

FRONTLINE

magazine by **THREATLOCKER**®



Never trust, always verify

Why Zero Trust is essential in the modern world

Leveling the playing field

AI cyberattacks are here. Is an AI response the answer?

The enemy within

Insider threats and the silent cybersecurity danger





2017

Danny and Sami Jenkins, along with John Carolan, incorporated ThreatLocker® and launched Allowlisting, a market-redefining Zero Trust solution.

2018

ThreatLocker signed its first enterprise customer in Florida and expanded its customer base to multiple states, marking the start of national growth and customer impact.

2019

ThreatLocker launched Ringfencing™ and Storage Control. Ringfencing was designed to control app behavior, while Storage Control protected data from rogue access and insider threats.

2020

Elevation Control was launched to reduce admin privilege exploitation and shrink the attack surface. ThreatLocker opened data centers in Florida and Virginia.

2021

With 27 employees, ThreatLocker hosted its first Zero Trust World (ZTW), expanded to Europe with a new office and data center in Dublin, and launched Network Control.

2022

ThreatLocker hired its 100th employee and acquired Thirdwall™ and HyperCube™ to expand its cybersecurity portfolio and platform capabilities.

2023

ThreatLocker released Detect, an EDR with advanced automatic response capabilities, expanded its data center network to include Sydney and Dubai, and grew to more than 200 team members.

2024

ThreatLocker was protecting 50,000+ organizations and debuted Cyber Hero® MDR. The company established a presence in Australia and the UAE and added data centers in Saudi Arabia and Illinois, USA.

2025

At ZTW 2025, ThreatLocker launched Web Control, Patch Management, Insights, User Store, and Cloud Control. The team grew to over 600 people, with members across more than 10 countries.

TABLE OF CONTENTS

4	Welcome note
6	On my mind: By Danny Jenkins
86	Where to find us



THREATLOCKER INTELLIGENCE BRIEF

10	Never trust, always verify Why Zero Trust is essential in the modern world
12	Key principles of a Zero Trust ecosystem The five core doctrines of information security
13	People-powered security Proven industry wisdom dictates a new security path
16	Best practice: Zero Trust Establish the methodology with help from ThreatLocker
20	ThreatLocker new solutions New suite of cybersecurity tools launched at Zero Trust World 2025
22	The impenetrable ring ThreatLocker Ringfencing is a world-exclusive security solution
24	macOS: Secure but not invincible Apple's OS may be tough, but handle its security with care
48	Assessing Starlink Mini ThreatLocker team on-the-go with Starlink Mini

BEHIND THE SHIELD

30	Zero Trust World 2025 The global gathering for IT pros
84	The human side of Zero Trust Building a security career by putting people first

SECURITY INSIGHTS

26	Leveling the playing field AI cyberattacks are here. Is an AI response the answer?
32	The enemy within Insider threats and the silent cybersecurity danger
34	Clearing the fog of war The critical role of logging and continuous monitoring
36	Hidden claws Mimikatz exploits the weakness beneath Windows' skin
37	Ghost in the shell RedRabbit demonstrates the malicious potential of PowerShell

HEAR IT FROM OUR CUSTOMERS

- 38** **Jack Thompson,**
Indianapolis Colts
Veteran turned
cybersecurity linebacker
- 52** **Shane Rogers,**
Harrison Steel Castings
On the growing importance
of digital security in industry
- 58** **Marc Menzies,**
Overview Technology Solutions
Real-world wisdom of a leading hybrid
solution provider
- 68** **Joe McGee,**
Advanced Medical Transport
Reshaping IT in healthcare
using emerging technologies
- 74** **Art Ocain, Airiam**
An incident response view
on the strength of Zero Trust
- 78** **Bo Olsen, Eastern Bank**
Protecting finance endpoints
and exploring the world

GLOBAL POLICIES

- 56** **CMMC 2: Defense redefined**
Inside the new U.S. DoD cybersecurity
regulations for 2025
- 72** **NIS 2: The need to know**
The EU's latest legislation is here,
with big implications

INDUSTRY FOCUS

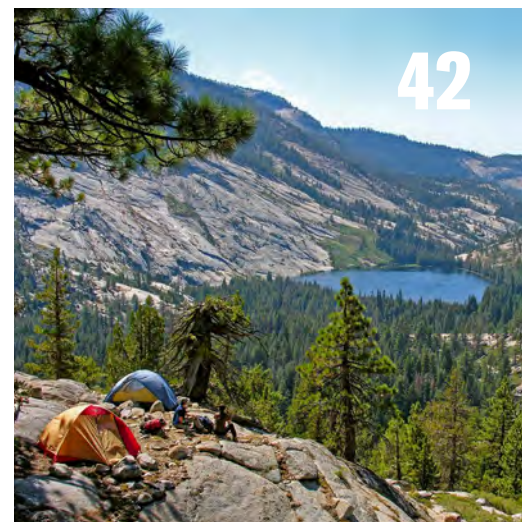
- 50** **Manufacturing**
How the most-attacked sector
can build back better
- 66** **Healthcare**
Cyberattacks kill—but poor security
in healthcare is not chronic

PEACE OF MIND

- 42** **Nature's prescription**
Battle burnout and stress in incredible
open-air locales
- 62** **Expert strategies for leadership**
Regulating the C-suite
with Katrina Lempenski

TRENDING

- 80** **Entangled evolution**
Quantum computers are set
to change security forever



WELCOME NOTE

Our number one goal is to help you become more secure, and this is why we developed a radically different, deny-by-default, allow-by-exception endpoint protection platform.

For over two decades, we've witnessed malware evade traditional antivirus detection, exploit weaknesses, and use sophisticated techniques to bypass security measures. We've dealt with zero-day exploits and seen the destructive impact on businesses. By 2014, we were constantly working on ransomware recoveries, watching lives and livelihoods destroyed. That's when we decided something had to change.

In 2017, we launched ThreatLocker® and implemented the first Zero Trust endpoint protection solution. Today, ThreatLocker protects over 50,000 businesses.

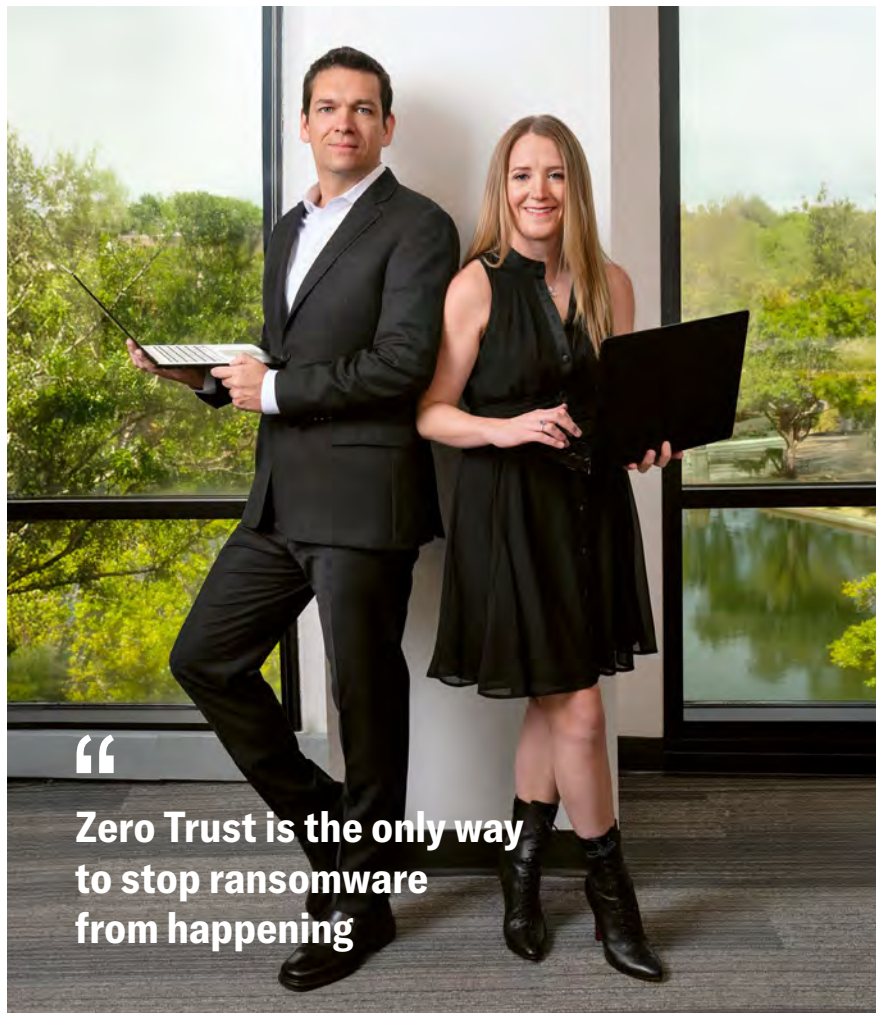
The Cyber Hero® story

Our first customer needed 24/7 support, but as a three-person team, we didn't offer it—yet. So, we stepped up, handling support calls in the middle of the night. At 2 a.m., when we were responding on live chat support, we needed to focus on fixing issues—not explaining why the CEO of the company was handling support. That's how the Cyber Hero name was born: we renamed the support chat to Cyber Hero to anonymize it slightly. While we no longer need to hide behind the name, every team member embodies the spirit of a Cyber Hero. The Cyber Hero is here to stay, 24/7/365.

Our mission

We built ThreatLocker to make default-deny solutions accessible to all businesses, enabling you to harden your environments with the most robust Zero Trust solutions.

We're also building a Zero Trust global community through ThreatLocker University, Cyber



Hero certifications, a growing customer base, and our annual Zero Trust World conference.

We operate with a high sense of urgency, relentless commitment, and a focus on securing you with the strongest, yet most agile tools to keep bad actors at bay—and drive them out of business.

Whether you're just starting with Zero Trust or are an experienced user of our solutions, we hope this magazine provides valuable insights to empower you and strengthen your defense against cyber threats.

So, dive in, read on, and stay cyber-strong.

Yours,

Danny Jenkins
CEO and Co-Founder, ThreatLocker

Sami Jenkins,
COO and Co-Founder, ThreatLocker

Stop trying to outsmart cybercriminals.

Lock them out instead.

You can't outthink every hacker—but you can outsecure them.

With ThreatLocker® Allowlisting, you automatically catalog and control applications, proactively blocking unnecessary access. Protect your systems from ransomware and other threats without adding complexity. It's a surprisingly straightforward process, too.



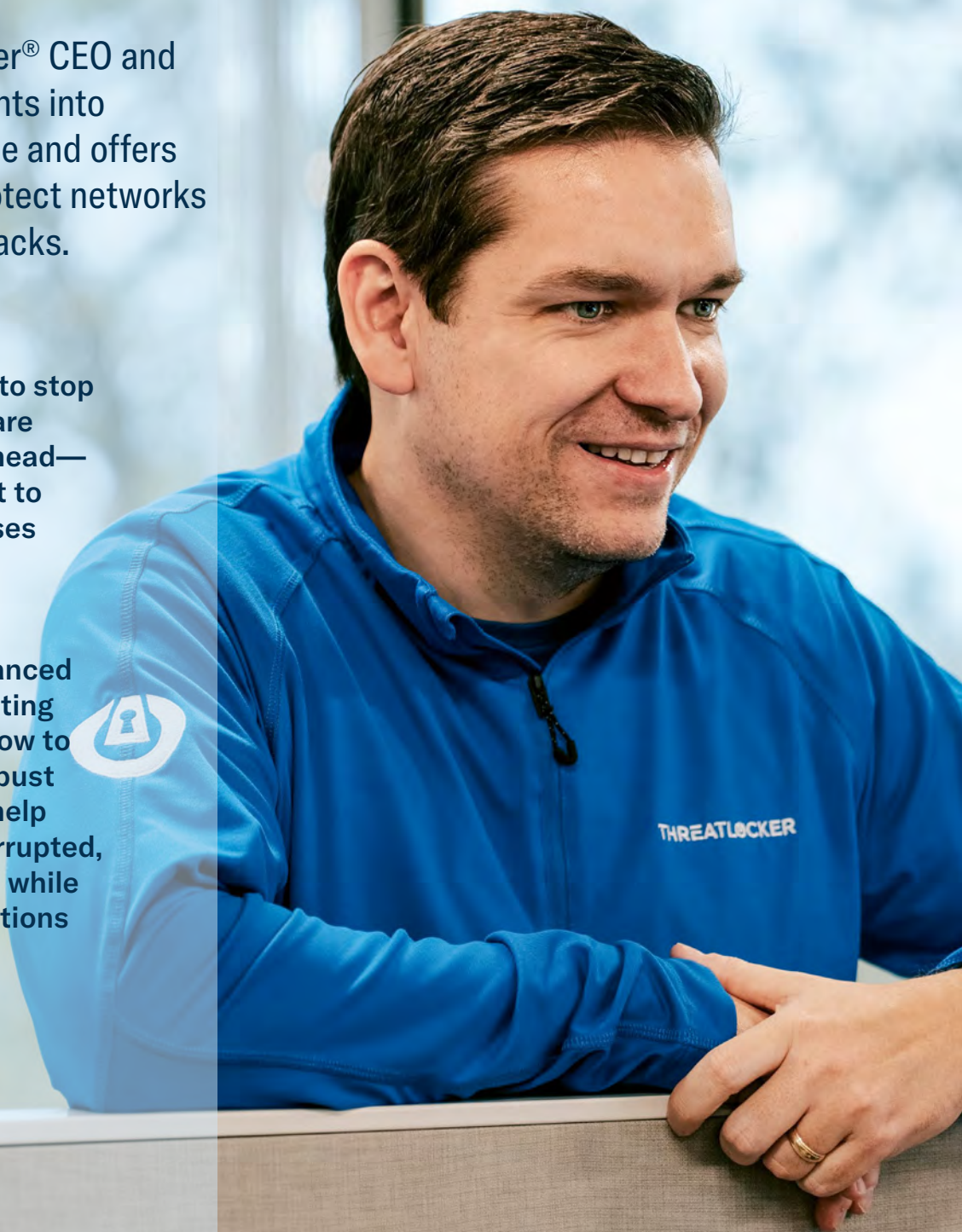
ON MY MIND

BY DANNY JENKINS

Danny Jenkins, ThreatLocker® CEO and Co-Founder, provides insights into the cybersecurity landscape and offers Zero Trust strategies to protect networks against inevitable cyberattacks.

ThreatLocker is on a mission to stop breaches in their tracks. We are flipping cybersecurity on its head—shifting from allow-by-default to only approving what businesses need first and then denying everything else by default.

As AI drives a barrage of advanced malware, we are heavily investing in educating businesses on how to fight back and provide the robust tools to do so. Our goal is to help organizations operate uninterrupted, even during malware attacks, while delivering the most agile solutions and peace of mind.



1

GET READY TO FIGHT MORE SOPHISTICATED CYBERCRIMINALS

As ransomware becomes more profitable, it's no longer a question of if, but when your business will be targeted.

Technology has evolved fast over the past 25 years. What once was a shared office email account is now a complex system vulnerable to ransomware attacks that can drain funds, encrypt data, or sell it on the dark web. Security is no longer just antivirus software—it's a full strategy to protect networks and data. For IT professionals, it is essential to align internally and across their organization on these threats, their consequences, and the best solutions to implement the strongest defenses.

Plus, you now have to be ready to fight AI-generated malware. While many cybersecurity professionals view AI as a powerful tool to enhance their defenses, it's a double-edged sword. AI can be used by cybercriminals to create sophisticated malware that often slips through traditional defenses unnoticed. This highlights the critical need for Zero Trust solutions.

2

STAY HUNGRY FOR EDUCATION

Education is key in fighting cybercrime. We attend 800+ events globally each year, where we lead training and thought leadership sessions on cybersecurity.

Each year, we host a conference with over 2,000 IT professionals. Our expert speakers provide the latest insights on cyberthreats and solutions, while our hands-on hacking labs empower IT professionals to learn how to strengthen their security.

We also offer free monthly webinars with security tips and hacks. Past sessions have included hacking Windows machines and showing companies how to prevent attacks.

In one demonstration, we used a drone to take over a company's Wi-Fi and intercept passwords, helping executives understand their network vulnerabilities. These demos quickly spotlight surprising vulnerabilities and the critical need to strengthen security. As we grow, we'll keep educating and demonstrating to ensure everyone has access to the most robust cyber protection solutions.

THREATLOCKER TIP



Instead of chasing every known and unknown threat, let's focus on the applications you need and then block everything else by default.

Zero Trust World is a key event to advance cybersecurity education





**There are only two types of
companies: those that have been
hacked and those that will be.**

Robert Mueller, former FBI Director

3

SIMPLE CONTROLS MAKE A MASSIVE DIFFERENCE

While major breaches like Colonial Pipeline, MGM, and Kaseya made headlines, many small businesses are quietly crushed by ransomware attacks.

Often, it's a dental office or a local business with just a handful of employees whose files are encrypted and held for ransom. Based on the stolen financial data, cybercriminals know what a company can afford and set ransom prices accordingly.

Even if businesses regain access to their data, they still face costly recovery efforts, such as cleaning up computers and servers.

One goal of cybersecurity is to slow hackers down enough that it becomes too costly and time-consuming to breach your systems. Simple controls can make a massive difference. Most people don't realize they're running hundreds of applications that can access all data in their files.

Limiting what apps can do on your network prevents data breaches. Invest in those security solutions. Enabling two-factor authentication on office accounts is another essential step.

Tools like ThreatLocker® Allowlisting and Ringfencing™ will protect your business when an employee accidentally downloads a piece of malware.

At the end of the day, identifying specific vulnerabilities is key to selecting the right cybersecurity tools for your organization.

“

Most people don't realize they're running hundreds of applications that can access all data in their files

4

PREPARE FOR THE INEVITABLE CYBERATTACK

Two years ago, I predicted more weaponized, undetectable, and unique malware. I didn't foresee AI generating such a significant amount of malware and the number of skilled hackers skyrocketing to virtually anyone being able to create phishing emails or cyberattacks with just a laptop and internet access.

Going forward, I expect more targeted attacks, increased cybercrime commercialization, and malware that's harder to spot.

As more businesses suffer, companies will realize the inevitability of attacks. This will push many to adopt a Zero Trust approach, where deny-by-default makes it much harder for cybercriminals to profit. ■

NEVER TRUST ALWAYS VERIFY

Cybersecurity has changed. In the early days of network computing, the fortress model made sense: secure the network perimeter, use firewalls to keep bad actors out of digital infrastructures, and assume everything within those walls should be safe. Cynical members of the cybersecurity community dubbed this practice “M&M security.” Within the network’s crispy outer shell lay a soft center, delicious to attackers—with enough heat or a sharp enough bite, cracks in the shell would allow them in.



Attackers have certainly been chipping away. Cybercrime is profitable, potentially costing the world USD 14 trillion by 2028[†]. Disruption is logistically valuable to rogue nations. The cost of handling breached data means paying attackers to unlock ransomware, which is often the most logical response by organizations to an attack. All this, while the way we work has changed. The rise of remote work, cloud services, and new computing models mean the walls of the fortress are no longer where they once were; every essential new IT service results in ceding a little more control.

The new normal

These shifts have fostered a hacker market that is now more sophisticated, professional, and commodified than ever. In response, the cybersecurity community has tirelessly worked to strengthen the fortress model, enhancing firewall capabilities and deploying more advanced endpoint protection. Yet, despite these measures, the reactive methodologies feel increasingly fragile in the face of relentless attacks.

“Detection shouldn’t be everything,” suggested Rob Allen, CPO of ThreatLocker®. “Because detection requires decisions on whether something is good or bad. The problem with that is if your detection tool gets a decision wrong and waves through something malicious, that’s effectively game over.” Therefore, while it is unwise to eliminate security measures, we can no longer consider a traditional perimeter entirely secure.

Core methodologies of Zero Trust

The introduction of Zero Trust offers a refreshing paradigm shift. The approach, fermented for over a decade and coined by Forrester’s John Kindervag in 2010, acknowledges the increased openness and communication of devices worldwide. It suggested, at the time, a change in posture, closing off communication by default and opening access only when needed.

“
**Zero Trust
is about
changing
your
mindset
and
rethinking
your
approach to
security**

Today’s Zero Trust model is a little different. At its core, Zero Trust challenges us to rethink how we interact with our systems and data. “There are three core elements to it,” explained Allen. “First, eliminate implicit trust in any one element, node, or service and add explicit trust in its place. Second, work from the principle that attackers are already in your network with full domain access and able to do whatever they want. How would you defend yourself in that case? And third, allow your users full access, but only to the bare minimum required to perform their jobs.”

A network keeps its traditional perimeter, but Zero Trust introduces a new layer that weaves between every interaction, offering a granular defense and encouraging constant vigilance. Zero Trust is a way for the enterprise to adopt a hyper-defensive stance. It acknowledges the shortcomings of reactive security and the weaknesses of perimeters and implements a coordinated and proactive response to digital threats. But it is not a switch that can just be flipped.

Mind over matter

“You can’t buy Zero Trust,” said Allen. “It’s a mindset. A way of looking at things. It starts with a firm decision to commit to and implement Zero Trust and go from there.”

Zero Trust can turn cybersecurity upside down, empowering organizations to rethink their approach. The “never trust, always verify” ideology is a scalable, resilient strategy—it’s as effective at protecting a single endpoint as it is defending an enormous enterprise. It’s agile, offering ongoing protection that’s immediately effective against zero-day threats. It’s resilient at its core, but it must be done right—and it’s a permanent change in methodology. “The important thing to remember is that, like happiness, Zero Trust is a journey and not a destination,” concluded Allen. “Zero Trust is a moving target, and it requires constant work.” ■

KEY PRINCIPLES OF A ZERO TRUST ECOSYSTEM

Maintaining a Zero Trust methodology means embracing a Zero Trust mindset – no exceptions, no excuses. While there are plenty of subtleties to consider, Zero Trust can be distilled into five core tenets that remain valid no matter where it is applied.



Anyone who takes their cybersecurity seriously should be looking at building a Zero Trust environment.

Terry Velivasakis, Systems Administrator, Sofwerx

Segmentation

A granular policy structure allows for broad-stroke security management as well as pinpoint changes. By dividing the network into smaller, individually secured segments, attackers lose the ability to move laterally. Even if a single segment is compromised, the rest of the environment stays secure.

Assume breach

There is no sense in hoping that breaches won't happen. A Zero Trust mindset assumes that they will occur and may have already occurred. This cynical viewpoint emphasizes the need for stringent access controls, monitoring procedures, and effective methods of response.

Continuous monitoring

Zero Trust moves from reactive to proactive security. Through a combination of strict verification procedures and constant monitoring of all user behavior, device health, and network activity, anomalies can be detected early, allowing for immediate response and resolution.

Least privilege

Everything that could be accessed, from data to applications, is offered on a "need to know" basis. Users receive only the bare minimum permissions necessary for them to perform their roles. This minimizes the risk of data exposure and, in case of a breach, severely limits what attackers may be able to access.

Verify explicitly

Every access attempt is authenticated, regardless of the source. An attempt could come from an on-site employee, a remote contractor, or an application process. Trust is never assumed, even after initial authentication, and continuous verification keeps each user's access as secure as possible.



PEOPLE-POWERED SECURITY

Sami Jenkins, COO & Co-Founder of ThreatLocker. Read Jenkins' product insight and best practice on Page 16

Cybercrime has never been more pervasive, more professional, or more dangerous. Attackers act on multiple divergent paths: scattergun attempts continue to rise, bespoke attacks are more powerful, and less technical disruptors are empowered with off-the-shelf, user-friendly ransomware with expert support.

Despite the complexities, the information security sector already possesses the foundational knowledge and strategies to combat these threats effectively. All it takes is a little reframing: applying the context of Zero Trust to the proverbs we live by proves that cybersecurity professionals can leverage their expertise to elevate security measures.

To an attacker, the checks and balances generally even out. Smaller companies might command a lesser prize than massive corporations, but a lack of cybersecurity maturity make them easier to target.

**“THERE ARE ONLY TWO TYPES
OF COMPANIES: THOSE THAT HAVE BEEN
HACKED AND THOSE THAT WILL BE.”**

ROBERT MUELLER, FORMER FBI DIRECTOR

In short, attackers can and will strike anywhere. The Zero Trust “assume breach” attitude helps lift the weight of impending attack from the shoulders of cyber pros: every action verified is an agile preventative measure. The probability and severity of successful attacks—which, again, will happen, whatever security model one follows—is severely reduced.

**“CYBERSECURITY IS 20% TECHNOLOGY
AND 80% PROCESS.”**

GINNI ROMETTY, FORMER IBM CEO

Adopting Zero Trust doesn’t do away with processes; if anything, it places security processes first in the queue. With technology itself moving at breakneck speed, cloud adoption, remote work, and IoT integration add new security challenges at every turn. Zero Trust allows cybersecurity experts to encourage and spearhead such growth without fearing the administrative headache that securing it might otherwise bring. A thorough process for classifying data and systems enables precise access controls and highlights where security resources are needed most. In essence, the process becomes the shield.

“

**Zero Trust makes
it easier for
organizations to
maintain compliance**

**“THE ONLY TRULY SECURE SYSTEM IS ONE
THAT IS POWERED OFF, CAST IN A BLOCK OF
CONCRETE, AND SEALED IN A LEAD-LINED
ROOM WITH ARMED GUARDS—AND EVEN
THEN, I HAVE MY DOUBTS.”**

GENE SPAFFORD, PURDUE UNIVERSITY

This is a quote from 1989 that rings just as true today, and aptly frames the idea of Zero Trust security. While information security teams do not have the luxury of whipping out the Quikrete, they can build an endless series of lead-lined rooms wherever they are required by constructing clever least-privilege access policies. Zero Trust gives cybersecurity professionals the confidence that, even if a breach occurs, the damage will be manageable and quickly contained, effectively protecting individual users, devices, and applications.

**“IT TAKES 20 YEARS TO BUILD A
REPUTATION AND FIVE MINUTES
TO RUIN IT.”**

WARREN BUFFET, PHILANTHROPIST

One breach could be all it takes. Many small businesses are compelled to cease operations after a cyberattack. While the often-cited figure of 60% may not be accurate, a significant number do close down. This is partly due to the prohibitive cost of recovery, but also the reputational damage that a breach can cause, and the regulatory nightmare that comes from data exfiltration. Zero Trust is a security strategy that reduces the impact of data breaches while constantly monitoring access and activities, making it easier for organizations to maintain compliance.



**HACKERS TAKE THE PATH OF
LEAST RESISTANCE. SO, BLOCK
THEM WITH THE PATH OF
LEAST PRIVILEGE.
SEE HOW.**



**“YOU CAN’T PROTECT WHAT
YOU DON’T KNOW.”** UNKNOWN

We include this perennial cybersecurity adage not because it is true, but because Zero Trust disproves it. Networks are inherently sprawling and difficult to manage, a situation made more challenging by the BYOD culture and the increasingly unregulated practices of remote work. Additionally, zero-day threats are lurking everywhere, and the criminal fraternity is consistently developing new attack methods. However, the structure of Zero Trust addresses these concerns. The framework’s monitoring and access control components essentially serve as self-audits—they protect against the activity of rogue devices and processes, ensuring that security teams are quickly alerted to any unusual behavior.

**“PEOPLE OFTEN REPRESENT
THE WEAKEST LINK IN THE
SECURITY CHAIN AND ARE CHRONICALLY
RESPONSIBLE FOR THE FAILURE
OF SECURITY SYSTEMS.”**

BRUCE SCHNEIER, HARVARD KENNEDY SCHOOL

Verizon’s 2024 Data Breach Investigations Report states that 68% of breaches involve a non-malicious human element, like falling victim to social engineering or making an error, and 35% are directly caused by internal actors. Zero Trust does not remove the need for users to behave securely, nor does it reduce the risk of attempted espionage, but strict access controls and an emphasis on classification limit the exposure of sensitive information and reduce the likelihood of data leaks. Even when an employee’s credentials are compromised, an attacker’s ability to reach high-value data is severely limited.

Security doesn’t wait.
ThreatLocker Cyber Hero
support team responds within
60 seconds, 365 days a year

**“CYBERSECURITY IS A CULTURE,
NOT A TECHNOLOGY.”** UNKNOWN

Too often, the response to increased threat is to layer on more protection and upgrade one’s hardware and software solutions to repel potential attacks. The industry cannot claim that this tactic has worked, especially considering that the global cost of cybercrime is projected to exceed USD 10 trillion in 2025 alone¹. Security needs to be the default, a culture shared by all. The ThreatLocker® method is robust, focusing on key security practices such as Allowlisting, Ringfencing™, and Network Control and detection, all essential components of a Zero Trust framework. This method facilitates the implementation of a Zero Trust mindset and fosters a significant cultural shift within the organization. By continuously emphasizing the importance of secure behavior, ThreatLocker keeps IT professionals and end-users engaged and vigilant at their respective endpoints, stressing that security is a shared responsibility rather than an afterthought. ■

“

**68% of breaches
involve the human
element**



BEST PRACTICE: ZERO TRUST

BY SAMI JENKINS

The cybersecurity world faces many known threats, from nation-state cyberattacks to the proliferation of IoT devices and advancements in AI to the risk of human error. Knowing these threats is only half the battle; dealing with the unknown is another matter entirely. Whether cybercriminals apply fresh methodologies to existing attack vectors or develop entirely new approaches, those on the defense must be prepared for anything, now and in the future.

The solution has crystallized as Zero Trust, a framework designed to mitigate unknown and brand-new threats. More than just a set of practices, Zero Trust represents a fundamental shift in the philosophy of cybersecurity. Embracing this approach demands dedication, commitment, and a willingness to rethink and adapt strategies in order to maintain a strong defense against threats.

First steps to Zero Trust

The initial phases of transitioning to a Zero Trust model heavily rely on the expertise of business analysts and information security professionals. It's crucial to establish a clear understanding of critical assets first. Identify data stores, applications, and vital infrastructure, and pinpoint the users, devices, and systems that absolutely require access. Next, logically break the network into microsegments to clearly define its boundaries. Use these insights to create detailed policies that segment access based on roles, behaviors, and context.

As these initial steps indicate, Zero Trust ultimately rests on effective policy definition, management, and enforcement. These policies specify exactly what can occur, with everything else being denied by default. However, the field of information security is not strictly black and white; it involves nuances and exceptions, with circumstances that may override even the most detailed policies. To truly embrace Zero Trust principles, information security teams need a platform that allows for consistent policy application while enabling swift decisions on exceptions. This is where ThreatLocker® comes into play.

ThreatLocker: The power to protect

The ThreatLocker Endpoint Protection Platform is the most comprehensive Zero Trust endpoint solution on the market, and it helps deliver a true Zero Trust approach. It is lightweight, user-friendly, and easy to implement. While whipping one's resources into shape may feel like a Herculean task, businesses can transition in a matter of days with the help of the ThreatLocker Cyber Hero® Team.

In the end, it's about empowerment. To meet compliance standards, safeguard sensitive data, and manage hundreds or thousands of vulnerable endpoints, IT professionals must leverage the best tools available to gain an advantage. Adopting a Zero Trust framework marks the beginning of their journey, and with the right resources, they can continue to move forward.

ThreatLocker Protect Platform

Tools to help maintain best practices through every step of the endpoint Zero Trust journey



ALLOWLISTING

Control which applications can run. Then block everything else by default.

- Automatically catalog and categorize all running applications.
- Select the apps you trust and block everything else—including current and future known and unknown threats.
- Stop ransomware in its tracks without worrying about the latest variations.



RINGFENCING™

Adds a vital layer of protection that limits an application from being able to interact with other applications, edit the registry, modify files, and access the internet.

- Granularly control how applications interact with each other and other system resources.
- Reduce the attack surface of approved applications.
- Minimize lateral movement even if an application is compromised.



NETWORK CONTROL

Defend against external threats with precision.

- Centrally managed firewall for endpoints and servers.
- Dynamic ACLs automatically open ports for trusted devices without requiring pre-defined IP addresses. For increased security, those ports close after five minutes of inactivity.
- Protect against untrusted internet traffic with unparalleled control.

Additional ThreatLocker solutions

ELEVATION CONTROL

Elevation Control revolutionizes endpoint privilege management by offering an application-centered approach. Rather than providing users with admin credentials, administrators can establish policies that temporarily elevate privileges for designated applications—eliminating the need for any credentials.

Why it matters:

Giving users admin privileges opens the door to cybersecurity risks. Users only need elevated access for specific applications. Elevation Control provides admin rights to specific applications—not users—and limits access to precise time frames if needed. This approach reduces both the attack surface and day-to-day disruptions.

CONFIGURATION MANAGER

Configuration Manager takes the ThreatLocker Protect Platform to the next level by enabling IT teams to develop and enforce effective configuration policies from a single console, regardless of how many Active Directory (AD) domains they have. Policies can be easily applied to individual endpoints, groups, organizations, or even across multiple tenants—all in one unified interface.

Why it matters:

Companies managing multiple AD domains often face challenges in standardizing Windows configurations. Configuration Manager simplifies the process of enforcing essential settings, such as automatic lock policies, disabling autoplay, or blocking SMBv1 throughout the network. This streamlines operations and also reduces the burden on IT staff.



STORAGE CONTROL

Storage Control lets you manage data access with precision. Policies can range from blocking USB devices to defining which applications or users can access specific files or backup shares.

Why it matters:

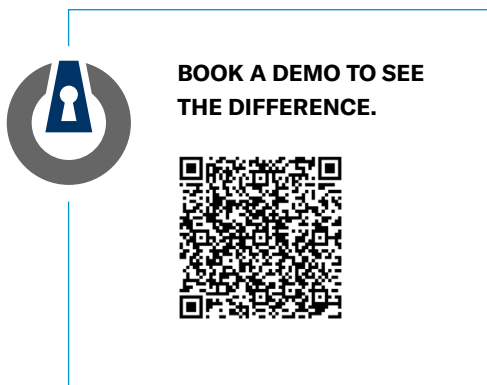
In the event of a breach, hackers often weaponize trusted applications. Granular Storage Control policies limit the damage they can cause. In addition, this is an excellent tool to protect against insider threats. With Storage Control, your data is safer. ThreatLocker® Unified Audit complements this solution by logging every instance of storage access—whether on the network or remote—down to the files copied and the external storage device's serial number.

DETECT

ThreatLocker Detect is a policy-driven Endpoint Detection and Response (EDR) solution. It monitors for unusual events or Indicators of Compromise (IoCs) and can send alerts or take automated actions when anomalies are detected.

Why it matters:

Detect leverages telemetry from ThreatLocker modules and Windows Event logs to provide critical insights. Its automated responses enable rules, isolate devices, or activate Lockdown Mode, blocking all activities to ensure security. From spotting abnormal Remote Desktop Protocol (RDP) traffic to detecting erased event logs, ThreatLocker Detect addresses threats before they cause harm.



“

Zero Trust ultimately rests on effective policy definition, management, and enforcement

WHAT IS THREATLOCKER CYBER HERO® MANAGED DETECTION AND RESPONSE (MDR)?

Cyber Hero MDR is an advanced add-on to ThreatLocker Detect. It delivers the expertise of the ThreatLocker Cyber Hero Team to monitor and respond to IoCs with world-class experience. When ThreatLocker Detect identifies a suspicious activity, the Cyber Hero Team investigates to confirm if it's a true IoC or a false positive. If a cyber incident occurs, they take swift action by adhering to the customer's runbook to isolate or secure the impacted devices while providing thorough insights into the situation, such as:

- The nature of the threat
- Where the threat originated
- What actions the threat attempted
- How the threat was blocked and mitigated

Why it matters

With 24/7/365 availability, the Cyber Hero Team provides around-the-clock MDR services, ensuring you are protected even outside standard operating hours. The average response time of about 60 seconds minimizes potential damage and offers unparalleled support in the face of cyber threats.

How it works

Combining the ThreatLocker Zero Trust Endpoint Protection Platform with Cyber Hero MDR allows organizations to reduce alert fatigue, bolster security, and comply with stringent incident response and mitigation requirements.

When it comes to safeguarding your endpoints, adopting a default-deny Zero Trust strategy proves to be the most effective cybersecurity solution. ThreatLocker stands out on the global market as the most comprehensive provider of default-deny endpoint protection. ■

ThreatLocker® drops new suite of cybersecurity solutions at Zero Trust World 2025

Committed to providing the strongest Zero Trust cybersecurity solutions, ThreatLocker has launched a new suite of tools that enhances both its platform's robustness and user experience.

ThreatLocker introduces new solutions

INSIGHTS

Designed to leverage data from millions of endpoints worldwide, this solution empowers organizations with the intelligence needed to make the best security decisions, fast. With real-time, actionable insights, cybersecurity professionals can skip tedious research and instantly view an application's typical behavior, making swift, informed decisions on what to allow and how to control it in their environments, strengthening their cybersecurity posture.

“

We're redefining Zero Trust—making it more accessible, practical, and much easier to manage. We are actively changing how people view deny-by-default, allow-by-exception security. We remain committed to making Zero Trust even simpler and more efficient, with a high focus on usability and strong security.

DANNY JENKINS, CEO & CO-FOUNDER, THREATLOCKER

PATCH MANAGEMENT

ThreatLocker Patch Management removes the burden of monitoring and researching software updates by consolidating alerts into a single, streamlined platform, eliminating the need to sift through multiple sources. To ensure every update is safe and reliable, the ThreatLocker Cyber Hero® Team rigorously tests each one in a controlled environment before deployment—so businesses stay secure without the risk of disruptions.

USER STORE

The ThreatLocker User Store is a catalog of pre-approved applications that lets users run the apps they need—without compromising organizations' cybersecurity posture. With the library of apps set up, cybersecurity professionals save time, reduce frustrations, and keep their security framework strong without extra effort as users install new apps. Any pre-approved application comes with optional temporary elevation. New Allowlisting and Ringfencing™ policies are automatically created, according to pre-set policies, to support an agile and streamlined Zero Trust environment with no security compromises.



Danny Jenkins introducing new ThreatLocker solutions at Zero Trust World 2025

WEB CONTROL

Web access control is a must-have for cybersecurity, but it often means adding yet another third-party tool to your stack. That also means more vetting, integration headaches, and potential security gaps. With the new ThreatLocker Web Control, you eliminate all these risks and extra work. In addition, the ThreatLocker browser extension enhances users' experience, letting them easily request permission to access blocked sites. ThreatLocker does all the heavy lifting. It builds and dynamically updates the library of website categories and applies the same controls to unmanaged devices accessing a company's network while delivering a greater end-user experience.

CLOUD CONTROL

ThreatLocker Cloud Control was developed as a powerful tool to protect companies against phishing attacks and token thefts. It leverages built-in intelligence to assess whether a connection from a protected device originates from a trusted network. By analyzing connection patterns from protected computers and mobile devices, Cloud Control automatically identifies and allows trusted connections. The result? Only users from IP addresses and networks deemed trusted by ThreatLocker can get in—automatically blocking phishing and token theft attacks. So, no matter how successful cybercriminals are with their phishing attacks and token thefts—all their efforts are now useless. No match. No entry.

DETECT DASHBOARD

The ThreatLocker Detect Dashboard consolidates your environment's incident and alert data into user-friendly bar charts, line graphs, and pie charts. Its intuitive design allows for quick insights, complete with tooltips for more in-depth analysis and rapid response. These insights provide details about the actions taken and the rationale behind each decision. As part of the incident response process, the Cyber Hero Team offers policy recommendations, including which ones to enable or disable, along with comprehensive guidance on how to tackle each incident. With just one click, you can address any incident response recommendation seamlessly. ■

“

Cybersecurity pros are always battling new threats, vetting apps, and securing systems—while keeping operations uninterrupted. Our latest innovations help teams make quicker decisions, gain deeper insights, save time with automation, and—hopefully—reduce stress while excelling at what they do. We're setting a new standard for rapid, reliable security and robust Zero Trust environments.

ROB ALLEN, CHIEF PRODUCT OFFICER, THREATLOCKER

THE IMPENETRABLE RING

How Ringfencing™ keeps you protected

BY BLAIN CURTIS, SOLUTIONS ENGINEER MANAGER



Every day, cybercriminals lurk in the shadows, searching for an opening. They don't kick down the door; instead, they slip in through the cracks, hijacking the very applications you trust. But what if you could create an impenetrable ring around these applications to stop cybercriminals in their tracks? That's exactly what ThreatLocker® Ringfencing does—acting as your first line of defense against threats that turn your own tools against you.

Ringfencing adds an extra layer of security, boxing in approved applications and preventing them from interacting with critical system components like the registry, the internet, sensitive files, and even other applications. It's the security solution you didn't know you needed, but once you have it, you won't want to be without it. And ThreatLocker is the only company in the world to offer it.

“

Cybercriminals' latest trick is fileless malware—an attack that operates directly in a system's memory, leaving no trace on the file system

We spoke to our customers to see how they leverage Ringfencing to safeguard their businesses. Here are some takeaways from them.

Real-world wins: How customers leverage Ringfencing to stay protected

▪ **Mitigating fileless malware:**

Cybercriminal's latest trick is fileless malware—an attack that operates directly in a system's memory, leaving no trace on the file system. This makes it difficult for traditional antivirus and endpoint detection systems to spot. Our customers use Ringfencing to counter this risk by blocking unauthorized actions that exploit trusted applications, stopping the attack before it can cause harm.



TO LEARN MORE,
REQUEST A DEMO.



Ringfencing adds an extra layer of security, boxing in approved applications and preventing them from interacting with critical system component

▪ Limiting application attacks:

You've likely heard of the SolarWinds Orion breach, where a single compromised software update gave attackers access to over 250 organizations, including Fortune 500 companies. For ThreatLocker customers, the story played out differently.

Ringfencing limited what SolarWinds' application could do, stopping malware downloads and blocking access to the internet. While others scrambled to contain the fallout, ThreatLocker customers were already protected. Ringfencing contained the attack, preventing the full-scale breach.

▪ Controlling data access:

Do all your applications need access to your entire system? The reality is that many applications have the same level of access as the logged-in user by default. That means trusted programs like PowerShell and tools like 7-Zip, could inadvertently become a vulnerability. With Ringfencing, our customers control what data applications can access, ensuring that only the necessary applications are given permissions, greatly reducing the risk of exploitation.

▪ Preventing unauthorized registry changes:

The Windows Registry is a common target for malware, which often hides there to avoid detection. ThreatLocker customers use Ringfencing for an extra layer of protection by preventing applications from making unauthorized changes to the registry, ensuring that malicious software can't embed itself and compromise your systems.

A real-life scenario: Stopping a ransomware attack others missed

A recent case highlighted the power of Ringfencing when a phishing campaign targeted the hospitality industry, using a fake email to impersonate Booking.com.

The email led users to a cloned website with a fake CAPTCHA that triggered remote code execution. The attackers used mshta.exe, a legitimate Windows tool, to execute scripts, while PowerShell attempted to download a malicious file from a Russian server.

Ringfencing's default PowerShell policy blocked the attack before it could spread, preventing PowerShell from accessing the internet, stopping the ransomware from being downloaded and halting the attack before it could do any damage. In contrast, other cybersecurity providers either flagged the system as breached—causing unnecessary disruptions—or failed to detect the attack altogether.

Next-level cybersecurity

ThreatLocker Ringfencing takes cybersecurity to the next level. By shrinking the attack surface and restricting application capabilities, it becomes increasingly difficult for cybercriminals to succeed. Even if hackers manage to infiltrate a trusted application, they quickly find themselves at a standstill. The ring holds firm, and the attack comes to a halt. ■

macOS: SECURE BUT NOT INVINCIBLE

BY SLAVA KONSTANTINOV

Apple's flagship operating system, macOS, has long been heralded for its robust security approach. The notion that macOS is impervious to vulnerabilities is, however, a misconception rooted more in marketing than reality. Despite its sophisticated security infrastructure, macOS, like any other major operating system, must contend with a myriad of threats that necessitate user awareness and caution.

It is true that Apple is a formidable defender, consistently rolling out security patches to address vulnerabilities, and the company's proactive approach to security includes features like System Integrity Protection (SIP), Gatekeeper, XProtect, Sandboxing, and Transparency, Consent, and Control (TCC). But while Apple's advertising campaigns of the late 2000s emphasized the absence of viruses on Mac computers, the growing popularity of macOS has made it an increasingly attractive target for cybercriminals—and Apple does not always get it right.

WORKING WITH A CLOSED SYSTEM

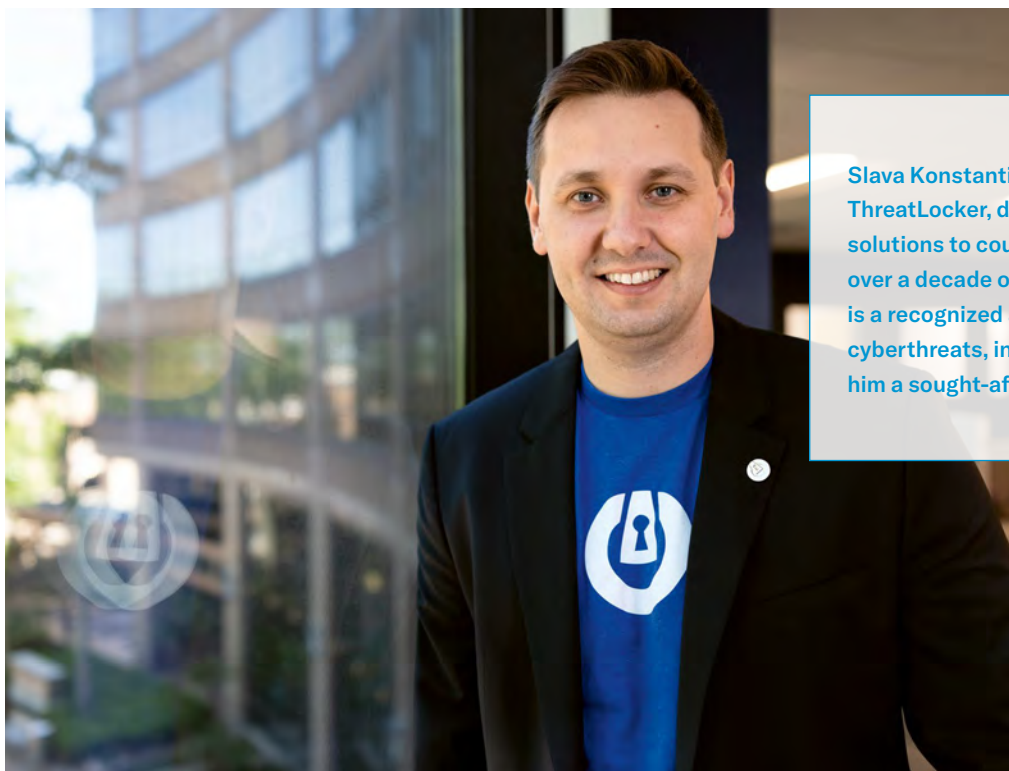
Apple's restrictive approach to its operating system architecture underpins its consistent approach to patching, but poses a unique challenge for third-party security developers. By denying access to the kernel, macOS limits the depth available to security tools, restricts security flexibility, and necessitates reliance on Apple's built-in measures. Incidents of macOS-targeted malware have recently surged, with adware and potentially unwanted programs (PUPs) becoming prominent threats, alongside sophisticated backdoor attacks.

Recently, a macOS update inadvertently disrupted third-party firewalls when the built-in firewall was enabled. Although Apple resolved this issue in

subsequent updates, users relying on third-party solutions during that interim period may have faced heightened risks. Apple's policy of supporting security updates only for the last three major macOS versions also leaves users of older systems vulnerable.

DEALING WITH RISING THREATS

The digital threat landscape as a whole continues to grow in complexity. Social engineering attacks are on the rise and becoming more difficult to detect, thanks to the presence of AI. State-sponsored cyber groups from countries like Russia, China, North Korea, and Iran are becoming increasingly active. And the rise of off-the-shelf Malware-as-a-



Slava Konstantinov, macOS Lead Architect at ThreatLocker, designs advanced cybersecurity solutions to counter sophisticated threats. With over a decade of experience in macOS security, he is a recognized authority defending against foreign cyberthreats, including nation-state actors, making him a sought-after voice in cybersecurity.

Service (MaaS) platforms, including offerings like Atomic Stealer, Banshee, and Cthulhu, has further democratized cybercrime. These platforms allow malicious actors to distribute pre-made malware on a subscription basis, lowering the barrier to entry for potential attackers.

Even considering Apple's usually stringent approach to security, macOS systems can be compromised through a variety of attack vectors. Common tactics include fake technical support scams, malicious browser extensions, and counterfeit software updates. Malware hidden in supply chain attacks and pirated applications also poses a significant risk, as do fake job postings that trick users into downloading malicious software under the guise of legitimate meeting apps. Zero-day exploits—vulnerabilities that are unknown to the software vendor at the time of exploitation—further underscore the importance of a multi-layered security approach.

A REAL-WORLD INCIDENT

One notable example of a macOS vulnerability involved a user attempting to update a suspicious application downloaded from the internet.

This seemingly benign software turned out to be a malicious executable, unknown to VirusTotal detection engines, that attempted to retrieve a payload from a server in Russia. Exploiting an unpatched macOS vulnerability, the malware sought to evade detection by bypassing the system's sandbox protections. Fortunately, a Zero Trust approach—treating all software and interactions as potentially malicious until verified—played a pivotal role in mitigating the threat.

So, while macOS delivers a secure environment with advanced integrated protective measures, it is clear that it is not immune to the dynamic tactics of cybercriminals and is under-supported by traditional security techniques. A cautious approach is a must: users should remain informed and proactive, combining Apple's built-in security features with best practices in cybersecurity. Through vigilance, education, and careful policy management macOS users can navigate the digital landscape with greater confidence and resilience. ■



The digital threat landscape as a whole continues to grow in complexity

LEVELING THE PLAYING FIELD

As criminals expand their use of AI in cyberattacks, the information security field is fighting back in kind—but can AI really defeat AI?



AI is everywhere. It is in places it should be, smoothing the customer service experience, detecting fraud in financial institutions, boosting healthcare processes to save more lives. It is also in places it shouldn't be, popping up to mistakenly replace perfectly solid processes when executives get unduly excited, or polluting the web with worthless, often incorrect content. And AI is in places it *really* shouldn't be: in the hands of cybercriminals, eager to use it to sharpen their attacks, gather more data, and collect more ransoms.

Every facet of AI is at play, from generative AI to machine learning and deep learning, creating new malicious tools and techniques, invading and poisoning networks, and disrupting legitimate AI tools. The attacks cybercriminals have relied upon for many years have been rejuvenated by AI, made stronger and more effective. Information security is undergoing a slow reset, where new methods of executing old attacks are replacing the reliable techniques that once safeguarded the world's networks.

Phishing 2.0

Phishing might be the most well-known attack vector, and it is definitely the most plentiful. It is said to account for a considerable portion of all emails, with some sources claiming (but not proving) that billions[†] of phishing emails are sent daily. Whatever the true number, phishing works. IBM's latest X-Force Threat Intelligence Report states that phishing is responsible for 41% of security incidents. CSO magazine, writing at phishing's peak at the height of the pandemic, reported a much higher number, over 80%.



60% OF RECIPIENTS
FALL VICTIM TO AI-GENERATED
PHISHING EMAILS[†]

The human element is the most vulnerable part of digital defense, after all. One tired employee, one rushed executive, one distracted individual with their guard down is all it takes to capture vital credentials, giving criminals fuel for the next stage of their attack. In the age of AI, however, the numbers don't paint the whole picture.

Phishing is predominantly a practice of throwing everything against the wall and seeing what sticks, but the world has become wise to scattergun phishing. Our email defenses are built strong, and little of the daily wave of phishing attempts makes it through. The Nigerian princes of the 1990s taught us well, so even the least tech-savvy employee will likely smell a rat if a random phishing attempt hits their inbox—but the same cannot be said of carefully crafted spear phishing emails. Designed to look and feel authentic, probably claiming to come from someone in a position of power, and possibly even originating from a previously compromised account, these are a different breed of attack altogether.

AI's potential influence here is likely rather obvious. Criminals use generative AI to skip most, if not all, of the hard work of preparing spear phishing attacks. They can train their models on publicly available data like social media posts or organizational charts, or even on breached data, known or unknown. AI can then generate highly realistic emails cognizant of everything from interpersonal relationships to the formatting, style, and writing tics of an individual.

The rise of deepfakes

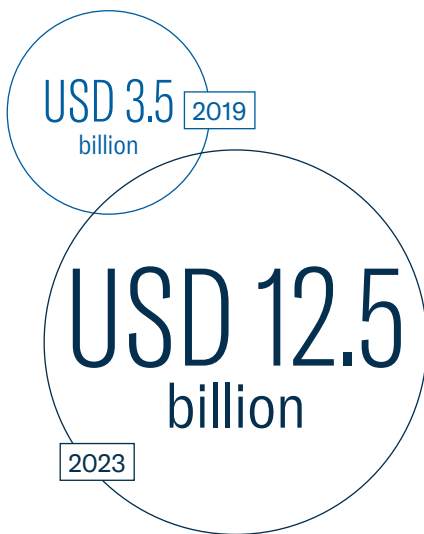
Text is not all that can be emulated, as the headlines have made all too clear. Generative deep learning AI trained on voice and video enables attackers to take a new route, striking via synthetic media—specifically, by so-called deepfakes. They might deploy phone calls supposedly from a friend, colleague, or family member, using information from social media to make conversations more personal and convincing. They can issue eerily realistic videos, mix the two, or even build filters to generate deepfake content live and on the fly.

The Department of Homeland Security sums up the threat of deepfakes, stating that it “comes not from the technology used to create it, but from people's natural inclination to believe what they see.” Today's attempts are noticeable to the trained eye, but the DHS suggests that “the severity and urgency of the current threat from synthetic media depends on the exposure, perspective, and position of who you ask.” The right fake in front of the wrong person could easily be the first step of a massive breach.

The threat is already here. Deep learning AI techniques are leagues ahead of their abilities and only getting more sophisticated. As the availability of high-end processing rises and its cost

lowers, the threat level, frequency, and convincing nature of deepfakes will increase—there is nothing as effective as confidence in encouraging a victim to drop their guard.

**AGGREGATE CYBERCRIME
LOSSES ROSE FROM
USD 3.5 BILLION IN 2019 TO
USD 12.5 BILLION IN 2023[†]**



Adaptive tactics

Equally as concerning as the human element, AI has begun dissolving the defenses that the information security sphere has built over the past few decades. Criminals no longer need to spend their time probing a network, because an AI can be trained to automatically analyze an institution's digital footprint. Automated reconnaissance allows potential attackers to discover vulnerabilities, map network structures, and essentially be presented with a plan of attack with little to no effort on their part.

Applied to the creation of malware, AI is equally insidious. Consumer-grade transformers like ChatGPT can, with the correct prompts, be coerced into writing malicious scripts. The controls which bind the output of chatbots are entirely circumventable; if a hacker wishes to create a damaging and undetectable PowerShell script, ready for deployment, they can.

Along similar lines, AI can design polymorphic malware, which changes its code or behavior to evade traditional antivirus detection methods, hugely increasing the level of remediation required to keep it at bay. It is even possible to use AI to coordinate DDoS attacks, optimizing and scaling them once it identifies the most effective vectors and patterns to overwhelm a system.

And cybersecurity professionals can't forget that AI is a two-way street. As workers rely more and more on AI to perform their day-to-day tasks, they also input increasing amounts of sensitive data into AI engines. That's an incredible amount of trust placed in a tool that may be spoofed, intercepted or insecure, a tool we already know can be tricked and exploited. Few companies have the resources to run a fully internal GPT, much less one with the power of the leading engines, meaning any data input into an AI engine is essentially being willingly placed out in the open.

Poisoning the well

For companies using AI to their advantage, it is important to realize that the AI battle is not one fought along a defined front. A criminal acting in enemy territory can disrupt the AI systems organizations are coming to rely on. By poisoning a data set, for instance, corrupted data could cause flawed or biased decision-making or encourage a public-facing AI to output undesirable responses. If an exploited AI is responsible for automation, it could cause a cascading failure before it is even noticed.

We've seen high-profile examples of poisoned AI before. One of Microsoft's earliest chatbots, Tay, was designed to develop conversational understanding by talking with humans on Twitter, learning from their posts. Even in 2016, Twitter offered a rather corrupt data set. Tay lasted just one day on the platform, which was all it took for a coordinated attack by a subset of Twitter users to teach the AI to be racist, antisemitic, and lewd.

Amidst the AI gold rush, many businesses are more interested in pulling the trigger on new AI innovations than checking that the safety is on. Microsoft's apology statement of 2016 reverberates today, almost a decade later: "To do AI right, one needs to iterate with many people and often in public forums. We must enter each one with great caution and ultimately learn and improve, step by step."



**THE GLOBAL COST
OF CYBERCRIME
IS ESTIMATED TO REACH
ALMOST USD 14 TRILLION
BY 2028[†]**

If AI is deployed without the proper safeguards in place, hackers need not even poison the data set. So-called adversarial attacks feed such systems maliciously crafted data, designed to manipulate them into making errors or breaking entirely. Even public-facing transformers have their quirks. It was recently discovered that ChatGPT's generation fails if it is asked to output certain people's names, for example—fine if one's use of AI is frivolous, but a disaster in a production context.

AI advantages

Logically, the information security sector must fight back with its own AI tools. There is nothing moving at quite the same pace nor growing in complexity in quite the same way as the world of machine learning and generative AI. However, dealing with the AI onslaught is not a task that IT professionals can complete manually.

Predictive models

The ability of AI systems to analyze vast amounts of data in real-time means they are well suited to identifying patterns and detecting anomalies that indicate possible cyberthreats. Predictive models may offer a glimpse into the future, helping to prevent future attacks based on prior knowledge. In essence, AI takes on the role of the seasoned information security professional—the person who always knows the answer. The more data AI can collect, the more seasoned it becomes.

Behavioral analytics

By flagging deviations from usual patterns, behavioral analytics can identify unauthorized access and even work to fight against insider threats. If a user with legitimate credentials behaves strangely—accessing things they typically wouldn't or logging on at unusual times—AI can detect this and trigger an automation to stop it.

Specialized AI

Used to spot inconsistencies in AI-generated media, specialized AI helps uncover deepfakes and reinforce trust in communications. AI can detect polymorphic malware through heuristic analysis and pattern recognition. It can sanitize data and inputs to preserve the integrity of AI models, analyze traffic to spot unusual activities, and automatically trigger an incident response if an intrusion is detected. With AI, information security efforts can fire as incidents happen rather than reacting after the fact. However, AI is not a complete answer—certainly not a drop-in solution.



THE AI CYBERSECURITY MARKET
WILL GROW TO OVER
USD 60 BILLION BY 2028[†]

An expanded defensive posture

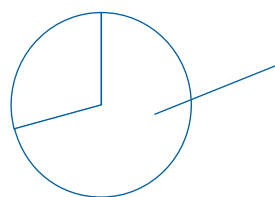
However difficult the process of developing and implementing them may be, AI-driven cybersecurity solutions must be part of the defensive toolkit. The scale of AI activity is simply too great. Those that ignore the unique advantages of AI tools will inevitably struggle against the sophistication and frequency of AI-driven attack techniques. AI may even prove cheaper than more manual security processes, with IBM suggesting that companies using AI enjoyed an average saving of USD 2.22 million[†] against those that did not. That does not mean, though, that defensive AI is the one true solution to the onslaught of AI hacks.

The fact is criminals have an innate advantage. Their singular focus allows them to remain one step ahead of any immature AI information security strategy. Institutions must pour time and effort into monitoring and updating all AI systems, including the AI engines hastily integrated into day-to-day business practices, to detect and mitigate adversarial attacks. Even then, it is safe to assume that criminals have as-of-yet unknown attacks ready to deploy.

Defensive AI is one tool of many—effective in the right places, but not infallible, and arguably less important than behaving in a proactive manner and getting the fundamentals right. AI may be able to offer alerts and guidance, but it does not make humans less vulnerable as an attack vector. Conducting regular security awareness training helps hammer home the importance of behaving in a safe and cynical manner.

GENERATIVE AI COULD PUSH AVERAGE
FRAUD **LOSSES** TO
USD 40 BILLION BY 2027[†]

As it always has, strong information security relies on multi-layered defense strategies. AI is one of these, but institutions may not be able to weather the storm without a culture of strong policy making, intelligent access controls, and a Zero Trust model that helps ensure such policies work as they are supposed to. There is no sense in being dazzled by the new and exciting, because the fundamental principles of security have not changed at all. ■



71% OF ORGANIZATIONS
HAVE UNFILLED CYBERSECURITY
POSITIONS[†]

ZERO TRUST WORLD 2025

Bigger, bolder, and more hands-on than ever

BY HEATHER HARTLAND, CMP, CMM VP EXPERIENTIAL MARKETING

In our 5th edition, Zero Trust World (ZTW) has reached a remarkable milestone. This year, over 1,800 attendees from 28 countries gathered for three days of in-depth cybersecurity sessions, engaging hands-on hacking labs, and a Solutions Pavillion packed with innovations to explore. This dynamic group of industry leaders and rising professionals joined forces to address the most pressing cybersecurity challenges. We came together to learn, collaborate, and celebrate every new Cyber Hero® who earned certification at ZTW.

A SPEAKER LINEUP PACKED WITH CYBERSECURITY HEAVYWEIGHTS

This year's speakers brought serious expertise to the stage, including:

Reggie Fils-Aimé

Former President & COO, Nintendo of America

Rob Allen

Chief Product Officer, ThreatLocker

Art Ocain

VP of Cybersecurity & Incident Response, Airiam

Chase Cunningham

Dr. Zero Trust

Trina Ford

CISO, iHeartMedia

Danny Jenkins

CEO & Co-Founder, ThreatLocker

Hector Monsegur & Chris Tarbell

Hacker & The Fed

David Sparks

Cybersecurity Journalist, CISO Podcast

Leo

Founder, PC Security Channel

CYBER HERO CERTIFICATION & GIVING BACK

Attendees had the chance to earn their Cyber Hero certification at the onsite exams—those who passed were refunded their registration fees. It required effort and preparation. Of 672 attempts from 339 contenders, 120 cybersecurity pros earned the coveted title. Congratulations to all new Cyber Hero pros who joined the ranks of elite defenders.

Meanwhile, ThreatLocker Cyber Hero Swag Store sales raised funds for the Ronald McDonald House Charities of Central Florida, with ThreatLocker matching every dollar. In a big finale, the auction of Danny Jenkins' Iron Man suit brought the total donation to USD 106,000.

DEEP-DIVE SESSIONS & HANDS-ON LABS

From our laptop-provided hacking labs to thought leadership on the mainstage, attendees enjoyed a selection of 61 sessions and earned over 17,000 clock hours of continuing education.





Adam Reid, Hector Monsegur, and Chris Tarbell during the “Hacker & The Fed” talk

With multiple hacking labs, our goal was to equip IT professionals with the mindset and skills to defend against hackers. We wanted attendees to walk away with a deeper understanding of how hackers think and operate—so they can anticipate threats, strengthen their defenses, and always stay ahead.

DANNY JENKINS,
CEO & CO-FOUNDER, THREATLOCKER

LABS COVERED:

- Methods for cookie theft and phishing
- Exploiting Active Directory vulnerabilities
- Use of Metasploit in real-world hacking scenarios
- Rubber Ducky techniques and malware development

KEY SESSIONS COVERED:

- The Zero Trust approach and the cybersecurity landscape
- Shadow IT risks, ransomware, and understanding the dark web
- Revolutionizing incident response and protecting against supply chain threats
- Preventing unintended lateral movement and the use of AI in security operations

A SUPER-POWERED AFTER PARTY

We celebrated all the heroic learning and connections with a comics themed party: Zero Trust, Justice, and a Better Tomorrow. The costumes were next-level, and we can’t thank our participants enough for going all out.

To everyone who joined us—attendees, speakers, and our incredible ThreatLocker team—thank you for making this our best Zero Trust World yet.

We can’t wait to see you all
March 6–8, 2026, in Orlando, FL.



Register at
ztw.com with code
ZTWMAGAZINE26
for USD 200 savings
at checkout.

THREATLOCKER
**ZERO TRUST
WORLD '26**

THE ENEMY WITHIN

You've locked down your firewalls and hardened every endpoint so no one gets in. But the enemy doesn't need to infiltrate—they're already inside.

The damage from insider threats, inflicted from within an organization's defenses, can be even more severe than attacks from outside the perimeter. Insiders—or users—are a ticking time bomb that is unpredictable, underestimated, and potentially absolutely devastating.

Two thousand twenty-four statistics suggest insider threats count for 35% of all data breaches[†], yet only 30% of CISOs rank insider threats as a major concern. It's a risk that's growing—insider breaches accounted for just 20% of the total in 2023—but is largely being swept aside in favor of louder and more obvious digital hazards.

“

Poorly configured access to critical resources can be a powerful source of accidental sabotage



THREATLOCKER TIP

Use ThreatLocker Storage Control and Unified Audit to control data access and instantly view all activity.

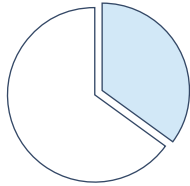
Insider threats first

If anything, insider activities should be at the top of the cybersecurity list, given that their varied and unknowable nature makes them so dangerous. This hazard exists outside of the archetype of the shadowy hacker, and can emerge from anywhere. Security professionals must be ready for anything, from the innocent to the malicious, and consider every user as a potential trojan horse. While active attacks are in the minority, accounting for only 27% of the total number of threats, employees or contractors working with malice are some of the most dangerous.

They might use their system access to deliberately steal data, install malware, or sabotage critical systems. External attackers, rival businesses, or criminal syndicates might also coerce those with legitimate access credentials to steal sensitive information or perform acts of fraud or espionage. A user doesn't even need to know they've been compromised; account credentials delivered to malicious hands through phishing attacks, shoulder surfing, or careless actions turn employees into unknowing accomplices.

The people problem

Psychologist B.F. Skinner wrote in 1969's *Contingencies of Reinforcement* that “the real problem is not whether machines think but whether men do.” Skinner's words predated the modern information society, but they ring truer than ever today. When one looks along the lines of negligence—the re-used passwords, the accidental attachments,



2024 STATISTICS SUGGEST
INSIDER THREATS
ACCOUNT FOR 35 %
OF ALL DATA BREACHES

the overworked and under-vigilant worker falling prey to attacks—that quote comes into focus. And it does not only apply to users. Oversight on the part of administrators and poorly configured access to critical resources, can be a powerful source of accidental sabotage.

It is vital that administrators do not ignore the explosion in potential attack surfaces that the modern hybrid environment provides. A planted USB drive, “lost” near an office and plugged in by a well-meaning employee, is a classic and not-quite apocryphal way of malicious software making itself into the bounds of the network perimeter. But there is so much more to contend with today: the IoT devices which have fallen behind in their update schedule, providing a backdoor for attackers; the messaging apps, from personal software like WhatsApp to corporate-sponsored platforms like Slack, which relax employees and may stop them thinking twice about sharing files they shouldn’t; the advanced espionage hardware, imperceptible USB keyloggers, data sniffers, or compromised Wi-Fi networks which sneak past traditional defenses.

Each of these, and countless more, serve as a reminder that modern security is not just about building and maintaining an impenetrable digital fortress. When one’s business consists of a thousand potential Trojan horses, it is as important to build behavioral awareness, operational vigilance, and an ingrained security culture that works to prevent potential insider attacks from ever happening willingly or accidentally.

On the defensive

A Zero Trust mentality forms a large part of these countermeasures. The point here, after all, is that no user, and no access, is inherently trustworthy. Strict access controls, identity verification and least-privilege policies go a long way to eliminating the possibility of insider attacks.

Administrators also need visibility. Behavioral analytics can detect suspicious behavior early, allowing it to be stopped before it turns into an attack. Anomalous logins, unusual file transfers, and excessive data downloads may all be indicators of espionage and can all be made visible to security personnel without compromising privacy.

On the ground, the key is buy-in from workers and executives alike. Cybersecurity is not only an IT issue; it’s a boardroom issue. Clear policies built around well-defined accountability structures encourage appropriate action from above, while regular training and clear messaging can ensure employees in the firing line remain hyper-aware.

“

**On the ground,
the key is buy-in
from workers and
executives alike.
Cybersecurity is not
only an IT issue; it’s
a boardroom issue**

The new cybersecurity posture

The solution to insider threats boils down to preparing for the inevitable. No strategy is bulletproof; Zero Trust behavior will minimize the impact, but it must go together with complex risk assessments, regular attack simulations, and well-formulated incident response plans. This is a case of safeguarding against human nature itself, outsmarting an enemy one cannot possibly know before they make a move. When the enemy is already within your walls, you can’t let your guard down for a second. ■

CLEARING THE FOG OF WAR

A security operative who fights blind is next to useless; they can be effective only with frontline intelligence derived from comprehensive logging and real-time monitoring.

The cybersecurity battlefield is consistent in its inconsistency. It's a never-ending, grinding fight against known and unknown threats, an enemy that is always changing shape and direction. These are muddy and miserable trenches, and those on the defense need every advantage they can get.

Belabored as that metaphor may be, it is true at its heart. While administrators have effective tools at their disposal to repel cyber threats, like the perimeter defenses of old and the Zero Trust methodology of modern times, dealing with amorphous threats demands a high level of understanding. Driving forward with Zero Trust principles means maintaining a proactive security posture, and this is only possible if robust logging and monitoring strategies support all efforts.

The Zero Trust assumption of potential compromise necessitates the kind of deep visibility that comes from inten-

sive log management and the rapid countermeasures such record-keeping makes possible. Continuous visibility, real-time threat detection, and adaptive response mechanisms both highlight and help deal with security threats as they occur.

EMBRACING MODERN LOG MANAGEMENT

Zero Trust is, in this sense, self-solving. It provides its own catalyst for activity analytics. The concept of monitoring and logging is inherent within its framework, such that adhering to its

A STANDARD
WINDOWS SERVER
GENERATES
65,000
LOGS PER DAY[†]

principles will naturally lead security professionals directly to the mechanisms required to do so.

For example, the Zero Trust approach to security is universal, suggesting that everything could be a threat. This encourages removing siloed and fragmented systems in favor of centralized, far-reaching policies layered with granular exceptions. In turn, this refactoring provides the opportunity to apply a log management system that covers endpoints, network devices, applications, and cloud services in a unified manner—one that can use tools like TLS inspection and machine learning—powered anomaly detection to detect unusual behavior even beneath the cloak of encryption.

Security events, whatever and wherever they may be, can be correlated, analyzed, and treated with the appropriate level of care and concern. Some separation cannot be avoided, of course. With the rise of distributed and hybrid environ-

ments, logs are naturally generated across diverse infrastructures. Anything can be an attack vector—and indeed, so can multiple things at once. Therefore, security teams must correlate these logs to analyze event patterns across on-premises and cloud-based assets and identify coordinated attacks.

Often, the clues are not so obvious. A sophisticated enough attack may fly under the radar and not immediately appear malicious, which only highlights the fragility of rules-based monitoring. Behavioral analytics can help uncover these hidden truths, revealing deviations from normal user behavior to emphasize potential threats like insider attacks, credential abuse, lateral movement, or anomalous privilege escalation. Malicious behavior comes before a breach; uncover it, and that breach may not happen.

ALIGNING MONITORING WITH ZERO TRUST

Essentially, all Zero Trust activities—continuous verification, least privilege access enforcement, and adaptive access controls—are built on a foundation of logging and monitoring. Continuously monitoring login attempts, device telemetry, and patterns of application access allows the construction of real-time adaptive authentication policies. Identity-centric monitoring hardens least privilege access controls, ensuring that unusual escalations trigger immediate alerts, access to critical systems is continuously validated, and compromised accounts are automatically isolated to prevent further damage.

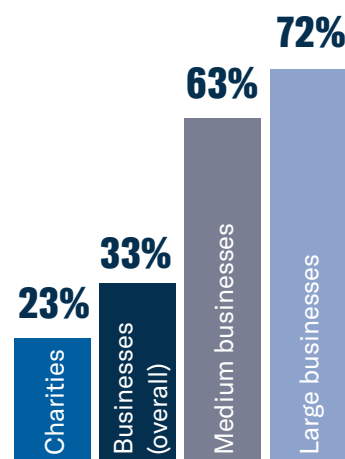
Given that the Zero Trust culture of micro-segmentation attempts to limit the breadth of attack surfaces, logging is fundamental here, too. It adds context to potential lateral movement attempts, allows minute details like API calls and microservice interactions to be brought to the forefront, and helps to identify unauthorized resource access. Logging, in a sense, builds better policies over time through the demonstration of potential vulnerabilities.

“

Modern security teams cannot afford to be overwhelmed by a constant stream of alerts: their job is to oversee and implement policies, not to directly micromanage every tiny network interaction

But these systems must also be smart enough to avoid overload. Modern security teams cannot afford to be overwhelmed by a constant stream of alerts: their job is to oversee and implement policies, not to directly micromanage every tiny network interaction. Automation is a core part of reducing such noise, whether blocking IP addresses exhibiting malicious behavior, placing MFA challenges in front of anomalous authentication attempts, or quarantining suspicious workloads or endpoints in real-time.

PERCENTAGE USING NETWORK SECURITY MONITORING TOOLS†:



MORE THAN JUST COMPLIANCE

For some, logging and monitoring have long been seen as tedious compliance checkboxes, helping businesses remain in line with regulatory frameworks like GDPR, HIPAA, and CISA mandates. It should be clear that this is far from the case. Yes, these processes keep one's business compliant, but they are also core pillars of Zero Trust security. They provide the ammunition required to strike down cybersecurity threats, pushing organizations from a reactive, defensive posture to a proactive stance, ready to repel any potential attack. ■

HIDDEN CLAWS

Mimikatz exploits the weakness beneath Windows' skin

Mimikatz began life wearing a white hat. Developed by French security researcher Benjamin Delpy as a proof-of-concept tool designed to demonstrate a major flaw in Windows' password handling routines, it immediately caught the attention of the black hat community—and when Microsoft initially all-but ignored his findings, Delpy felt compelled to release the tool to the world.

Mimikatz has, in the 13 years since its release, maintained its position as what Wired Magazine calls “one of the world's most widespread and powerful password stealers.” By exploiting an issue inherent in Windows' native Local Security Authority Subsystem Service (LSASS), the tool simply sniffs out user credentials stored in RAM, along with the keys required to decrypt them, trivialising the process of extracting passwords, hashes, PINs and Kerberos tickets.

If an attacker can find a way to gain administrator- or system-level privileges on a host—by injecting into a suitable application, for example, or exploiting an OS process that many security tools whitelist by default—they can run Mimikatz and subsequently use its tools to gain the credentials required to gain elevated access network-wide.

Microsoft's stance has inevitably changed, patching many key features of Mimikatz since its release. Windows 8.1 offered the option to switch off WDigest, a vital component of the exploit, while

Windows 10 and 11 disabled it by default. However, legacy systems remain as vulnerable as ever, and many organizations rely on digest authentication through WDigest, so they cannot simply disable it entirely.

Mimikatz, too, has progressed over its lifetime. Not only has Delpy continued to update it in the years since its release, adding additional features including (amusingly) the ability to cheat at Minesweeper by extracting the position of its bombs from memory, but its open-source nature has seen hackers build Mimikatz functionality directly into effective and damaging ransomware and worms.

With the exploit tied so closely to the operation of the Windows OS, the only real solution is to apply the principle of least privilege to ensure a strong security posture that does everything to mitigate the exploitation of such vulnerabilities. As Delpy told Wired in 2017, “If Mimikatz has been used to steal your passwords, your problem is not Mimikatz.”

WHAT CAN MIMIKATZ DO?

- Pass-the-hash attacks allow hackers to impersonate a user by injecting an extracted hash in place of a password.
- Pass-the-ticket attacks use Kerberos authentication tokens to impersonate users without even needing their credentials.
- Pass-the-cache attacks exploit UNIX-format access tickets (from a Mac or Linux machine, for example) to perform a pass-the-ticket authentication.
- Overpass-the-hash attacks obtain hashed passwords from domain controllers and use them to impersonate users.
- Silver ticket attacks exploit password hashes for key services like file shares or SQL servers to create a fake Kerberos service ticket and gain access.
- Golden ticket attacks enable hackers who obtained the Kerberos server password to gain non-expiring admin credentials for any machine on the network.

GHOST IN THE SHELL

RedRabbit spotlights the unreasonable power of simple scripting

PowerShell is a formidable scripting language that has become a foundational element of modern system administration because of its reach and versatility. The flexibility and strength of PowerShell mean it can be used to access system processes, files, and network configurations directly. It can be employed for automation and task management, allowing the construction of complex operations with minimal overhead. It is, unquestionably, very useful.

Its power is also its greatest weakness: the extensive control it offers combined with the deep integration of PowerShell into the Windows OS make it an attractive target for malicious actors. It runs directly in system memory, evading the reach of traditional file-based antivirus; for those developing living off the land attacks, PowerShell is the ideal tool. It is little wonder that PowerShell is (ab)used in over 90% of ransomware attacks today[†].

But PowerShell can also be used to highlight its own vulnerabilities. For example, RedRabbit, a sophisticated penetration testing tool designed for Red Team investigations, is fully self-contained within a single 60KB, 3000 line PowerShell script. Designed by British security engineer Ash Moran, RedRabbit incorporates a long list of powerful infiltration and reconnaissance tools. A pen tester need only obtain administrator access and run the script to begin. The script can also be executed remotely using PowerShell's `iex` (Invoke-Expression) cmd let, bypassing any local script restrictions which may be in place. Its functions range from the relatively benign to the extremely dangerous. The first option amongst the 23 included tools offers testers a quick recon, listing the users, groups, admins and installed

programs on a host, for example. At the other end of the spectrum, it can deploy a keylogger and/or clipboard logger as a hidden process. Its network scanning capabilities allow RedRabbit to hunt for hosts and file shares on a network; other functions allow it to brute force password protected ZIP files, initiate control via a reverse shell or extract locally stored passwords.

The key is that RedRabbit does all of this within a PowerShell session, using only the built-in functionality of PowerShell's scripting language. It is not some advanced malware; really, RedRabbit is a little more advanced than a script, just one designed to use its own features against it. Any malicious script, allowed to run, could do the same, without needing a pretty menu or even any way for a user to know about it.

ThreatLocker® CPO Rob Allen suggests that tools like RedRabbit—and vulnerabilities in other applications, which could be used to call PowerShell—mean security professionals must consider internal tools as readily as they do external threats, and control applications to limit their potential reach. “Realistically,” says Allen, “why does anything need to call PowerShell? Does PowerShell need to access the internet in most cases? Does it need to access documents, the desktop, file shares or storage locations? No. So we need to focus on denying by default and permitting by exception. Most applications don’t need to interact with any other applications when they’re running. Ringfencing™ controls such interactions to prevent what is often the first stage of a major attack.” ■



“

It's not every day
you get to protect a
brand you've loved
your whole life.





SECURING THE COLTS

Jack Thompson's mission to protect data and trust

When most fans think of the Indianapolis Colts, they imagine thrilling touchdowns and game-day excitement. But behind the curtains, Jack Thompson works tirelessly to secure every facet of the organization. From protecting sensitive player data to ensuring fans' trust in digital transactions, Thompson has turned the Colts' cybersecurity posture into a proactive force that protects the organization's reputation and legacy. As the Director of Information Security, Risk, and Compliance for the Indianapolis Colts, Thompson combines his military-honed expertise with a deep commitment to the team he grew up rooting for.

Thompson's journey to this role is anything but conventional. "I started in the military doing all-source intelligence for the U.S. Army and later transitioned to cyber intelligence and operations in the Air Force," Thompson shared. This blend of investigative acumen and technical expertise laid the groundwork for his passion: identifying vulnerabilities and fortifying defenses against threats.

Afterward, Thompson worked in various industries, including healthcare, manufacturing, and logistics, before joining the Colts in September 2022. "When I saw the opportunity to work for my hometown team in a field I'm passionate about, it was a no-brainer," he said. "It's not every day you get to protect a brand you've loved your whole life."



Jack Thompson and Kyle Earnest work tirelessly to secure every facet of the Colts' data

“

The reliance on data for analytics and performance insights is growing weekly. That means more technology and, by extension, more risks to manage

As one of the NFL's most recognized teams, the Colts face a unique set of cybersecurity challenges. Professional sports organizations must protect a wide range of sensitive data, from fan information and payment details to player health records and intellectual property. “The scope of what we secure is vast,” Thompson explained. “We’re protecting personal information for fans, payment card data for ticketing, and even our internal strategies. Cybersecurity at the Colts means we are protecting our information and therefore people’s lives.” Thompson notes that the team’s operations go beyond the field. The Colts’ stadium infrastructure is categorized as critical under federal guidelines, requiring a heightened focus on cybersecurity.

“We have to think about physical security, cybersecurity, and how the two intersect,” he said. “It’s a responsibility we take very seriously.”

When Thompson joined the Colts, the organization operated in a largely reactive cybersecurity posture. “We were using traditional tools like next-gen antivirus and endpoint detection and response, but it always felt like we were a step behind,” he said. That changed with the implementation of ThreatLocker®, a Zero Trust solution that Thompson first encountered at a cybersecurity conference. “The ThreatLocker proactive approach completely transformed our posture,” he said. “Instead of reacting to threats, we’re now in a position to prevent them from materializing.”

“As I listened to Danny Jenkins, CEO of ThreatLocker, on that stage, what caught my eye was his background in technology and being a practitioner. His passion for the product and his understanding of the challenges we face made the difference.” The ThreatLocker Application Allowlisting and user-friendly interface made it an ideal fit for the organization. “It simplified what

is often a complicated process,” Thompson said. “The tool allowed us to move quickly, with fewer false positives and less time spent on implementation. It’s been a game-changer.”

Thompson credits a large part of his success to the support of the Colts’ ownership and leadership. “Trust starts at the top,” he said. “The ownership understands the importance of cybersecurity and has given me the resources and freedom to build a strong program.” This support extends to the team’s broader culture, which values security and mental well-being. “The Colts have a dedicated foundation, Kicking the Stigma, that focuses on mental health awareness,” Thompson said. “It’s inspiring to work for an organization that prioritizes not just the safety of its data but also the well-being of its employees and community.” That culture of trust influences Thompson’s approach to fan data, as he believes fans benefit from the team’s behind-the-scenes efforts. “Our fans might not think about cybersecurity daily, but they can rest assured they are one of the best-protected fan bases in professional sports.”

“

We were using traditional tools like next-gen antivirus and endpoint detection and response, but it always felt like we were a step behind

As the sports industry becomes increasingly digital and data-driven, cybersecurity will play an even more significant role in shaping its future. “The reliance on data for analytics and performance insights is growing weekly,” Thompson stated. “That means more technology and, by extension, more risks to manage.”

Thompson envisions a continued evolution for the Colts’ cybersecurity program. “We’re going through a digital and cultural transformation, and I’m committed to ensuring security is a central part of that,” he said. Despite the challenges, Thompson finds deep fulfillment in his role. “Being able to give back to the team I love while knowing we’re doing right by our fans and community is incredibly rewarding.” For Thompson, cybersecurity is his way of defending the legacy of a team that means so much to him and the Indianapolis community. As he looks to the future, his mission remains clear: to keep the Colts secure, resilient, and ready to win more championships. ■



The Colts’ stadium infrastructure is categorized as critical under federal guidelines, requiring a heightened focus on cybersecurity

NATURE'S PRESCRIPTION

El Capitan is a vertical rock formation on the north side of Yosemite National Park



FOR DIGITAL DEMANDS

For IT professionals, the high-pressure demands of safeguarding digital infrastructures can lead to chronic stress and burnout. Hiking in remote natural settings offers an antidote, combining physical activity with mental rejuvenation.

Research consistently shows spending time in nature reduces cortisol levels, lowers blood pressure, and improves mood by increasing serotonin. Silence amplifies these benefits, fostering introspection and grounding. Hiking through forests or mountains also exposes the body to phytoncides, natural compounds emitted by trees that boost immunity and reduce inflammation. By choosing remote trails, technology professionals can step away from their digital routines, recharge their minds, and gain clarity. Here's where to take your next nature retreat.

Glacier National Park, Montana

Known as the “Crown of the Continent,” Glacier National Park offers dramatic landscapes of rugged peaks, crystal-clear lakes, and pristine forests. Begin your visit with a drive along the Going-to-the-Sun Road, a 50-mile scenic route with breathtaking views and photo opportunities. Wildlife enthusiasts can spot grizzly bears, mountain goats, and eagles throughout the park.

For hikes, try the Highline Trail for stunning vistas and wildflowers, or the Grinnell Glacier Trail, where you'll pass turquoise lakes and towering glaciers. Families can explore the Trail of the Cedars, a short, serene walk through ancient forests. During summer, boat tours on Lake McDonald or St. Mary Lake provide unique perspectives of the park's grandeur. End your day stargazing, as Glacier is also an International Dark Sky Park, perfect for nighttime photography and quiet reflection.

WHERE TO STAY: UNDER CANVAS GLACIER

Located just 10 minutes from Glacier National Park, this eco-friendly glamping site offers safari-style tents with high-end touches like king-size beds, private bathrooms, and wood-burning stoves. Surrounded by pine forests and mountain views, the camp's amenities include on-site dining with locally sourced dishes and nightly s'mores by the campfire. Activities like yoga sessions, live music, and guided park tours enhance stays. Guests can also borrow bikes or embark on nearby trails directly from the property.

Under Canvas
Deluxe bedroom
with Hive by Bailey
Made Studio





Above: Panoramic backcountry camping over Merced Lake

Right: AutoCamp Clubhouse features sleek Airstream caravans in a serene forest setting

Yosemite National Park, California

Yosemite National Park is a natural wonderland with granite cliffs, towering waterfalls, and ancient sequoia groves. Start at Yosemite Valley, accessible year-round, where iconic sights like El Capitan, Half Dome, and Bridalveil Fall await.

For hikers, the Mist Trail leads to Vernal and Nevada Falls, while the Glacier Point Trail rewards with panoramic views of the valley. For an easier trek, Mariposa Grove offers a walk among giant sequoias, some over 2,000 years old. Adventurers can climb Half Dome, which requires a permit and plenty of stamina.

Other activities include wildlife watching, rock climbing, or floating on the Merced River in summer. Fall brings vibrant foliage, while winter is perfect for snowshoeing.



WHERE TO STAY: AUTOCAMP YOSEMITE

AutoCamp Yosemite redefines camping with a contemporary touch. Located just outside the park, this upscale retreat features sleek Airstream trailers, luxury tents, and spacious cabins, all designed for comfort and style. On-site amenities include a clubhouse, fire pits, and a heated pool. Guests can rent bikes, join yoga classes, or savor craft meals from The Kitchen. AutoCamp also has an on-site shuttle stop for easy access to Yosemite's entrance, via YARTS (Yosemite Area Regional Transportation System).

Dogwood Canyon Nature Park, Missouri

In the Ozarks, Dogwood Canyon Nature Park is a 10,000-acre paradise filled with waterfalls, caves, and wildlife. Start at the Visitor Center, where you can learn about the park's conservation efforts before heading out to explore.

Hiking trails in the area range from easy to moderate difficulty. Scenic highlights include Pine Ridge Pass and Hickory Ridge, which feature meandering streams and cascading waterfalls. Consider renting a bike to explore the trails for a different perspective of the park.

Guided wildlife tram tours allow visitors to see bison, elk, and longhorn cattle in the park's managed herds. Fishing enthusiasts can enjoy casting their lines in the trout-filled streams, while horseback riders can book majestic trail rides. Families will appreciate the Treehouse built by Animal Planet's "Treehouse Masters" and the interactive exhibits throughout the park.



WHERE TO STAY: BIG CEDAR LODGE

Big Cedar Lodge, in Ridgedale, blends rustic charm with modern luxury. Nestled within the Ozark Mountains, this resort offers log cabins, private lodges, and cozy cottages, all with stunning views. Top notch amenities include world-class golf courses, a spa, and water activities on Table Rock Lake. Guests can explore nature trails, enjoy outdoor adventures, or indulge in award-winning dining experiences featuring genuine Ozarks hospitality and breathtaking views. Big Cedar Lodge is an ideal escape for families, couples, or solo travelers seeking relaxation in a quiet wilderness setting.

Below: World-class golf courses between nature pursuits at Big Cedar Lodge





Above: All-levels hiking trails in Great Smoky Mountains National Park

Great Smoky Mountains National Park, Tennessee

The Great Smoky Mountains National Park straddles Tennessee and North Carolina, offering lush forests, mist-covered peaks, and rich biodiversity. Begin your visit at Clingmans Dome, the park's highest point, for panoramic views.

Hiking trails abound, including the Alum Cave Trail to Mount LeConte and the untamed Cades Cove Loop, where you can spot deer, black bears, and turkeys. For waterfalls, the Grotto Falls Trail allows you to walk behind a cascading waterfall, while the Appalachian Trail winds through the park for those seeking a longer trek. Other activities include auto-touring, horseback riding, and fishing in pristine mountain streams. Vibrant foliage attracts photographers in the fall, while spring brings wildflower blooms.

WHERE TO STAY: TREEHOUSE GROVE

Treehouse Grove offers a magical stay amidst the Great Smoky Mountains. Designed by Pete Nelson and the Nelson Treehouse & Supply Team from the TV show “Treehouse Masters” on Animal Planet, these elevated cabins combine whimsical design with modern amenities like full kitchens, private decks, and cozy interiors. Located in Gatlinburg, Tennessee, the treehouses provide easy access to the national park while offering a serene retreat after a day out. Guests can enjoy stargazing, campfires, and the wild sounds of the Smokies.



Left: *By The Creek* houses at Treehouse Grove, Gatlinburg

Above: Inside *The Black Jack Oak* treehouse

DuPont State Recreational Forest, North Carolina

Year-round, DuPont State Recreational Forest offers a 12,500-acre wonderland of waterfalls, lakes, and lush woodlands. The forest's diverse ecosystems make it a haven for birdwatchers and photographers. Start with the Triple Falls Trail, a moderate hike featuring three waterfalls. Nearby, the High Falls Trail leads to a 150-foot waterfall with a covered bridge above, ideal for picnics.

For a longer trek, the Lake Imaging Loop reveals the park's clear lakes and forested landscapes. The forest is also popular for mountain biking, horseback riding, and fishing. Don't miss visiting Bridal Veil Falls and other recognizable film locations from "The Hunger Games."

WHERE TO STAY: DUPONT YURTS

Located near the forest, DuPont Yurts offer an off-the-grid retreat with creature comforts. Ideal for nature lovers seeking an intimate escape, these cozy yurts are equipped with plush beds, heating, and outdoor fire pits for stargazing nights. Surrounded by woodland, the yurts provide a serene base for exploring or simply unwinding in a closer-to-nature setting. 



THE GEAR

The Starlink Mini, the smallest offering from the SpaceX-affiliated satellite internet service, is the ideal solution for those who need to roam but can't bear to lose connectivity even in their downtime.

It features a built-in router, low energy consumption, and the ability to provide speeds up to and over 100 Mbps. Starlink's Roam service plan can even operate while moving at speeds up to 100mph, making off-grid on-grid.



[READ FULL ARTICLE ON PAGE 48](#)

Assessing Starlink Mini:

A COMPACT INTERNET SOLUTION FOR REMOTE LOCATIONS

The Starlink Mini stands out as a compelling choice for those needing dependable internet access while on the move. Its compact design and minimal power requirements make it easy to toss into a backpack alongside your laptop and portable power bank. This lightweight device is perfectly suited for travelers, remote workers, and anyone in areas with spotty connectivity.

SETUP AND EASE OF USE

Setting up the Starlink Mini is a breeze. Power it on and connect your device to its Wi-Fi—there's no need for lengthy configurations. The optional mobile app adds extra features, like optimizing satellite orientation, setting up a Wi-Fi password, and watching network statistics. It also tracks uptime, service interruptions, speed tests, and power usage, providing valuable insights into the performance of your connection.



Starlink Mini offers plug-and-play design with fast activation

PERFORMANCE AND CONNECTIVITY

When we tested it out in urban and rural environments, the Starlink Mini delivered solid download speeds with low latency, thanks to Starlink's low-Earth orbit satellites positioned within 350 miles of the surface. However, upload speeds were inconsistent at times, though they typically stabilized quickly. The performance was sufficient for general office work and video conferencing, though heavy data uploads may require some patience.

The power consumption remains low, averaging around 25–30 watts under load. This makes it last several hours with a standard portable battery bank. While the Starlink Mini is limited to Wi-Fi 5, the real-world impact is minimal, given Starlink's bandwidth limitations.

DESIGN AND DURABILITY

The Starlink Mini boasts a weather-resistant design, rated IP67, ensuring it can withstand the elements, although we have yet to put it to the test in harsher conditions. The supplied power cable is not only sufficiently long but also weatherproof at both ends,



Above: Low latency and decent speeds make it possible to stay connected even in remote locations

Below: Starlink Mini is compact and lightweight, making it ideal for travel and remote work



enhancing its durability for outdoor applications. Moreover, the Starlink Mini includes an Ethernet port, though an Ethernet cable is not part of the package. For outdoor setups, it's advisable to use a weather-resistant cable.

FINAL THOUGHTS

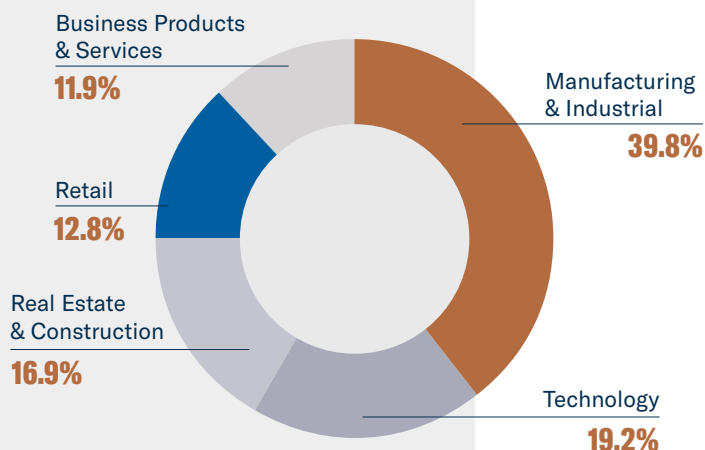
The Starlink Mini is a well-designed, portable connectivity solution that effectively combines user-friendliness with solid performance. While you may experience some fluctuations in upload speeds and the limitation posed by Wi-Fi 5, the overall speed, latency, and portability make it an appealing choice for those needing internet access in remote or mobile locations. If reliable connectivity on the go is essential for you, then the Starlink Mini is worth considering. ■

SECURITY CHALLENGES IN MANUFACTURING

Digitalization has transformed the manufacturing sector. Now, manufacturers need to focus on building their defenses in the face of rising security attacks.

Harrison Steel Castings

Most ransomware attacked industries 2024[†]



The manufacturing sector's cybersecurity challenge

The manufacturing sector is the lifeblood of the global economy. "Nothing can be made except by makers," Henry Ford famously said. The essential nature of manufacturers puts them in a uniquely vulnerable position on the world stage, one which cybercriminals are all too willing to exploit. The National Institute of Standards and Technology (NIST) reports that manufacturing is now the most targeted industry for cyberattacks. IBM's X-Force Threat Intelligence Report states that 25% of all security incidents strike manufacturing targets.

This is partly a problem of the sector's own making. The shift towards advanced digitalization in manu-

facturing, known as Industry 4.0, began to accelerate in the mid-2010s, before the development of much of what we now understand about cybersecurity, leaving the sector in limbo. Operational technology has been mixed with information technology, accruing all the risks that come with it yet, often, without the same security priorities or capabilities that modern equipment enjoys.

Facing the security challenge

Bringing security into the future is a distinct challenge for manufacturers. Although IBM's report also states that 85% of incidents at critical infrastructure organizations could be mitigated with patching, multi-factor authentication, and least-privilege principles, the industry is often not well-equipped to create and maintain robust cybersecurity protocols.

Sometimes, they cannot do so even if the spirit is willing; certain legacy systems and machinery, built for long-term durability rather than digital security, have been brought kicking and screaming into this new age. The growing Industrial Internet of Things (IIoT) offers potential attackers an expanded attack surface. And threat actors, whether private or state-sponsored, will not stop. The stakes are too high.

A prime target in transition

Cyberattacks are devastating when they strike manufacturing businesses. A single attack could impede a manufacturer's ability to operate. The knock-on effects on the supply chain—missed shipments, strained relationships, global shortages—cause an explosion in real-terms costs. Given most manufacturing operations' precision and tight margins, even a brief disruption could lead to outsized consequences.

Zero tolerance for downtime makes manufacturers a prime target for ransomware. Focused criminals tend to concentrate on the targets most likely to pay; an industry heavily dependent on continued operation is a prime candidate. Moreover, manufacturing is a sector more affected by compliance issues than many others. Cybercriminals often attack manufacturers not to disrupt machinery but, as with other sectors, to steal information and harvest credentials. State-level privacy acts, global legislation like GDPR, and industry-specific directives like CMMC mean a breach could lead to significant, business-ruining fines.

New industry, new tricks

In many ways, manufacturing's problems are not unique at all. According to IBM, cybercriminals caused 48% of attacks across all industries by entering enterprise environments using legitimate credentials. These attackers did not break in—they simply walked through an open door. Tomorrow's tools will also come into play. Just as manufacturers are transitioning to Industry 4.0, threat actors are innovating and steadily moving towards cybercrime 2.0—a landscape in which generative AI will lead to more identity-based attacks.

“

Manufacturers must begin to view cybersecurity as a core component of their operational strategy—and by also fostering a culture of vigilance, cybersecurity leaders can work to safeguard their businesses against attack

Fighting back against attacks

Manufacturers are not as powerless as they might seem. A route to effective cybersecurity in manufacturing begins with policy management and least-privilege access controls, which ThreatLocker® can help administer. But even before that, it requires executive leadership buy-in. Statista data puts the average data breach cost in the industrial sector at USD 5.56 million. In that context, investment in security infrastructure is a positive bargain. Manufacturers must begin to view cybersecurity as a core component of their operational strategy—and by also fostering a culture of vigilance, cybersecurity leaders can work to safeguard their businesses against attack. ■



We sat down with Shane Rogers, IT Director at century-old Attica, IN manufacturer Harrison Steel, to explore how leadership is critical in protecting operational continuity, preventing downtime, and fostering resilience in the manufacturing space.

READ FULL ARTICLE ON PAGE 52

BUILDING CYBER RESILIENCE IN MANUFACTURING

Shane Rogers
Harrison Steel Castings

Shane Rogers has dedicated over 28 years to managing and evolving the IT infrastructure of this prominent steel foundry. Starting his journey as a technician, Rogers has seen the company's digital landscape grow from a handful of computers to a complex system supporting various departments. In this interview, Rogers sheds light on the unique cybersecurity challenges facing the manufacturing sector, the impact of ThreatLocker® on his incident response approach, and his views on the future of cybersecurity in industrial settings.

What made you step into cybersecurity at a young age, and how did you evolve into your current role at Harrison Steel?

I began my career right out of school when I joined Harrison Steel as a technician. The tech landscape was much simpler back then—we had only a few computers, one server, and fundamental tech issues like fixing printers. Over the years, as technology rapidly evolved, so did my role. I moved up from technician to lead tech, then IT manager, and eventually to Director of IT. I oversee a much larger and more complex infrastructure with around 45 servers and hundreds of endpoints. This shift reflects the

growth of IT in the manufacturing sector, where we've become central to supporting the production process and ensuring that our operations remain secure and efficient. Looking back, it's been interesting to witness how much technology has transformed what we do here.

As a “technology-driven international engineering and manufacturing organization,” can you share more details about Harrison Steel and how IT needs transformed your work?

Harrison Steel is a steel foundry primarily focused on serving the mining industry. We create heavy-duty steel parts—some weighing as much as 18,000 pounds—that play a crucial role in our clients' operations. In a traditional sense, steel

“

Protecting our IT infrastructure is as critical as maintaining our equipment on-site

Rogers in the heart of tech operations in a bustling server room, ensuring seamless operation of essential systems



manufacturing might not be the first industry you'd think of as tech-dependent. However, IT has become increasingly important here over time. We now handle everything from CAD (computer-aided design) systems for design to automation and monitoring tools on the shop floor. IT supports every step of the manufacturing process and has to be constantly vigilant about security to prevent downtime or data loss, which would directly impact our production. There's a real need to balance legacy systems with newer technology, a unique challenge in our industry.

Given your long tenure, what have you observed in the role of cybersecurity, specifically within manufacturing?

The cybersecurity landscape has changed dramatically, especially in the past decade. When I first started, cybersecurity wasn't much of a concern—we focused mainly on keeping our systems running and addressing technical issues as they arose. But now, as manufacturing processes are more connected and reliant on technology, we're seeing more targeted attacks against our industry. Hackers have realized that manufacturing environments can be vulnerable, and a successful attack could shut down production, resulting in significant losses. So, we've had to take cybersecurity a lot more seriously, investing in tools like ThreatLocker to protect our network better and prevent unauthorized access to sensitive systems and data. Protecting our IT infrastructure is as critical as maintaining our equipment on-site.

You mentioned a production shutdown. How do cyberthreats impact a company like Harrison Steel, and how do you and your team support operation teams if an incident occurs?

Production downtime from a cybersecurity incident has far-reaching effects. While we've been fortunate to avoid downtime caused by security breaches—thanks to our protective measures—I can tell you how it could unfold if it happened. For one, our automated production lines would stop functioning correctly. We could switch to manual operations, which would drastically slow everything down.

Our custom-built applications and monitoring tools are crucial for tracking parts throughout the production process. If those went offline, we'd lose visibility over our workflow, which could further stall operations. Even if some production could continue slowly, we wouldn't be able to ship products without our shipping systems running. This would delay customer orders and payments, creating a financial ripple effect that impacts the entire organization.

Systems malfunctions directly create challenges for the whole workforce as downtime affects employees and their work. My team's role is to use the right mindset and tools to ensure these worst-case scenarios don't happen.

“

Zero Trust is less about restricting people and more about safeguarding the integrity of our operations



Harrison Steel is a steel foundry primarily focused on serving multiple heavy industries

Speaking of tools, how has ThreatLocker® changed your approach to cybersecurity and incident response?

ThreatLocker has been a game-changer for us, especially in incident response. Before we implemented it, our defenses were primarily reactive, so if a breach occurred, we'd deal with the consequences after the fact. With ThreatLocker, we now have a proactive layer of security that limits what applications can run on our network. It's like having an extra guard to prevent potential threats from executing. One recent example that stands out involved a phishing email that, had it not been for ThreatLocker controls, could have allowed malicious software onto our network. ThreatLocker blocked the program from running, which saved us from what could have been a very disruptive incident. This tool has made our network more resilient and given us peace of mind, knowing we have a system in place that catches threats before they cause damage.

“

Cybersecurity is challenging, but it's also rewarding because you're protecting something tangible

What unique challenges do you face in securing a manufacturing environment compared to other sectors?

One of the biggest challenges is dealing with legacy systems. In manufacturing, we often use equipment that's been around for decades and still serves its purpose well, but these systems weren't built with modern cybersecurity in mind. Compared to other sectors that can replace or update software more frequently, we can't swap out our machines every few years. So, we have to find ways to protect them without disrupting production. Another challenge is the industrial control systems (ICS) that run our manufacturing processes—they must be secured, but operate with minimal downtime. Any interruption can halt production and have a significant financial impact. So, our approach is more layered and has to account for these operational realities. It's a balancing act, ensuring security while running our processes smoothly.

Keep in mind that hackers are constantly evolving their methods, and we're seeing more targeted attacks rather than random malware or viruses. For example, phishing attacks have become incredibly refined, often mimicking legitimate communications that are difficult to spot.

Ransomware is another growing threat that’s especially dangerous for manufacturing because it can bring production to a halt. To protect against these threats, businesses need a multi-layered security approach. It’s about having solid defenses like ThreatLocker and educating our employees to recognize potential threats. For us, regular training and reminders about best practices have been essential.

Zero Trust is becoming a popular security strategy, but it is seen as complex. How do you implement and communicate Zero Trust principles at Harrison Steel?

Zero Trust is an intimidating concept for those outside of IT. Still, as you know, it’s about assuming that no one, inside or outside the network, is automatically trustworthy. We’ve taken a simplified approach to Zero Trust by focusing on limiting access based on role and enforcing strict permissions. For example, someone in accounting doesn’t need access to our engineering systems, and vice versa. ThreatLocker helps with this by ensuring that only approved applications can run. When explaining Zero Trust to our team, I emphasize that it’s about protecting our work and ensuring everyone can do their job without unexpected disruptions. It’s less about restricting people and more about safeguarding the integrity of our operations.

With everything we’ve discussed, what would you say keeps you motivated in this field?

I’ve been with Harrison Steel for nearly three decades, and I’m still motivated by the impact we can have. Cybersecurity is challenging, but it’s also rewarding because you’re protecting something tangible. Every day is different, and there’s always something new to learn. The stakes are high—keeping our systems secure means keeping our production on track and supporting the livelihoods of everyone who works here. It’s a responsibility I take seriously, and I’m always looking for ways to improve. Seeing how far we’ve come and knowing that our efforts make a real difference for the company and its people is what drives me to keep pushing forward. ■■

“
It’s about having solid defenses like ThreatLocker and educating our employees to recognize potential threats

Keys to robust cybersecurity in manufacturing

Integrated security and operations	Supply chain considerations	Employee training and awareness	Preparation for cyber incidents	Strict access controls
Cybersecurity must be a core part of IT in manufacturing, bridging IT and operational technology to protect legacy systems and keep up with evolving threats.	A stable supply chain is critical. An attack on partners can disrupt operations, so manufacturers must collaborate with companies demonstrating strong cybersecurity strategies.	Human error is the leading cause of breaches. Training staff to spot unusual activity and avoid phishing can significantly reduce risks.	Downtime isn’t an option. A strong incident response plan, regular backups (including offline copies), and equipment redundancy minimize disruption and ensure quick recovery.	ThreatLocker access policies protect even legacy systems by limiting attackers’ network movement, tracking actions, and verifying credentials. Even compromised accounts remain restricted.



CMMC 2.0

DEFENSE REDEFINED

The U.S. Department of Defense will implement revised regulations in 2025; here are the essential takeaways.

WHAT IS CMMC 2.0?

Aimed at hardening security within the Defense Industrial Base sector, the Cybersecurity Maturity Model Certification (CMMC) 2.0 is a framework developed by the U.S. Department of Defense (DoD) to standardize cybersecurity practices among its partner organizations and contractors. Above all, though, CMMC 2.0 is an exercise in simplification, placing the DoD's requirements in line with other well-known standards like NIST SP 800-171 and helping balance security with cost efficiency to make compliance more achievable.

SIMPLIFIED LEVELS

CMMC 2.0 restructures and streamlines the tiered compliance system of the original framework, replacing the complex initial quintet with just three levels to make compliance more accessible. In essence, the trio of new levels depends on the sensitivity of one's environment: level one assures basic cybersecurity for organizations working with Federal Contract Information, level two protects Controlled Unclassified Information, while level three addresses advanced cybersecurity for the most sensitive environments.

CMMC levels

Level 1: Foundational

15 requirements based on FAR 52.204-21 Annual self-assessment and affirmation

Level 2: Advanced

110 requirements aligned with NIST SP 800-171 (Revision 2) Annual affirmation, assessment or self-assessment every three years

Level 3: Expert

134 requirements – as level 2, plus 24 from NIST SP 800-172 Annual affirmation, assessment every three years by DIBCAC

FLEXIBLE ASSESSMENTS

Under the original CMMC, all levels required third-party assessments, a prohibitively costly expense for smaller contractors. CMMC 2.0 reduces this requirement, tying it to risk. Annual self-assessments are now available at level one and for organizations considered lower risk at level two. Third-party audits are still required for higher-risk level two organizations and all level three entities. The idea is that compliance efforts are now proportionate to the sensitivity of the information being protected, aiding accessibility for smaller businesses without removing strict oversight.

COMPLIANCE AT A COMFORTABLE PACE

There's no expectation for immediate perfection. Under CMMC 2.0, as with its predecessor, contractors can address their security gaps over time using a Plans of Action & Milestones (POA&M) document. If an organization can provide a clear, realistic, and properly documented plan of action for cybersecurity improvement, it is free to bid on DoD-related contracts—perfect for small businesses that might otherwise struggle to catch up in time.

ALIGNMENT WITH ZERO TRUST

Adopting a Zero Trust approach helps partner organizations align with the DoD's new framework, even though the regulations do not explicitly require it. Strict access controls support CMMC 2.0's core information protection requirements, but Zero Trust comes into its own in more sensitive environments. At the highest level, CMMC mandates advanced requirements based on NIST SP 800-172, emphasizing strategies like enhanced identity verification, system isolation, and continuous monitoring—the bread and butter of a Zero Trust architecture.

SLOWING THE ROLLOUT

The DoD introduced the proposed rules for CMMC 2.0 in late 2023 and formalized them in late 2024, but compliance requirements for defense contracts have yet to be added. This is partly due to the similarity with the NIST security requirements, which have been mandatory for DoD contractors since 2017. The first stages of CMMC 2.0 allow assessments to begin, ready for its more formal introduction. CMMC 2.0 will see a phased contractual rollout expected to begin in Q4 2025, with compliance a requirement of all defense contracts by the end of 2028. ■

“ CMMC has become a benchmark for reliability and integrity in security practices

Marc Menzies, Founder of
Overview Technology Solutions, Inc.

READ THE FULL INTERVIEW ON PAGE 58



WE'RE LIKE A SWISS ARMY KNIFE OF SOLUTIONS

Marc Menzies,
Overview Technology Solutions, Inc.

Marc Menzies shares about cybersecurity, the role of CMMC, common industry pitfalls, and the future of security in our digital world.

Background and vision

Can you tell us about your background and what inspired the founding of Overview Technology Solutions?

I was a physics major at Stony Brook University in New York, and I was always interested in technology from a young age—taking apart VCRs and picking up computers off the side of the road. It's been fascinating to watch the progression from dial-up to where we are today.

When I was around 22, I founded my first company doing B2C and some B2B work, which eventually evolved into Overview Technology Solutions. Technology appealed to me because you could dive into any specialty relatively easily, and I loved that openness to learn and adapt.

For me, the field of technology was always about accessibility and the ability to learn continuously. I was passionate about making a difference and solving problems with tech. That was the drive behind founding Overview. I've also seen how people from different academic backgrounds—sociology and philosophy—can thrive in tech if they're curious and committed. It's something you can enter at any age if you're willing to learn.



Can you explain what you do for someone unfamiliar with Overview Technology Solutions?

We're like a Swiss army knife of solutions. We call ourselves a hybrid solution provider because we cover consulting, infrastructure management, assessments, and more. Essentially, we solve business problems using technology. We support companies in various industries, especially in the defense industrial base that the Department of Defense uses to fulfill contracts, where compliance with state and federal regulations is critical. A lot of our work involves helping companies become compliant or working with their IT departments to handle specific challenges.

How do you integrate cybersecurity into a broader IT strategy when architecting a solution for your clients?

Every conversation with a client boils down to risk. Everything in technology and cybersecurity revolves around risk—every decision, every piece of equipment, and every policy comes down to evaluating risk. For example, choosing a laptop involves weighing performance, durability, and

cost. In the same way, implementing cybersecurity measures involves understanding which areas pose the most significant risks and prioritizing accordingly. Sometimes, regulatory requirements are unclear, or clients might be limited by budget. In those cases, we walk them through the potential risks: threats, fines, potential audits, operational impact, and ethical considerations. Ultimately, our goal is to ensure clients fully understand their risk landscape and make decisions with eyes wide open. Once they do, we create a plan of action, implement it, and keep that cycle going. This is what seasoned IT professionals should be doing, and it's a standard to which we hold ourselves.

CMMC and industry impact

You mentioned compliance. Can you tell us specifically about the Cybersecurity Maturity Model Certification (CMMC)? Can you explain what it is in your own words and why it's important for companies in the defense sector?

The CMMC is a set of standards created by the U.S. Department of Defense (DoD) to ensure contractors handling sensitive information meet specific cybersecurity requirements. It's based on a combination of cybersecurity practices and controls that have been distilled from various standards. The goal is to protect the defense supply chain as breaches among smaller subcontractors have previously exposed sensitive information.

Essentially, CMMC acts as a framework for contractors to follow, helping to ensure that the defense supply chain remains secure, even at the subcontractor level. Compliance with CMMC is a challenge for some companies due to costs and resource constraints, but it's crucial for maintaining eligibility for DoD contracts. For companies that don't comply, there's a risk of losing business or being phased out of the supply chain.

CMMC and its latest revision has set new standards, and it's really pushing companies to prioritize cybersecurity as a core component of their business. More than meeting regulatory requirements, it creates a culture of security. CMMC provides a structured framework, where companies aren't just ticking boxes—they're building a layered approach to security. This helps organizations protect their data and builds trust with their clients and partners, which is incredibly

valuable. For industries like defense, where compliance is critical, CMMC has become a benchmark for reliability and integrity in security practices.

What challenges do you see businesses facing when implementing CMMC, and how do you help your clients navigate these?

A big challenge is that compliance doesn't equal security. CMMC lays out standards to follow, but achieving compliance doesn't necessarily make a company fully secure. I often find that companies, particularly smaller ones, are overwhelmed by the requirements and sometimes don't even know what data they need to protect.

We work with companies to help them understand their specific risk profiles, guiding them through the scoping process and ensuring they identify what needs to be protected. Many companies try to implement controls without first understanding what's necessary, which is inefficient. By starting with a proper risk assessment and scoping, we support clients make informed, efficient decisions about their cybersecurity investments.

Looking forward, how do you see the future of cybersecurity evolving?

I think we'll see an increasing convergence of compliance and security, though I hope compliance frameworks will adapt to be more flexible and aligned with actual security needs. The cybersecurity landscape is constantly changing, with threats becoming more sophisticated. Organizations will need to stay agile, using data-driven, risk-based approaches to stay ahead of these threats. Compliance standards like CMMC will likely continue to adapt as well, but I believe that companies need to remember that compliance is just one part of the equation. A mature, risk-based approach that combines compliance with real-world security practices will be essential for businesses to remain resilient against evolving threats.

ThreatLocker® role and influence

You've been a strong advocate of ThreatLocker and even serve on the advisory board. Could you share how the ThreatLocker Zero Trust model fits into your work and how it impacts your clients?

I became a customer of ThreatLocker around 2020, and it's been a game-changer. ThreatLocker is built on a Zero Trust model, meaning we only allow specific, pre-approved actions and applications to run on our systems. The Zero Trust approach has been incredibly challenging to implement effectively, especially for smaller organizations, but ThreatLocker software and support make it accessible.

What I appreciate most is that ThreatLocker focuses on making Zero Trust manageable. They've simplified a complex process with excellent customer support, so our team always feels supported and knowledgeable. With ThreatLocker, we've been able to streamline our operations, reducing the number of security tools we use while enhancing security. This has allowed us to focus more on incident response and provide quicker, more efficient support for our clients.

How do you view the role of Zero Trust in the current cybersecurity landscape, and what challenges do companies face when adopting it?

Zero Trust is becoming essential. It's a shift away from the traditional perimeter-based model, which doesn't work as effectively in a world of remote work and cloud adoption. Many companies are interested in Zero Trust, but implementing it requires more than just technology. It's a complete mindset shift. Zero Trust requires a company to limit access to only what's absolutely necessary, creating multiple layers of security and minimizing potential damage from insider threats or compromised accounts. It's complex, but for many organizations, it's the best way forward.

In your experience, what are the common missteps organizations make when approaching cybersecurity?

One of the biggest pitfalls I see is a reactive rather than a proactive approach. Many companies wait until an incident happens to implement security measures; by then, they're already playing catch-up. Security needs to be woven into every aspect of a business—from product development to employee training. When organizations only react to breaches, they're always one step behind, leaving them vulnerable to repeated issues. A proactive stance, where cybersecurity is embedded in the organization's lifecycle, can make a huge difference in resilience.

The reality is that many clients come to us with only a surface-level understanding. We often hear clients say they want cybersecurity, but they don't realize it's more than just "installing protection." It's about understanding your assets, managing risks, and making educated decisions based on that.

In fact, a common misconception is that cybersecurity is just for analysts digging through logs or running forensic scans, but it's much broader than that. Cybersecurity is for anyone in IT who touches operations, management, or engineering. This misconception is why we have a talent shortage; people aren't exploring the full spectrum of roles in cybersecurity. So, educating our clients and the industry is a big part of what we do.

Final thoughts

As an advocate for mental health, can you share more about the challenges of working in cybersecurity?

Absolutely. Mental health is incredibly important in the cybersecurity industry, where burnout is a common issue due to the high pressure and fast pace. There's a misconception that IT and cybersecurity are "just tech jobs," but the reality is that they require constant learning, adaptability, and resilience. We're dealing with continuous, evolving threats, and that can take a toll on mental well-being.

I co-founded Tech Degenerates, a group focused on raising awareness about mental health in the tech industry, specifically in cybersecurity. Our mission is to create open conversations around mental health, provide support, and encourage practices that help prevent burnout. Only if we acknowledge these challenges and support each other can we help create a healthier, more sustainable work environment for cybersecurity professionals.

Given the pressure in the industry, how do you maintain your passion and avoid burnout?

For a long time, my motivation was personal—being my own boss and building something from the ground up. But since starting a family, my perspective has shifted. My family keeps me grounded, and they're the reason I've redefined my relationship with my work. I want to build something meaningful that my kids can be proud of and, hopefully, that will continue to benefit people even after I'm gone.

At the same time, mental health is a huge issue in our industry. I talk openly about it with my team, and I support them in taking care of themselves. Burnout is common in cybersecurity because of the 24/7 demands and the constant changes. It's important to check in with your people and make sure they're doing okay.

The first piece of advice I'd give is to set boundaries. Cybersecurity is a field that never sleeps, and it's easy to feel like you need to be "on" all the time, but it's crucial to take time for yourself. I tell my team to prioritize breaks, disconnect when possible, and have a healthy work-life balance. It's not only about protecting systems; it's about protecting yourself as well. ■



EXPERT STRATEGIES

for leadership growth and optimal performance

Executive Coach **KATRINA LEMPENSKI**, Founder of **THE EDEN COLLECTIVE**, shares her deep expertise in positive psychology, leadership development, and global economics to coach high-level executives—including IT professionals—looking to advance their leadership skills and improve team dynamics.

Drawing from over a decade of consulting with top-tier organizations like IBM, Atlassian, and Goldman Sachs, Katrina Lempenski combines her applied knowledge and certifications—including a certification in applied positive psychology (CAPP) and professional coaching through Martha Beck Inc.—to guide leaders toward optimal performance and impactful growth.

Her methodology integrates evidence-based strategies to help C-suite professionals navigate complex challenges, foster resilience, and build cohesive, high-performing teams in high-stake environments. Below, she shares some of her best practices around stress reduction, effective communication, and conflict resolution that have proven to cultivate individual and team success aligned with organizational goals.

Stress management

A regulated nervous system is one of the greatest assets for any leader, especially a CISO navigating the high-pressure demands of their role. Research shows that leaders with a balanced nervous system are more resilient, make better decisions, and foster positive, productive team environments. They can manage stress effectively, respond calmly to challenges, and connect deeply with others—key traits for anyone leading a team, project, or organization.

That's why I prioritize central nervous system regulation in every executive coaching engagement. Neuroleadership emphasizes the importance of working with the brain's natural mechanisms. Our brains are wired for survival, constantly scanning for threats. Stressful workplace interactions—harsh criticism, difficult conversations, or tough feedback—activate the sympathetic nervous system, triggering a fight-or-flight response. In these moments, the amygdala, the brain's emotional center, takes over, while the prefrontal cortex, responsible for problem-solving and decision-making, steps back. For cybersecurity professionals, who make critical decisions daily, this shift can hinder effectiveness.

I teach clients to use tools like the KIND process to regulate their nervous systems and bring their prefrontal cortex back online. In just a few deep breaths, they can reset and regain focus. Practicing this daily for just five minutes equips leaders to handle stress throughout their day.

My approach is highly personalized, helping clients identify a regulation tool that aligns with their needs and style. By mastering nervous system regulation, leaders can enhance resilience, decision-making, and overall performance, even in the face of relentless challenges.

“

By mastering nervous system regulation, leaders enhance resilience, decision-making, and overall performance, even in the face of relentless challenges

PRACTICING KINDNESS

The KIND process is a simple yet powerful practice for grounding and self-awareness. Begin in a comfortable seated position, taking deep breaths.

K: Know your body

Perform a body scan from head to toe, noticing sensations without judgment. How does your body feel today?

I: Inhabit your emotions

Check in with yourself. How am I feeling today? No judgement, just observe your emotions as they arise.

N: Notice your mind

Acknowledge your thoughts. Are you calm, stressed, or anxious? Name these thoughts and gently let them go.

D: Direction

Take a deep breath then ask yourself: “What personal direction do I need today to stay balanced?” Allow these insights to emerge naturally. End with a few deep breaths.

This practice takes just a few minutes and helps center the mind and body, and prepares professionals to navigate their day with clarity and calm.

Effective listening for executive teams

I frequently observe executive leadership teams in action to identify communication patterns and interpersonal dynamics. Ineffective communication is a recurring challenge I uncover in many of these sessions. Most of us unconsciously “listen to reload,” meaning we focus on crafting our response or defending our point of view rather than truly understanding what the other person is conveying.



**Most of us unconsciously
“listen to reload”**

To address this, I teach the best practice of listening to understand. This involves two steps:

1. Suspend judgment and planning:

As someone speaks, avoid preparing a rebuttal or forming an opinion. Instead, focus entirely on their words, body language, and tone, absorbing their message fully.

2. Mirror back what you hear:

After the person finishes, pause and restate what you understood. For example, “What I’m hearing you say is X, Y, Z. Is that correct?” This simple practice ensures clarity, invites confirmation or elaboration, and fosters trust.

Another tool I use successfully is the **DFIT Model**, particularly with teams prone to interrupting or debating instead of engaging. I organize the leadership team in a semicircle so that each person can see one another as each executive takes their turn to move through the four steps of the communication exercise.

For example, one executive focused on the key decisions they had to make in week ahead and the interdependencies across the executive leadership teams that were affecting those decisions. Another discussed annual reoccurring revenue targets and the challenges they were facing with the pipeline and sales reps.

THE DFIT MODEL

The 4-step process

D: Describe the situation:

Briefly outline the topic at hand.

F: Note the facts:

Address what is currently playing out and your feelings about it.

I: Highlight the impact:

Discuss how the situation affects the business, team, and/or stakeholders.

T: Turn it over:

State your intention for raising the topic and your desired outcome.

During a 90-minute session, I guide teams to practice DFIT alongside mirroring in real-time to create a “listening roadmap” that shifts team dynamics toward deeper understanding and constructive dialogue that ultimately improves decision-making and fosters a healthier, more productive workplace culture.

Expanding communication range

One valuable tip for technology executives is to expand what I call your “communication range.” I once coached a CISO client who was informal, reserved, and indirect in their communication style. Together, we worked on broadening their range to enhance their presence and effectiveness.

We began by identifying a leader he admired for his assertive and impactful communication. We then analyzed elements of that leader’s style—such as a more formal tone, directness, and fact-focused advocacy—that my client could adopt. Through role-playing real-life scenarios, he practiced asserting himself, advocating for resources, and commanding a room. The results were immediate: key stakeholders began paying closer attention and responding more positively.

Conversely, if you are naturally direct and assertive, you may need to swing the pendulum the other way—adopting a more reserved, listening-focused, and accommodating approach when the situation calls for it. Expanding your communication range allows you to adapt to different circumstances, gain buy-in, and lead effectively.

Conflict resolution

Conflict resolution is a critical workplace skill. At its core, it involves addressing disagreements among key parties and finding mutually acceptable solutions. The process works best when it emphasizes mutual benefit, active listening, open communication, and often times, negotiation. When coaching clients, I emphasize clarity on what conflict resolution means. I ask participants to define what success would look like. This helps establish clear expectations and shared goals. While reaching a clear agreement on a solution and next steps is often helpful, a productive process doesn’t necessarily end with a perfect resolution. It may result in two parties saying, “Now I really understand where you’re coming from.” Or it could lead to intangible outcomes like better mutual understanding, reduced tension, improved collaboration, and stronger relationships.

When engaging in conflict resolution, I often utilize Amy Gallo’s “HBR Guide to Dealing with Conflict,” which incorporates three pillars outlined below. ■

“

Conflict resolution is a critical workplace skill

HBR GUIDE TO DEALING WITH CONFLICT

The three essential components

Meet interests: Ensure the resolution addresses as many of your own and the other party’s needs as possible.

Fairness: The solution should be reasonable and equitable, and both parties should feel it can be defended to others.

Maintain relationships: The resolution should preserve or improve the relationship, avoiding outcomes that foster resentment or damage trust.

By applying these principles with honest, open dialogue, teams co-create solutions that enhance teamwork, boost consensus, and lead to a healthy, more productive work environment.

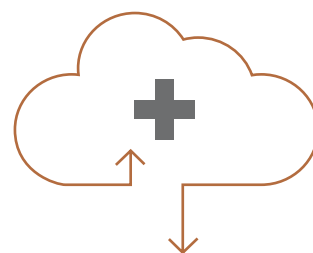
SECURITY IN HEALTHCARE

The healthcare sector is ill-equipped to cope with cyberattacks—but an ounce of prevention is worth a pound of cure. The right mindset and the use of proper tools can protect even difficult legacy devices, and save lives along the way.

Cybercriminals are all too happy to exploit the unique vulnerabilities of healthcare organizations. The sector's position as a heavily regulated holder of the most personal information makes it a prime target—one that is, on the one hand, struggling to remain prepared and, on the other, actively positioning itself in dangerous territory. Rapid modernization and digitalization have pushed hospitals and healthcare facilities to open up, making sensitive data more accessible than ever before—essential for interdepartmental and inter-facility working as much as it is for establishing instant rapport with patients. Healthcare organizations operate under stringent regulations like HIPAA and fall into the scope of growing worldwide directives such as NIS 2. A single breach

can lead to devastating consequences, from severe financial penalties to stinging reputational damage. Thus, the dual requirement to maintain accessibility and security is a delicate balancing act. Get it wrong, and the red tape will never stop.

To focus on the bureaucratic consequences is to ignore the most serious of all: cyberattacks kill. It is estimated that between 2016 and 2021, vital equipment locked down by ransomware was directly responsible for the deaths of up to 67 Medicare patients in the U.S. alone[†]. While disruption in other industries might cost money, in healthcare, it costs lives—and criminals know that this means a successful hit on a healthcare facility is the route to a quick, lucrative payout.



92 %

OF HEALTHCARE
ORGANIZATIONS
**EXPERIENCED A
CYBERATTACK
ATTEMPT**
IN 2024[†]

IN 2023, 88% EXPERIENCED AT LEAST 40 CYBERATTACK ATTEMPTS[†]

Beyond disruption, there is a rich prize available for criminals. CNBC reports that medical records sell for USD 60 on the dark web; some slightly overexcited sources put the price closer to USD 1,000. Even on the low end, a single medical record is valuable compared to a social security number (anywhere from USD 1 to 15) or a credit card number (USD 5). By that metric, 2024's Change Healthcare breach—which recent reports suggest compromised the records of over 100 million Americans—would be worth USD 6 billion on the black market.

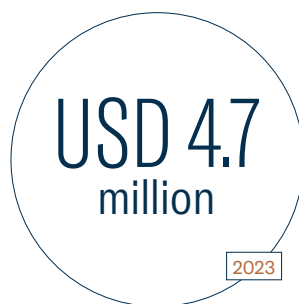
The healthcare sector is soft. It relies on legacy systems, often under-patched or poorly defended, working with outdated protocols and insecure data transfer methods. A hospital's fast-paced, stressful environment often uses shared workstations and, in turn, shared passwords and credentials, creating a weak link in the security chain. Security architectures in healthcare are fragmented, comprising different tools, procedures, and policies that form sticking-plaster defenses. A hacker easily rips them off with a little knowledge of their target system.

This occurs in an undersupported sector that struggles with chronically low cybersecurity budgets. Healthcare's priorities are, understandably, with its patients, but it must rethink its approach to cybersecurity. A proactive stance emphasizing modern defenses, collaboration, and awareness is the only way to hold back the tide of attacks.

In part, healthcare's security turnaround is already underway. The sector is well aware that cyberthreats are growing, and the statistics back this up: between 2018 and 2023, The HIPAA

Journal reports a 239% increase in hacking-related data breaches and a 278% increase in ransomware attacks. There is increasing resolve to fight against cybercriminals, a movement that will begin with a united front.

ESTIMATED COST OF A HEALTHCARE CYBERATTACK[†]



Unity among healthcare organizations—sharing knowledge, resources, and best practices—allows the sector to create a collective defense. There is a necessarily high level of data sharing between healthcare units, which means criminals need to search for only one weak point in the entire landscape to cause a significant breach. While specific targets may prove more prosperous, even the smallest could offer an attacker more than enough data or disruption to make their work worthwhile.

IN 2023, 42% OF ATTACKED HEALTHCARE ORGANIZATIONS PAID RANSOMS; IN 2024, THIS NUMBER INCREASED TO 53%[†]

What form healthcare's defenses take will vary, just as the systems and organizations that make up the sector do, but there is no question that a Zero Trust approach plays a big part in the future of healthcare security. It is a comparatively simple way to take back control of fractured systems that have become loosely guarded—and those that old defensive measures can't guard.

Without Zero Trust software like ThreatLocker® to support endpoints, and a commitment to the philosophy, criminal incursions will continue to wound deeply. With Zero Trust, they will merely constitute a sharp scratch. And as unrealistic as the idea of the entire industry changing its security philosophy overnight might be, healthcare's commitment to collaboration means any one organization could be the nucleus of a cure. ■

“ A proactive stance is the only way to hold back the tide of attacks

Joe McGee, Advanced Medical Transport's Director of IT

READ THE FULL INTERVIEW ON PAGE 68

JOE MCGEE

SECURING THE FRONTLINES OF EMERGENCY CARE

Advanced Medical Transport's Director of IT shares insights on cybersecurity challenges and opportunities.



ThreatLocker offers robust protection without hindering AMT's operations

Joe McGee, Director of IT at Advanced Medical Transport (AMT), brings nearly two decades of IT expertise to the healthcare sector. With a rich background spanning insurance, consulting, and optometry, McGee's journey to AMT reflects his continuous drive for growth and innovation. Now, as the leader of AMT's IT operations, McGee navigates the unique cybersecurity challenges posed by a highly mobile and essential emergency care organization. In this interview, McGee shares his professional journey, the critical importance of cybersecurity in healthcare, and the role of emerging technologies in shaping the future of his field.

Can you share your professional journey and current role at AMT?

I've been in IT for about 18 years, with the last five and a half focused on healthcare. My career began as a consultant at State Farm Insurance, where I gained a strong foundation in large-scale IT operations. I eventually moved into technical roles, managing thousands of endpoints and mentoring new team members. After earning my MBA, I transitioned into healthcare IT, first building an IT department from the ground up at Keplr Vision and now leading IT at AMT. Joining AMT felt like a natural progression—a way to tackle the high-pressure, mission-critical challenges unique to emergency medical services.

What specific cybersecurity threats does AMT face, and how do these differ from those encountered by hospitals?

AMT's mobility creates a distinct set of challenges. We operate over 70 ambulances across multiple cities, each essentially a mobile office equipped with connected devices for real-time patient care. This mobility increases the risk of equipment loss or theft, which isn't as prevalent in stationary healthcare facilities like hospitals. Additionally, healthcare is a prime target for cyberattacks, with phishing being a major threat across the board.

For us, it's about ensuring that even if a device is compromised, the data remains protected and inaccessible to unauthorized users.

How does AMT's mobility introduce unique cybersecurity risks compared to stationary healthcare providers?

Our ambulances rely on secure, reliable connectivity for everything from patient charting to transmitting vital data to hospitals in real-time. This creates vulnerabilities not typically seen in hospitals. For example, if a device is left unattended or if a passerby gains access to an ambulance, there's a real risk of data exposure. Our systems need to account for these scenarios, ensuring encryption, endpoint protection, and Zero Trust principles to mitigate threats.

Can you tell us how you navigate healthcare compliance standards, such as HIPAA, to ensure patient data protection?

Compliance is non-negotiable. We hold ourselves to the same standards as hospitals, but HIPAA guidelines can sometimes leave room for interpretation. For instance, a requirement for lock screen timers doesn't specify an exact duration, so we tailor policies to fit our workflow. Tools like



McGee conducting systems maintenance in the data center adjacent to AMT's dispatch center

“

Even if a device is lost or stolen, the platform's Application Allowlisting and endpoint protection ensure that bad actors can't exploit it

ThreatLocker® play a crucial role in meeting these standards by offering granular control over system access, ensuring we can confidently demonstrate compliance to auditors.

What misconceptions about cybersecurity compliance have you encountered?

One common misconception is that compliance equates to security. While compliance provides a framework, it's not a guarantee of protection. Another is the idea that technology alone solves all problems. People often overlook the importance of training and culture. Cybersecurity is not just a set of tools but people understanding and adhering to best practices.

How does ThreatLocker enhance AMT's cybersecurity?

ThreatLocker has been a game-changer for us. Its Zero Trust architecture ensures that nothing runs on our systems without explicit permission, significantly reducing the risk of malware or unauthorized access. Even if a device is lost or stolen, the platform's Application Allowlisting and endpoint protection ensure that bad actors can't exploit it. The visibility and control ThreatLocker

provides give us peace of mind, knowing that our systems are secure even in the most unpredictable situations.

How do emerging technologies like AI influence your approach to cybersecurity?

AI is a double-edged sword. On the one hand, it offers incredible potential for threat detection and automating routine tasks. On the other, it's also a tool that bad actors can exploit. For example, AI can lower the barrier for entry into hacking by helping novices create scripts or identify vulnerabilities. It's a constant race to stay ahead, but when used responsibly, AI can significantly enhance our ability to protect data and systems.

What are the biggest cybersecurity challenges you foresee for organizations like AMT?

One major challenge is the outdated technology often used in healthcare. Many vendors are years behind in implementing modern security features like SAML authentication, complicating our efforts to maintain a strong cybersecurity posture. Additionally, the increasing sophistication of cyberattacks means we must continually evolve our defenses to stay ahead of threats.

If you could implement one industry-wide change to improve cybersecurity in healthcare, what would it be?

I'd advocate for greater accountability among software vendors to adopt modern security standards. Too often healthcare IT systems are built on outdated technology, creating unnecessary vulnerabilities. Pushing vendors to modernize their platforms would go a long way in reducing risks across the industry.

How do you balance the need for strong security measures with the operational demands of emergency care?

It's a delicate balance. Security controls can't interfere with our ability to provide timely, quality care. This is where tools like ThreatLocker shine, offering robust protection without hindering our operations. Ultimately, it's about striking the right equilibrium between safeguarding data and enabling our team to focus on what matters most: saving lives.

What advice would you offer to other IT leaders in healthcare?

Build relationships with your leadership team and communicate the value of cybersecurity in terms they understand. Focus on creating clear, actionable business cases for your initiatives. And perhaps most importantly, invest in ongoing education—not just for yourself, but for your entire organization. Cybersecurity is a team effort, and everyone has a role in protecting sensitive data. ■

“

Ultimately, it's about striking the right equilibrium between safeguarding data and enabling our team to focus on what matters most: saving lives

AMT's professional IT team around McGee, in the center



NIS 2

THE NEED TO KNOW

Europe's most impactful security regulation has arrived, with huge worldwide information security implications.

WHAT IS NIS 2?

The second edition of the EU Network and Information Security directive aims to increase the cyber resilience of important and critical entities operating in the European Union by imposing stronger requirements on a broader field than the 2018 original. The intention is to reduce security inconsistencies, align the EU's cyber defenses, build confidence and trust, and help actors implement a plan to cope with data crises.

WIDER SCOPE

NIS 2 sees the EU acknowledging the importance of security and resilience in many more business sectors. Notably, these now include ICT service management and public administration—deemed “essential,” critical for societal and economic activities—and digital providers in the less-supervised “important” category. This group includes services like social networks, search engines, and online marketplaces.

Ten areas of concern for NIS 2

- Risk assessments and security policies.
- Proper use of cryptography and encryption.
- System security, including handling and reporting vulnerabilities.
- Asset and access control, particularly surrounding sensitive data.
- Use of multi-factor and continuous authentication.
- Self-evaluation of the effectiveness of security measures.
- Cybersecurity training and best practice adherence.
- Incident planning, including post-incident resolution.
- Supply chain security and relationships.



IN EFFECT BUT NOT YET ENFORCED

The NIS 2 regulations went into effect on Oct. 17, 2024, but their enforcement is beholden to the EU's broad range of member states, and each one must transpose them into its own national law, adding friction to the process and realistically slowing Union-wide adoption. Stricter rules also increase the challenge of achieving full compliance. This task will likely take affected entities many years, and while we should expect a brief moratorium on fines, it cannot be guaranteed.

EXTRA LIABILITY

Until now, authorities rarely enforced the first NIS regulations and did not define any penalties. However, this time, non-compliant organizations could be fined EUR 10 million or up to 2% of total turnover for those deemed essential within scope. Management can now be held liable for infringements, with the EU instituting compliance audits to check up. For important entities, these audits will happen post-incident, but authorities can inspect essential entities at any time.



The European Parliament voted to adopt NIS 2 in late 2022; less than two years later, it went into effect

Four proactive steps towards NIS 2 compliance

- Assess existing cybersecurity practices through audits to identify gaps with NIS 2 guidelines.
- Develop a comprehensive risk management framework to encourage proper security controls and continuous monitoring.
- Establish clear reporting procedures in line with NIS 2 requirements and train staff to anticipate and spot security threats.
- Engage with experts to thoroughly understand obligations, both Europe-wide and within local implementations.

WORLDWIDE IMPLICATIONS

If an in-scope business operates in the EU, its European activities are subject to NIS 2 regulations wherever its headquarters happens to be. This has obvious implications for online entities, which will struggle to avoid operating in the EU, and those selling digital products for use in Europe. EU customers will necessarily be more diligent over their purchases, too—if a device or its supply chain cannot prove that it helps meet NIS 2 standards, it may become quite unpopular.

REGULATORY CROSSOVER

Resilience is the order of the day in the EU right now. Much of NIS 2's content overlaps with the recently ratified Digital Operational Resilience Act (DORA), specifically targeting the financial sector and taking precedence for financial institutions. The EU's Critical Entities Resilience Directive (CER) also covers much of the same ground and affects the same organizations, though CER extends beyond cybersecurity into physical threats to continuity. ■■

USING THREATLOCKER® POST-BREACH IN AN ACTIVE INCIDENT RESPONSE CASE

Art Ocain – Airiam

Art Ocain, a cybersecurity expert with over 25 years in IT, currently leads the incident response (IR) team at Airiam. In this interview, Ocain shares his journey into cybersecurity and how ThreatLocker has enhanced post-breach containment. He also discusses the challenges small and large organizations face in securing their infrastructure. His insights on Zero Trust, evolving threats, and building resilience reveal the complexity and necessity of cybersecurity today.

As you walk us through your journey, can you share why you decided to focus on cybersecurity and how you joined Airiam?

I've been in IT for about 25 years now, and it all started back when I was in college. I studied mathematics, but I was also working for web hosting companies and data centers to help cover expenses. This gave me hands-on experience early on, and I realized I enjoyed working with systems and understanding how they fit together. Over the years, I've worn many hats: system administrator, network administrator, cloud administrator, and, eventually, cybersecurity specialist.

As I continued in the field, I saw the rapid rise of cybersecurity challenges and recognized the critical importance of responding effectively to cyber incidents. Before Airiam, I was the president and COO at MePush, where I launched our incident response team. When Airiam acquired us, it made sense to keep building that side of the business. It's fulfilling work—there's nothing quite like helping a company recover from an attack and knowing you're making a real difference in their resilience and security.

How has your diverse experience shaped the way you approach incident response for clients?

I am drawn to roles where I can see a direct impact on people and businesses, and incident response allows me to do that every day. When I launched our IR team, the goal was to help clients get back on their feet as quickly as possible. It's a high-stakes role where speed and accuracy matter immensely.

What I appreciate about Airiam is that it's a place where I can use my experience across various aspects of IT to help clients, whether they're small businesses or large enterprises. Each brings unique challenges, but

“

There's nothing quite like helping a company recover from an attack and knowing you're making a real difference in their resilience and security



Art Ocain at MITRE's ResiliencyCon 2022 talk on "Accidental Resiliency"

one thing is consistent: you need a structured approach to build resilience. After an incident, it's not enough to get the client back up and running—we also need to identify weaknesses, strengthen defenses, and ensure they're better prepared for the future. That's the kind of approach we emphasize at Airiam, and it shapes every IR project we handle.

Given your experience working with both small businesses and large companies, what unique challenges do small businesses face in cybersecurity compared to larger enterprises?

Small businesses face a lot of unique challenges because attackers often see them as easy targets. Larger enterprises generally have the resources and budget to invest in comprehensive cybersecurity measures—often employing entire teams dedicated to managing security. Small businesses, on the other hand, are often limited by cash flow and tend to view IT expenses as something that's reactive rather than proactive.

This lack of preparation can be a huge vulnerability. Many small businesses don't have a structured IT budget and often have outdated hardware and software, which presents additional risks. When an attack happens, they're

caught off guard. Larger businesses may have better cyber insurance and can absorb the financial hit, but for a small business, a cyber incident can be devastating—it can be a business-ending event. That's why it is important for small businesses to work with managed service providers (MSPs) who understand these challenges and can provide guidance on how to build a resilient IT strategy, even with a limited budget.

In your experience, what are some of the most common missteps companies make before they engage with an incident response provider like Airiam?

One of the most common missteps is not enabling multi-factor authentication (MFA) across all accounts. Often, companies will have MFA enabled for executives but overlook shared accounts or generic ones like marketing@company.com. These shared accounts, without the protection of MFA, are an easy entry point for attackers.

Another common issue is relying on outdated infrastructure. Many businesses are still using end-of-life hardware and software because they see it as a cost-saving measure, but that's a huge risk. Staying updated is fundamental for resilience; outdated systems create vulnerabilities that attackers exploit. These missteps are often things we identify in incident response, and we always advise clients to address them to prevent future breaches.

How do you ensure that incident response is not just reacting to threats but also preparing companies for long-term resilience?

Our approach to incident response goes beyond simply stopping the immediate threat. We want to get companies back on their feet, but we also want them to understand the underlying vulnerabilities that led to the incident. After containment, we conduct a thorough analysis to understand what went wrong, and we recommend specific measures to improve their cybersecurity posture.

The goal is to turn an incident into a learning experience so they can build a more resilient infrastructure. We discuss things like network segmentation, endpoint security, and how to layer defenses in a way that's manageable. We want to make sure that the company is better prepared so they're not in the same position if another attack happens.

Many businesses find the idea of Zero Trust intimidating. How do you simplify this concept for your clients, and what role does it play during incident response?

Zero Trust can be a daunting concept because it's often misunderstood as a lack of trust in your own employees or systems. In reality, it's about assuming that any access point could be compromised and taking steps to minimize risk. I often frame it in terms of an "assume breach" mindset—think of it as acting like there's already someone inside your network and what steps you'd take to prevent them from moving around freely.

“

ThreatLocker ensures that only pre-approved applications can run, which makes it nearly impossible for an attacker to execute unauthorized commands

When it comes to incident response, Zero Trust is invaluable. ThreatLocker® plays a key role in our Zero Trust strategy because it restricts actions within the network. It ensures that only pre-approved applications can run, which makes it nearly impossible for an attacker to execute unauthorized commands. Zero Trust is a strategic approach to reducing exposure and containing threats.

How has ThreatLocker changed your approach to handling post-breach scenarios? Can you share a specific example?

ThreatLocker has been a game-changer in incident response because it allows us to respond immediately.

We once had a partner reach out to us after spotting ransomware in their environment. They had ThreatLocker but hadn't fully enabled it in secured mode yet. We immediately set it to secured mode, which completely stopped the attack. Some machines were already affected, but no further damage was done after activation.

This level of containment is something we hadn't achieved so quickly with other solutions. The capability of ThreatLocker to stop unauthorized actions is unique—it doesn't just monitor for suspicious behavior; it blocks it outright.

Without ThreatLocker, containment would typically take much longer, which means more damage could occur. Now, we can achieve containment quickly and begin the recovery process sooner. It's a tool that prioritizes prevention by design, blocking any unapproved actions from the outset.

How have you seen hackers evolve their tactics since you started your career, and what are the most effective ways businesses can protect themselves from these constantly changing threats?

Hackers have definitely evolved. In the early days, most attacks involved malware or viruses that traditional antivirus software could detect. Now, attackers use legitimate system administration tools to blend in, making it harder to detect them. They might log in through VPNs or use admin tools to move around the network, which is why behavioral-based detection is essential.

To stay protected, businesses should use multi-factor authentication, keep all software updated, and invest in advanced security solutions that go beyond traditional antivirus. ThreatLocker, for example, stops suspicious activities before they can even start, which is a different approach from traditional EDR (Endpoint Detection Response) that relies on behavioral

analysis. It's about staying ahead of the tactics by layering protection.

Cybersecurity is increasingly becoming part of boardroom discussions. How do you think the relationship between executive leadership and IT professionals is changing, and what steps should we take to bridge the gap?

Cybersecurity has a bad reputation in the boardroom because some leaders view it as a blocker rather than an enabler. Security teams often get labeled as the “department of no” because we tend to highlight risks, which can slow things down. To change this, cybersecurity professionals need to approach the board with a business mindset, focusing on risk rather than technical details.

We need to communicate how security enables agility and growth by protecting the business' assets and reputation. Effective communication is key—explain what's at risk in a way that resonates with leadership. Showing how a tool like ThreatLocker can speed up incident response and reduce down-

time helps the board see cybersecurity as a worthwhile investment, not just an expense.

What emerging threats should businesses be most concerned about in the next few years, and how can they prepare?

Looking ahead, state-sponsored attacks are likely to be an increasing concern. We're already seeing attackers who move “low and slow,” infiltrating networks over time and waiting for the right moment to strike. For businesses, this means adopting an “assume breach” mentality and strengthening defenses at every level.

For business leaders without a deep technical background, what are the most critical aspects of incident response they need to understand?

The biggest thing to understand is that cyber incidents aren't just technical issues—they're business risks. A breach can have significant financial and operational impacts, from the

direct cost of incident response to reputational damage and customer loss. Leaders should focus on quick containment, resilient recovery, and building a security culture within the organization. Budgeting for the right tools and resources in cybersecurity is as essential as any other core business function.

Looking ahead, what drives you to stay passionate about the evolving field of cybersecurity, and what do you hope to see change in the industry?

The constant evolution in cybersecurity keeps me engaged. New tactics emerge all the time, and staying one step ahead is both a challenge and a motivator. What drives me is helping clients adapt and protect themselves, turning threats into manageable risks.

Looking forward, I'd love to see cybersecurity shift from a reactive approach to a proactive one, where organizations embed security into every part of their business strategy to support innovation and agility rather than seeing it as a roadblock. ■



“

Cybersecurity has a bad reputation in the boardroom because some leaders view it as a blocker rather than an enabler

BANKING ON ZERO TRUST



A blueprint for cybersecurity excellence

Eastern Bank is known for its track record of innovation driven by the belief that its customers deserve a banking experience centered around their needs. In the digital-first world we live in, safeguarding sensitive financial data is no small feat.

Bo Olsen, Security Engineering Manager, plays an important role in ensuring the implementation of Zero Trust, so the bank's endpoints are consistently protected.

When Bo Olsen joined Eastern Bank over a decade ago, cybersecurity was a simpler landscape. Antivirus software and spam filtering were the main lines of defense. Today, Olsen manages an advanced security framework, spearheading the bank's Zero Trust initiative to counter any threat.

Founded in 1818, Eastern Bank has thrived by embracing change. This adaptability, coupled with forward-thinking leadership, has positioned

the bank as a leader in cybersecurity within the financial sector.

Olsen's path to Eastern Bank reflects his passion for protecting endpoints and users. Beginning his career at antivirus companies, he developed expertise in understanding malware behavior and crafting defenses. "I fell into cybersecurity by chance, but it quickly became something I loved. My natural curiosity drove me to research what was happening and find ways to protect our users from these threats," he recalled. When the opportunity at Eastern came up, he joined in a role where he was tasked with integrating new technologies.

Over the years, Olsen has witnessed a seismic shift in cybersecurity. "The threat landscape is no longer about reacting to what's already happened. It's about anticipating and preparing for what could

“

ThreatLocker saves us time by streamlining processes and reducing the need for constant monitoring

happen,” he explained. This proactive philosophy underpins the bank’s adoption of Zero Trust, a framework that requires verification at every level. Zero Trust is a mindset. The philosophy is simple: trust nothing, verify everything,” Olsen explained.

Central to the bank’s Zero Trust journey was ThreatLocker®, with its set of Zero Trust solutions, that provided valuable flexibility and visibility. “The ability of Threatlocker to enforce granular micro-segmentation and monitor activities in real-time has been extremely valuable,” Olsen said.

“ThreatLocker saves us time by creating more efficient processes. The level of protection it provides allows us to focus on other strategies and skills to ensure optimal security measures.” Olsen emphasized.

Ransomware and phishing remain top threats, but Olsen credits Zero Trust with mitigating their impact. “Zero Trust is helping to mitigate the impact of threats in a cyber secure environment.”

Olsen’s passion for cybersecurity is evident in his approach to leadership and innovation. “What drives me is knowing that what we do

matters,” he said. “Our customers trust us to protect their most valuable assets, and that’s a responsibility we take seriously.”

Looking ahead, Olsen is excited about emerging technologies like AI, which he believes will shake up the industry. “AI has the potential to enhance both security and customer experience,” he noted. “It’s an exciting time to be in cybersecurity.”

As Eastern Bank continues to innovate, Olsen remains committed to delivering the highest quality environment. “I’m proud to be part of a team that values both its customers and its employees, and helping them to achieve their goals.”

Eastern Bank has long built a reputation for innovation, including through Eastern Labs, where it’s working with digital innovations and fintech. Eastern Bank’s IT team is similarly innovating, across a range of areas, including how it addresses cybersecurity. With colleagues like Olsen, that is only expected to continue. ■

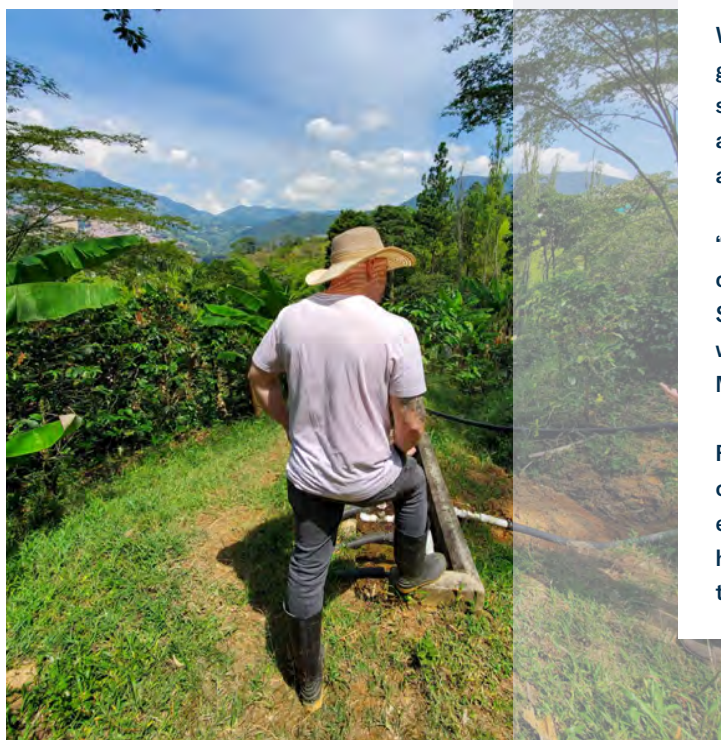
BEYOND THE BANK: A CULINARY EXPLORER

When Bo Olsen steps away from his role at Eastern Bank, he dives into another passion: discovering the world through its food and coffee. A devoted traveler, Olsen enjoys exploring diverse cuisines and immersing himself in local cultures.

Whether starting at a spot from the prestigious 50 Best list or a hidden gem recommended by new friends, Olsen dives deep into local cultures, savoring their flavors and forging connections. “Food tells the story of a place and its people,” Olsen said. “It’s a window into traditions, history, and creativity.”

“South America is one of my favorite destinations, providing not just rich culinary experiences but also the perfect environment to practice my Spanish and Portuguese. Europe holds its charm too, especially Greece, where I gather with friends each November to run the Athens Authentic Marathon—the route of the original marathon.”

For Olsen, fitness and nutrition are as much a part of his travels as the culinary adventures. Staying active clears his mind and fuels his ability to enjoy the indulgences of his trips. It’s a balance he’s mastered—training hard, running marathons, and, as he humorously notes, earning the right to eat ridiculous amounts of incredible food along the way.



ENTANGLED EVOLUTION

Quantum computers will alter the course of technology

Quantum computing will, one day, change the technological landscape, revolutionize our understanding of science and the universe, and alter the entire focus of society. That day is not today. At a CES investor Q&A, Nvidia CEO Jensen Huang suggested that real-world applications of quantum computing could be 15-30 years away. Given Nvidia's position as the driving force of today's cloud computing industry, Huang was speaking from what must be considered a position of some bias—but quantum's true transformative potential is far over the horizon.

Next-generation change

Quantum computing is expected to drive significant advancements. In medicine, quantum simulations could model complex molecular interactions, enabling new drug discoveries or bespoke medical treatments. Quantum algorithms could advance financial investment and fraud detection as well as accelerate machine learning by dealing with larger data sets and more complex training models.

Security might be the most important field. With quantum computers aiding more classical methods, the security field is expected to be able to boost key sharing and secure authentication as well as potentially introducing new secure communication mechanisms through quantum networks. But equally, quantum computing poses a cryptography challenge.

Problems and solutions

Quantum computers could soon render even today's most complex cryptographic methods obsolete. The NIST Report on Post-Quantum Cryptography suggests that breaches of 2048-bit encryption might come as soon as 2030.

This vulnerability is being taken seriously on both sides of the fence. Attackers have begun collecting encrypted data in the hopes that they will one day be able to decrypt it. Major governments are aware that quantum-resistant encryption algorithms are a vital component of cybersecurity's future. NIST's Computer Security Resource Center has, following a public research and submission process, selected an initial batch of four, while NIST itself is set to release comprehensive guidance on post-quantum cryptography in the near future.

Quantum mechanics: A complex challenge

Quantum computing's primary challenge is its early stage of development combined with its extreme complexity. It works on intricate principles from the field of quantum mechanics, which, while well documented, are inherently non-intuitive. To quote the late Richard Feynman, "If you think you understand quantum mechanics, you don't understand quantum mechanics." What's more, the building blocks of quantum computing, qubits, can only exist by maintaining highly delicate operating conditions, in many cases an environment cooled close to absolute zero. The difficulty of ensuring coherence, a stable quantum state, makes qubits highly error-prone.

Perhaps this is why Google CEO Sundar Pichai calls the company's 2019 quantum supremacy event—where the company's nascent Sycamore quantum computer outperformed the fastest supercomputers in a single computational task for the first time—merely the field's "hello world" moment. "In the long arc of scientific progress," stated Pichai on Google's Keyword blog, "it was just one step towards making quantum applications meaningful to human progress."

Charting the next steps

The field is now focused on error correction. In 2023, Google's Quantum AI lab demonstrated the prototype of a logical qubit, an error-correcting quantum bit, marking the second milestone of its ambitious six-part roadmap to practical quantum computing. Microsoft's Azure Quantum team is working on the development of topological qubits, also positioned as a potential solution to stability.

Canada's D-Wave Systems is exploring quantum annealing, a method that uses the natural behavior of qubits to discover optimal solutions rather than relying on potentially noisy logic gates.

Despite the challenges ahead, the progress in quantum computing is exciting and full of potential. As researchers continue to make strides in error correction, the industry is poised to tackle the next big milestone: scalability. Today's quantum computers work with very few qubits, a few hundred in the largest cases. However, attaining a quantum advantage for general-purpose tasks

“

The stakes have never been higher, and the race to secure our digital future is on

IBM Quantum's modular System Two, seen in its debut installation in Yorktown Heights, New York



means employing thousands or millions of qubits. This presents a fascinating engineering opportunity to innovate and develop the hardware necessary to keep such a large collection of qubits stable and deal with new, unpredictable outcomes from operating on a quantum level at scale.

The future is now

Quantum computing is difficult, but the slow progress of its early years looks set to ramp up as each technological hurdle is overcome. Like the supercomputer scene of old, the race now revolves around singular, unique machines. Most striking is the IBM Quantum System Two, a modular quantum computer initially built to house a trio of the company's Heron QPUs and heavily focused on scaling. Using in-house quantum coupling technology, IBM expects to link numerous System Two units together, creating a quantum circuit able to handle a billion operations by 2033.

Intel has, somewhat inevitably, thrown its own silicon expertise into the quantum ring with a chip named Tunnel Falls. Just 50 nanometers square, Tunnel Falls can be reproduced using existing, well-worn fabrication processes, essential for placing its 15 qubits into the hands of as many research institutions as possible. It also demonstrates silicon spin qubits, a technology that allows quantum chips to function at warmer temperatures than the frigid requirements of the leading QPUs.

Looking ahead

Google has grabbed the headlines most recently, at least in large numbers. Demonstrating its Willow QPU at the end of 2024, it spent five minutes performing a calculation that would take traditional computers more than 10 septillion years. Interestingly, Google claims Willow has "passed the error correction threshold," suggesting that quantum's next step may have already been taken.

Yes, the qubits are limited, and the definitive applications as yet unclear. But there is plenty to be mined in computing's second gold rush. And perhaps it's even more vital than that. As Sundar Pichai told the BBC in 2020, "I view it as the most profound technology that humanity will ever develop and work on. If you think about fire or electricity or the internet, it's like that – but even more profound."

Next steps for cybersecurity

Access to quantum computing platforms is relatively limited but growing. IBM Quantum offers an SDK through which developers can create quantum applications and a cloud platform on which they can run, and others like Google, Nvidia, Microsoft, and Amazon have begun building quantum components into their cloud offerings.

Hackers do not yet have their hands on enough qubits to defeat 256-bit encryption, but it may only be a matter of time before they do.

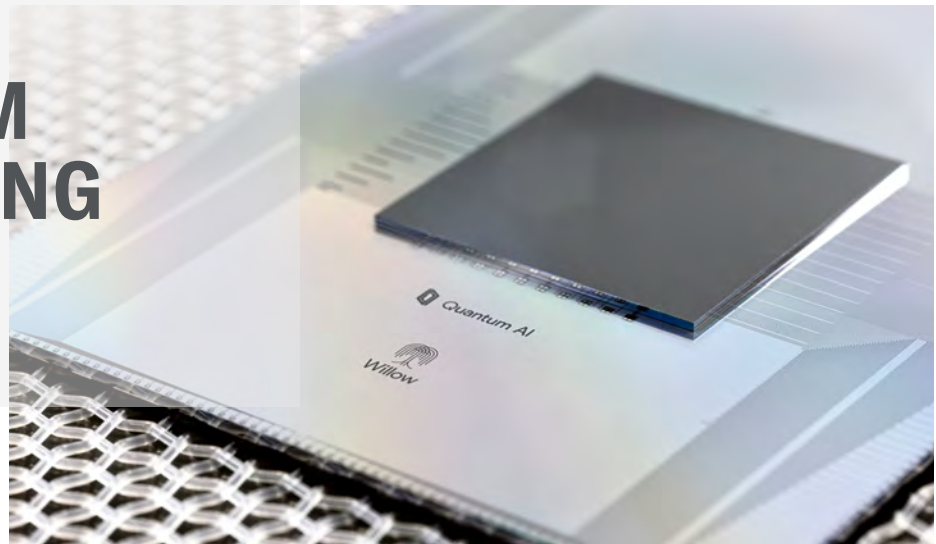
Naturally, there is scepticism over the practical uses of today's quantum computers and the future scalability and applications of tomorrow's machines. Some consider quantum computation to still be speculative technology; Université Montpellier physics professor Mikhail Dyakonov states that his vision of a practical quantum computer "would have to be able to manipulate – on a microscopic level and with enormous precision – a physical system characterized by an unimaginably huge set of parameters, each of which can take on a continuous range of values. Could we ever learn to control such a system? My answer is simple. No, never."

Nonetheless, in security any possibility must be considered a certainty. When – if – existing encryption standards are broken, everything becomes vulnerable at once. Whether that happens 15 or 30 years in the future, or hackers find a way to unleash a quantum attack tomorrow, those businesses following mature, considered, limited-access security policies will endure. And when processor-intensive quantum-resistant encryption algorithms become feasible to employ, their implementation alongside Zero Trust methodologies will be critical. ■

“

**Despite the challenges ahead,
the progress in quantum computing
is exciting and full of potential**

HOW QUANTUM COMPUTING WORKS



Google says the design of its latest QPU, Willow, allows it to reduce errors when its qubits are scaled up

Traditional computers use bits that exist in a binary state, either zero or one. Quantum computers deal with quantum bits, otherwise known as qubits. These can exist as a zero or one state, but the phenomenon of quantum superposition allows qubits to be both zero and one at the same time—Schrödinger's bits if you will. Two quantum bits allow four potential states to be put into superposition; with 20, that number grows to a million, 27 over a billion, and so on.

Qubits are also subject to entanglement, which means one can be correlated to another, sharing information instantly. This combination enables quantum computers to perform complex calculations at unprecedented speeds. Where a standard computer would need to evaluate each possible solution to a problem in series, one at a time, a quantum computer can (in theory) explore multiple possible solutions simultaneously. ■■

SCHRÖDINGER'S BITS: THE QUANTUM PARADOX EXPLAINED

Schrödinger's Cat is a thought experiment that Austrian Physicist Erwin Schrödinger created to illustrate the strange nature of quantum mechanics. In this scenario, a cat resides inside a sealed box equipped with a mechanism that activates based on a quantum event. If a radioactive atom decays, it triggers a reaction that kills the cat; if it doesn't decay, the cat stays alive. According to quantum theory, until someone opens the box and observes the situation, the atom exists in a superposition of decayed and not decayed, meaning the cat is both alive and dead at the same time. This paradox highlights the puzzling concept of superposition and emphasizes how observation influences reality.

THE HUMAN SIDE OF ZERO TRUST



Jherome DeGuzman's passion for cybersecurity began long before his role as Manager of Enterprise Solutions Engineers at ThreatLocker®. With nearly 30 years of experience across major tech companies, his career in technology has been shaped by a personal experience with online security during the early days of the internet. Now, Jherome plays a key role in helping businesses navigate the shift to Zero Trust security, offering hands-on expertise while building strong relationships with customers.

For Jherome, the journey to becoming a leader in the Zero Trust space started long before joining ThreatLocker. With nearly three decades in the tech industry, Jherome's resume reads like a tour through some of the biggest names in technology: Sun Microsystems, Oracle, CME Group, and IBM. Along the way, he has taken on roles like Network Engineer, Project Manager, and Pre-Sales Engineer, each position providing a fresh perspective on security and risk. But his passion for cybersecurity started much earlier, with a personal experience that left a lasting impression.

"During the era of 14.4kbps modems, I received an Instant Message through my AOL account asking me to confirm my password," Jherome recalled. It was a straightforward scam, but it was eye-opening

how easily someone could fall victim. "At the time, it seemed remarkably easy for anyone to be tricked into sharing their password," he said. "That moment immediately heightened my awareness of the importance of cybersecurity, not just for myself, but for my family and friends as well."

Fast forward to today, that mindset hasn't changed. If anything, it's evolved into a full-blown passion for protecting businesses from modern cyberthreats. When the chance to join ThreatLocker came along, it was a no-brainer. "I was looking for something that could help me control how applications interact with sensitive data, and ThreatLocker Storage Control was the perfect solution," Jherome said. "It's rare to find a product that actually delivers what it promises, but this one does."

Now, as Manager of Enterprise Solutions Engineers, Jherome plays a key role in helping customers implement ThreatLocker tools. “There’s really no such thing as a typical day,” he said. “While I do have a general list of tasks I need to accomplish, the day-to-day collaboration is unpredictable and often the most rewarding part of my work.”

One of Jherome’s most memorable experiences came when a longtime customer faced a major setback after an administrator left the company. “They had become proficient and were successfully managing things on their own for over a year,” he shared. But with overly permissive rules in place, operations were at risk. “At that point, it was crucial for us as product experts to step in and provide hands-on support from start to finish,” he added. Rebuilding configurations across a multitude of endpoints wasn’t easy, but Jherome and his team worked alongside the customer to get them back on track.

For Jherome, the human side of cybersecurity is just as important as the technical side. “As a Solutions Engineer, I view myself as an extension of the customer’s team,” he said. “In many ways, I act as their ‘Zero Trust’ department.” He takes pride in helping customers navigate the shift to Zero Trust, offering as much support as they need—whether it’s two months or two years.

The relationships Jherome has built with customers are one of the most rewarding parts of his job. Events like Zero Trust World give the solutions engineer a chance to connect face-to-face with the organizations he works with every day. “Last year, around seven different organizations I partnered with came by to say hello and express their

appreciation for the work we’ve done together,” he said. “It was one of those moments when I genuinely felt like a movie star!”

It’s not just customers who notice Jherome’s hard work. His dedication hasn’t gone unnoticed—his coworkers voted him “Cyber Hero® of the Year,” and the company honored his achievement by awarding him a Porsche.

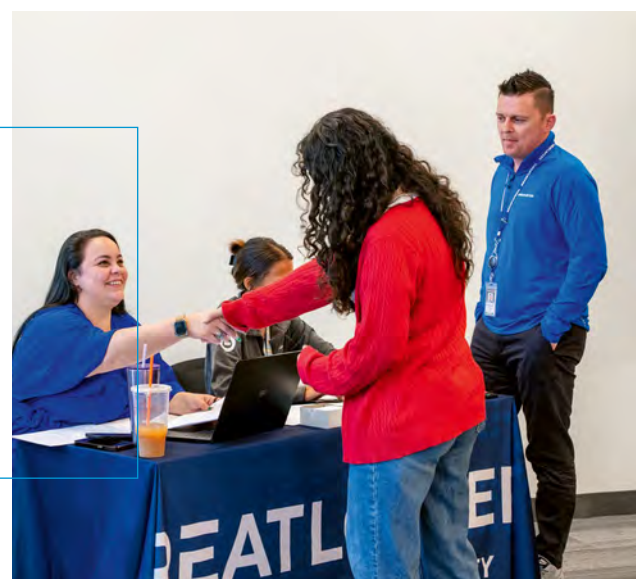
When he’s not busy leading his team or sharing his expertise with customers, you’ll probably find Jherome spinning tunes as a DJ, training dogs, or volunteering in his community. “I’m always looking for ways to give back,” he said. “If there’s an opportunity to make a difference, I’m all ears.”

When it comes to cybersecurity, Jherome believes it all comes down to balance. “Zero Trust is about finding that sweet spot between security and usability,” he explained. “ThreatLocker makes that balance simple. It gives businesses the tools they need to stay secure without making things complicated for their users.”

With a hands-on approach, technical expertise, and genuine passion for his work, Jherome has become a driving force behind the success of ThreatLocker. Whether mentoring the team, solving a customer’s challenge, or just sharing his love for Zero Trust, one thing is clear: Jherome’s in it for the long haul. And as he puts it, “If you love what you do, it doesn’t feel like work.”



SCAN FOR CAREER OPPORTUNITIES



UPCOMING EVENTS: JOIN US AND CONNECT

Stay on top of new threats, discover agile and robust solutions, and meet our Cyber Hero® Team at these top cybersecurity conferences and tradeshows. Join us at these upcoming events, where we share practical ideas to build a safer future together.

June 10–12
Las Vegas, US
Info-Tech LIVE

July 29–31
Nashville, US
GTIA ChannelCon2025

August 5 - 6
São Paulo BR
Conferência Gartner Segurança & Gestão de Risco 2025

August 6–7
Las Vegas, US
Black Hat USA 2025

August 10–14
National Harbor, US
ILTACON 2025

September 30–Oct 1
Toronto, CA
SecTOR

October 6–8
Miami Beach, US
Kaseya DattoCon

October 20 - 23
Orlando, US
Gartner IT Symposium/Xpo

October 27–29
Lake Buena Vista, US
InfoSec World

October 27–30
Nashville, US
EDUCAUSE Annual Conference

November 5–7
Orlando, US
IT Nation Connect Global

November 11–13
Austin, US
SpiceWorld 2025





June 3–5
London, GB
Infosecurity Europe

June 4–5
Frankfurt, DE
Cloud & Cyber Expo Frankfurt

September 30–Oct 1
London, GB
International Cyber Expo

November 5–6
Paris, FR
Cloud & Cyber Security Expo

November 10–13
Barcelona, ES
Gartner IT Symposium/Xpo

Riyadh
 Dubai

October 6–8
Dubai, UAE
Gartner CIO & Executive IT Conference

November 24–26
Riyadh, SA
Black Hat MEA

July 3
Sydney, AU
SydneySEC

September 8–10
Gold Coast, AU
Gartner IT Symposium/Xpo

October 15–17
Melbourne, AU
Cybercon Melbourne

October 28–30
Sydney, AU
Kaseya DattoCon Asia-Pacific

December 2–4
Da Nang, VN
Canalys Forum

Da Nang

Gold Coast
 Sydney
 Melbourne

THREATLOCKER

Danny Jenkins | Co-Founder and CEO

Sami Jenkins | Co-Founder and COO

Shane Deegan | Chief Revenue Officer

Rob Allen | Chief Product Officer

Aliona Groh | Sr. Vice President, Brand Marketing

Paola Garcia | Director of Graphic Design

Collaborators

Ben Goodman | Brand Marketing Partnerships Manager

Heather Hartland | VP Experiential Marketing

Kieran Human | Special Projects Engineer

Izzy Martinez | Graphic Designer

Nicholas Minton | Content Engagement Specialist

Magazine concept & production by

THE RETHINK HUB LLC

Nathalie Grolimund | Publisher

Daisy Vieira | Editorial Manager, Copywriter

Mareike Walter | Graphic Designer

Amber Hunter | Copy Editor

Alex Cox | Tech Copywriter

Nora Walsh | Lifestyle Copywriter

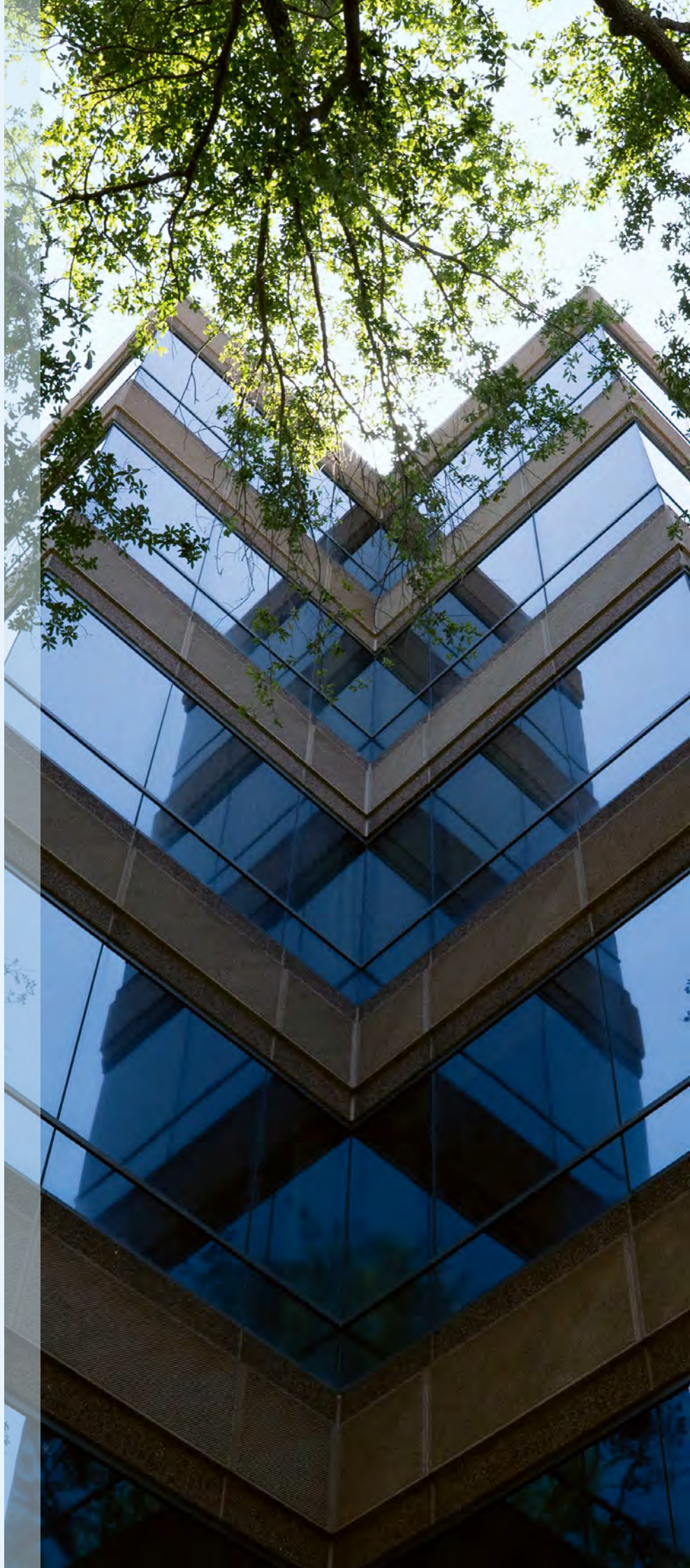
David Burghardt | Photo Editor

Rüdiger Breidert | Photo Editor, Pre-Press

Photo credits: ThreatLocker® (pages 1, 2, 4, 5, 6, 7, 10, 13, 15, 21, 25, 30, 31, 47, 48, 49, 84, 85, 88); MUTI (pages 8, 12, 18, 26); Rob Allen (page 37); The Colts (pages 38, 40, 41); Dan Warsinger - AutoCamp Yosemite Press Images (page 42); Under Canva (page 43); Kenny Karst (page 3, 44 top); Erin Feinblatt (page 44 bottom); Big Cedar Lodge (page 45); Tennessee Department of Tourism & Development (page 46 top); Tim Allison (page 46 bottom left); Andrew Mills Photography (page 46 bottom right); Harrison Steel Castings (pages 50, 53, 54); Andrea Izzotti (page 56); Marc Menzies (page 59); Peter Hurley (page 62); Shutterstock—Master1305 (page 65); Advanced Medical Transport (pages 68, 70, 71); Alexandros Michailidis (page 72); Airiam (pages 75, 77); Bo Olsen (pages 78, 79); Christopher Tirrell—IBM Quantum (page 81); Google (page 83).

¹Data Sources: (pages 11, 15) Statista *Estimated cost of Cybercrime Worldwide 2018-2029*; (page 27) IBM X-Force 2025 Threat Intelligence Index, CSO Magazine, Harvard Business Review; (page 28) FBI Internet Crime Report 2023, Statista; (page 29) Markets and Markets, IBM Cost of a Data Breach Report, Deloitte Center for Financial Services, World Economic Forum Global Cybersecurity Outlook 2024 Insight Report; (page 32) Verizon, Proofpoint Voice of the CISO Report 2024, Kaspersky; (page 34) Defense.com; (page 35) UK Government Cyber Security Breaches Survey; (page 37) SonicWall 2024 Mid-year Cyber Threat Report; (page 50) IBM X-Force 2024 Threat Intelligence Index, NIST, IBM; (page 66) STAT, HIPAA Journal; (page 67) Ponemon Healthcare Cybersecurity Report 2024, CNBC, HHS/OCR, Microsoft Digital Defense Report 2024.

Every effort has been made to identify the copyright holders of material used and accuracy of the information in this publication. The publisher cannot accept responsibility for any errors, and you can contact us for any correction. Reproduction in whole or in part without written permission is strictly prohibited. All information is correct as of press time. Printed in May 2025. © 2025 ThreatLocker. All rights reserved.



What happens if a user is compromised?

With us, hardly anything.

With ThreatLocker® Allowlisting, Ringfencing™, and Network Control, you are in complete control.

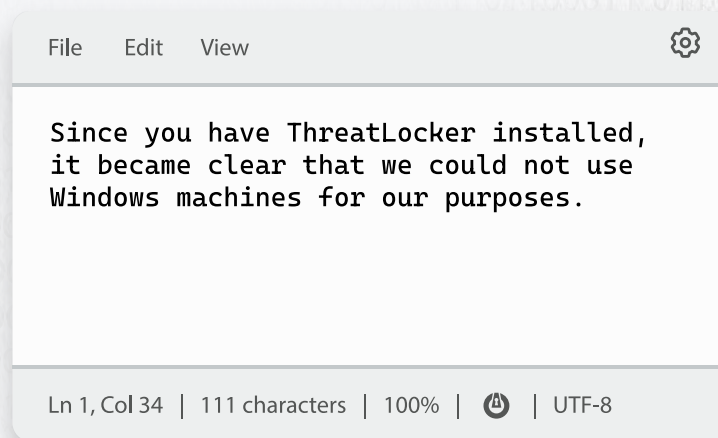
- ✓ **Choose what to trust:** Allow only authorized applications and users.
- ✓ **Restrict interactions:** Control how trusted apps access your data, preventing lateral movement.
- ✓ **Isolate threats:** Contain the damage when credentials are compromised.
- ✓ **Rest easy:** ThreatLocker® Orlando-based Cyber Hero® Team responds in about 60 seconds.

THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM



Ready to take control?
Book a demo now to redefine
your cybersecurity approach.

**this is why
hackers
hate us.**



– A real message from
an actual hacker.

**this is why
you will
love us.**

Do you know your current
systems' vulnerabilities?
**Order your free
software health report now.**

THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM



threatlocker.com