INTERVIEW

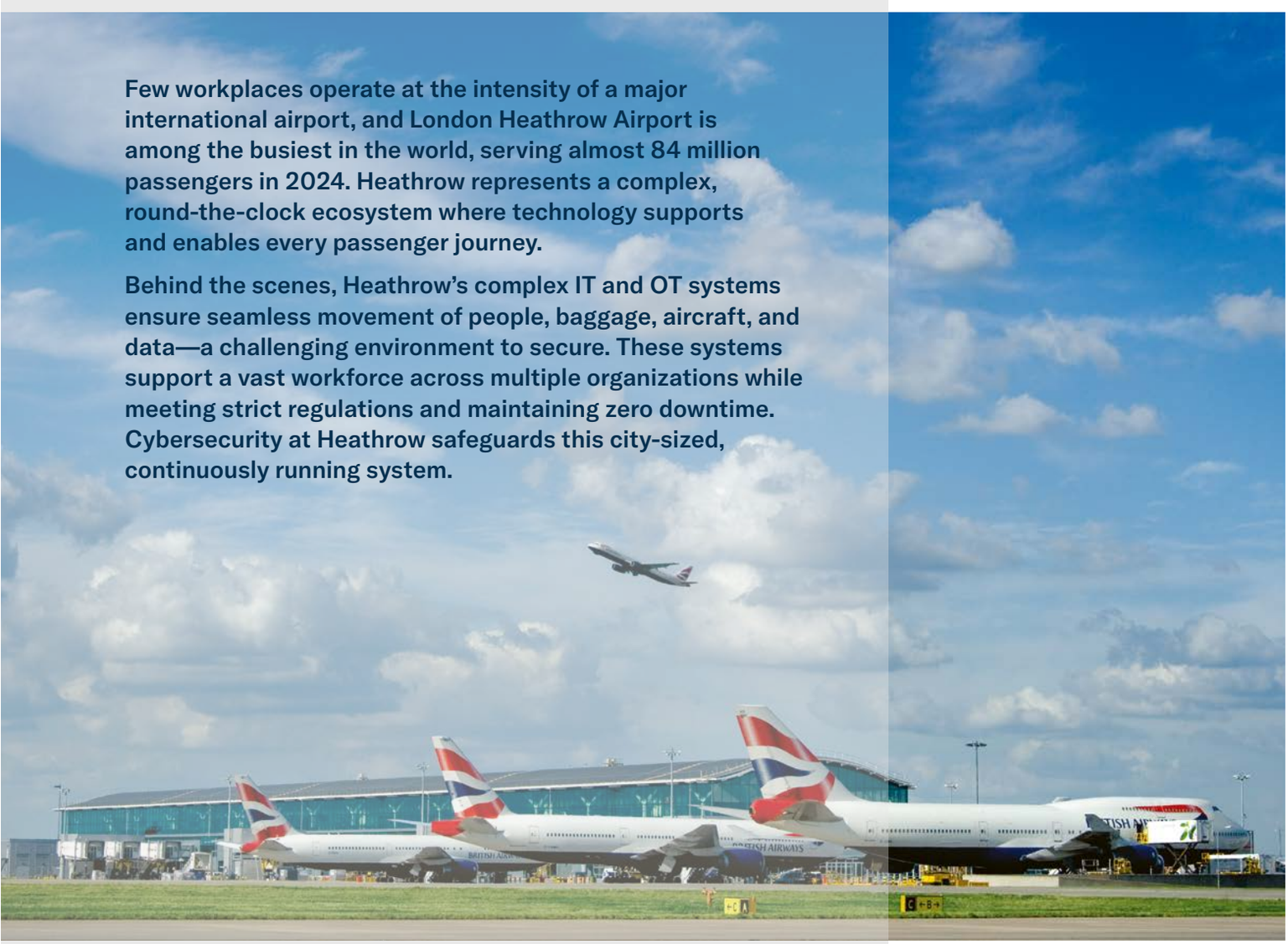
SECURING HEATHROW'S DIGITAL RUNWAY

Jeremy Parsons and Rob Thackeray, London Heathrow Airport

> "On an average day, we deal with 1,400 flights, and between 200,000 and 250,000 passengers passing through

Few workplaces operate at the intensity of a major international airport, and London Heathrow Airport is among the busiest in the world, serving almost 84 million passengers in 2024. Heathrow represents a complex, round-the-clock ecosystem where technology supports and enables every passenger journey.

Behind the scenes, Heathrow's complex IT and OT systems ensure seamless movement of people, baggage, aircraft, and data—a challenging environment to secure. These systems support a vast workforce across multiple organizations while meeting strict regulations and maintaining zero downtime. Cybersecurity at Heathrow safeguards this city-sized, continuously running system.



How does operating at Heathrow's scale make you think about cybersecurity and infrastructure differently?

JEREMY: There are 90,000 people working at Heathrow across the supply chain. It's the largest single-site employer in the U.K. On an average day, we deal with 1,400 flights, and between 200,000 and 250,000 passengers passing through. To offer an example in terms of IT, we run in excess of 3,500 Wi-Fi access points and 10,000 CCTV cameras. It's enormous. We essentially run IT for a city, and we're operating 365 days a year.

The times when other businesses might be able to shut down for maintenance—Christmas, holidays, the weekends—are our busiest. So, we're very aware that we can't do this on our own. We use the concept of "Team Heathrow." On a standard day, we might deal with 12 different organizations, and we have a highly collaborative approach.

The window to maintain all critical systems at Heathrow is very small, in terms of IT or OT. We tend to work between Monday and Thursday, very early morning, after the last flight and before the first. Maintenance crews might resurface just 33 feet of a runway at a time, because you can't take out a whole runway. The same is true of technology—we need to create well-thought-out migration plans, structure changes in small chunks, and build in multiple opportunities to achieve an objective if an airport operational issue gets in the way. You have to be extremely organized to deliver change at Heathrow.

How has Heathrow's technology evolved over the past twenty years?

JEREMY: Like many organizations, we've adopted a more hybrid structure, and over the past decade, we've increasingly relied on the cloud. However, we'll never be a cloud-only organization—there are no cloud-based baggage control systems, for example. While there will always be on-premises elements, we are open to collaborating closely with third parties. Zero Trust aligns well with our approach, as we need a comprehensive security philosophy that prioritizes safety in all situations, involving all parties.

ROB: It's all about integration—more partners, increasing data flow, and the need to align everything with the complexity of operating flights. It has always been complex, but that complexity has grown massively over the years. The process of constant small changes has helped us build a very modern and well-managed estate. Still, certain aspects are more difficult to upgrade and update—we innovate where we can, but stability is the primary factor in operational decision making.

After evaluating several candidates, Jeremy Parsons and Rob Thackeray found ThreatLocker® to be the most intuitive, enterprise-ready tool

> "Zero Trust isn't something you can come along and implement in an existing organization. It's a journey, and ThreatLocker is a vital component of our Zero Trust architecture

Do you feel you're up against a unique level of cyberthreat?

ROB: I believe the cyberthreats Heathrow faces are similar to those encountered by many other companies. Everyone out there, whether they realize it or not, is constantly under attack. The difference is that Heathrow is more of a target. It's something that, for whatever reason, bad actors would like to break. We're a high-value target, a prize, which increases the risk.

In the current climate, I'd say ransomware is probably the biggest threat. Denial of service is a huge issue. And threats are constantly evolving. But you need to make sure you're in a position to adapt to them. We do have a slight advantage as an organization—the nature of aviation, the physical threats that come along with that, means that security is well embedded within Heathrow. That helps with security buy-in.

How did your partnership with ThreatLocker come about? How does it fit into your architecture?

JEREMY: There was a requirement for us to be able to do application control on the estate. Rob and I evaluated a large number of products and trialed them internally on our own devices.

> "ThreatLocker was the most intuitive solution we tested [...] It's great to have an ongoing relationship with a company that's so responsive to our requests

This helped us figure out how suitable they would be to roll out to Heathrow, given that we have to be able to do it with no downtime at all.

There were a number of potential candidates, but none that would have the same level of impact as ThreatLocker. It's unique in the way it operates. Running in monitor mode to understand the impact on the business before putting it into action is critical to us. If we didn't have that functionality, there's no way we would have been able to roll it out across the entire estate. We needed an enterprise-ready tool, and ThreatLocker absolutely fit the bill.

← Cybersecurity at Heathrow safeguards the city-sized, continuously running system

↑ With 1,400 flights and up to 250,000 passengers a day, securing Heathrow's data is paramount

ROB: I've also got to mention the ease of ongoing management. ThreatLocker® was the most intuitive solution we tested. And the responsiveness of the organization—the willingness to engage with us, set up a demo, and work with us on weekly audit reviews—was very good. It's great to have an ongoing relationship with a company that's so responsive to our requests.

Which came first, ThreatLocker or your Zero Trust practices?

JEREMY: Zero Trust isn't something you can come along and implement in an existing organization. It's a journey, and ThreatLocker is a vital component of our Zero Trust architecture. And as we take our systems through their refresh cycle, that Zero Trust mindset is always there.

ROB: Having rolled out ThreatLocker to our end-user estate, it's really helping to establish and enforce Zero Trust. It has had a big impact, actively changing the actions of some of our user base, because they're seeing that deny-by-default model in action.

JEREMY: And on top of that, where bad practices have been discovered on the estate, ThreatLocker provides technical control, which stops those bad practices from happening. We're using ThreatLocker Application Control, Ringfencing™, and Detect in certain environments. In the future, we will roll out Storage Control, too.

Can you describe the impact ThreatLocker has had?

JEREMY: There's a lot we can't talk about for security reasons, but I can tell you that it identified applications we didn't know were running. In a small number of cases, we found things on the network which we would not necessarily have approved of, or programs accessing a service they shouldn't have. But sometimes these are things our partners need, whereas in the past we might have had to block them entirely. We've been able to use ThreatLocker to find these applications and control the context in which they can operate. Ringfencing, in particular, has been key to improving our security.

Heathrow Airport announces plans for expansion to enhance capacity and improve traveler experience

> We work with so many partners, components, and applications, ThreatLocker allows us to minimize the blast radius if something goes wrong

ROB: We've also been able to demonstrate multiple "what if" scenarios by running labs to show what would happen in case of a disaster and how we would respond. In our line of work, control of lateral movement is essential. We work with so many partners, components, and applications, ThreatLocker allows us to minimize the blast radius if something goes wrong.

Why did you decide to switch to a Zero Trust strategy in the first place?

JEREMY: Like lots of organizations, we have had to pivot from the semi-trust model; it's a risk that's leading us to Zero Trust. It means a change in architecture and a change in tooling, of which ThreatLocker is a key component.

ROB: A lot of the principles and techniques aren't new. Least privilege access has always been something we've adhered to at Heathrow. Zero Trust aligns with industry best practices, and our existing mindset and strategy have helped us evolve in that direction, but we're still on the journey. The key challenge with Zero Trust is getting the balance right between making the service secure while still delivering the service. It's a real art form. If the model you implement restricts operations too much, people will inevitably find a way around it.

What makes working at Heathrow special for you?

JEREMY: No two days are ever the same. The scope of our work is vast—from working on an end-user computer one day to speaking with the team managing the railway or Heathrow's power generation system the next. We end up working with everything and anything.

ROB: And don't forget the planes. Our office is on the airport perimeter, and when visitors arrive, they often look out in awe at the runways. Meanwhile, we're working on many different, diverse systems, so we almost forget that planes are just outside.

Heathrow has its challenges, but we've got a strong team and a strong culture, and we're only one part of the passenger journey. The important thing is that passengers get away, on time, safely, with their baggage. Sure, it would be nice if people knew or appreciated what we're doing to make things secure, but they shouldn't need to know. Traveling through an airport is a naturally stressful thing to do, and we just want to make that as smooth as possible.

FEATURE PROFILES

Rob Thackeray leads the end-user computing estate at Heathrow, focusing on secure, modern technology for staff and contractors. His team manages everything that interfaces directly with users, often pioneering the use of new tools and processes such as Zero Trust with service providers like ThreatLocker. Thackeray first joined Heathrow in 1999 under the former BAA group, rising to Lead IT Infrastructure Architect before moving into industry roles with HP and other firms. He returned about two-and-a-half years ago to a now stand-alone Heathrow, where he works closely with Jeremy Parsons to align day-to-day IT operations with wider cybersecurity strategy.

Jeremy Parsons is a Cybersecurity Architect at Heathrow, overseeing both IT and OT systems across the airport. His remit covers any technology with a network connection—from operational equipment to core IT infrastructure—taking a holistic, city-scale view of security. With more than 20 years in IT consulting for both public and private sectors before joining Heathrow over a decade ago, he brings a broad industry experience. Parsons previously held Rob Thackeray's current role, giving him insight into end-user operations as well as strategic security architecture.