Lookout

Case Study

Airbus expands its confidence in Lookout by protecting all 160,000 global employees



© AIRBUS

The Challenge — Reduce Mobile Cyber Risk

Airbus, global leader in aeronautics and space services, manufactures a comprehensive line of civilian aircraft including helicopters, airplanes and military vehicles.

As with every large enterprise, Airbus has grappled with the paradigm shift of work in recent years. Some workers are fully remote, while others are distributed or hybrid, which has created a fundamental reliance on mobile devices. This has subsequently blurred the lines between corporate and personal use of these devices — posing potentially high risk for Airbus. For their team, it was critical to maintain a fully integrated security ecosystem for its fleet of corporate iOS and Android endpoints — extending Zero Trust access and proactively monitoring for threats in order to protect against a broadening array of mobile risks.

Previously, Airbus had built its mobile security strategy around access control. This platform was based in an integrated ecosystem of mobile device management (MDM), a security incident and event manager (SIEM) platform, and single sign-on (SSO) to simplify mobile access via the organization's cloud access security broker (CASB) to ensure safe access to cloud resources.

AIRBUS

The Customer:

Airbus is a leading global aerospace company that designs, manufactures, and delivers commercial aircraft, helicopters, defence and space equipment. The company is the largest aeronautics and space company in Europe and a major worldwide competitor in the aerospace industry. As one of the world's leading aerospace companies with a global workforce of more than 160,000 employees Airbus is dedicated to maintaining comprehensive mobile endpoint security and protecting its cybersecurity reputation.

Industry: Aerospace

Challenges:

- Extending Zero Trust and EDR to mobile devices in order to secure and protect access to sensitive cloud data.
- Gaining visibility into mobile risk and protecting employee mobile devices against mobile malware, device compromise, network attacks and more.
- Deploying seamlessly to corporate iOS and Android endpoints, with an intuitive but unobtrusive interface for employees in the field.

The Solution: Lookout Mobile Endpoint Security (MES)

The Results:

- With seamless deployment to new and existing mobile devices, Airbus now protects more than 160,000 employees who rely on their iOS and Android devices every day.
- By implementing Lookout Continuous Conditional Access, Airbus is able to extend its Zero Trust strategy to mobile endpoints and create a unified endpoint access strategy.
- With the advanced protections provided by Lookout, Airbus can now proactively detect and protect against mobile threats while implementing tight privacy controls.
- Extended visibility into the comprehensive landscape of mobile threats has given Airbus unmatched insights into potential inbound attacks against their organization.

As a global aerospace leader, Airbus has a core cultural ideology to maintain a world-class security posture and adopt leading edge technologies. As the company embraced digital transformation and mobile connectivity, it became clear that Zero Trust and enhanced mobile security were critical tenants to achieving those goals.

But given the sharp rise of remote work and mobile connectivity, even prior to the pandemic, Airbus Security Product Manager Sébastien François understood that the enterprise would need more comprehensive and sophisticated security measures to protect its corporate-managed mobile endpoints. Moreover, Airbus was contending with the evolving and multi-layered mobile threat landscape. In addition to high-profile attacks like Pegasus and Scattered Spider targeting large enterprises, zero-day vulnerabilities and the challenge of managing security across a variety of corporate devices made it clear that Airbus needed to prioritize mobile security and Zero Trust.



© AIRBUS 2019 — Photo by S. COLDING / Mango Producciones

The Solution

Over the course of seven years together, Lookout and Airbus have built a strong relationship of trust. With that experience, Sébastien and his team knew that Lookout could continue to grow and evolve with them as they focused on key initiatives such as:

- Implementing a consistent deployment and security model across a growing fleet of both company- and employee-owned mobile devices.
- Extending Zero Trust to mobile productivity, email, and collaboration apps while maintaining a balance between security and operational efficiency.
- Securing mobile endpoints against mobile cyber threats, while providing proactive visibility, detection, and remediation against any emerging threats.
- Integrating with its MDM and smoothly deploying to its fleet of more than 160,000 corporate endpoints from a cloud-based platform.
- Providing an easy-to-use, non-intrusive interface for employees who work in the field.

After seven years of successful operation with Lookout, Airbus conducted a rigorous RFP process, and this evaluation confirmed that Lookout's technology continues to be the most effective choice. As a result, Airbus is expanding its deployment of Lookout's protection solution from 100,000 to more than 160,000 devices across its mobile fleet.

> *"Throughout the RFP process, we really dug into the threat detection capabilities of each security vendor and their integration with our evolving IT and security environment. It became clear that Lookout is still at the top of the field. As we continue our Zero Trust journey with our cloud-based infrastructure, we are confident that Lookout will enable secure access to all of our cloud data, now and in the future."*
>
> **— Sébastien François, Security Product Manager, Airbus.**

The Results

Working closely with the Lookout customer success team, Airbus has successfully deployed Lookout Mobile Endpoint Security to more than 160,000 corporate iOS and Android endpoints. Immediately, Airbus was able to implement global policies that allowed only devices installed with Lookout to access cloud-based corporate data in their Google Workspace platform. Moreover, Airbus was able to implement stringent mobile access policies through the Lookout Continuous Conditional Access service — enabling Zero Trust across every mobile device for all cloud-based corporate data.

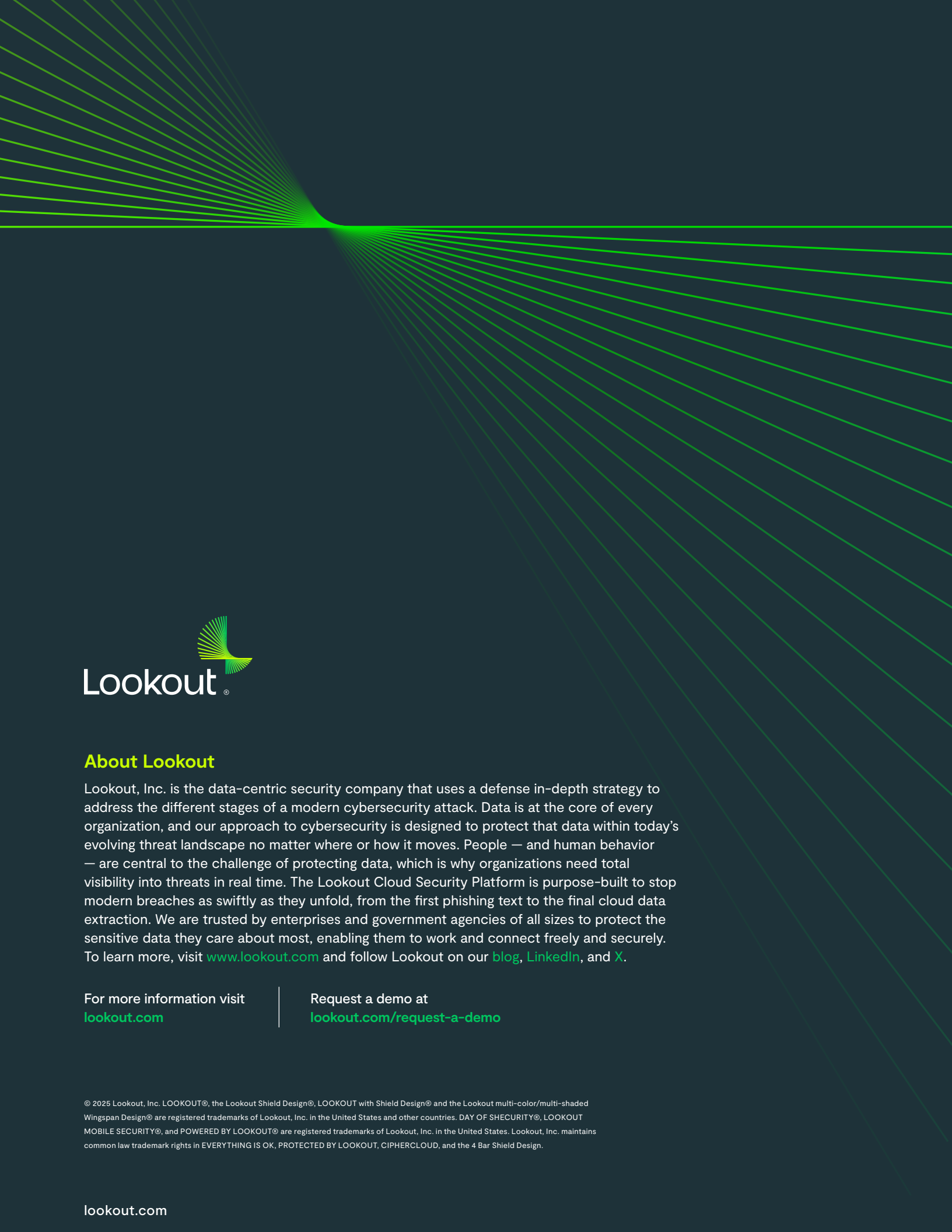
Airbus also gained complete visibility into the full spectrum of mobile risks. The organization was able to immediately implement robust detection and protection capabilities that could protect against even the most evasive mobile threats. Airbus is more confident in its mobile security and alignment with ever-shifting compliance and data sovereignty standards.

> *"Airbus has greatly benefited from a close partnership with Lookout since 2017. This collaboration has provided the dedicated support necessary to manage our large-scale deployment.*
>
> *The employee education provided by Lookout, featuring in-app educational resources and close engagement from the Lookout support team, has been straightforward and effective for both our technical and non-technical users."*
>
> **— Sébastien François, Security Product Manager, Airbus.**

With Lookout, Airbus benefits from the industry's leading mobile security and threat intelligence protections. Every day, Lookout inspects roughly 100,000 applications for malicious activity and nefarious intent and has analyzed over 400 million apps overall. By automatically scouring every version of every app across the world's largest app stores, third-party stores, and more, the artificial intelligence that backs Lookout MES identifies and auto-convicts nearly 10,000 new malicious apps each day. This automated analysis, combined with the industry's best threat researchers, keeps Airbus continuously informed and protected against the emerging landscape of mobile threats.

Airbus has tens of thousands of employees working in the field. Lookout gives Airbus the peace of mind that those workers are protected throughout the full lifecycle of the user and device. This ensures that users do not fall prey to any mobile threats, whether they be man-in-the-middle attacks, connections to rogue Wi-Fi networks, jailbreak vulnerabilities, or more; and that any non-compliant or malicious behavior — at both the device and application level — is automatically identified and remediated on the device and alerted to the Airbus security operations team.

As a global leader in commercial and military aerospace, Airbus is now confident in its mobile security posture across its global workforce. With Lookout, Airbus can fully pursue its global digital transformation initiatives and embrace the shift to remote, decentralized work, while maintaining its secure reputation as an aerospace and technology pioneer worldwide.



About Lookout

Lookout, Inc. is the data-centric security company that uses a defense in-depth strategy to address the different stages of a modern cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data within today's evolving threat landscape no matter where or how it moves. People — and human behavior — are central to the challenge of protecting data, which is why organizations need total visibility into threats in real time. The Lookout Cloud Security Platform is purpose-built to stop modern breaches as swiftly as they unfold, from the first phishing text to the final cloud data extraction. We are trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and securely. To learn more, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and X.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo

© 2025 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design® and the Lookout multi-color/multi-shaded Wingspan Design® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, and the 4 Bar Shield Design.