Airbus Deploys Lookout Mobile Endpoint Security to 100,000+ Global Workforce

© AIRBUS 2019 - photo by S.RAMADIER

The Challenge – Reduce Mobile Cyber Risk

Every large enterprise, with the changing paradigm of work in the wake of COVID-19 – where workers are remote, distributed and hybrid – has to rely more and more on mobile devices. This has subsequently blurred the lines between corporate and personal applications and devices. In order to maintain a fully integrated security ecosystem for its fleet of corporate iOS and Android endpoints, Airbus wanted to extend Zero Trust access, and proactively monitor threats while preventing these devices across a broadening array of mobile risks.

Zero Trust and enhanced mobile security became core strategies for embracing the company's digital transformation and mobile connectivity.

AIRBUS

The Customer:

About Airbus

Airbus pioneers sustainable aerospace for a safe and united world. The Company constantly innovates to provide efficient and technologically-advanced solutions in aerospace, defence, and connected services. In commercial aircraft, Airbus offers modern and fuel-efficient airliners and associated services. Airbus is also a European leader in defence and security and one of the world's leading space businesses. In helicopters, Airbus provides the most efficient civil and military rotorcraft solutions and services worldwide.

Industry: Aerospace

Challenges:

- Implementing a Zero Trust strategy for every mobile endpoint, to secure and protect cloud-based data and applications.
- Securing employees' mobile endpoints against a broad range of attacks, while providing complete visibility into cyber risk.
- Providing a seamless deployment to corporate iOS and Android endpoints, with an intuitive but unobtrusive interface for employees using mobile devices in the field.

Solution: Lookout Mobile Endpoint Security

Results:

- Lookout Mobile Endpoint Security (MES) deployed to more than 100,000 iOS and Android devices.
- Zero Trust strategy extended to corporate mobile endpoints with Continuous Conditional Access from Lookout.
- Detection and protection against device and application threats as well as tight privacy controls.
- Fully visible mobile threat landscape.

Solution

Even prior to the pandemic, to prevent high-profile attacks like Pegasus or Trident targeting large enterprises, Airbus had always implemented the most comprehensive security measures to protect its corporate-managed mobile endpoints. Zero Trust access enables the company to manage security across a variety of corporate devices, while securing both company and employee-owned mobile endpoints with a consistent security and deployment model.

Lookout Mobile Endpoint Security was deployed to more than 100,000 Airbus corporate iOS and Android endpoints. Stringent mobile access policies were implemented via Lookout Continuous Conditional Access – enabling Zero Trust across every mobile device for all cloud-based corporate data.

Moreover, to protect against even the most evasive mobile threats, robust detection and protection capabilities were implemented throughout the organisation, while maintaining the alignment with ever-shifting compliance and data sovereignty standards.

The Lookout team provided Airbus with the right level of dedicated support needed to manage its large-scale deployment. Employee education from Lookout was straightforward for technical and non-technical users alike, with in-app Lookout educational resources and close engagement from the Lookout support team.

Lookout Mobile Endpoint Security is powered by the Lookout Security Graph, which analyzes telemetry data from more than 200 million devices and 150 million apps, and continuously ingests and analyzes millions of URLs every day. By using machine intelligence, Lookout secures organizations against phishing, app, device and network threats in a manner that respects user privacy. The use of machine learning on data in the Lookout Security Graph enables Lookout Mobile Endpoint Security to automatically detect and respond to threats even if they have never been seen before.

Lookout enables the protection of all employees 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.

Results

- Zero Trust was extended to corporate data over email, collaborative and home-built apps while maintaining a balance between security and operational efficiency;
- Secure mobile endpoints against mobile cyber threats, while providing proactive visibility, detection, and remediation against and protection against any potential emerging threats;
- Smooth deployment to its fleet of more than 100,000 corporate endpoints from a cloud-based platform;
- Provide an easy-to-use, non-intrusive interface for employees who work in the field.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more about Lookout Mobile Endpoint Security, visit lookout.com/products/mobile-endpoint-security.