

Fallstudie

Airbus führt Lookout Mobile Endpoint Security für mehr als 100.000 Mitarbeiter weltweit ein



© AIRBUS 2019 – Foto von S. RAMADIER

Die Herausforderung: Eindämmen der Cybersicherheitsrisiken für Mobilgeräte

Im Zuge der Coronapandemie hat sich die Arbeitswelt gewandelt und große Unternehmen müssen sich auf mobilere, dezentrale und hybride Arbeitsplätze einstellen, an denen Mobilgeräte zunehmend an Bedeutung gewinnen. Um für sämtliche firmeneigene iOS- und Android-Endgeräte eine voll integrierte Sicherheitsumgebung zu schaffen, hat Airbus den Zero Trust Access ausgeweitet. Bedrohungen werden proaktiv überwacht und die Geräte vor immer vielfältigeren Risiken geschützt.

Zero Trust und die Sicherheit mobiler Endgeräte spielen für Airbus seit jeher eine zentrale Rolle bei der Strategie für Digitalisierung und mobile Konnektivität.

Airbus hat schon immer umfangreichste Sicherheitsmaßnahmen zum Schutz der vom Unternehmen verwalteten mobilen Endgeräte ergriffen. Aufgrund der Auswirkungen der Pandemie auf das Arbeitsumfeld musste jedoch die Zero-Trust-Strategie ausgedehnt werden, um auch die Sicherheit auf den vielfältigen Firmengeräten sicherzustellen und gleichzeitig sowohl die geschäftlichen als auch privaten mobilen Endgeräte der Mitarbeiter mit einem einheitlichen Sicherheits- und Bereitstellungsmodell zu schützen.

AIRBUS

Der Kunde:

Über uns

Airbus ist Pionier einer nachhaltigen Luft- und Raumfahrt für eine sichere und vereinte Welt. Das Unternehmen arbeitet ständig an Innovationen für effiziente und technologisch fortschrittliche Lösungen in den Bereichen Luft- und Raumfahrt, Verteidigung sowie vernetzte Dienstleistungen. Airbus bietet moderne und treibstoffeffiziente Verkehrsflugzeuge sowie dazugehörige Dienstleistungen an. Airbus ist auch führend in Europa im Bereich Verteidigung und Sicherheit und eines der größten Raumfahrtunternehmen der Welt. Im Bereich Hubschrauber stellt Airbus die weltweit effizientesten Lösungen und Dienstleistungen für zivile und militärische Hubschrauber bereit.

Branche: Luft- und Raumfahrt

Herausforderungen:

- Einführung einer Zero-Trust-Strategie für alle mobilen Endgeräte zum Schutz cloudbasierter Daten und Anwendungen.
- Schutz der mobilen Mitarbeiterendgeräte vor verschiedensten Angriffen sowie umfassende Transparenz bezüglich Cyberrisiken.
- Nahtlose Bereitstellung für iOS- und Android-Firmenendgeräte mit intuitiver, aber nicht-intrusiver Benutzeroberfläche für Mitarbeiter, die Mobilgeräte im Außeneinsatz nutzen.

Die Lösung: Lookout Mobile Endpoint Security

Das Ergebnis:

- Implementierung von Lookout Mobile Endpoint Security auf mehr als 100.000 iOS- und Android-Geräten.
- Zero-Trust-Strategie mit Continuous Conditional Access von Lookout auf mobile Firmenendgeräte ausgeweitet.
- Erkennung und Schutz vor Geräte- und Anwendungsbedrohungen sowie strenge Datenschutz-Kontrollmechanismen.
- Vollständige Übersicht über mobile Bedrohungslage.

Die Lösung

Über Lookout Continuous Conditional Access wurden strenge Richtlinien für den mobilen Zugriff eingeführt – und so Zero Trust für alle cloudbasierten Unternehmensdaten auf sämtlichen Mobilgeräten ermöglicht.

Darüber hinaus wurden im gesamten Unternehmen robuste Erkennungs- und Schutzfunktionen eingeführt – ohne die Einhaltung der sich immer wieder ändernden Compliance-Standards und Bestimmungen zur Datenhoheit einzuschränken – um selbst die am schwersten aufspürbaren Bedrohungen aufzudecken.

Das Team von Lookout stellte Airbus angemessenen, individuellen Support bereit, um diese groß angelegte Implementierung zu betreuen. Die Mitarbeiter wurden von Lookout ungeachtet ihrer technischen Vorkenntnisse unkompliziert mit Lehrinhalten in der Lookout App und unter enger Einbindung des Lookout Supportteams geschult.

Lookout Mobile Endpoint Security basiert auf dem Lookout Security Graph, der tagtäglich Telemetriedaten von über 200 Millionen Geräten und 150 Millionen Apps auswertet und kontinuierlich Millionen von URLs erfasst und analysiert. Mithilfe von maschineller Intelligenz schützt Lookout Unternehmen vor Phishing sowie App-, Geräte- und Netzwerkbedrohungen unter Achtung der Privatsphäre der Anwender. Durch die Anwendung maschinellen Lernens auf die Daten im Lookout Security Graph kann Lookout Mobile Endpoint Security selbst bisher unbekannte Bedrohungen automatisch erkennen und auf sie reagieren.

Lookout ermöglicht den Schutz aller Mitarbeiter über den gesamten Lebenszyklus eines Benutzerkontos und Geräts hinweg. So lässt sich vermeiden, dass Benutzer Opfer von Bedrohungen auf Mobilgeräten werden – seien es Man-in-the-Middle-Angriffe, Verbindungen mit unkontrollierten WLANs, Schwachstellen durch Jailbreaking oder ähnliches. Zudem können Richtlinienverstöße oder böses Verhalten sowohl auf Geräte- als auch Anwendungsebene automatisch erkannt und auf dem Gerät beseitigt sowie dem Sicherheitsteam von Airbus gemeldet werden.

Das Ergebnis

- Ausdehnung von Zero Trust auf per E-Mail, über Kollaborations-Apps und firmeneigene Apps übertragene Unternehmensdaten bei Wahrung der Balance zwischen Sicherheit und betrieblicher Effizienz
- Vor Cyberbedrohungen geschützte mobile Endgeräte und gleichzeitige proaktive Sichtbarkeit, Erkennung und Beseitigung von Bedrohungen sowie Schutz vor potenziellen neuen Bedrohungen
- Reibungslose Bereitstellung auf mehr als 100.000 Firmenendgeräten über eine cloudbasierte Plattform
- Bereitstellung einer einfach zu bedienenden, nicht-intrusiven Benutzeroberfläche für Mitarbeiter im Außeneinsatz

Mehr über Lookout Mobile Endpoint Security erfahren de.lookout.com/products/endpoint-security.

Auf mehr als 100.000 firmeneigenen iOS- und Android- Geräten von Airbus wurde Lookout Mobile Endpoint Security implementiert.



Über Lookout

Lookout, Inc. ist das Unternehmen für Sicherheit von Endgeräten bis in die Cloud speziell entwickelt für die Schnittstelle zwischen Unternehmens- und persönlichen Daten. Durch unsere einheitliche, Cloud-native Sicherheitsplattform schützen wir Daten über Geräte, Anwendungen, Netzwerke und Clouds hinweg – eine Lösung, die so fließend und flexibel ist wie die heutige digitale Welt. Indem wir Unternehmen und Privatpersonen mehr Kontrolle über ihre Daten geben, ermöglichen wir ihnen, ihr Potenzial voll auszuschöpfen und erfolgreich zu sein. Unternehmen jeder Größe, Behörden und Millionen von Privatpersonen vertrauen auf Lookout, um sensible Daten zu schützen, damit sie frei und sicher leben, arbeiten und sich vernetzen können. Um mehr über die Lookout Cloud Security Plattform zu erfahren, besuchen Sie www.lookout.com und folgen Sie Lookout auf unserem [Blog](#), [LinkedIn](#), und [Twitter](#).

Für mehr Informationen
lookout.com

Demo anfordern
lookout.com/demo-anfragen

© 2023 Lookout, Inc. LOOKOUT®, das Lookout Shield Design®, LOOKOUT mit Shield Design®, und SIGNAL FLARE® sind eingetragene Marken von Lookout, Inc. in den Vereinigten Staaten und anderen Ländern. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, und POWERED BY LOOKOUT® sind eingetragene Marken von Lookout, Inc. in den Vereinigten Staaten. Lookout, Inc. unterhält Common Law Markenrechte an EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, dem 4-Balken-Schild-Design und dem Lookout Multi mehrfarbigen/mehrschattigen Wingspan-Design.

lookout.com