ZIMPERIUM

Major Global Airline Adopts Mobile-First Security Strategy

Industry

Airline and Transportation

Location

International Scope

Solution

Zimperium Mobile Threat Defense (MTD) / Mobile EDR

Customer Profile

As a leading US-based airline with ambitions to become the largest in aviation history, this global carrier plans to grow by 50% over the next few years. With a workforce of approximately 100,000 employees and a worldwide network of hundreds of destinations, the airline is committed to providing exceptional customer experiences through modern aircraft and cutting-edge IT solutions. As a result, the airline has adopted a mobile-first strategy to streamline operations, reduce costs, enhance productivity, and boost revenue with mobile technology.

The Challenge

Attackers are turning their attention to the aviation industry now that travelers have returned to frequent travel. Various cyber threat actors, including nation-state actors, advanced persistent threat (APT) groups, organized cybercriminals, and hacktivists, target the commercial aviation sector. These groups aim to steal sensitive data, disrupt operations, extort money through ransomware, or gain geopolitical advantages. Additionally, the widespread adoption of digital technologies and their connectivity to aviation systems has created a vast and complex attack surface for airlines. As a result, managing cybersecurity risks has become increasingly difficult due to the various malicious actors, services, devices, and data involved.

This interconnected nature means that a breach in one area can have widespread implications for both national security and critical infrastructure. Recent cyber incidents in the aviation sector include data breaches and DDoS attacks on major airlines. Recognizing the crucial role of security in national infrastructure, the airline had been advised by top government agencies on the evolving threat landscape, particularly those surrounding mobile devices.

Understanding the urgency and potential impact, the airline identified the necessity for a comprehensive mobile endpoint security solution. To ensure the highest standards of protection, they sought a solution that closely aligned with the National Institute of Standards and Technology (NIST) 800 guidelines and the Open Worldwide Application Security Project (OWASP) framework. This alignment would not only help them stay ahead of mobile threats but also ensure compliance with industry best practices and regulatory requirements.

As a “mobile-first” company, the airline manages a vast fleet of mobile devices across various operations, including:

- **In the Cockpit:** Pilots use iPads to manage aviation-related information and flight plans.
- **In the Cabin:** Flight attendants use iPhones for work duties, accessing flight and passenger information, processing transactions, and maintaining communications during flights.
- **On the Ground:** Ground crews use multiple types of mobile devices for service tracking, scanning new parts, and operational coordination.
- **During Training:** Trainees use iPads equipped with software and features that simulate various flight scenarios, emergency situations, and training exercises.
- **For Corporate Personnel:** Smartphones enable employees to access corporate resources continuously.

> *"As we evaluated several vendors, it became clear that none could match Zimperium. Many competitors leaned too far into being an MDM rather than a true Mobile Threat Defense solution. The strong relationship we've built and the seamless integration into our operations reinforced our decision. Choosing Zimperium made perfect sense for us regarding capability, interface, and overall value."*
>
> -CISO of a Global Airline

With over 125,000 devices in use—including employee-owned, corporate-issued, and specialty devices—the airline recognized the significant challenge of maintaining visibility and protection for a vast number of devices. They required a solution they could easily manage and seamlessly integrate with their existing security systems, providing a frictionless experience and single pane of glass visibility.

Real-time Visibility
Mobile devices are exposed to numerous connectivity threats due to their portable, always-on nature. These threats include network risks, web threats, and vulnerabilities in both default and third-party apps. Managing these risks is crucial to maintaining device and data security. Traditional endpoint detection and response technologies are inadequate for providing the real-time visibility needed to monitor the status and security of all mobile devices and applications. A more advanced and responsive mobile endpoint solution is required to ensure real-time visibility to safeguard against device compromises, phishing attacks, network threats, and mobile malware.

Mobile App Vetting
Using mobile apps from various sources, whether developed in-house or obtained through app stores, without thorough vetting significantly increases the risk of mobile attacks. Conducting advanced analysis of apps used on devices that access corporate resources is essential for enhancing security. This process is crucial for preserving the security and privacy of the workforce and the airline's operations.

Integration with Existing Security Systems
Integrating mobile security measures with existing security systems poses a significant challenge. The airline needed a solution that seamlessly integrated with its current cybersecurity infrastructure, ensuring comprehensive protection across all platforms without creating security gaps or inefficiencies.

Compliance and Regulatory Requirements
To meet NIST 800 standards, the airline must navigate and comply with emerging regulations from the US Government's Transport Security Administration (TSA). Additionally, the airline must address requirements from the Federal Aviation Administration (FAA) and other regulatory bodies, such as the General Data Protection Regulation (GDPR), which impose further privacy and security mandates on their mobile endpoints.

The Solution

The airline implemented Zimperium Mobile Threat Defense™ (MTD) to address these challenges. Zimperium MTD is a privacy-first application designed to provide comprehensive mobile security. It offers security teams mobile risk and vulnerability assessments, valuable insights into the risks of mobile applications, and threat protection to secure employee and corporate-owned devices from advanced persistent threats across device, network, phishing, and app risks and malware vectors.

Key Features of Zimperium MTD:

- **Zero-Day Threat Detection:** Powered by Zimperium's Dynamic On-Device Detection Engine, MTD detects and protects against the latest mobile threats, including zero-day malware.
- **Real-time Visibility:** Provides increased visibility into the status and security of all mobile devices and applications.
- **Advanced Mobile App Vetting:** Conducts in-depth analysis of apps used on corporate devices to identify and mitigate potential security and privacy threats.
- **Seamless Integration:** Integrates smoothly with enterprise SIEM, IAM, UEM, and XDR platforms, ensuring a comprehensive and cohesive security approach.
- **Compliance Assurance:** Enables airlines to navigate and comply with regulatory requirements, including NIST 800 standards and OWASP standards, FAA mandates, and GDPR.

The Benefits

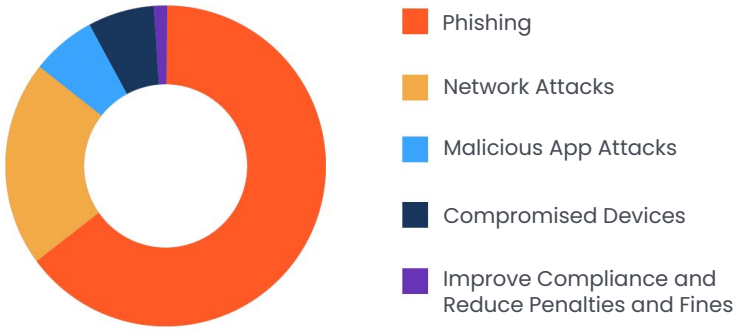
The airline has seen substantial benefits from implementing Zimperium MTD, which has significantly enhanced the safety and compliance of its operations.

Here are three key advantages:

- **Enhanced Security Monitoring:** MTD offers comprehensive vulnerability reporting and continuous monitoring, ensuring near real-time detection of suspicious activities or security incidents affecting a mobile device's ecosystem.
- **Improved Risk Management:** MTD provides valuable insights into mobile app and device risks, allowing the airline to proactively address privacy and security vulnerabilities.
- **Regulatory Compliance:** MTD facilitates ongoing compliance and configuration management, ensuring all devices adhere to established standards and control objectives that are aligned with regulatory requirements.

Additionally, implementing Zimperium's MTD offers a significant return on investment, potentially saving up to $17.5 million over three years by preventing data breaches. Phishing and network attacks are primary methods attackers use to gain unauthorized access or steal credentials. By preventing data loss from malicious attacks on mobile devices, the airline can save $15 million. This prevention helps avoid larger breaches that could disrupt operations, incur compliance and regulatory costs, and result in the loss of intellectual property and sensitive data.

Benefit by Threat Category: 3 Year



$17.5M	$1.8M	13 Mos.
Total Benefits	3 Month Cost of Delay	Payback Period

Discover how Zimperium MTD can safeguard your airline's mobile-first operations. Contact us today to learn more and schedule a demo.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244