Zimperium Protects 275,000 Mobile Devices for U.S. Government Agency

This case study highlights how Zimperium helped optimize mobile security across a complex and highly sensitive federal environment with unique requirements. Due to the classified nature of its work, this U.S. federal agency will be referred to as "The Agency" in this document.

ZIMPERIUM®

Client

U.S. Federal Government Agency

Deployment Size

275,000 Mobile Devices

Challenges

A government agency that handles classified national security data requires a comprehensive solution for Mobile Threat Defense beyond what MDM can provide.
With air-gapped systems and siloed data, The Agency needed a team of experts who could dig deep, customize their product and implementation strategy, and design a FedRAMP-compliant solution that would implement seamlessly, provide real-time analysis, and not compromise national security.

Result

In four months, Zimperium implemented a secure system that works seamlessly with the government agency's current MDM.

Today, Zimperium's Customer Success Manager meets weekly with The Agency's cybersecurity staff to provide ongoing support, introduce new features, and help them get the most out of the MTD platform while keeping their evolving priorities in mind.

A major U.S. government agency selected Zimperium to safeguard 275,000 of its mobile devices that are vital to daily operations and national security.

Facing critical challenges–such as intentional air gaps between systems handling classified data–The Agency required a mobile security solution that could integrate seamlessly without the need for internet connectivity. Zimperium met these requirements and successfully transitioned The Agency from a pilot program to a large-scale deployment in only four months.

As part of the ongoing relationship, Zimperium's customer success team meets weekly with the client's cybersecurity team to navigate the evolving security landscape, tailor new solutions, and maximize the effectiveness of their Mobile Threat Detection (MTD).

Challenge: MDM is Not Enough

In 2018, The Agency's security team relied solely on policy and security features within their Mobile Device Management (MDM) system. While this was common practice at the time, emerging mobile threats exposed security needs that MDM can not address.

These needs included the ability to detect and mitigate advanced mobile threats in real time, as well as insight into mobile applications installed on agency devices. The Agency recognized that malicious or vulnerable applications posed a serious risk to national security, thus requiring a solution that could proactively vet applications before they were allowed into the mobile environment.

> **“Protecting national security data across a vast and complex mobile environment demands more than just technology—it requires deep collaboration, precision, and an unwavering commitment to mission success. At Zimperium, we’re proud to deliver mobile security that meets the highest standards and supports the critical work of this agency,”** said Shridhar Mittal, CEO of Zimperium.

After rigorously testing several solutions, The Agency selected Zimperium based on the company’s ability to deliver comprehensive mobile threat detection through a hybrid (on-premise and cloud-based) deployment. The decision was further reinforced by Zimperium’s on-device detection capabilities which operate independently of an internet connection, ensuring continuous protection in an air-gapped environment.

Solution: Protect Against Mobile Threats and Maintain National Security Protocols

The Agency valued the competence and expertise of Zimperium’s dedicated customer success team; whose hands-on approach ensured a successful implementation and ongoing support.

Prior to its partnership with Zimperium, The Agency developed multiple architecture scenarios to address their security needs, including an air-gapped separation between systems to protect sensitive data. Based on that existing architecture, The Agency initially required an on-premise solution.

As planning progressed, The Agency realized the reliability and security of Zimperium’s mobile security solutions would meet their needs and opted for the company’s cloud-based FedRAMP-authorized solution. A mobile security architecture was designed that would better serve The Agency’s current and future needs.

Implementation: A Strategic 3-Phase Approach

1 First 30 Days: The Plan

- Gather requirements via 1:1 sessions between Zimperium and The Agency
- Configure MTD to integrate with The Agency's MDM
- Develop a phased rollout and strategic communications plan

2 Month 2: Pilot

- Deploy Zimperium's solution in a controlled segment of The Agency
- Collect real-time feedback and refined policies based on findings
- Adjust configurations to ensure a seamless user experience

3 Month 4: Refine and Rollout

- Execute a phased rollout strategy to systematically expand deployment
- Monitor effectiveness and adapt security policies as needed
- Create a comprehensive knowledge base and localized messaging for agency personnel

The flexibility of Zimperium's solution allowed the team to support the agency's unique requirements, such as:

- **Compatibility with The Agency's MDM** to allow for seamless deployment and ongoing policy management.
- **CAC-based authentication** to align with federal security standards.
- **Ability to mask personally identifiable information (PII)** to maintain strict data privacy protocols.
- **Optimized sync processes** to enhance the efficiency of security updates without disrupting operations.
- **Identify and mitigate security risks** associated with third-party and internally developed mobile applications before they are installed on devices.

> **“The Zimperium platform gives us unparalleled visibility into mobile threats without disrupting operations. Their team works as an extension of our own, providing expert guidance and rapid response whenever needed,”** said one agency representative.

Results: A Secure, Scalable Mobile Security Solution

Zimperium continues to meet weekly with The Agency to identify opportunities for improvement and implement new features. Recently, The Agency integrated zero-touch activation, which allows for updated configurations to be pushed directly to devices via The Agency’s MDM without any action needed from the end users.

Additionally, Zimperium’s mobile app vetting solution has significantly strengthened The Agency’s security posture by preventing vulnerable or malicious applications from compromising classified data. With automated risk assessments and detailed app behavior analysis, The Agency now confidently allows only safe applications within its network.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244