ZIMPERIUM

Enhancing Mobile Device Security for the Department of Defense

Mobile devices often store sensitive and classified data, making their protection a critical priority. Additionally, with requirements such as the Cybersecurity Maturity Model Certification (CMMC), the Defense Industrial Base (DIB) partners are required to meet stringent cybersecurity standards, including those for mobile devices. This program is designed to enforce the protection of sensitive, unclassified information that is shared by the Department with its contractors and subcontractors.

The Challenge: Protecting Sensitive Data in a Mobile World

An agency within the Department of Defense sought an effective solution to secure their mobile devices, which had been approved for usage. The agency had multiple unique requirements, like an on-premises console, including the need for comprehensive protection against all four mobile threat vectors: device compromises, network attacks, malicious apps, and phishing. Additionally, due to their responsibility for securing a high volume of devices, they required an on-premises centralized management platform capable of giving them detailed analytics and robust defense against both known threats and zero-day attacks.

What Data's At Risk?

Individuals who use their devices could jeopardize the following information:

- **Sensitive and Classified Information:** The agency deals with sensitive and classified data related to national defense and security. This could include military plans, intelligence reports, communications, and other confidential information critical to the nation's defense. If mobile devices were compromised, this sensitive data could be at risk of unauthorized access or theft.
- **Access to Government Systems:** Mobile devices in the defense sector may have access to government networks and systems. Unauthorized access to these systems could have significant consequences, potentially allowing malicious actors to manipulate or steal sensitive information.
- **Operational Data:** Military operations and mission-critical activities often rely on mobile devices for communication, coordination, and access to real-time operational data. Compromised mobile devices could disrupt these operations and compromise mission objectives.
- **Security Policies:** Information about security policies and protocols within the public sector should be safeguarded to ensure compliance with regulatory standards and maintain a strong security posture.
- **Communication Logs:** Mobile devices often contain call and message logs. These logs can contain sensitive customer or employee interactions and must be protected.
- **Mobile Device Information:** Information about the mobile devices themselves, including their unique eSIM, operating systems, and security configurations, is essential to protect and maintain the security and privacy of providers.

Given the nature of the Department of Defense agency's work, the protection of all these types of data is critical to national security and the overall effectiveness of Zero Trust operations. Therefore, implementing robust mobile device security measures, as outlined in the use case, was essential to mitigate the risks associated with potential data breaches or compromises.

Our Solution: Zimperium MTD

Zimperium's mobile security solution emerged as the ideal choice for addressing the agency's security challenges and on-premises requirements. Zimperium's on-device detection capabilities provided real-time protection against all four mobile threat vectors, ensuring the agency's mobile devices remained resilient to a wide range of threats. The centralized management platform offered by Zimperium simplified the task of securing a large number of devices efficiently. Furthermore, Zimperium's solution provided continuous updates to protect against known threats and zero-day attacks, enhancing the agency's overall mobile device security posture.

MTD™