

Zimperium MobileThreat Defense (MTD)

Solution Overview for Government

A World of Rapidly Evolving, Mobile Threats.

Device, network, application, and phishing threats intensify daily, with concerted, targeted attacks on the rise. Threats to organizations, confidential corporate data, and personally identifiable employee information are now ubiquitous. Further, within the public and private sectors, the rise of bring-your-own-device (BYOD) exacerbates these risks, specifically targeting organizations and their employees.

Malware signature and definition-based protection help to prevent the known, but what about the unknown? What about protection in a disconnected situation when unable to validate a mobile threat without a connection to a cloud-based server? Traditional methods of mobile threat detection miss zero-day attacks, failing to provide protection when severed from cloud resources.

According to Zimperium's 2023 Global Mobile Threat Report, between 2021 and 2022, the total number of malware samples detected by Zimperium increased by 51%; traditional detection methods are challenged at best and subject to complete compromise.

80% of phishing sites target mobile devices.



Users are 6-10 more likely to fall for SMS phishing attacks.

Fortunately, there's a way to stop them. Zimperium.

Zimperium's Dynamic On-device Detection is unique in the industry, enabling the patented Dynamic Detection Engine to succeed where other mobile threat defense technologies fail.

Underpinned and driven by some of the world's most advanced and sophisticated research, Zimperium delivers the industry's only fully on-device protection solution. Zimperium doesn't require an internet connection to provide protection or rely on updates that address only the known. In a recent independent test from AV-Test, Zimperium's mobile threat defense solution delivered top-tier results—better than 99% accuracy in about all scenarios, including offline detections.

90,000

Ransomware attacks were detected and protected by Zimperium in 2022.

With the ability to protect an entire mobile device or a single mobile application, Zimperium's Dynamic Detection Engine allows for true flexibility, protecting users, their data, and the enterprise from evolving mobile threats.

Protection for diverse environments and needs

A Component of a Larger Security Solution

Zimperium was the first FedRAMP-authorized solution providing security teams with visibility into the threats and vulnerabilities across all mobile devices in the organization to enable assessment of risk, identification of security gaps and rapid enactment of remediation. Zimperium's experience with the private sector, federal, state, and local governments, make Zimperium an ideal partner and component of an end-to-end mobile solution.

Full Device Protection

Zimperium Mobile Threat Defense (MTD) - formerly zIPS - delivers threat and attack protection for the entire device, whether a corporate or employee-owned device. MTD is the world's first mobile-first security solution that protects iOS, Android, and ChromeOS devices against four major attack vectors: device, network, application, and phishing. Zimperium MTD provides comprehensive detection, analysis, and remediation, enabling private sectors and government agencies to activate a Mobile-First Security Strategy. Zimperium was the first FedRAMP-authorized solution providing security teams with visibility into the threats and vulnerabilities across all mobile devices in the organization to enable assessment of risk, identification of security gaps and rapid enactment of remediation. Zimperium's experience with the private sector, federal, state, and local governments, make Zimperium an ideal partner and component of an end-to-end mobile solution.

Protection of Corporate Mobile Apps

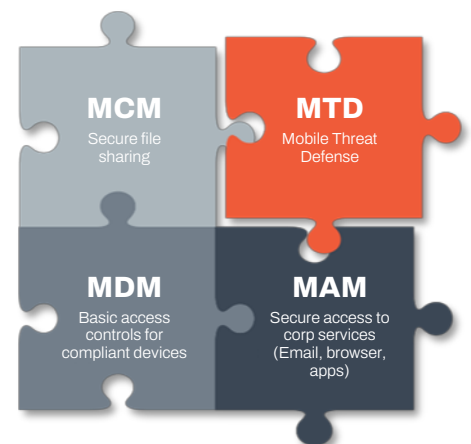
Zimperium's zDefend SDK ensures that mobile applications remain safe from attacks by providing immediate device risk assessments and threat alerts, minimizing exposure of sensitive data, and preventing customers' and partners' data from being jeopardized by malicious and fraudulent activity. Zimperium Mobile Threat Defense (MTD) - formerly zIPS - delivers threat and attack protection for the entire device, whether a corporate or employee-owned device. MTD is the world's first mobile-first security solution that protects iOS, Android, and ChromeOS devices against four major attack vectors: device, network, application, and phishing. Zimperium MTD provides comprehensive detection, analysis, and remediation, enabling private sectors and government agencies to activate a Mobile-First Security Strategy. Zimperium was the first FedRAMP-authorized solution providing security teams with visibility into the threats and vulnerabilities across all mobile devices in the organization to enable assessment of risk, identification of security gaps and rapid enactment of remediation. Zimperium's experience with the private sector, federal, state, and local governments, make Zimperium an ideal partner and component of an end-to-end mobile solution.

Flexible deployments that adapt to your needs

Enterprise Mobility Management (EMM) and Mobile Device Management Platforms (MDM) are important components of mobile device security. However they fail to provide comprehensive protection for the entire spectrum of mobile threats. These solutions have vulnerability gaps, resulting in exploited mobile devices due to a lack of on-device remediation. Several endpoint providers have partnered with Zimperium for being the best technology for mobile detection and remediation.

Zimperium provides the missing piece of the mobile protection puzzle and will work with your vendor of choice.

Zimperium's technology is unique as it can be installed on-premises or in the cloud. It's highly flexible, configurable, and cloud-agnostic — allowing us to conform to your environment. Not the other way around.



For more information or to request a demo, visit www.zimperium.com.