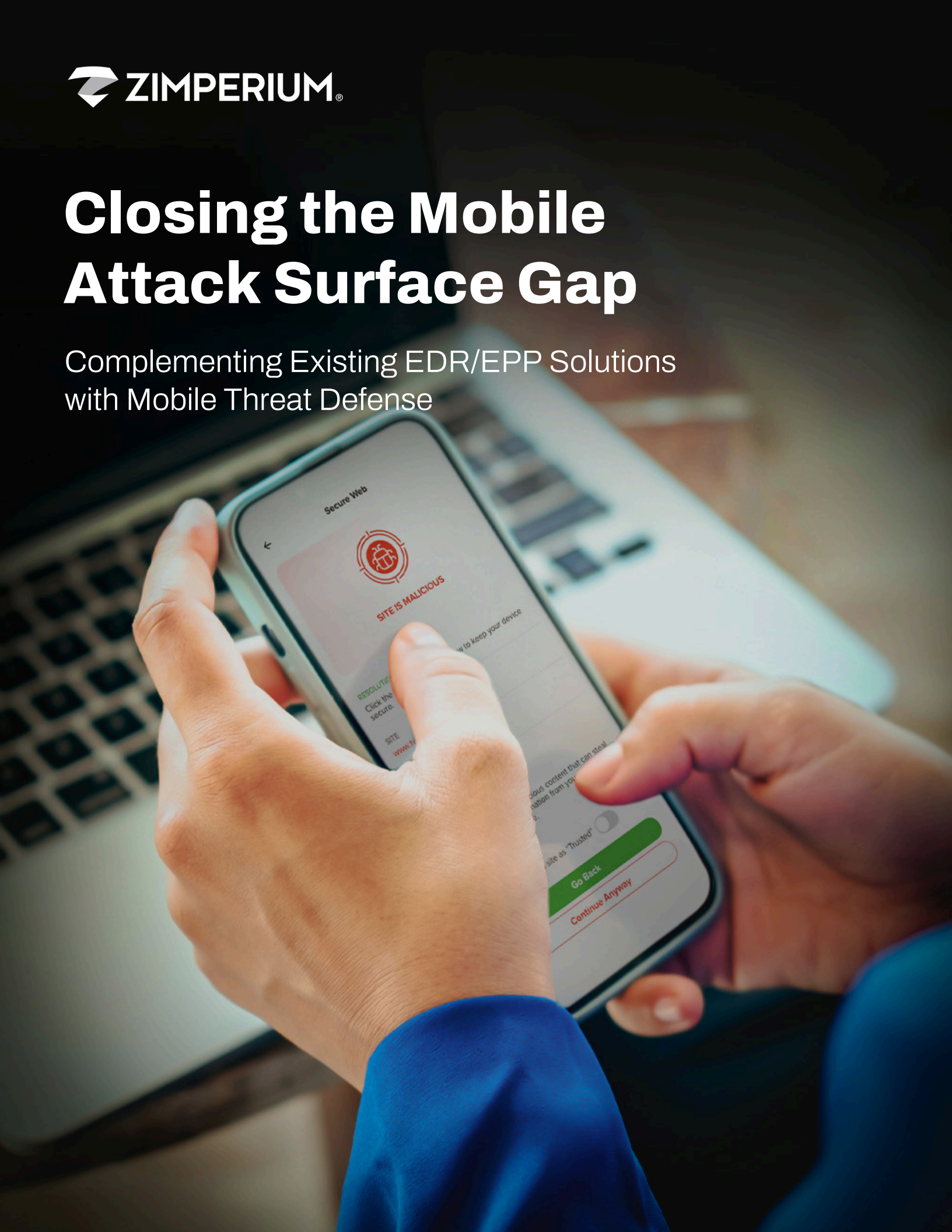
ZIMPERIUM®

Closing the Mobile Attack Surface Gap

Complementing Existing EDR/EPP Solutions with Mobile Threat Defense



Modern Endpoint Detection and Response (EDR) and Endpoint Protection Platforms (EPP) have become a standard play among enterprises globally, replacing outdated endpoint security systems with advanced visibility, detection, and response capabilities supporting the modern workforce. However, these modern security solutions alone cannot provide sufficient coverage for a significant number of mobile endpoints connected to corporate systems, leaving critical gaps in the enterprise attack surface. To complicate security concerns, **enterprises report that over 66% of smartphones in the enterprise are employee-owned, limiting security team's access and control over the device.**[1]

The Gap in Mobile Endpoint Visibility

In today's modern day workforce, enterprises and employees rely on mobile endpoints for daily productivity and work, making it even more critical that security teams are able to provide the same advanced level of security and protections to these devices.

"Threats to mobile applications and devices pose security risks to global enterprises. Security and risk management technical professionals responsible for IT security, especially inorganizations with high security or compliance needs, must have an in-depth strategy to defend mobile devices."

- Patrick Hevesi, Gartner Analyst

"Advance and Improve Your Mobile Security Strategy," August 9 2022

In 2021, 42% of organizations reported that mobile devices and web applications led to a security incident.[2] Solutions like mobile device management (MDM) lack the functionality necessary to detect a majority of threats, focusing more on device management and local policies. The rise of bring your own device (BYOD) options also hinders MDM due to privacy and liability concerns due to the ownership of the mobile devices themselves creating a gap in security measures.

The modern employee is conducting work beyond their laptop, accessing data on the go from tablets and mobile phones far outside the reach of security teams. More often than not, mobile endpoints are accessing critical data without any enterprise-grade security or threat visibility.

How Mobile Endpoint Security Differs from Traditional Endpoint Security

Traditional endpoint security platforms lack the comprehensive mobile access necessary to monitor and assess mobile OS security postures. Users are the admins; they decide when to upgrade their OS, what networks to connect to and what apps to install. Beyond the user risk, mobile apps operate in containers and sandboxes but not fully protected from manipulation and exploitation by mobile malware and attacks. But mobile operating systems are locked down, rendering traditional EDR solutions ineffective because they rely on kernel access for detection. And ultimately, consumer-centric mobile security tools lack the enterprise-critical features necessary for monitoring, response, and remediation without impacting user privacy.

How Malicious Actors Are Attacking Mobile Endpoints

Device
Attackers' primary goal on mobile is to fully compromise a device in order to be persistent and weaponize it for "land and expand" lateral movements.

Network
Attackers use rogue access points (RAPs) and man-in-the-middle (MITMs) to steal data and also to deliver targeted exploits to compromise the device.

Phishing
Mobile phishing,especially SMISHING via text/messaging apps and personal email, is a highly-effective way to steal credentials and deliver targeted exploits.

Apps
Malicious apps can create fraud, steal information and also deliver device exploits.

Legacy solutions are unable to scale to the modern threats and risks to mobile threats. Enterprise connected mobile endpoints, whether they are corporate-managed or BYOD, require an advanced security approach: **mobile threat defense**. No matter the mobile threat, from unknown, "zero-day" attacks to compromised networks, malicious application, phishing, and more, the advanced on-device detection provided by mobile threat defense delivers the necessary security and threat telemetry to enterprise security teams. With the on-device protection, security practitioners are also capable of assessing privacy and security risks in legitimate mobile apps and detect known and unknown risks and attacks. With mobile threat defense, security teams are capable of closing the security gap in their growing attack surface and apply the same advanced security capabilites to mobile security as applied to traditional devices.

How Zimperium Can Help

Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - is an advanced, mobile threat defense solution capable of providing the critical technology to protect against the modern, mobile threats while also providing security teams the critical visibility into the mobile attack surface.

Zimperium MTD is the only mobile threat defense to provide the machine-learning powered, on-device threat detection and response capabilities to enterprises without impacting the privacy of personally owned devices.

How MTD Delivers Value to Your EDR/XDR Strategy

Zimperium MTD customers are able to integrate critical monitoring services directly from the Zimperium zConsole cloud management platform into their existing monitoring toolsets using either direct integrations, or standards based feeds such as API and SYSLog.

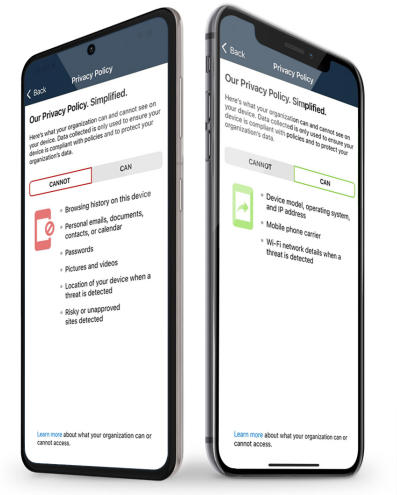
From security operations using SIEM and SOARS, to EDR toolsets capable of accepting Syslog or consuming external APIs, enterprise security teams are able to receive threat alerts and take actions from one console. Once alerts through the security team's security console of choice, threats and attacks requiring more advanced responses can be quickly addressed directly through Zimperium zConsole, both on-demand, and through automated policy.

Zimperium customers are able to integrate the following actions into existing security management toolsets:

- Users and Roles: Retrieves a list or details about users and lists roles, and also updates a role for a user.
- Devices: Retrieves list or details about devices.
- Events: Retrieves a list or details about threats.
- Apps: Retrieves information about device applications, such as classifications and reports.
- Risks: Retrieves information on risky apps and devices; such as devices and apps that require updates.
- Tenants and Users: Creates, reads, updates, and removes a tenant.
- Privacy Policies: Retrieves various information about privacy policies for a tenant.

The Mobile Attack Surface, Reduced with MTD

The mobile attack surface represents one of the largest unaddressed and unsecured attack surfaces in an enterprise, and with each new employee, BYO device, and new application, the complication surrounding the risks only increase. The opportunity each mobile device represents to threat actors through phishing, network attacks, application vulnerabilities, or device compromise puts enterprises and their critical systems at risk. Detection, prevention, and threat telemetry is necessary from each of these mobile devices for security teams to stay ahead of the modern day threat.



Whether integrating into an existing security operations center or maintained individually, Zimperium's advanced endpoint protect delivers the critical information needed to detect, respond, and mitigate advanced mobile threats. Zimperium MTD delivers the coverage in real time and response tools necessary to protect their complete mobile attack surface, from BYOD to corporate owned assets. And as a crucial part of any incident response, security teams will be confident in the forensic data provided from the mobile endpoints, reducing the mean time to recovery.

To learn more about Zimperium's MTD Solution, contact us today.

Sources

1 https://www.zimperium.com/global-mobile-threat-report/
2 https://www.zimperium.com/global-mobile-threat-report/