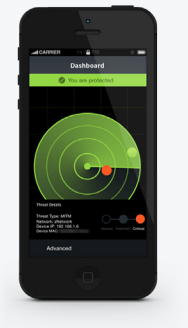
ZIMPERIUM

The Leader in Advanced Mobile Threat Defense

The explosion of mobile devices has changed the way people live and work. Existing network security solutions lack the visibility required to be able to protect mobile devices once they leave the corporate network. Advanced attacks are on the rise and signature based technology can't protect against unknown threats. With more business being conducted on the go, outside of the office, on unsecured public WiFi networks than ever before, the risk of a targeted cyberattack is significantly increased. One attack can result in a security breach, compromising an organization's data, assets and brand. Today's organizations need protection against advanced attacks without impacting the employee's experience, privacy and productivity on a mobile device.

Securing Organizations in an Increasingly Mobile World

Zimperium Mobile Threat Defense Suite uses patented behavioral analytics that sit on the device to detect network and host-based threats in real-time. Zimperium Mobile Threat Defense features:



IPS

The world's first mobile intrusion prevention system (Mobile IPS) app that defends mobile devices against both network and host cyberattacks wherever they go.

Console

A mobile threat management platform to monitor security incidents on zIPS-protected mobile devices with unprecedented mobile forensic detail.

ANTI

A mobile penetration testing toolkit that lets security managers assess the risk level of a network with the push of a button, and even simulates an advanced attacker to identify the techniques they can use to compromise the corporate network.

Leading Threat Detection

Secure enterprises from breaches in BYOD environments with the only advanced threat detection developed specifically for mobile devices. Zimperium protects the whole device from multiple attack vectors including:

- Spearphishing attacks (e.g., malicious URLs, PDF files)
- Malicious apps (e.g., "time bombs", self-modifying apps)
- Network traffic redirection attacks (e.g., "man-in-the-middle")
- SSL stripping techniques
- Rogue WiFi access point
- Rogue basestation/femtocell
- Reconnaissance scans

Benefits

- Prevent your mobile devices from being compromised by network and host based attacks
- Prevent a compromised mobile device from gaining access to your network
- Provide actionable reporting about every incident on your mobile devices including who, where and how attacks occurred
- Enforce risk-based policy management for all mobile devices in your organization remotely from a web-based, easy to use console
- Enable productivity while preserving the security of your corporate data
- Offers pervasive platform coverage (iOS, Android, etc.) to support your BYOD program
- Works seamlessly with your enterprise environment, integrating with leading MDM and SIEM solutions

ZIMPERIUM

Z9 Threat Detection Engine

The security experts at Zimperium developed z9, a revolutionary cyberattack detection engine that uses statistical models to dynamically detect advanced host and network-based attacks on mobile devices. Unlike other threat detection systems, the z9 engine monitors the whole device for malicious behavior (not just scanning apps) without reliance on signatures. This approach allows Zimperium to find and protect against both known and unknown threats in real-time, regardless of how they are delivered to the device.

The behavioral detection engine sits on the device, within the zIPS app, to detect threats and prevent a compromised device from gaining access to the corporate network. This unique approach protects the end user's privacy and prevents excessive battery drain that occurs when data is sent to the cloud. This global security intelligence fuels the Zimperium Mobile Threat Defense Suite to monitor, detect and prevent cyberattacks that evade traditional security technologies.

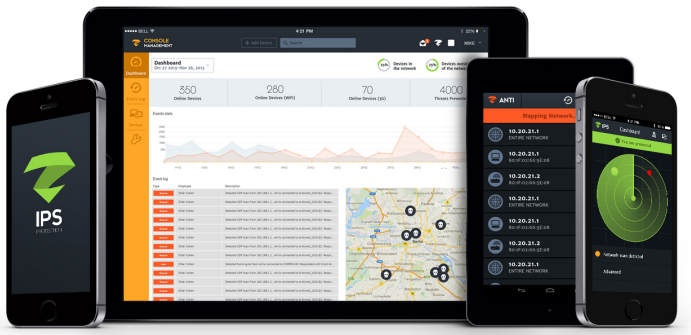
Unparalleled Mobile Security

Zimperium partners with leading mobile device management (MDM) vendors to deliver the most comprehensive protection against the next generation of advanced mobile threats. Together we integrate with your existing enterprise, enable ease of deployment and upgrades and deliver superior protection for your corporate network.

ZIMPERIUM MOBILE THREAT DEFENSE	MOBILE DEVICE MANAGEMENT
Detect against both known and unknown threats in real-time, regardless of how they are delivered to the device (via network, mobile app, email, etc.)	Manage all enrolled corporate-owned, employee-owned and shared devices
Protects against network-based mobile attacks such as man-in-the-middle attacks, SSL stripping, rogue AP, and reconnaissance scans	Secure access to corporate resources such as corporate email, corporate WiFi & VPN, Intranet and line of business apps
Protects against host-based mobile attacks such as spearphishing attacks, malicious apps, and malicious	Perform device commands (pin code enforcement, remote lock, find device, selective wipe)
Provide actionable reporting about every mobile security incident on the network	Prevent a compromised or non-compliant mobile device from gaining access to your network via risk-based policy management

Scalable Enterprise Architecture

Zimperium Mobile Threat Defense delivers advanced threat detection that seamlessly integrates with your existing security infrastructure. Built on scalable, multi-tenant architecture, Zimperium can handle hundreds of thousands of devices to keep up with the growing demands of any enterprise.



ZIMPERIUM

Zimperium is a privately owned mobile security company that defends organizations from advanced cyber-threats in an increasingly mobile workplace. Founded in 2010 by mobile security experts, Zimperium is the first company to use on-device, behavior-based analytics to detect and protect devices against network and host-based threats wherever business takes them.

Contact Us

560 Mission Street
San Francisco, CA **94105**
Main: **415**.992.8922 | Toll Free: **844**.601.6760
www.zimperium.com