ZIMPERIUM

Zimperium for Microsoft Intune

Enabling complete end-to-end mobile threat protection

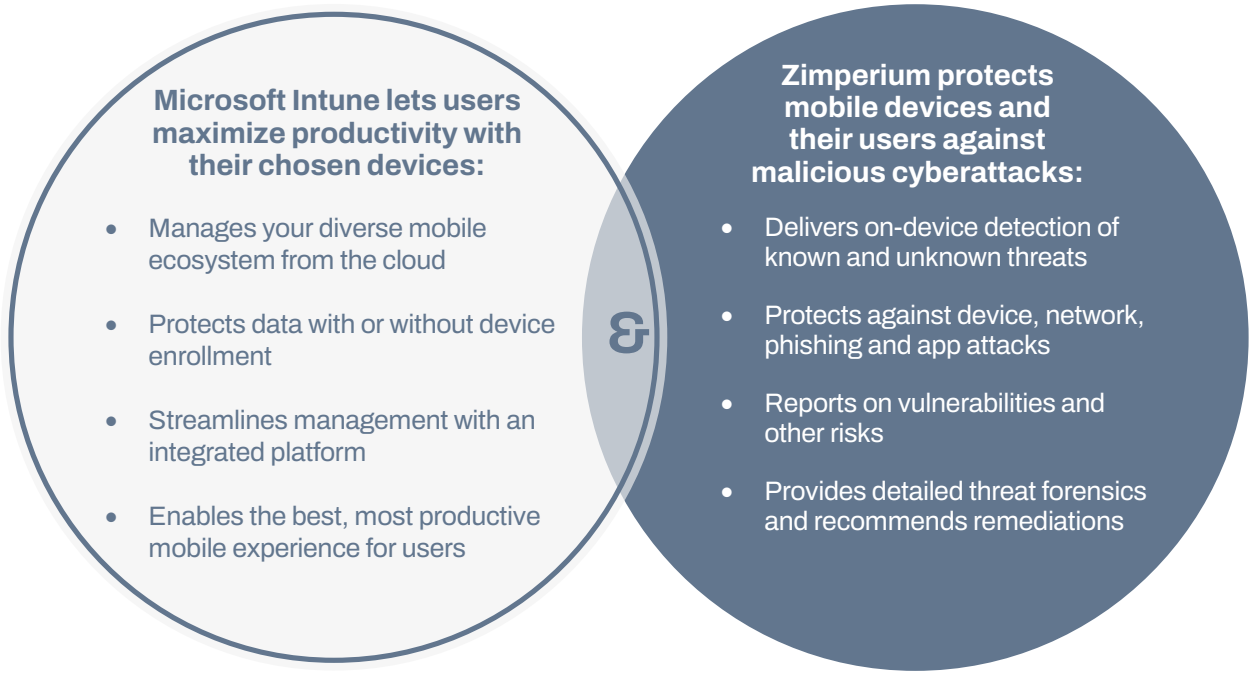
Complete Mobile Security

Microsoft Intune and Zimperium have partnered to provide a complete enterprise mobile security solution that delivers sophisticated threat protection for mobile devices against known and unknown threats to ensure corporate data and networks are not compromised by a mobile attack.

Together, Microsoft Intune and Zimperium enable enterprises to manage and secure mobile devices against the broadest array of device, network, phishing and malicious app attacks.

Zimperium continuously detects and analyzes risks and threats and provides Microsoft Intune with the visibility to enact risk-based policies to protect mobile devices.

The integrated solution provides IT Security Administrators with a way to safely enable corporate and BYO device initiatives. The combination enables a balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices and the enterprise against advanced threats.



Together enact risk-based policy to prevent a single mobile device from compromising the enterprise

Key Benefits

Built from the ground up for mobile devices, Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - uses machine learning technology optimized to run on the device without requiring an internet connection. Zimperium's non-intrusive approach to securing mobile devices provides protection around the clock without impacting the user experience or violating user privacy. Built on a scalable architecture and seamlessly integrated with Microsoft Intune, Zimperium supports the demands of any large enterprise.

Zimperium and Intune: How it Works

Deployment / Activation

› Intune deploys Zimperium to devices.

› Zimperium authenticates via AAD SSO.

› Device activates after authentication and reports to Intune.

Risk-Based Detection and Reporting

› Zimperium utilizes Microsoft EMS device threat levels to define risk posture threshold.

› Device threat level and threat data are reported to Intune.

› Intune designates compliant devices by using Zimperium threat data.

Remediation

› Intune enforces conditional access policies for noncompliant devices like removing access to Exchange or apps.

› Zimperium notifies Intune when the threat is mitigated in order to reinstate device and user access.

Available in Azure

Deploying mobile threat detection in Azure simplifies Enterprise Mobility + Security + Mobile Threat Defense. Zimperium is the first mobile threat defense solution that is deployed in Azure, making life simpler for IT admins when enabling Single Sign-on (SSO) and Azure Active Directory (AAD).

FEATURES & BENEFITS	MICROSOFT INTUNE	ZIMPERIUM
Access controls to corporate email, VPN, app delivery and removal	✓	
Secure corporate document sharing and web security	✓	
Ability to revoke access from non-complaint mobile devices	✓	
"Always on" protection on the device	✓	✓
Detect if device has proper security enabled (e.g. pin, encryption)	✓	✓
Jailbreak detection	✓	✓
Root / compromise protection	✓	✓
Network attack (e.g. MITM, rogue access points) detection		✓
OS compromise and exploitation detection		✓
Malicious app and profile detection		✓
Mobile phishing detection		✓
Provide detailed app risk and privacy analysis		✓
Reconnaissance scan detection		✓
Detailed mobile threat intelligence and forensics		✓

Contact us

Contact us today to enable mobile threat defense for Intune and to define your risk and protect your devices against device, network and application attacks!

For more information, visit
www.zimperium.com.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244