ZIMPERIUM®
MOBILE THREAT DEFENSE

Integrating Zimperium-detected Mobile Threats Into Defender ATP

THE NEED TO EXTEND MICROSOFT DEFENDER ATP TO MOBILE ENDPOINTS

Microsoft Defender Advanced Threat Protection (ATP) is a unified platform for preventative protection, post-breach detection, automated investigation and response. It has advanced endpoint detection and response (EDR) capabilities for systems utilizing traditional operating systems like Windows, Linux and MacOS. These capabilities provide attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach, and take response actions to remediate threats.

But there is a problem--a problem shared by almost every EDR solution. Today, the majority of endpoints are mobile devices that do not utilize traditional operating systems. 60% of endpoints accessing a typical organization today, run iOS and Android operating systems. These operating systems have unique characteristics - like hardened kernels and containerized apps - requiring a new security approach known as mobile threat defense (MTD).

As the global leader of enterprise MTD solutions, Zimperium is perfectly positioned to help Microsoft Defender ATP customers close the mobile endpoint security gap. This is why Zimperium and Microsoft have partnered to integrate Zimperium's detailed mobile threat alerts and forensics directly into the Microsoft Defender ATP dashboard.

ZIMPERIUM & MICROSOFT PROVIDE ADVANCED MOBILE SECURITY

The combination of Microsoft's management and security solutions and Zimperium's unique on-device mobile device security delivers unequaled protection for managed and unmanaged BYOD devices. This partnership has delivered numerous innovations for customers:

- Zimperium's MTD is integrated with Microsoft's Enterprise Mobility + Security (EMS) Solution;
- Zimperium and Microsoft jointly developed the BYOD unenrolled device solution that is the foundation for the Intune MAM - BYOD offering;
- Zimperium is the only MTD solution that is capable of running natively on Azure; and

- Advanced Integration with Microsoft Defender ATP for forensic level threat visibility and hunting.

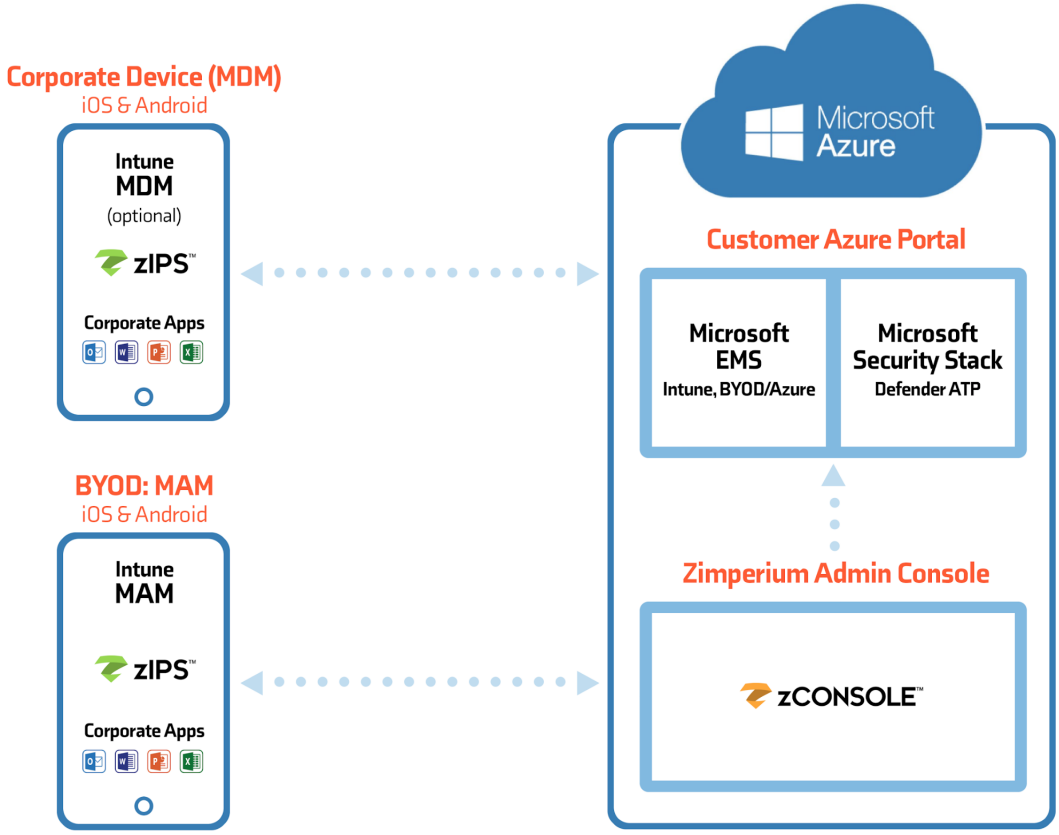

Figure 1: Key Integrations Between Zimperium & Microsoft

ZIMPERIUM: THE MOST COMPREHENSIVE MTD SOLUTION FOR MICROSOFT DEFENDER ATP CUSTOMERS

In order to have the best mobile threat data in Microsoft Defender ATP, organizations need the most enterprise-ready MTD solution: Zimperium zIPS. zIPS leverages our award-winning machine learning-based engine, z9, to detect more device compromises, network attacks, phishing attempts and malicious apps than any other MTD provider.

In addition to proven detection advantages, enterprises and government agencies around the world continue to select zIPS in record numbers because of its clear and significant operational benefits, including:

- Most deployment options, including Shared SaaS, Dedicated SaaS and On-Premises;
- Only MTD solution available on any cloud--including Microsoft Azure;
- Only solution that enables multiple UEMs in a single console; and
- Unmatched, comprehensive mobile threat forensics.

Zimperium's combination of unparalleled mobile threat detection and forensics is a large part of why it is the best choice for Microsoft Defender ATP customers looking to cover mobile endpoints.

The Zimperium MTD integration with Microsoft Defender ATP provides customers with a single pane of glass view within Microsoft Defender ATP for viewing, hunting and taking actions on mobile threats in the same console they currently use for managing threats from traditional endpoints like laptops and desktops running Windows, Mac and Linux.

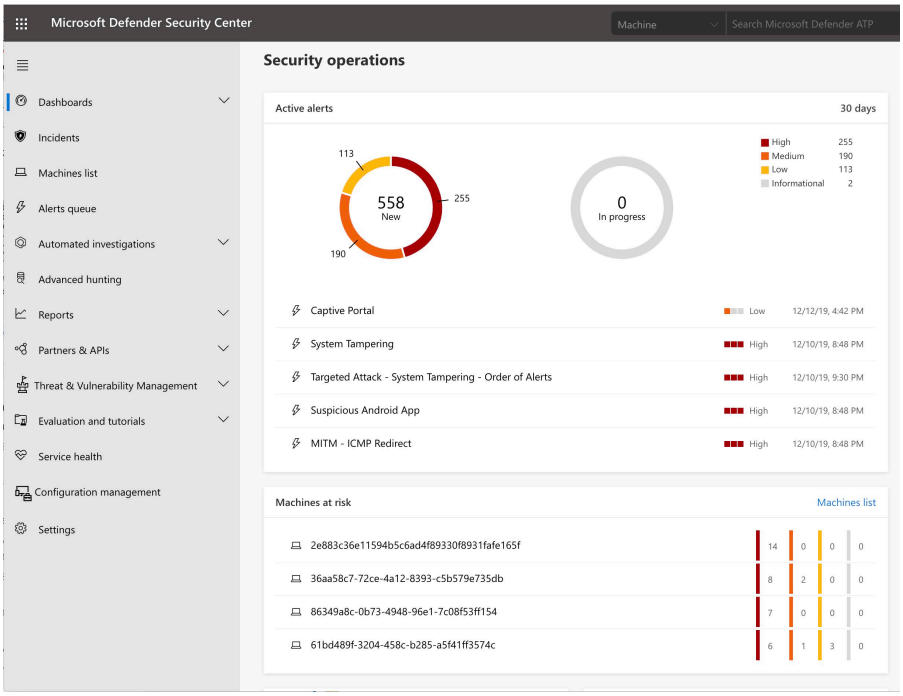

Figure 2: Microsoft Defender ATP with Zimperium Mobile Threats

Some of the specific benefits include:

- Comprehensive Endpoint Visibility - Administrators have a complete view of the security posture of all of the endpoints (laptop, desktop, tablet, phone) an employee leverages in their day-to-day work as they access corporate resources;

- Threat Hunting - Security administrators can now hunt for mobile threats by user or devices within Microsoft Defender ATP (e.g. show me list of threats affecting my CFO) and identify threat patterns that are indicators of a targeted attack on the organization;
- Advanced Threat Forensics - Zimperium provides Microsoft Defender ATP with threat forensic data not available from any other MTD solution; and
- Real-Time Device Status - The integrated solution automatically delivers threat status updates in Microsoft Defender ATP as threats are resolved on mobile devices.

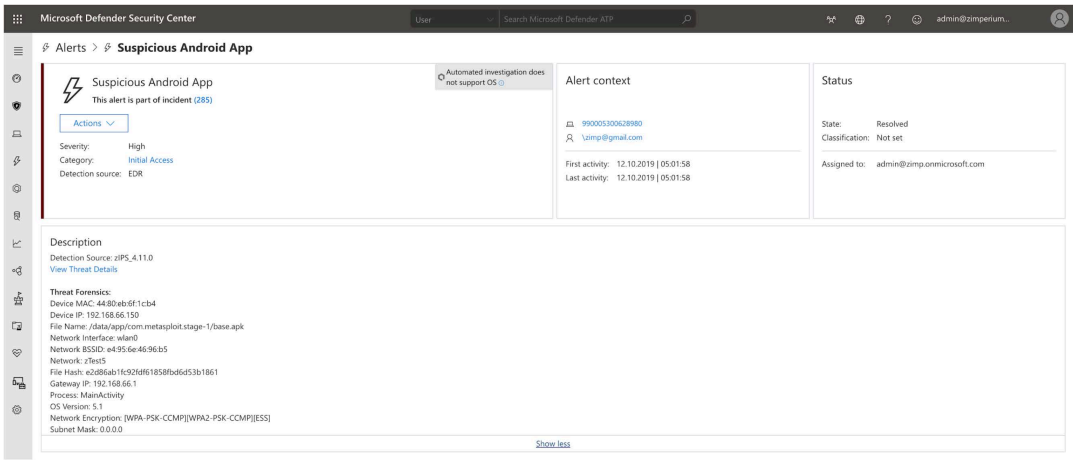

Figure 3: Example of Zimperium Mobile Threat Forensics

LEARN MORE

Zimperium zIPS is the only real-time, on-device, machine learning-based solution for mobile devices. Backed by zLabs research and millions of mobile endpoints, Zimperium provides complete protection for the 60% of endpoints that are currently exposed and introducing risk to organizations--mobile devices. Now Zimperium's unmatched threat detection alerts and forensic data are available directly inside Microsoft Defender ATP to assist in mobile EDR efforts.

To learn more about Zimperium & Microsoft Defender ATP or receive a demonstration, contact us today.