ZIMPERIUM®

Leveraging Zimperium and O365 for an Effective Zero Trust Strategy

Combining the Power of O365 with Advanced Mobile Threat Defense for Enhanced Zero Trust Architecture

Enterprise adoption of Microsoft Office 365 (O365) skyrocketed to over 258,000,000 users in 2020 and continues to climb into 2021, with 70% of Fortune 500 organizations purchasing licenses to the productivity toolset. Enabling cross-platform productivity and communication across traditional and mobile endpoints allowed companies to shift to distributed and remote workforces with minimal disruption to daily activity.

Organizations are investing heavily in meeting the requirements laid out by advanced security architectures and frameworks like Zero Trust and XDR that are designed to shore up endpoint and data access security. But despite the investments, mobile devices are often left unsecured even with the increased reliance on mobile data access and the complications of securing mobile bring your own (BYO) endpoints that are unmanaged within most mobile policies.

Ultimately, the rise of mobile adoption with corporate owned and BYOD access has exposed enterprises to potential attacks from increasingly sophisticated cyber threats as many of these new security layers still focus almost exclusively on traditional endpoints.

Adversaries need only find one unprotected device to wreak havoc on an enterprise's infrastructure. According to the MITRE ATT&CK Matrix, legacy-based mobile security layers, such as mobile device management (MDM) products, virtual private networks (VPNs), and multi-factor authentication (MFA), do not sufficiently address the increased risk from these endpoints.

While enterprises are accelerating their reliance on Zero Trust and MFA strategies in light of the new era of remote work, the Achilles heel is already exposed: mobile endpoints. Without implementing mobile threat defense (MTD) solutions to address this increased mobile attack surface, companies are leaving major gaps in their Zero Trust architectures.

But there is a way to strengthen these mobile endpoints, reduce risk, and increase security confidence. Zimperium and Microsoft together enable O365 administrators and users to reduce the operational risk while increasing identity access confidence across mobile devices for enterprise data.

Together, the solutions deliver the necessary device attestation for security administrators to properly enable Zero Trust frameworks with mobile devices, covering both BYO and corporate owned devices with ease and confidence.
As enterprises continue to advance BYOD and corporate-owned mobile endpoint adoption in order to support the distributed workforce, they must provide two core technological capabilities to secure O365 users and support Zero Trust initiatives:

- **Unified Endpoint Management (UEM):** The ability to manage and remediate risks and threats is foundational to securing endpoints. For O365 implementations, the logical solution is Microsoft Endpoint Manager.
- **Mobile Threat Defense (MTD):** UEMs are not capable of detecting modern, mobile threats on mobile endpoints. Device, network, phishing, and malware attack detection strategies must include real-time MTD solutions.

> **"It is essential to know that no single specific technology is associated with Zero Trust architecture. The Zero Trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default; a holistic approach to network security that incorporates a number of different principles and technologies."**
>
> **— Ludmila Morozova-Buss, Security Researcher**

Manage Mobile Endpoints with Microsoft Endpoint Manager

To establish a strong security perimeter around mobile endpoints, organizations of all sizes can use Microsoft Endpoint Manager as a solid management foundation. Microsoft Endpoint Manager provides a management framework for mobile endpoints and apps, including O365. Microsoft Endpoint Manager helps answer the following Zero Trust related endpoint considerations:

- Are the right people on the correct devices accessing the proper information?
- Is the data protected at all times?
- Are the applications used to access data protected with policies?
- Are all of the endpoints manageable from one location to ensure security and policy consistency across all platforms?

Secure Mobile Endpoints with Zimperium zIPS

Organizations of all sizes must apply the same security mindset they maintain with traditional endpoints to their mobile environment in order to minimize their attack surface, gather essential device data, and fully integrate mobile endpoints into Zero Trust frameworks. Zimperium zIPS delivers critical mobile device risk attestation, essential for these Zero Trust considerations:

- Does this mobile device meet the security requirements for data access?
- Are there any rogue, unapproved, or risky applications installed?
- Is the device operating with required security configurations?
- Is the device connected to a secure access point?

Zimperium zIPS: Truly Mobile Machine-Learning Based Protection

Zimperium zIPS provides continuous protection for mobile devices, providing the risk intelligence and forensic data necessary for security administrators to raise their mobile security confidence. As the mobile attack surface continues to expand and evolve, so does Zimperium's on-device, machine learning-powered detection. Built on the z9 machine learning platform, zIPS detects threats across the kill chain: device, network, phishing, and app attacks.

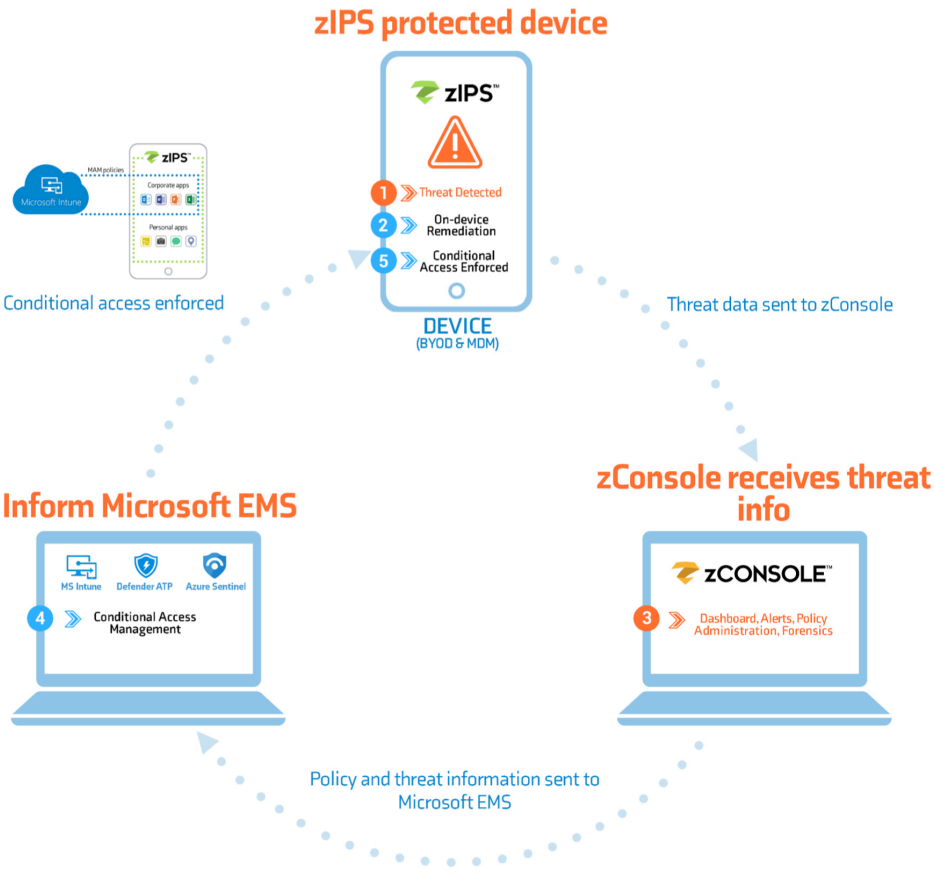
With zIPS, Incident Response teams finally have visibility into mobile threats and risks through integrations with leading UEM, SIEM, SOAR, and XDR systems. The unmatched forensics provided by zIPS prevent a single compromised device from turning into an outbreak. Collecting forensic data on the device, network connections, and malicious applications, security operations teams are enabled to secure this growing threat vector and minimize their total attack surface with confidence.

Zimperium zIPS and Microsoft: Complete Mobile Zero Touch Capabilities

UEMs, like Microsoft Endpoint Manager, were not designed to detect active attacks, and organizations still need to implement an MTD solution to complete protection. By implementing Zimperium zIPS into the mobile security stack, security teams can fill the legacy applications' security gaps while integrating seamlessly into existing workflows.

Zimperium zIPS' unique ability to detect on-device and in real-time is critical to protecting and supporting Zero Trust initiatives. If MTD protection is not always on, security gaps could prevail, a dependency on a cloud connection disables Zero Trust posture by default. Zimperium zIPS protects O365 users, and Zero Trust access simultaneously by ensuring mobile endpoints and the connected networks are not compromised.

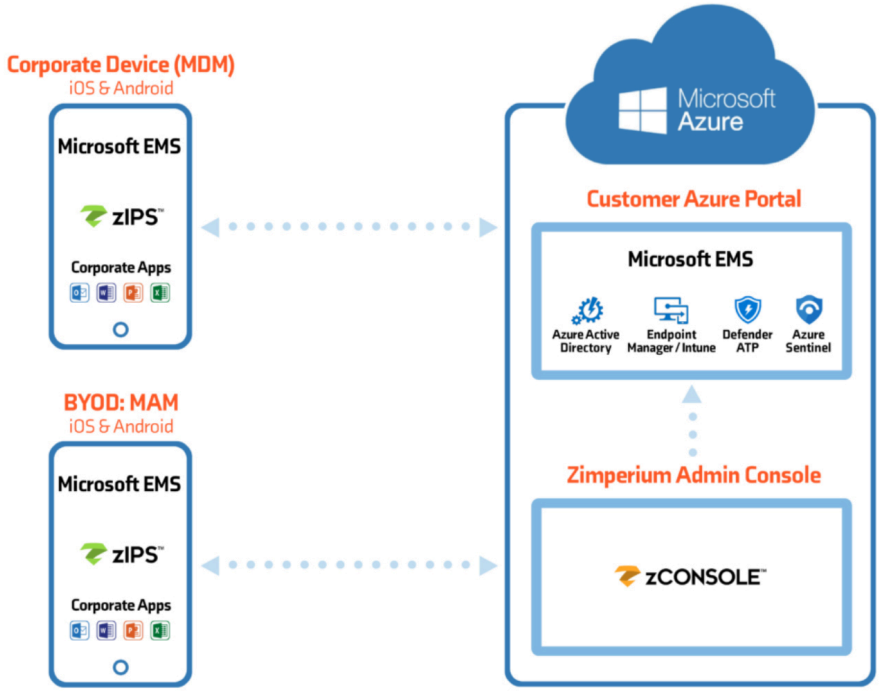
Zimperium zIPS protects O365 users, and Zero Trust access simultaneously by ensuring mobile endpoints and the connected networks are not compromised. zIPS not only provides advanced technology to the mobile endpoint space, it is also enterprise-ready. Along with its integration with Microsoft Sentinel, zIPS supports Microsoft environments as the only major MTD solution operating on Azure cloud. And Zimperium zIPS is the first mobile threat defense solution to receive FedRAMP authority to operate (ATO), supporting security compliance of any enterprise with federal contracts.



Microsoft and Zimperium, Fully Integrated

Zimperium paired with Microsoft enhances Zero Trust architectures by delivering comprehensive mobile risk posture data. Together, the solutions advance mobile security, bringing Zero Trust capabilities to mobile endpoints and enabling IT and security administrators to decrease their attack surface and increase their overall security confidence.

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. And with full support of managed and unmanaged devices, security administrators can remain confident that their data is being accessed by the right people from the correct device, every time.



Contact Us

Microsoft Office 365 users and Zero Trust initiatives can be enhanced and secured through advanced mobile threat defense. Zimperium zIPS provides scalable, machine-learning designed from the start for enterprises, securing mobile endpoints and the corporate data they access.

Want to learn more? Contact us and we would be happy to discuss it further or show you why we are so confident in making that statement.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, **contact us** today.

ZIMPERIUM®

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

Zimperium, Inc
4055 Valley View, Dallas, TX 75244