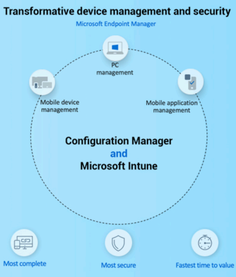
Microsoft ZIMPERIUM.

Top 5 Ways to Secure All Remote Workers

1 Manage corporate endpoints with Microsoft Endpoint Manager MDM

Begin with a solid foundation - Microsoft Endpoint Manager, which helps focus on outcomes:

- Are the right people on the right devices accessing the right information?
- Is the data protected at all times?
- Is the system automatically detecting and responding to any threats, whether internal or external?
- Are the applications you use to access data protected with policies?
- Are my corporate PC's, and mobile devices manageable from one location to ensure consistency in security and policy across all platforms?

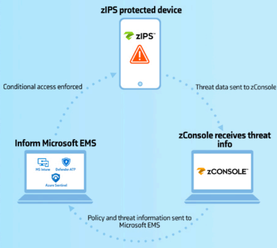


2 Secure your traditional corporate endpoints with Microsoft Endpoint Manager and Defender ATP

Defender ATP resides within the Microsoft Endpoint Manager console, where settings can be configured and deployed. From one location, you have a consistent view of your security configuration, and a place to deploy settings to both your cloud connected and on-premises PC's.

3 Secure your corporate mobile endpoints with Zimperium zIPS

Enterprises are realizing mobile devices can no longer be viewed as "the forgotten endpoint." While mobile platforms have some built-in protection such as app container isolation and vetted consumer app stores, these platforms remain vulnerable to attacks. As more employees use devices for work and to access sensitive data, the information from mobile threat defense (MTD) solutions can help protect devices and resources.



Our best of breed zIPS solution is the only real-time, on-device machine learning-based detection offering that protects known and unknown threats on Android and iOS devices. zIPS runs locally on any mobile device and detects device, network, phishing and malicious app cyberattacks without a connection to the cloud. When it detects suspicious activities on-device, it sends detailed threat forensics data that can be used for SOC analysis.

4 Enable BYO use cases with Microsoft Endpoint Manager MAM

App protection policies are built into all the core Microsoft Office apps, as well as the top 3rd party, and line of business (LOB) apps used for productivity. They are available on iOS and Android; and referred to as Windows Information Protection in the context of Windows. IT admins can configure settings in the areas of data protection, access requirements, and conditional launch.

Data protection settings govern behaviors like data transfer between managed and unmanaged contexts; access requirements specify PIN or corp credential requirements to get into the corporate context of the app; and conditional launch is a set of 'conditions' that a device or app must meet in order to allow the end user to get into their corporate data.

Intune's app protection policies can be used with or without device enrollment into an MDM provider. One scenario they enable is protection of corp data for organizations with BYOD programs.

5 Secure BYO endpoints with Zimperium zIPS + Endpoint Manager MAM

- MTD on enrolled devices is now available. BYOD users can now be blocked from accessing corporate content on their Android and iOS devices if an integrated Intune MTD solution detects their device is risky.
- This is a unique offering from other UEMs. Uniqueness comes from the integrated Office experience.
- No longer need a require enrollment to take advantage of MTD.
- This is not a conditional access (CA) feature. This is a pure App Protection feature.

Learn More

Visit Zimperium's Website
View Zimperium on Microsoft's Azure Marketplace
Contact Zimperium