{e} mazzanti®
technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Endpoint Management: A Gamechanger for Today's Complex Digital Landscape

Every cell phone, laptop, and point of sale device connected to the network creates a potential doorway for hackers. And yet business leaders who would never leave a side door unlocked at night often leave these electronic doorways wide open. A critical component of cyber security, endpoint management protects and manages connected devices.

Endpoint management involves the tools and policies to protect and support each device that connects to the network. This includes applying software updates, managing remote access, enforcing password policies, and monitoring devices for possible threats. It also includes the ability to remotely shut down a compromised device.

The benefits of endpoint management extend beyond cyber security. For instance, it increases productivity by ensuring that devices stay well-maintained and that users have quick access to the services they need. Additionally, the right endpoint management system will allow employees to use BYOD devices without diminishing security or productivity.

Complex Environment Presents Challenges

Even a small business typically includes hundreds of connected devices using a variety of operating systems and platforms. Employees work from anywhere, often starting a task on one device and switching to another device halfway through. This makes it difficult to track device location and status.

At the same time, ensuring that each device has the right applications and security settings can prove complicated. And keeping track of patch management to make certain that each device and application gets security updates requires careful coordination. IoT devices such as cameras and printers add another layer of complexity.

Best Practices for Securing and Managing Devices

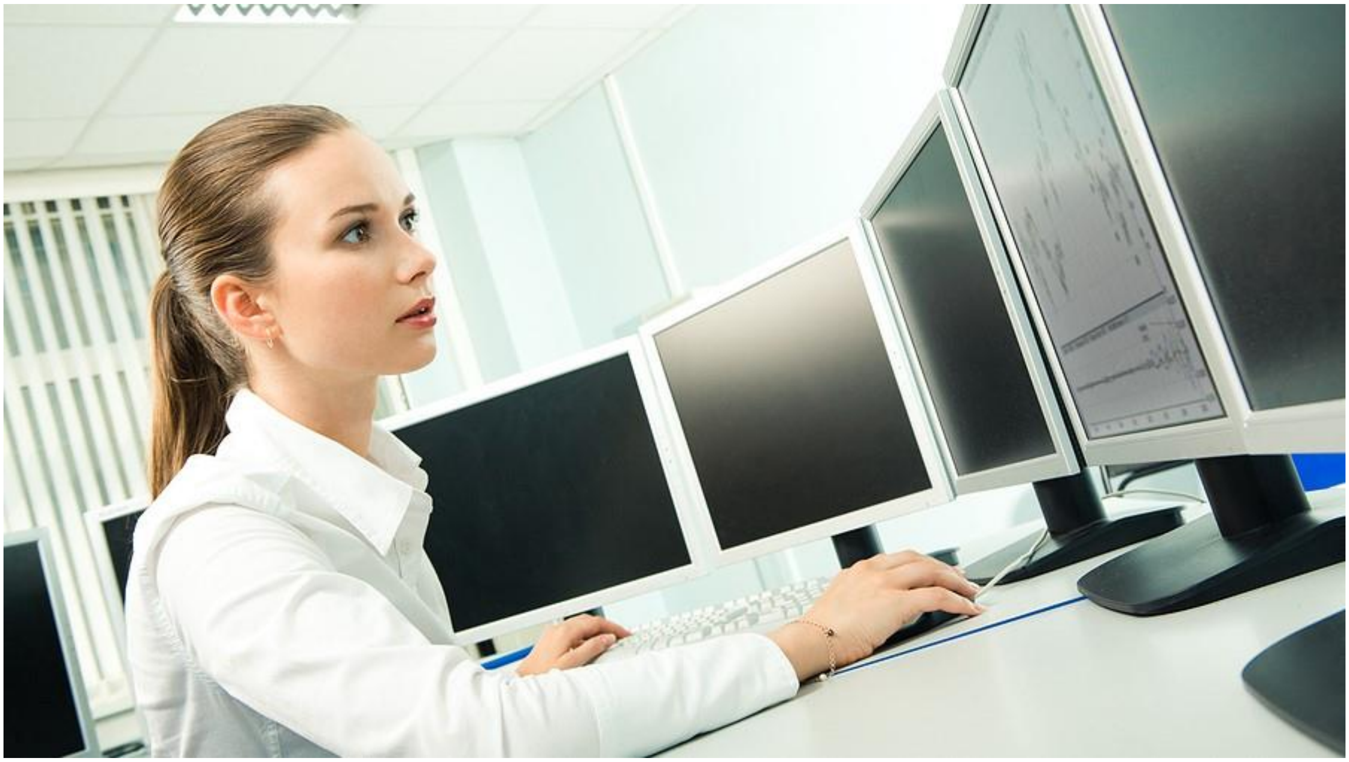
Endpoint management practices and systems need to evolve to keep up with the increasingly complex digital landscape. This begins with choosing the right endpoint management system. For instance, an effective system must have the ability to manage all endpoints from any operating system, including BYOD devices.

The endpoint management system should provide centralized visibility into all devices connecting to the company network and services. This includes tools to discover connected devices and audit them to determine device performance, health, and security status.

Best practices also include automating processes such as device deployment, patch management, and regular backups. Automating policies such as multi-factor authentication and conditional access proves essential, as well. And a good endpoint management system will include the ability to execute policies remotely across all endpoints.

To provide additional security, organizations should consider segmenting endpoints into groups based on factors such as risk level, function, or compliance requirements. With segmentation, IT can then apply different settings and rules to different device groups.

Finally, the endpoint management system should integrate with other IT services, from identity and access management to cloud management and threat intelligence.



Microsoft Tools for Endpoint Management

Microsoft provides several sophisticated security tools to help organizations manage their endpoints. Deeply integrated with Microsoft 365, the Intune family of products offers a unified endpoint management solution. A cloud-based system, it streamlines endpoint management across multiple operating systems, as well as both on-premises and cloud environments.

The Microsoft solution simplifies endpoint management by allowing administrators to view and manage all devices through a centralized console. It also strengthens security by applying advanced security features like conditional access, data loss prevention, and threat protection. And it enhances productivity by giving users seamless and secure access to needed services.

Major components of Microsoft endpoint management include:

- Intune Admin Center – This web-based, centralized admin center allows administrators to manage and monitor mobile devices, users, and applications. It also provides the capabilities to create and manage policies.
- Configuration Manager and co-management – The Configuration Manager provides on-premises endpoint management. Co-management connects on-premises management with the cloud-based features of Microsoft Intune. This includes features in the Intune Admin Center.
- Endpoint analytics – This service analyzes the health and performance of Windows devices.
- Intune Suite – This involves a set of advanced solutions including remote help, endpoint privilege management, advanced endpoint analytics, and the Microsoft Tunnel VPN for mobile app management of devices not enrolled in Intune. It also improves management of specialty devices.

- Microsoft Entra ID – Intune uses this cloud-native service to manage identities of and apply Intune policies to devices, users, and groups.
- Windows Autopilot – Using Windows Autopilot, administrators can preconfigure new devices and reconfigure existing devices.

Optimize Endpoint Management with Expert Help

The cyber security experts at eMazzanti work with organizations to choose and implement an endpoint management system tailored to business needs. And as a four-time Microsoft Partner of the Year, they offer the specific expertise necessary for those who deploy Microsoft endpoint management.