LIGHTSPIRE TECHNOLOGIES

https://www.lightspire.tech
info@lightspire.tech
(717) 216-0114

EndpointGuard Managed Service

Overview

Our managed endpoint services empower organizations to secure and streamline their endpoint management with expert oversight and proactive protection. By leveraging Microsoft Intune's cloud-based device management and Microsoft Defender's advanced threat detection, we ensure your endpoints are consistently compliant, patched, and resilient against modern cyber threats. Whether you're scaling operations or tightening security, this service delivers the support, control, visibility, and protection your organization needs—without the complexity or massive time investment.

Objectives

EndpointGuard is an ongoing managed service offering design to compliment your team by providing ongoing support and administration of Microsoft Intune and Defender for Endpoint solutions within your environment. Examples of in-scope items include:

Tenant Administration – Deployment, configuration and support of assignment filters, dynamic device groups, enrollment restrictions, ADMX templates, policy sets, and more.

Intune Connectors - Deployment, configuration and support of Intune supported connectors such as Windows 365, Defender for Endpoint, TeamViewer, ServiceNow, Certificate deployment, etc.

Windows Device Management - Deployment, configuration and support of common Windows device administration objects such as Win32 application deployments, device configuration profiles, windows update for business rings, Defender for Endpoint policies, BitLocker, Windows LAPS and more…

Third-Party Application Updates – automatic deployment of updates to an extensive list of supported third-party applications for Windows devices.

iOS/iPadOS/macOS/Android Device Management - Deployment, configuration and support of common Apple/Google device administration objects such as application deployment, device configuration profiles, compliance policies, update policies, File vault disk encryption and more…

Monitoring of the Defender for Endpoint Vulnerability Management - Weekly reports sent to stakeholders with recommended actions to reduce attack surface area.

Monthly Program Review – Endpoint management environment health review; Review of open support requests; Discussion on Customer goals & priorities

Outcomes

Application Deployment Support: Centralized deployment and configuration of business applications on user endpoints.

Device Configuration/Compliance Support: centralized, scalable, and policy-driven control over how devices are set up, secured, and used.

Ongoing, Managed Third-Party Application Updates: Limit attack surface area by ensuring applications on endpoints are patched regularly while monitoring compliance.

Windows Device Hardening Assistance: Using industry recommended tools and configurations to protect endpoints and organization data, regardless of platform or device type.

Endpoint Protection Support: NextGen antimalware combined with leading endpoint detection and response and threat & vulnerability management capabilities from Microsoft Defender for Endpoint