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

Windows Endpoint Hardening Services

Overview

Our Windows Endpoint Hardening Services provide a comprehensive security solution designed to protect Windows devices from modern cyber threats. Leveraging Microsoft Intune and other Microsoft 365 Defender tools, our consultants ensure that all endpoints are configured, monitored, and maintained according to industry best practices and compliance standards.

Objectives

Policy-Based Configuration Management

- **Microsoft Intune:** Centralized management of security baselines, device compliance policies, and configuration profiles.
- **Custom Security Baselines:** Tailored hardening templates based on Microsoft Windows standards.
- **Automated Deployment:** Seamless rollout of security configurations across all Windows endpoints.

Threat Protection & Monitoring

- **Microsoft Defender for Endpoint:** Real-time threat detection, response, and remediation.
- **Attack Surface Reduction (ASR):** Enforce rules to block executable content, scripts, and untrusted processes.
- **Endpoint Detection and Response (EDR):** Advanced analytics and behavioral monitoring to detect sophisticated attacks.

Vulnerability Management

- **Microsoft Defender Vulnerability Management:** Continuous scanning for misconfigurations and missing patches.
- **Patch Management via Intune:** Schedule and enforce Windows Update for Business policies to ensure timely updates.

Access Control & Identity Protection

- **Windows Hello for Business**: A secure, password less sign-in solution that enables seamless access to Windows devices and single sign-on to corporate resources
- **BitLocker Encryption Enforcement:** Ensure all devices have full disk encryption enabled.
- **Credential Guard & Secure Boot:** Enable hardware-based isolation for sensitive processes and credentials.

We offer flexible ways to work with you, no matter where you are in your journey to secure and strengthen your Windows Endpoint environment.

Outcomes

Improved Endpoint Security Posture: Devices are protected against modern threats with hardened configurations and real-time monitoring.

Reduced Attack Surface
Implementation of least privilege, application control, and exploit protection reduces exposure.

Enhanced Visibility & Control
Centralized management and reporting through Microsoft 365 security tools.

Regulatory Compliance Support
Alignment with security frameworks helps meet internal and external compliance requirements.

Operational Efficiency
Automated policies and streamlined management reduce manual overhead and response time.