PRESIDIO®

SOLUTIONS BRIEF

Microsoft Defender for Endpoint Quickstart

THE CHALLENGE

Organizations today face increasingly sophisticated cyber threats across diverse hybrid and cloud environments. As remote work, endpoint proliferation, and advanced cyberattack tactics expand, maintaining robust endpoint security becomes more challenging. The adoption of AI tools and automated processes further increases the need to protect devices from threats like malware, ransomware, and zero-day exploits. Balancing productivity with security, ensuring consistent threat response, and eliminating blind spots demand a unified and scalable endpoint protection solution.

THE SOLUTION

Microsoft Defender for Endpoint provides a comprehensive endpoint security solution that helps organizations prevent, detect, investigate, and respond to threats in real time. With advanced threat analytics, automated response capabilities, and seamless integration with Microsoft 365, Defender for Endpoint offers deep visibility and control over your entire endpoint environment. Its Zero Trust approach ensures that endpoints remain secure while maintaining productivity. Defender for Endpoint's AI-powered threat protection helps mitigate risks, enforce security policies, and keep organizational assets safeguarded.

Presidio supports organizations in strategizing, implementing, and optimizing Microsoft Defender for Endpoint to achieve superior endpoint protection. We tailor our solutions to your business needs, ensuring smooth integration with your existing infrastructure and tools. By combining technical expertise with a focus on operational efficiency, we help you protect your endpoints, enhance threat response, and maintain trust.

MICROSOFT DEFENDER FOR ENDPOINT QUICKSTART

Review Endpoint Security Posture

Identify Endpoints

- Review current endpoint security platform on laptops, servers, and mobile devices and determine approach for migration to Microsoft Defender

Threat and Vulnerability Management

- Assess endpoint security configurations and vulnerabilities as it relates to Microsoft Defender deployment
- Prioritize mitigation actions to reduce security risks with Microsoft Defender

Threat Detection and Response

- Enable Microsoft Defender for Endpoint sensors on all devices.
- Review real-time alerts and threat analytics for potential risks.

Review Security Policies And Controls

Access Control

- Implement role-based access control (RBAC) for endpoint management.
- Define privileged access policies to limit exposure to critical systems.

Zero Trust Principles

- Apply conditional access policies for endpoints.
- Enforce multi-factor authentication (MFA) and endpoint compliance policies.

Security Tools Integration

- Integrate with Microsoft Sentinel for centralized monitoring.
- Enable automated threat response using Defender for Endpoint capabilities.

Microsoft Defender for Endpoint Quickstart

Review Threat Response and Automation

Automated Response

- Configure automated investigation and remediation (AIR).
- Set up attack surface reduction (ASR) rules for proactive threat defense.

Incident Management

- Review processes for incident detection, investigation, and resolution.
- Enable notifications and alerts forhigh-severity threats.

Integration with Security Operations

- Ensure seamless communication with your Security Operations Center (SOC).
- Integrate Defender for Endpoint with other Microsoft security tools for a unified response.

Review Deployment Requirements

Licensing Needs

- Confirm licensing for Microsoft Defender for Endpoint (Plan 1 or Plan 2).
- Validate integration with existing Microsoft 365 or Microsoft Entra subscriptions.

Compatibility Check

- Ensure endpoint devices meet the compatibility requirements.
- Verify integration with Windows, macOS, iOS, Android, and Linux environments.

Deployment Strategy

- Plan phased deployment for endpoints across the organization.
- Develop a communication plan for end-user awareness and training.

Delivery timelines generally range from 2 to 6 weeks.

KEY BENEFITS

- **Rapid & Secure Deployments –** Our Microsoft Defender for Endpoint QuickStart enables swift deployment, helping you protect endpoints with minimal disruption.
- **Enhanced Endpoint Security –** We ensure critical devices are secured with the latest threat protection technologies and aligned with best practices.
- **Automated Threat Response –** Leverage automated investigation and response to reduce dwell time and mitigate threats before they spread, helping you protect endpoints with minimal disruption.
- **Operational Efficiency –** A unified approach to endpoint security streamlines processes, enabling your team to focus on strategic initiatives.

WHAT MAKES US DIFFERENT

- **Tailored Security Solutions:** We customize Microsoft Defender for Endpoint implementations to match your unique security landscape and operational requirements.
- **Accelerated Deployment:** Our QuickStart approach ensures rapid setup and integration, minimizing disruption and quickly enhancing your security posture.
- **End-to-End Support:** From strategy to execution, we provide comprehensive guidance to ensure your endpoint security and threat response objectives are achieved.

Contact Presidio today: www.presidio.com