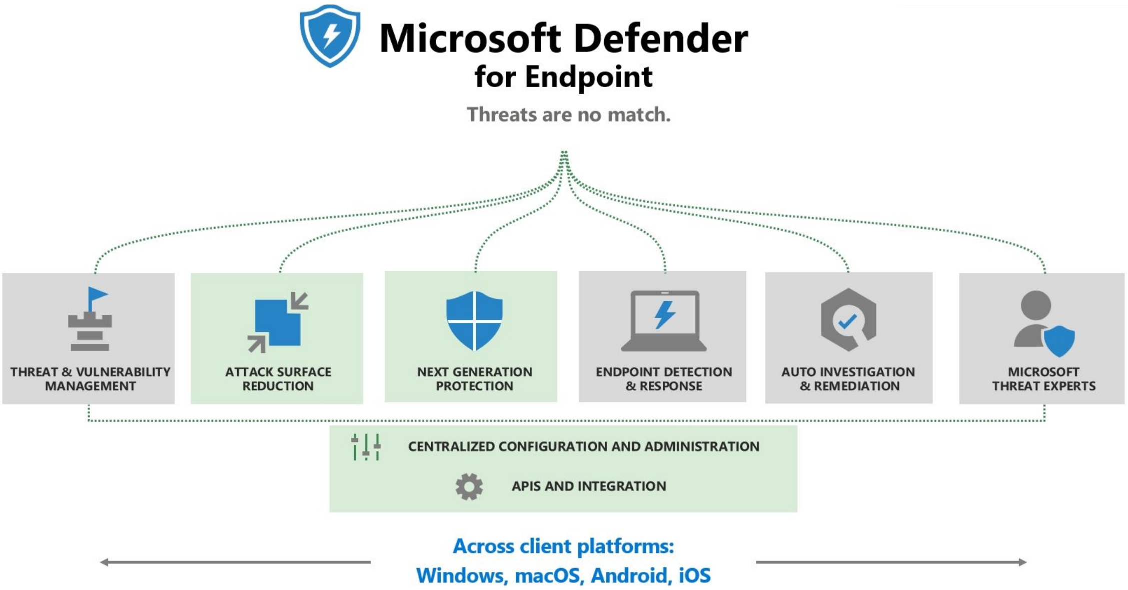
Microsoft
Defender

Assessment Service Documentation

by **Smart Technologies (BD) Ltd.**

Endpoint Security with Microsoft 365 Defender

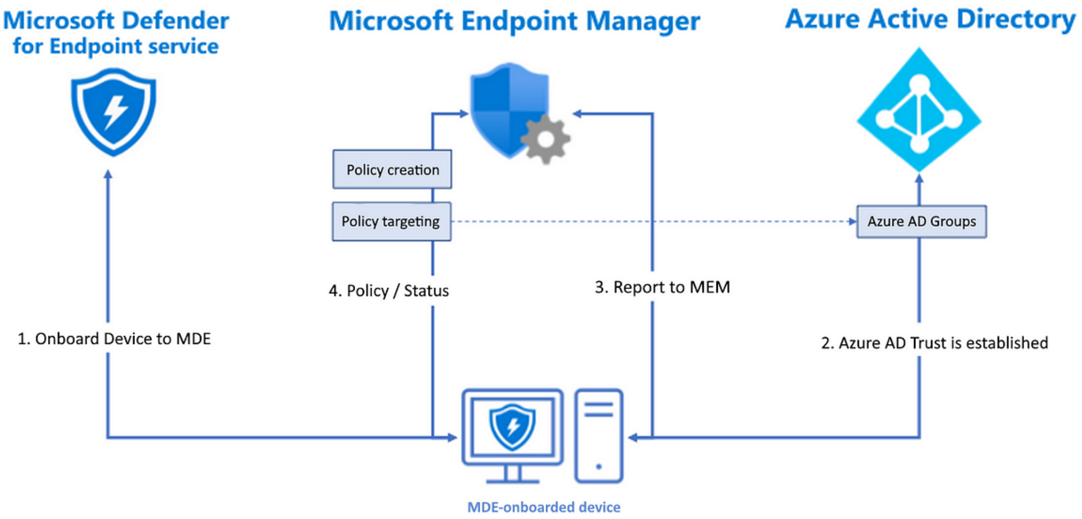

Microsoft Defender
for Endpoint
Threats are no match.
THREAT & VULNERABILITY MANAGEMENT
ATTACK SURFACE REDUCTION
NEXT GENERATION PROTECTION
ENDPOINT DETECTION & RESPONSE
AUTO INVESTIGATION & REMEDIATION
MICROSOFT THREAT EXPERTS
CENTRALIZED CONFIGURATION AND ADMINISTRATION
APIS AND INTEGRATION
Across client platforms:
Windows, macOS, Android, iOS

Empower your organizational security with confidence. Our 7-day Microsoft 365 Defender for Endpoint Assessment enhances endpoint security, protects sensitive data, and unleashes the full potential of your workforce – all with minimal disruption. This documentation provides additional insights into the key features of Microsoft 365 Defender for Endpoint and how our assessment aligns with your organizational goals.

Defender for Endpoint uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

- Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.
- Cloud security analytics: Leveraging big-data, device learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data.

How does it work?



Strengthen Threat Protection

Microsoft 365 Defender for Endpoint enables you to detect and respond to advanced threats using cutting-edge security intelligence and AI-driven analysis, elevating your organization's defense against sophisticated cyber threats.

Proactive Incident Response

Minimize the impact of security incidents through swift and effective response measures, enhancing your organization's readiness to respond to security incidents and reduce downtime.

Endpoint Security Optimization

Ensure your endpoints are resilient against evolving threats, providing a secure foundation for your organization. Optimize your organization's endpoint security strategy for maximum effectiveness.

Empowered Workforce

Provide secure access to corporate resources and applications, boosting productivity and collaboration for your workforce. Empower your employees with secure and seamless access to essential tools and resources.

Our assessment ensures robust threat protection, proactive incident response, and comprehensive endpoint security.

Our Assessment Focus:

- Threat Landscape Analysis
    - Identify vulnerabilities in the current threat landscape.
    - Assess the organization's exposure to advanced cyber threats.
- Defender Configuration & Optimization
    - Evaluate Microsoft 365 Defender for Endpoint settings and configurations.
    - Identify areas for optimization to fortify endpoint security.
- Incident Response Readiness
    - Assess the organization's preparedness to respond to security incidents.
    - Strengthen incident response capabilities for swift and effective actions.

Deliverables in 7 Days:

1. Comprehensive Threat Report:
    a. Detailed report outlining identified vulnerabilities.
    b. Recommended enhancements for improved security.
    c. Strategic implementation roadmap as a blueprint for fortifying the organization against emerging threats.
2. Cost-Benefit Analysis:
    a. Thorough analysis detailing potential return on investment.
    b. Insights into the benefits of strengthened security measures.
    c. Understanding of the optimized incident response's impact on organizational productivity.
3. Clear Action Plan:
    a. Clear and actionable plan for seamlessly integrating Microsoft 365 Defender for Endpoint.
    b. Roadmap ensuring a smooth transition and fortification against evolving threats.