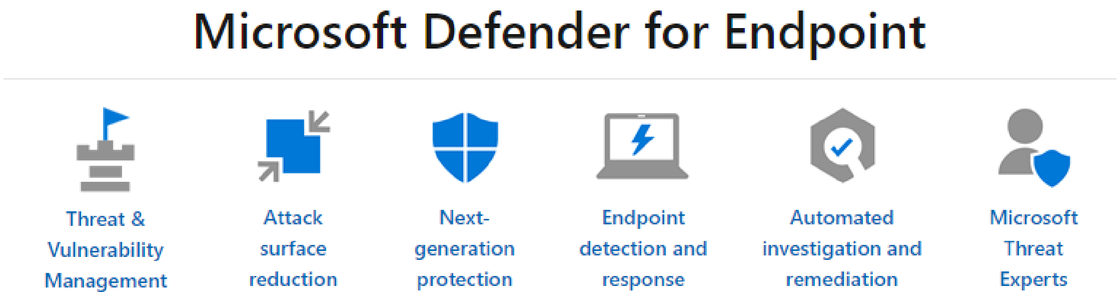
Microsoft Defender for Endpoint

By: RyanStewart


Microsoft Defender for Endpoint
Threat & Vulnerability Management
Attack surface reduction
Next-generation protection
Endpoint detection and response
Automated investigation and remediation
Microsoft Threat Experts

The following capabilities are enabled with Microsoft Defender for Endpoint:

- Threat and vulnerability management provides real-time visibility and helps identify ways to improve your security posture.
- Attack surface reduction eliminates risky or unnecessary surface areas and restricts dangerous code from running.
- Advanced protection uses machine learning and deep analysis to protect against file-based malware.
- Endpoint detection and response monitors behaviors and attacker techniques to detect and respond to advanced attacks.
- Use artificial intelligence to automatically investigate alerts and remediate complex threats in minutes.
- Microsoft threat experts bring deep knowledge and proactive threat hunting to your security operations Center.

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

- **Endpoint behavioral sensors**. Built-in in to Windows 10, these sensors collect and process behavioral signals from the operating system. The sensors send the data to your private, isolated cloud instance of Microsoft Defender for Endpoint.
- **Cloud security analytics**. Uses big data, machine 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 and security teams, and augmented by threat intelligence provided by partners, threat intelligence enables

Microsoft Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.