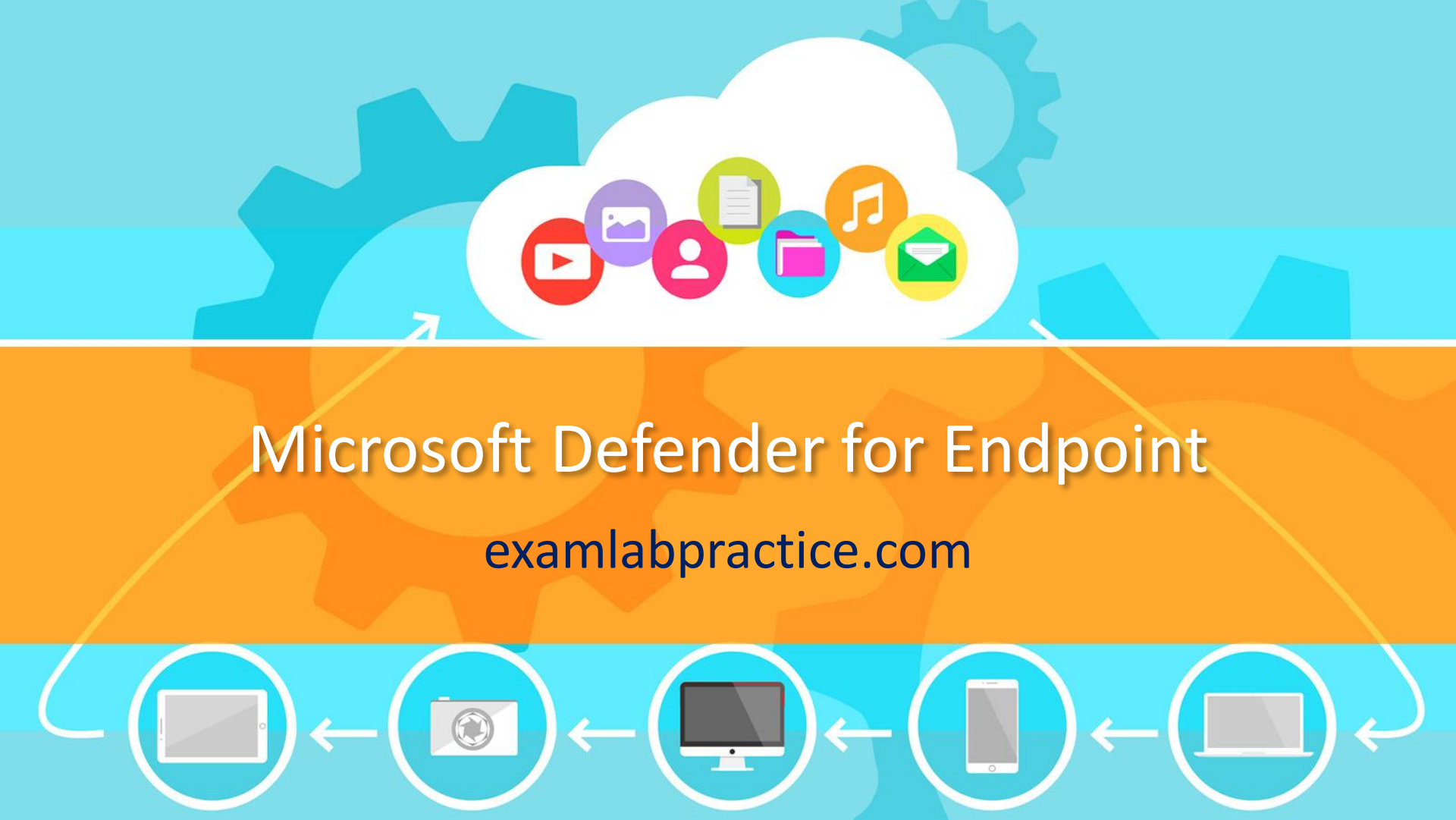
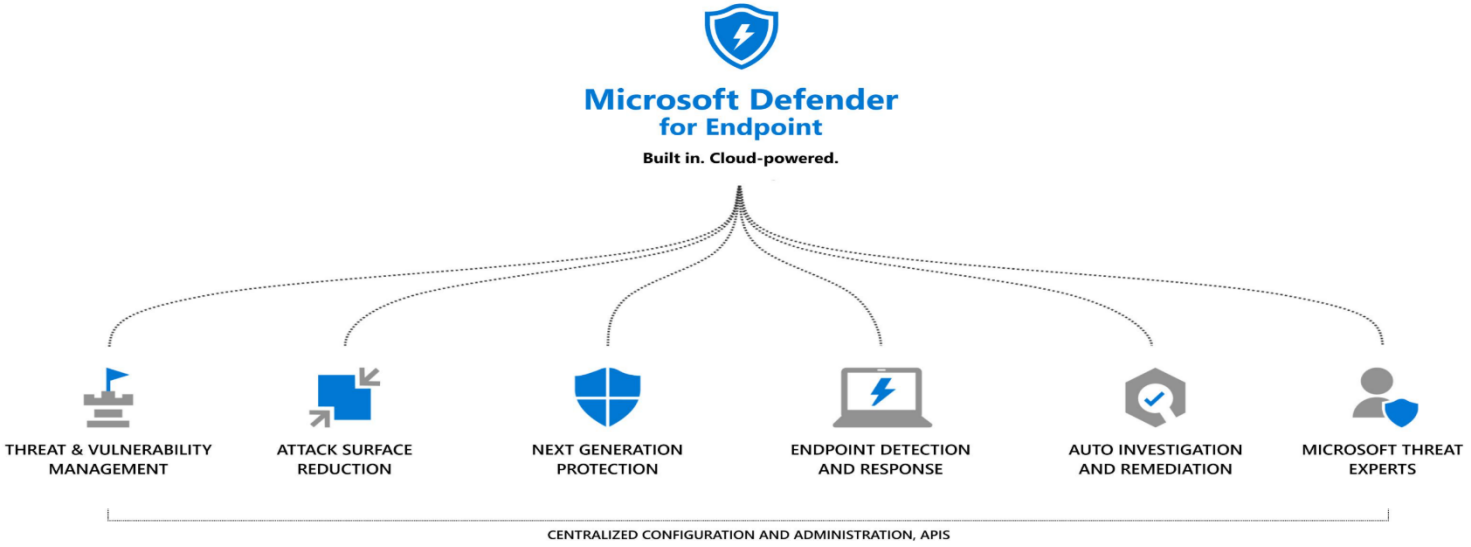


Microsoft Defender for Endpoint

examlabpractice.com

What is Microsoft Defender for Endpoint?

Microsoft Defender for Endpoint is built to be an enterprise grade endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.



Capabilities Provided

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

- **Endpoint behavioral sensors**

Embedded in Windows, 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.

Capabilities Provided (Continued)

- **Threat & Vulnerability Management**

This built-in capability uses a game-changing risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations

- **Attack surface reduction**

The attack surface reduction set of capabilities provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs.

- **Next-generation protection**

To further reinforce the security perimeter of your network, Microsoft Defender for Endpoint uses next-generation protection designed to catch all types of emerging threats.

- **Endpoint detection and response**

Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars. Advanced hunting provides a query-based threat-hunting tool that lets you proactively find breaches and create custom detections.

Capabilities Provided (Continued)

- **Automated investigation and remediation**

In conjunction with being able to quickly respond to advanced attacks, Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

- **Microsoft Secure Score for Devices**

Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve the overall security of your organization.

- **Microsoft Threat Experts**

Microsoft Defender for Endpoint's new managed threat hunting service provides proactive hunting, prioritization, and additional context and insights that further empower Security operation centers (SOCs) to identify and respond to threats quickly and accurately.

Integration with Microsoft solutions

- Azure Security Center
- Microsoft Sentinel
- Intune
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Defender for Office 365