Microsoft Security

ITie

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
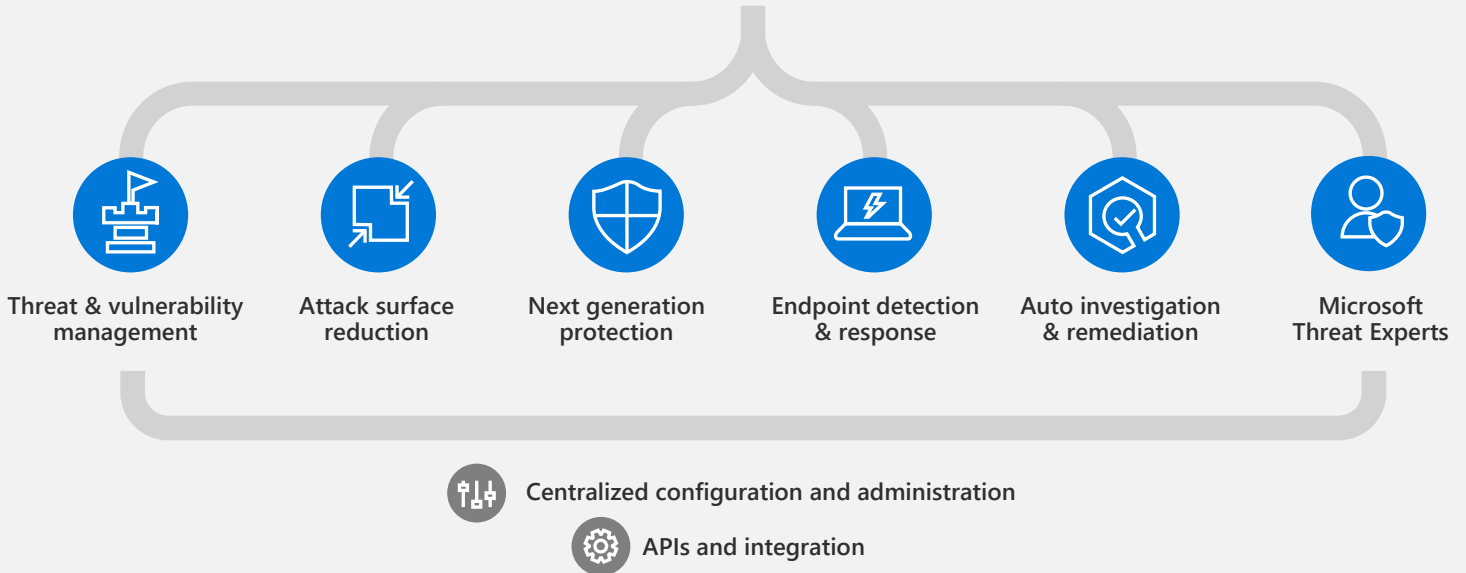
Microsoft Defender for Endpoint is an industry-leading, cloud-powered endpoint security solution that helps to secure against ransomware, file-less malware, and other sophisticated attacks on Windows, macOS, Linux, Android, and iOS. Our comprehensive solution helps to rapidly stop attacks, scale your security resources, and evolve your defenses.

Top 10 Microsoft Defender for Endpoint advantages   = unique value

1. Agentless, cloud-powered

Save time and resources with no additional infrastructure and no agents to deploy on your Windows endpoints. Defender is seamlessly integrated in the platform and always up to date.

2. Infinite scale and built-in multi-tenancy

Built on cloud technologies, Microsoft Defender for Endpoint can scale above and beyond a million endpoints on a single tenant, also enabling customers to further partition their tenant to hundreds of sub-tenants.

3. Unparalleled optics

The widest threat optics, signal, and world-class human intelligence is built into the product, offering you a unique advantage against the latest and most sophisticated threats.

4. Machine learning, behavioral detections and known threat library

Leverages combined client and cloud-based Machine Learning and behavioral algorithms to detect and block known and unknown threats.

5. Award-winning protection

Trusted by organizations across the globe, our award-winning solution is one of the best in class with top ratings in analyst evaluations and consistently high scores in independent tests.

6. Built-in automation

The only vendor to apply out-of-the-box AI-based automation to investigate alerts to understand if a threat is real and take automatic remediation actions to quickly fix impacted machines.
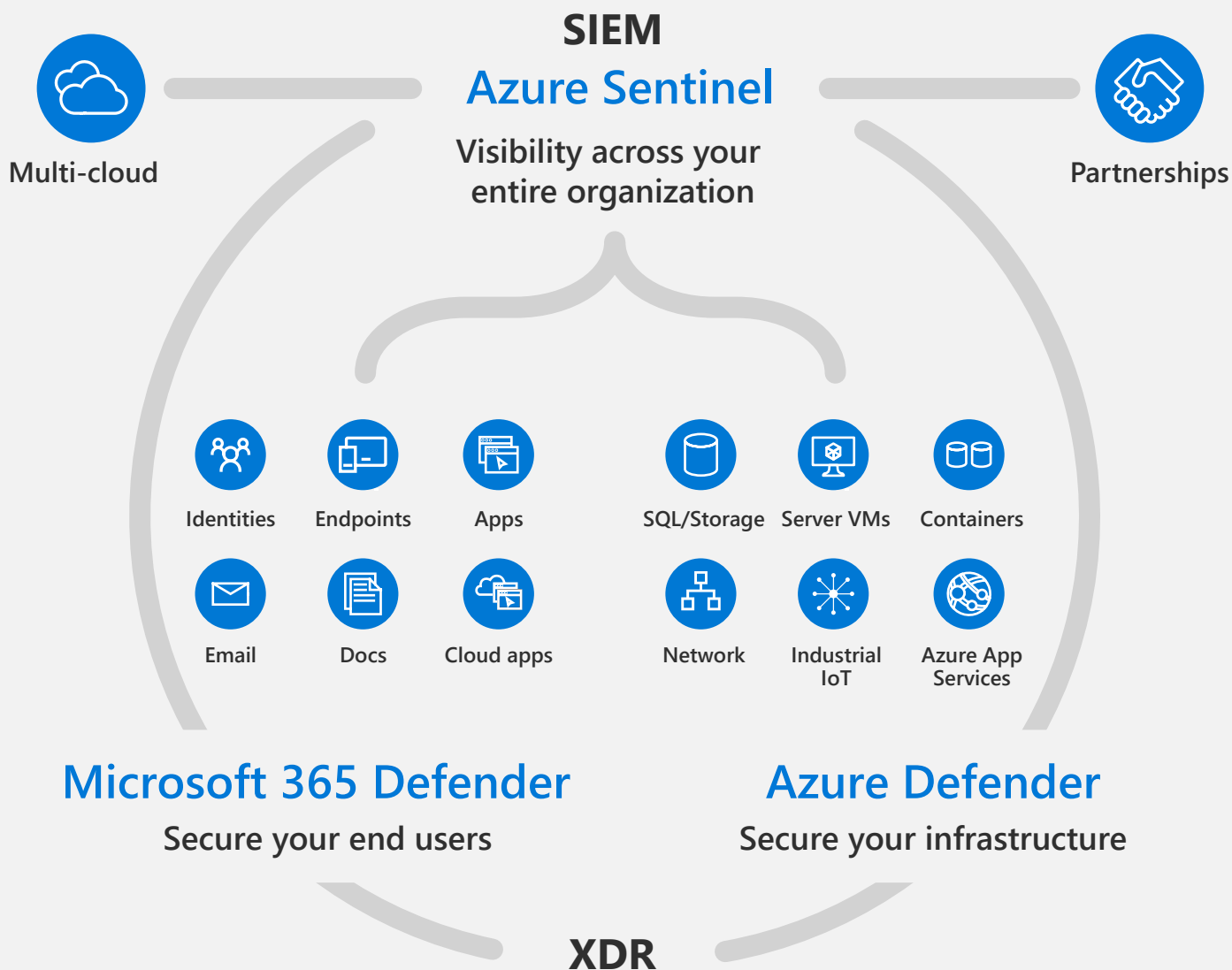
7. Threat hunting

Microsoft Defender for Endpoint provides security teams with the ability to hunt for compromise over six months of historical data across the organization. Security teams can build their own custom hunting queries and custom detections.

8. Threat analytics

Threat analytics reports allow organizations to quickly understand new global threats, see if they are currently impacted, assess their exposure and take mitigation actions to increase their resilience to these threats.

9. Threat and vulnerability management

Microsoft Defender for Endpoint monitors for Microsoft and third-party software vulnerabilities and security configuration issues. It then automatically takes actions to mitigate risk and reduce exposure.

10. Microsoft Threat Experts

Microsoft Threat Experts provide Security Operations teams expert level oversight and analysis to help ensure that critical threats in their unique environments don't get missed.

Stay ahead of attackers with a unified SecOps experience

SIEM
Azure Sentinel
Visibility across your entire organization

Multi-cloud

Partnerships

| Identities | Endpoints | Apps | | SQL/Storage | Server VMs | Containers |

| Email | Docs | Cloud apps | | Network | Industrial IoT | Azure App Services |

Microsoft 365 Defender
Secure your end users

Azure Defender
Secure your infrastructure

XDR

Microsoft Defender for Endpoint is part of an integrated set of threat protection solutions from Microsoft that offer a holistic view of security for your organization.

Microsoft 365 Defender and Azure Defender deliver the most comprehensive XDR solution on the market and Azure Sentinel is an innovative cloud-native SIEM. With the integration of these tools, defenders have more actionable context than ever so they can focus on stopping threats across the entire enterprise.

Microsoft Defender for Endpoint
Rapidly stop threats. Scale your security. Evolve your defenses.

Windows   macOS

Android   iOS

Cisco
Juniper Networks

HP Enterprise
Palo Alto Networks

Endpoints and servers

Mobile device OS

Network devices