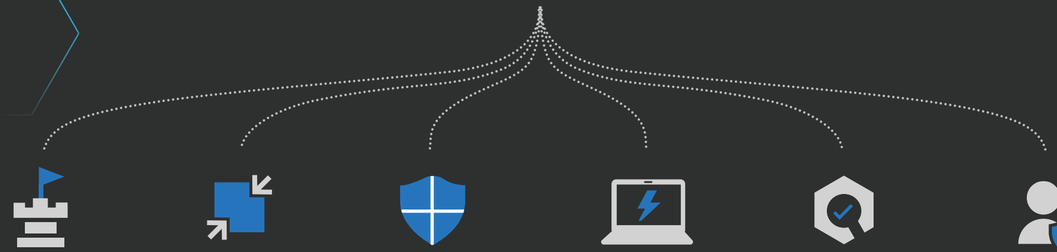
Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.

Unified platform for automated protection, detection, investigation, and response



THREAT & VULNERABILITY MANAGEMENT

Discover, prioritize and remediate vulnerabilities.

ATTACK SURFACE REDUCTION

Increase your endpoints' resistance to threats.

NEXT GENERATION PROTECTION

Protect your business from advanced threats.

ENDPOINT DETECTION & RESPONSE

Detect those who want to stay undetected.

AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale.

MICROSOFT THREAT EXPERTS

Human guidance, threat monitoring and prioritization.

CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

Threat & vulnerability management

Provides real-time visibility and identifies ways to improve your secure score.

- Discover vulnerabilities and misconfigurations continuously in real-time
- Prioritization is based on your business context and the dynamic threat landscape
- Correlation of vulnerabilities with endpoint detection and response (EDR) alerts
- Built-in end-to-end remediation process to bridge the gap between security and IT teams

Attack surface reduction

Eliminates risky or unnecessary surface areas and restricts dangerous code from running.

- Block exploitation of unpatched vulnerabilities and 0-days
- Browse safely within a hardware-based isolated session
- Prevent devices from contacting exploit sites and malicious locations on the internet
- Simplify application control based on your logic and reputation data from the Intelligent Security Graph

Next generation protection

Leverages machine learning and deep analysis to protect against file-based and fileless malware.

- Defend against never-seen-before polymorphic and metamorphic malware threats
- Address malware including fileless attacks using an AI-based solution that is coupled with runtime emulation, sandboxing, reputation analysis, script and memory scanning

Endpoint detection & response

Monitors behaviors and attacker techniques to detect and respond to advanced attacks.

- Visually investigate forensic evidence across your endpoints to easily uncover the scope of breach
- Proactively hunt and investigate across six months of historical data across endpoints
- Write your own queries, save them, and turn them into custom detections
- Submit suspicious files for a deep inspection and see a full capability report in minutes

Auto investigation & remediation

Leverages artificial intelligence to automatically investigate alerts and remediate complex threats in minutes.

- AI-based automatic investigation of alerts
- Investigates and remediates memory-based / fileless attacks
- Automatically investigates alerts, determines if a threat is active and determines what course of action to take to perform required remediations
- Investigates across multiple alerts and automatically remediates threats on all impacted endpoints

Microsoft Threat Experts

Brings deep knowledge and proactive threat hunting to your Security Operations Center.

- Provides expert level threat monitoring and analysis
- Proactive hunting across your data for critical threats
- Environment-specific context delivered through alerts to enable you to respond with confidence
- Experts on demand: direct access to world-class hunters

Why Microsoft?

Agentless, cloud-powered.
No additional deployment or infrastructure.
No delays or update compatibility issues.
Always up-to-date.

Unparalleled optics.
Built into Windows 10, shares with the Microsoft Intelligent Security Graph to deepen insights.

Threat hunting over rich data.
Six months of historical data and real-time search to hunt across all your cyber data and entities.

Automated security.
Take your security to a new level by going from alert to remediation in minutes—at scale.

Part of Microsoft Threat Protection.
Protect across your devices, identities, apps, and data for a seamless investigation experience.

Synchronized defense.
Microsoft Threat Protection shares detection and exploration across devices, identities, and information—to speed up response and recovery.

Get started with Microsoft Defender ATP

Learn more.
https://aka.ms/mdatp

Start your free trial.
Sign up for a free trial of Microsoft Defender ATP today and onboard as many machines as you need. Nothing to deploy, start better protecting your organization today!

"Aced protection tests 12 months in a row." Proven protection in the field, backed up by consistent top rankings on industry comparison tests (AV-TEST, SE Labs).

Gartner names Microsoft a Leader in the August 2019 Magic Quadrant for Endpoint Protection Platforms.

Forrester names Microsoft a Leader in The Forrester Wave™: Endpoint Security Suites, Q3 2019.

Demonstrated **industry-leading optics and detection capabilities** in MITRE ATT&CK-based evaluation.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Microsoft

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.

Trusted by IT.
Loved by security teams.

Endpoint security through the power of the cloud, machine learning, and behavior analytics.

Vulnerabilities prioritized based on your business context.
Discover, prioritize, and remediate endpoint vulnerabilities and misconfigurations in real-time. The built-in remediation processes speeds up your mitigations.

Eliminate risks by reducing the surface area of attack.
Use hardware-based isolation, exploit and network protection, and app control to dramatically reduce the surface area of attack.

Block and tackle sophisticated threats and malware.
Take advantage of an AI-based solution to stop never-seen-before threats from impacting devices.

Detect and investigate advanced persistent attacks.
Use behavior monitoring, ML, and security analytics to detect 0-days, advanced attacks, and data breaches.

Automatically remediate threats from affected endpoints.
Automatically investigate alerts to understand if a threat is active and determine a course of action to perform remediation. Prevent users from accessing sensitive data from devices at risk.

Managed threat hunting by Microsoft Threat Experts.
Microsoft Threat Experts provide your Security Operations Center with deep knowledge, expert level threat monitoring, analysis, and support to identify critical threats in your unique environment.