Microsoft Security

E-book Series

Microsoft Defender for Endpoint

Disrupt ransomware with industry-leading endpoint security across Windows, Linux, macOS, iOS, Android, and IoT.

Today's threat landscape calls for dynamic, AI-powered endpoint security

In just the past few years, cyberattacks have become far more sophisticated than ever before, virtually unrecognizable from the attacks of the 2010s. Past attacks took a more randomized "spray and pray" approach, but today's attacks are persistent, adaptive, and precisely targeted so that once they land, attackers work surgically to achieve maximum impact.

Microsoft has more insight into attacker behaviors than anyone

78T	signals synthesized per day*
10K	security and threat intelligence experts*
1M	Microsoft Security customers*

* **Source:** Microsoft Digital Defense Report, 2024

Before, attackers targeted organizations through a single domain such as endpoints, whereas today they have a comprehensive understanding of your device estate and target your entire company across domains. They can operate relatively undetected, leveraging compromised accounts to move laterally.

Campaigns are now customized to your specific environment, combining human and artificial intelligence with the availability of generative AI. After each action taken by a security team or security software, attackers recalculate and pivot.

As attacks have advanced, so too has their impact. Successful campaigns are now all but guaranteed to cause catastrophic and visible business damage after just a short period of time.

Attacks used to take days before impacting organizations, but today thousands of devices can be encrypted in less than 5 minutes. Therefore, even if your security team is operating at its very best, there is often little they can do to protect your organization from large-scale damage.

That's why traditional endpoint detection and response is simply no longer enough to protect organizations. Today's security solutions must take a multilayered approach and be automated, dynamic, and operate in real-time.

Microsoft Defender for Endpoint is an industry-leading endpoint security solution that is specifically designed to keep you ahead of these modern, sophisticated attacks. It delivers defense in depth, going way beyond just antivirus protection to safeguard your digital estate with everything from proactive posture management to automatic attack disruption of in-progress campaigns.

Defender for Endpoint doesn't just protect you from active attacks but looks at the entire attack graph to determine the potential blast radius and stop intruders in their tracks. It is powered by AI and the industry's broadest threat intelligence, including deep analysis of tens of thousands of attacks. It delivers this comprehensive protection across all devices and platforms and is integrated into the Microsoft Defender XDR platform for unmatched, cross-domain visibility across your organization.

Defender for Endpoint provides comprehensive protection across all platforms and devices

As the threats against each device type and platform vary significantly, we purposely build protections accordingly: how you secure a Windows laptop for an office worker differs significantly from a Linux server for a healthcare facility. Defender for Endpoint protects all platforms and devices, from mobile to servers to IoT, including Windows, macOS, iOS, Linux, and Android.

Posture management

Next-generation protection

Auto-deployed deception techniques

Automatic attack disruption

Endpoint detection and response

I wanted a Swiss Army Knife solution that could expand into endpoint configuration, firewall management, and data loss prevention. We've fulfilled that hope by adopting Defender for Endpoint.

Esmond Kane

Chief Information Security Officer,
Steward Health Care

What's different about Microsoft Defender for Endpoint?

Auto-deployed deception techniques

Create early-stage, high-fidelity signals with built-in deception techniques that automatically create an artificial attack surface in minutes. Think of it as a series of trip wires across your network that attackers cannot see.

Automatic attack disruption

A built-in self-defense capability that uses multi-domain signal, the latest TI & AI-driven machine learning models to automatically stop attacks like ransomware early in the kill chain, and block lateral movement and remote encryption across all your devices.

Posture management

Monitor for Microsoft and third-party software vulnerabilities and security configuration issues—taking action to mitigate risk and reduce exposures. Ensure strong endpoint security posture from day one and improve your security configuration with in-console, prioritized recommendations.

Microsoft Security Copilot

Use natural language to speed up daily tasks such as investigating and responding to incidents, prioritizing alerts, and upskilling. Security Copilot combines the world's leading generative AI with Microsoft's global threat intelligence.

Next-generation protection

Leverage machine learning models trained on cloud-scale data and behavior-based detection to protect against malware and malicious activity.

Microsoft Threat Intelligence

We see more threat vectors than any other vendor in the industry. Our threat intelligence is informed by 78 trillion daily signals from across the world's largest clouds, over a billion endpoints, and more than 10,000 cross-disciplinary experts across 72 countries.

Microsoft Defender XDR integration

Ramp up seamlessly from endpoint protection to the industry's broadest XDR platform for detection, response, and exposure management capabilities based on automatically correlated signals across domains—from endpoints and identities to email, documents, and cloud apps.

Effective security should be easy to deploy and manage

Just as important as effective protection are safety and ease of use, and Microsoft continually delivers innovations that dramatically simplify the SOC experience and deliver critical protections while ensuring operational resiliency. Keeping you ahead of the evolving threat landscape requires continual enhancements to Defender for Endpoint, but our top priority is to deploy these updates safely to protect you and your organization. We also invest continually in making Defender for Endpoint easy to deploy and manage so that your team can focus on what really matters.

Empower your team to work smarter and faster with Security Copilot

Security Copilot combines the world's leading generative AI with Microsoft's security-specific model trained on our unique global threat intelligence and more than 78 trillion signals daily. Embedded into the Defender for Endpoint experience, analysts can use natural language to speed up daily tasks such as investigating and responding to incidents, prioritizing alerts, and upskilling.

Flexible controls for your enterprise

Strike the desired balance between protection and productivity by applying Defender for Endpoint's granular controls to meet your organization's distinct requirements.

Simplified settings management for easier deployment

Streamline operations across your security and IT teams with a single source of truth for endpoint settings and policy management. Admins can choose to onboard devices and author policies in the Defender portal without ever leaving the experience or team up with IT to manage all endpoint security settings with Intune.

Safe agent architecture and deployment practices

Our agent architecture is engineered for security and reliability, where we used optimized sensors within the highly privileged kernel mode for data collection and enforcement. The remainder of the security solution occurs isolated within user mode, where reliability issues have less impact.

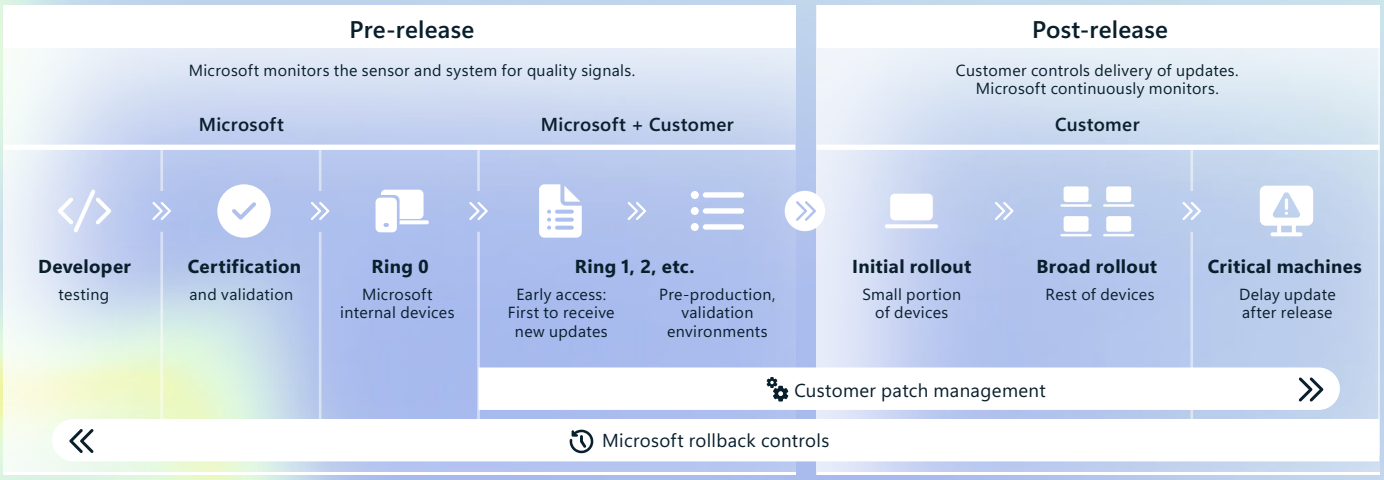
As we deliver updates to Defender for Endpoint, our number one priority is to do so in a safe, responsible way. Updates go through several phases of testing and validation, then rollouts start internally at Microsoft across thousands of devices before gradually proceeding through staged external rollout rings. You can control delivery of these updates to your devices by managing device groups and timing.

Microsoft has long invested in these best practices, and we look forward to broader adoption of this approach to reduce the likelihood of incidents across the industry.

Tailor-made protection for servers

Securing endpoints means every device in the network, not just productivity devices or mobile phones. Whether they are on-prem or in the cloud, servers are especially critical to secure. We take a tailored approach to protecting servers with custom detections for attacker techniques that target different server roles—web server, file server, and so on.

Best practices for safe deployment



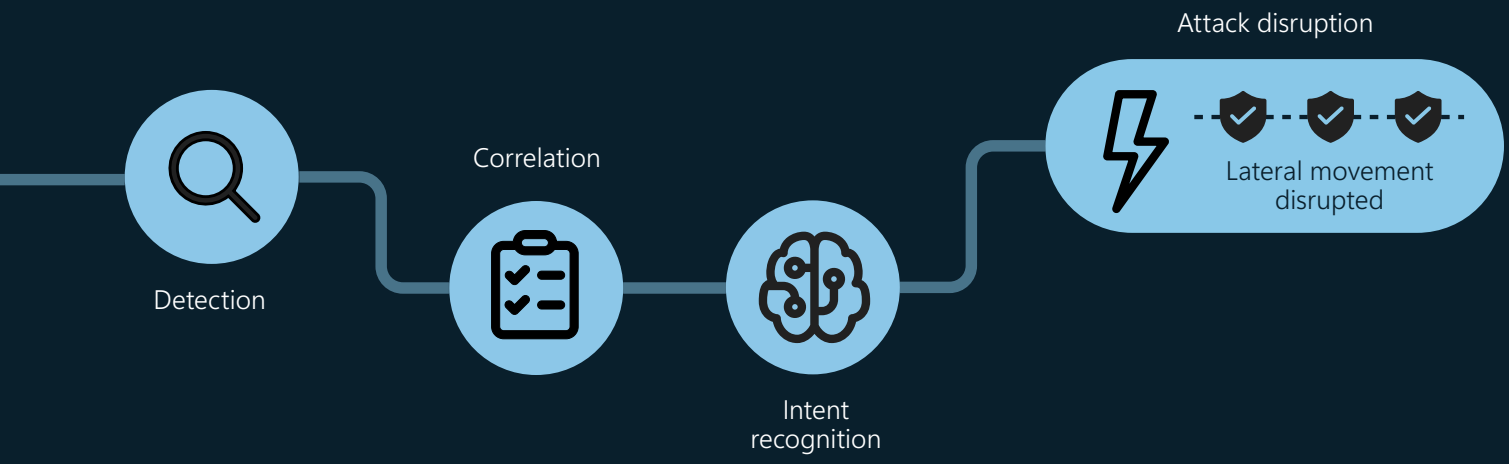
Built-in self-defense to automatically shut down cyberattacks early

No matter how effective your prevention is, you need best-in-class detection and response in case of an attack.

Automatic attack disruption is our built-in, automated response capability that stops in-progress attacks by analyzing the attacker's intent, identifying compromised assets (like devices, identities), and containing them in real time. This capability uses trillions of collected signals, the latest threat intelligence and machine learning models to accurately predict the attack path and adaptively respond to block an attacker's next move before it happens.

While other endpoint security solutions look at attacks in pieces, Defender for Endpoint analyzes them from the attacker's perspective: at the organizational level based on the evolving attack graph and intelligent complex logic that is continuously updated based on 78T daily signals.

Defender for Endpoint can also distinguish malicious behavior from benign behavior even on a single device, and therefore can contain threats granularly, with minimal impact to your organizational productivity. This capability is unique to Microsoft– just one of the ways we protect you against some of the most sophisticated and multi-domain attacks.



We disrupt ransomware attacks in an average of 3 minutes. In these attacks, identities and devices are the primary targets for gaining initial access, and we disrupt 16,000 such incidents each month. In fact, we disabled and contained 50,000 compromised user accounts in the last 6 months alone and saved over 180,000 devices at the same time.

Today, we disrupt some of the most sophisticated types of attacks, including ransomware, business email compromise, malicious OAuth app abuse and attacker-in-the-middle scenarios.

To strike the right balance between protection and business continuity, disruption doesn't kick in until Defender for Endpoint has reached above 99.99% confidence in the presence of an attack.

This is a capability that only Microsoft can develop and maintain given its native breadth of signal and best of breed components all integrated into the unified security operations platform.

> Defender for Endpoint 'lit up a Christmas tree' with hundreds of alerts, and attack disruption kicked in to save the day.

Anonymous

Healthcare company

3 minutes
average time to disrupt ransomware*

120,000
disabled user accounts in the last six months*

35,000
incidents disrupted per month*

180,000
devices saved from an attack in the last six months*

* **Source:** Microsoft Internal Research

Defender for Endpoint helps you prevent attacks and manage your exposure

Endpoints represent a significant part of your attack surface. The complex relationship they have with your identities, apps and data make it a real challenge to understand the role they play in your exposure to threats. Defender for Endpoint helps to ensure that the posture of your endpoints is strong from day one through offering vulnerability management capabilities that allow organizations to take a holistic and continuous approach to managing risk and staying ahead of cyber threats.

For instance, our vulnerability assessment capabilities provide your team with a prioritized view of how individual vulnerabilities can be chained together in a breach to reach your sensitive data. By viewing these attack paths, you can understand and receive guidance on how to address each vulnerability, making it easy to prioritize efforts and implement improvements.

Continuously discover and monitor assets

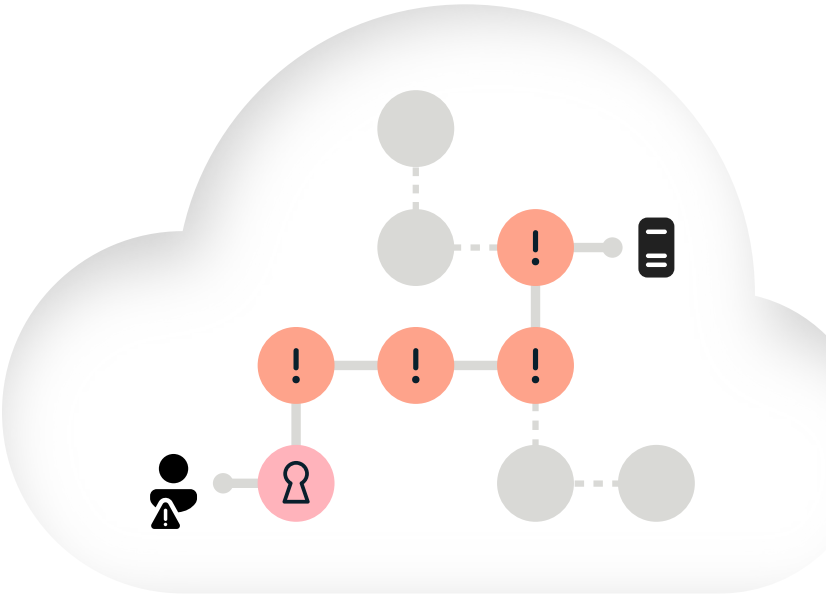
Eliminate periodic scans with continuous monitoring and alerts. Detect risks even when endpoints are not connected to the corporate network.

Focus on what matters

Prioritize the biggest vulnerabilities on your most critical assets using Microsoft's threat intelligence, breach likelihood predictions, and business contexts.

Track and mitigate risks with ease

Bridge the gap between security and IT teams to seamlessly remediate vulnerabilities with robust contextual recommendations, built-in workflows, and application block capabilities to enable protection faster.



Use attack path analysis to identify and remediate the vulnerabilities that have the greatest potential for exploitation in your environment.

These capabilities are part of our growing list of built-in preventative controls for endpoints—like security baselines—giving you a comprehensive set of features to manage your exposure.

You can quickly expand from vulnerability management of endpoints and tap into broader exposure management across your entire digital estate spanning identity, cloud, app, network, and data.

Consolidate your posture silos into a single source of truth for security teams and decision-makers in Microsoft Defender Exposure Management. This provides a contextual, comprehensive, and risk-based view that helps map your organization's digital attack surface and implement strategies to reduce risks.

> With Microsoft Defender, we have the information we need to assess employee behavior and make risk-based decisions. The visibility we gain with Defender for Endpoint is mind-boggling.

Suresh Gumma

Director for Cyber Strategy and Architecture
DXC Technology

Industry analyst recognition

Of course, our work is never done, and we're committed to continually optimizing and innovating Defender for Endpoint to stay ahead of today's attacks and anticipate tomorrow's challenges.

Gartner

Microsoft is a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the 5th time in a row. [1]

MITRE | ATT&CK®

Microsoft delivered 100% protection and technique level detections across all attack stages for Linux and macOS threats with zero false positives in MITRE's 2024 ATT&CK evaluation. [2]

IDC

Microsoft has the largest worldwide market share in modern endpoint security. [3]

FORRESTER®

Microsoft is a Leader in Forrester's 2023 Endpoint Wave and 2024 XDR Wave with the highest scores in the strategy, current offering, and market presence categories. [4]

Source:
[1] 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms
[2] 2024 MITRE ATT&CK® Evaluations: Enterprise
[3] Forrester Endpoint Wave, 2023
[4] Worldwide Modern Endpoint Security Market Shares, 2023: Evolving to Address New Work Modalities, 2023

Ramp up seamlessly from endpoint protection to XDR

One thing we hear consistently from industry analysts is the value of Defender for Endpoint being part of the Defender XDR platform. In fact, Microsoft Defender is recognized as a Leader in both the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms and the 2024 Forrester Wave: Extended Detection and Response (XDR) platforms.

Why does this matter? Attackers think in graphs, expertly traversing across your network by moving between the seams of siloed tools. So, when you have incomplete protection, or multiple solutions stitched across different platforms, you are left with gaps in coverage that attackers know how to exploit.

That's why it's so important that Defender for Endpoint is integrated into the Defender XDR platform, which correlates a wide breadth of signals across endpoint, identity, email, SaaS apps, data, and cloud workloads. This provides a unified vantage point across your estate and delivers cross-workload protections like exposure management and automatic attack disruption.

> This is the silver bullet for a SOC. Having high quality detections is not easy to build and more difficult to find in 3rd party [vendors]."

Anonymous

Microsoft Defender XDR customer

> Once our security professionals gained confidence with the technology…they quickly became some of our strongest advocates for Microsoft Security solutions. We highly value Defender for Endpoint and Identity as primary layers of protection for our environment.

Glauco Sampaio

Chief Information Security Officer,
Cielo

Advanced cyberattacks are pushing the boundaries and highlighting the shortcomings of traditional endpoint security solutions. It has never been more critical to have a dynamic and comprehensive solution to protect your digital estate, and Microsoft Defender for Endpoint is exactly that.

Beyond incident-based investigation and response, Defender for Endpoint includes AI-powered vulnerability management, auto-deployed deception techniques, and automatic attack disruption. It comes with Security Copilot to drive SOC efficiencies and is built on the world's broadest threat intelligence to stay ahead of increasingly sophisticated attackers. Microsoft Defender is available on all platforms and devices, and tailor-made for each.

Keep up with the evolving attack landscape and see what AI-powered, intelligence-driven endpoint protection can do for your security team.

Get started today
Connect with our sales team to learn more