News Endpoint security Microsoft Defender for Endpoint
5 min read

Microsoft Defender for Endpoint now stops human-operated attacks on its own

By Rob Lefferts, Corporate Vice President, Microsoft Threat Protection

October 11, 2023

SIEM and XDR

Microsoft Defender

Microsoft Defender XDR

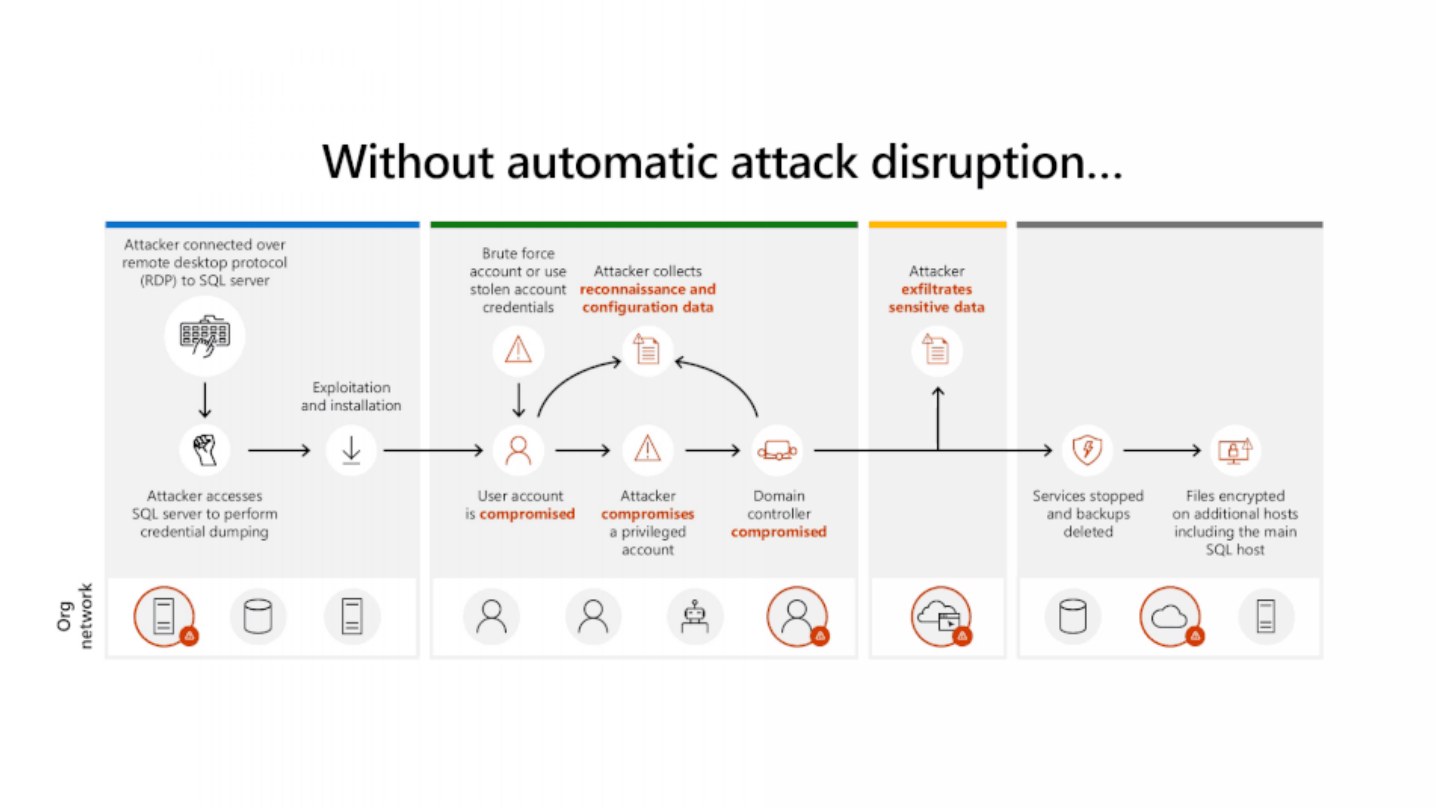
Microsoft 365 Defender is now Microsoft Defender XDR. Learn more.

Defenders need every edge they can get in the fight against ransomware. Today, we're pleased to announce that Microsoft Defender for Endpoint customers will now be able automatically to disrupt human-operated attacks like ransomware early in the kill chain without needing to deploy any other capabilities. Now, organizations only need to onboard their devices to Defender for Endpoint to start realizing the benefits of attack disruption, bringing this extended detection and response (XDR) AI-powered capability within reach of even more customers.

Automatic attack disruption uses signal across the Microsoft 365 Defender workloads (identities, endpoints, email, and software as a service [SaaS] apps) to disrupt advanced attacks with high confidence. Basically, if the beginning of a human-operated attack is detected on a single device, attack disruption will simultaneously stop the campaign on that device and inoculate all other devices in the organization. The adversary has nowhere to go.

Attack disruption achieves this outcome by containing compromised users across all devices to outmaneuver attackers *before* they have the chance to act maliciously, such as using accounts to move laterally, performing credential theft, data exfiltration, and encrypting remotely. This on-by-default capability will identify if the compromised user has any associated activity with any other endpoint and immediately cut off all inbound and outbound communication, essentially containing them. Even if a user has the highest permission level and would normally be outside a security control's purview, the attacker will still be restricted from accessing *any* device in the organization. As a result of this decentralized protection, attack disruption has saved 91 percent of targeted devices from encryption attempts.[1]

Until now, detecting these campaigns early posed significant challenges for security teams since adversaries typically perform activities disguised as normal user behavior. And while other vendors may detect these attack techniques, only Microsoft 365 Defender can automatically disrupt them around the clock even when your security team might be offline. Backed by Microsoft's breadth of signal and deep user behavioral analysis, security teams now possess a robust new tool to effortlessly stop sophisticated ransomware attackers at scale.



This capability has been quietly disrupting attacks for real organizations since 2022. For example, in August 2023, hackers compromised the devices of a medical research lab. With lives and millions of dollars in research at stake, the potential reward for hackers to encrypt the devices and demand a ransom was high. During the hands-on keyboard attack, hackers manually executed commands and used remote desktop protocol to connect to one of the organization's SQL servers. From there, the hackers performed credential dumping—the first step in trying to access 55 other devices in the network. However, they were unaware that the moment they connected to the SQL server, that would be the last step in their ransomware campaign. They were immediately shut out from accessing any of the lab's devices. And the security analysts didn't even have to lift a finger.

This research lab was just one of a handful of Microsoft customers involved in the preview of this industry-first capability. Since August 2023, more than 6,500 devices have been spared encryption from ransomware campaigns executed by hacker groups including BlackByte and Akira, and even red teams for hire.[1]

Automatic attack disruption levels the playing field

Ransomware is one of the most common human-operated attacks organizations face. In 2022, there were nearly 236.7 million ransomware attacks worldwide with the projected cost rising to USD265 billion annually by 2031.[2] With increasing volume and impact of attacks like ransomware, security analysts need the sophisticated automation of previously manual responses that attack disruption offers to effectively scale their defenses.

To help defenders in this asymmetrical battlefield, in November 2022 Microsoft 365 Defender introduced automatic attack disruption: an industry-first capability that stops attacks at machine speed by using the correlation of cross-domain signal into one high-fidelity incident. Combined with automated incident and response capabilities, Microsoft 365 Defender is the only XDR platform that protects against ransomware attacks at the organizational and device levels.

In addition to ransomware, attack disruption covers the most prevalent, complex attacks including business email compromise and adversary-in-the-middle. These scenarios each involve a combination of attack vectors like endpoints, email, identities, and apps, posing a significant challenge for security teams to pinpoint where the attack is coming from. Most security vendors lack the high-fidelity signal to accurately identify if an attack is even happening, let alone can take disruption actions. Automatic attack disruption solves this problem by confidently detecting and disrupting at the attack source, giving defenders time to respond before the

adversary can inflict damage.

Expand your coverage with more signal

As the security adage goes, it's not a matter of if you'll be breached, but a matter of when. Endpoint security requires a depth of defense through multiple protective layers and mechanisms such as patching vulnerabilities, using next-generation antivirus to neutralize threats at the perimeter, harnessing auto investigation and response to remediate at the individual device level and automatic attack disruption at the organization level to further limit the spread of an attack.

Attack disruption's effectiveness and coverage increases with every product that is integrated into Microsoft 365 Defender. While the majority of ransomware attacks happen on the endpoint, it's important to deploy the entirety of the security stack across apps, identities, email, and collaboration to protect against prevalent scenarios like business email compromise, adversary-in-the-middle, and future scenarios. This enables organizations to benefit not only from disruption capabilities but all the rich features across the most critical security workloads.

Protect customers of all sizes with automatic attack disruption today

Every day, more and more organizations around the world are taking advantage of automatic attack disruption to successfully disrupt human-operated attacks. The new contain user disruption capabilities will help customers of all sizes stay automatically protected against ransomware attacks. For small and medium businesses (SMBs), who often lack access to sophisticated security solutions or expertise, this "on by default" capability helps them stay protected from the latest threats, while they focus on running their business.

These capabilities are now available in public preview in the following endpoint protection offerings:

- Microsoft Defender for Endpoint Plan 2 and associated bundles.
- Defender for Business standalone and associated bundles.

To ensure you have the latest agent deployed and your devices are onboarded to take advantage of this capability, read the documentation.

To learn more:

- Dive deep into how automatic attack disruption worked in protecting the cancer research lab and in fending off the Akira threat group in this article.
- Tune into the live Ninja show on October 12, 2023.
- Join us for the upcoming Ask me Anything session on October 24, 2023.
- Watch a demo of automatic attack disruption in action.

Small and medium business resources:

- Learn about automatic attack disruption in Defender for Business through our documentation.
- Learn more about SMB security solutions from our website.

Learn more

Learn more about Microsoft Defender for Endpoint.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X, formerly known as Twitter, (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1]Microsoft internal data.

[2]100+ Ransomware Attack Statistics 2023, Astra. August 4, 2023.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy