

Search the blog

[Best practices AI and machine learning Microsoft Copilot for Security](#)

4 min read

## Defend against human-operated ransomware attacks with Microsoft Copilot for Security

By [Microsoft Security for Copilot Team](#)

March 4, 2024



Microsoft Defender

Microsoft Defender for Endpoint

Microsoft Defender XDR

Organizations everywhere are seeing an increase in human-operated [ransomware](#) threats, with Microsoft's own telemetry showing a 200% increase in threats since September 2022.<sup>1</sup> When an entire organization is attacked, they need every advantage they can get to protect against skilled, coordinated cyber threats. The availability of [Microsoft Copilot for Security](#), brings SecOps teams a new tool with the power of generative AI to help outpace and outsmart threat actors. In the following demonstration videos, we take a detailed, step-by-step look at how it can help surface, contain, and mitigate a human-operated ransomware attack.

### Microsoft Copilot for Security

Powerful new capabilities, new integrations, and industry-leading generative AI.

[Learn more >](#)

## The power of Microsoft Defender XDR with Microsoft Copilot for Security

[Microsoft Defender XDR](#) coordinates detection, prevention, investigation, and response across endpoints, identities, email applications, and the cloud to provide integrated protection against sophisticated ransomware threats. In this series of demonstration videos, we share real-world scenarios where Copilot is helping SecOps teams navigate threat detection, investigation, and managed response. To begin, we look at a situation where a human-operated ransomware attack has just taken place. The incident started with suspicious activity on two devices, where a credential theft tool was detected and stopped by [automatic attack disruption](#) within Microsoft Defender XDR.

Watch the video: [\(Humor\) Human Operate Ransomware](#)

### Respond at the speed and scale of AI

Bad actors can move through a system with damaging speed. And with the ever-increasing frequency and sophistication of attacks—paired with the ongoing shortage of security talent—it can be difficult for leaders to staff security teams completely. When every second counts—like during an active ransomware incident—Copilot for Security brings together critical context so security professionals can share clear, concise, and comprehensive summaries of active incidents—giving affected parties a deep

understanding of the situation, even when an incident happens after business hours. With the power of AI, Copilot is helping analysts write up these incident narratives 90% faster than in the past.<sup>2</sup>

In the case of this human-operated ransomware incident, [Microsoft Defender for Endpoints](#) had the first alert, detecting possible human operated malicious activity on a device. Many complex and sophisticated attacks like ransomware use scripts and tools like PowerShell and Mimikatz to access and manipulate files, tamper with system recovery settings, and delete file backups. In this incident, attackers also attempted to access Primary Refresh Tokens (PRT) and used Windows Sysinternals tools for evasion. But with line-by-line script examination in Copilot, security analysts could immediately understand what each section of code does, to quickly identify a script as malicious or benign. This Copilot capability directly helps junior security analysts “upskill” their expertise by learning the context behind the code.

## Gain critical incident context

When faced with a complex attack, Copilot for Security can help analysts understand what’s happening quickly, so they can protect and defend their organization at machine speed and scale. In an examination of the same ransomware incident, our next demonstration video shows how the Copilot incident summary focused in on a PowerShell script, leading analysts to a critical piece of the incident puzzle.

Watch the video: [Defender Embed to Standalone Copilot](#)

Without enough time and without PowerShell expertise, it could be difficult for a security analyst to fully understand the ramifications of an attack like this. But this is where Copilot can help—it quickly analyzes the PowerShell script, providing a plain English explanation of key steps within it. This helps analysts gain a full understanding of the incident and prioritize the containment and mitigation work that matters most. Copilot also works with [Microsoft Defender Threat Intelligence](#) to investigate the script hosting, determine it’s malicious and share evidence connecting the script to a known threat actor. Moving from Microsoft Defender to the stand alone Copilot experience allows analysts to connect to [Microsoft Sentinel](#) and [Microsoft Intune](#), surfacing a key piece of information in this serious incident—a device that was noncompliant with current security policies, missing a key compliance update that may have prevented this attack. In just a few minutes, Copilot surfaced the right information to provide remediation steps and advance organizational understanding to proactively prepare for (and hopefully prevent) future attacks.

## Augment critical expertise and upskill analysts

In our last demonstration video, we look at how security teams can utilize Copilot to stretch their skill sets, understand incidents more completely, and gain an extra hand when resources are hard to come by.

Watch the video: [User account research](#)

Copilot for Security enables junior security analysts to complete more complex tasks with skills like natural language to Kusto Query Language translation and malicious script analysis. In this ransomware incident, analysts used Copilot to generate a PowerShell script to validate the configuration of all affected systems. By then looking at a compromised device, analysts learn the source of the compromise and discover the device wasn’t compliant because it was mis-grouped when it was first assigned. With this information and more, surfaced and organized at the speed of AI by Copilot, analysts now have a more complete understanding of how the ransomware attack happened and how it can be prevented in the future. When a single ransomware incident can turn any organization upside down, security analysts can lean on Copilot for global threat intelligence, industry best practices, and tailored insights to outpace and outsmart adversaries.

## Learn more

[Join us online](#) at Microsoft Secure on March 13, 2024, to discover new ways to try Microsoft Copilot for Security. Experience world-class threat intelligence, end-to-end protection, and industry-leading, responsible AI through hands-on demos. And [register now](#) for our three-part webinar series “[Intro to Microsoft Copilot for Security](#).” The first of three webinars takes place on March 19<sup>th</sup> on the basics of generative AI, followed by the second webinar on March 26<sup>th</sup> about how to get started with Copilot for Security. And lastly, the third webinar will take place on April 2<sup>nd</sup> and delves into Copilot for Security best practices.

[Learn more](#) about how Microsoft Copilot for Security can help your team protect at the speed and scale of AI. And for more helpful tips and information, [view the Copilot for Security Playlist](#) on the [Microsoft Security Channel](#) on YouTube.

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 ([@MSFTSecurity](#)) for the latest news and updates on cybersecurity.

<sup>1</sup>[Microsoft Digital Defense Report 2023 \(MDDR\) | Microsoft Security Insider](#)

<sup>2</sup>[Randomized Controlled Trial for Microsoft Security Copilot](#), Benjamin G. Edelman, James Bono, Sida Peng, Roberto Rodriguez, Sandra Ho. November 29, 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](#)

