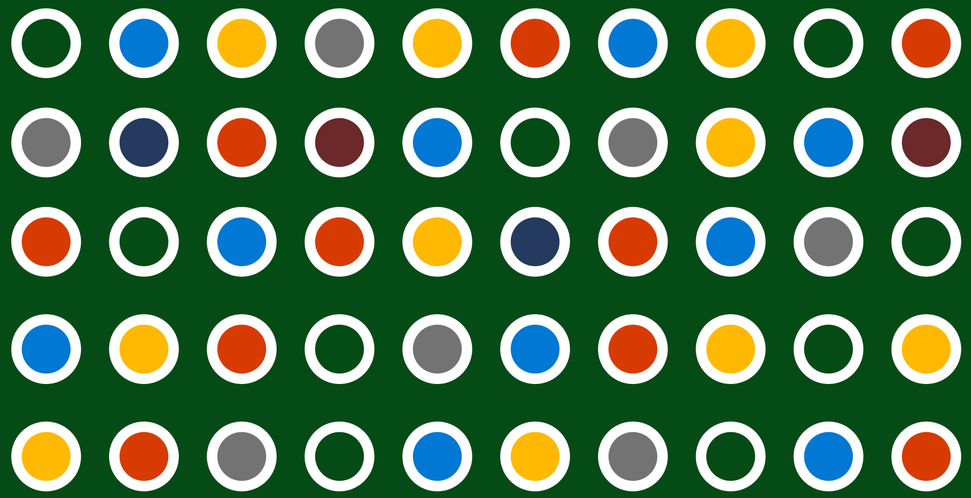
Microsoft Security

Microsoft Defender XDR

The solution to modern cyberattacks

1 Outpacing today's cybercrime tactics requires a new approach to security



The average organization uses 50 different security tools to manage their security operations.[2]

The magnitude of cybercrime in the current landscape is immense, and it has never been more critical for organizations to have a strong security operations center (SOC). Security teams have seen cyberattacks escalate relentlessly, growing in frequency, speed, and sophistication. Unfortunately, cyberattacks are also becoming more targeted as highly motivated malicious actors develop new ways to get to precisely the assets they're after.

Sobering statistics on the state of cybercrime validate the pressure SOC teams are feeling every day. Just a few of the challenges they face include:[1]

There are 4,000 password cyberattacks every second, a tenfold increase in 2023 alone.

There are more than 156,000 business email compromise (BEC) cyberattacks daily.

Human-operated ransomware cyberattacks have increased 200% since 2022.

In the race to protect their environments, security teams have had to react quickly to new cyberthreat vectors. In doing so, many have adopted a patchwork of siloed tools to cut off potential vulnerabilities in email, endpoints, identities, cloud applications, data, and even cloud workloads. As these disparate tools accumulate, the work of SOC teams can become overwhelmingly complex. The average organization uses 50 different security tools to manage their security operations.[2]

Security analysts with too many tools are forced to context-switch between isolated tools, then manually correlate a multitude of alerts. This leads to alert fatigue and keeps analysts stuck in the weeds, making it harder for them to see the bigger picture of sophisticated cyberthreats. Given these challenges, security teams are weathering an era of high stress and mounting turnover rates.

Cyberattacks across multiple domains raise the stakes for SOC teams

One of the most pressing concerns SOC teams must deal with is advanced campaigns carried out by nation-state actors. These cyberattacks are so well resourced that they can be difficult to stop completely once malicious actors have gained access to an organization's network.

Typically, these cyberattacks cross multiple security domains, are complex to detect, and are difficult to stop early. They tend to progress systematically, starting by identifying the path of least resistance within a compromised network, then moving laterally to exfiltrate target data or encrypt data to prepare for ransom. Some of the most damaging cyberattacks SOC teams are facing today include human-operated ransomware, BEC campaigns, and data exfiltration campaigns.

Cybercriminals frequently target the gaps between an organization's security tools to carry out these financially devastating cyberattacks. That's why it's more important than ever to find solutions that can unify disparate tools, allowing security teams to work faster.

A unified security operations platform not only closes gaps, but it also gives security teams the panoramic visibility they need to understand the full scope of a cyberattack. An end-to-end extended detection and response (XDR) solution such as Microsoft Defender XDR can help security teams achieve just that kind of visibility so they can prioritize alerts, respond quickly, and move from reactive to proactive mode.

2 XDR: Where modern cyberattacks meet their match

XDR solutions combine a variety of powerful tools to establish a holistic, simplified approach to security operations. Used together, these tools provide streamlined protection against advanced cyberattacks and give SOC teams a complete view of the cyberattack chain through a single dashboard. Having this end-to-end visibility simplifies investigating and responding to cyberthreats across multiple domains. The connectivity XDR creates also lays the foundation organizations need to use the most recent cybersecurity innovation: generative AI tools such as Microsoft Copilot for Security.

Endpoint detection and response (EDR) solutions alone can't provide security teams with the visibility, tools, and threat intelligence they need to protect against the advanced cyberthreats we're seeing today. XDR solutions provide a much more complete view of the cyberattack chain than EDR by correlating signals across endpoints, email, identity, software-as-a-service apps, and more. This allows security teams to see much more of the attack while reducing the need for manual investigating upfront. Then XDR takes it to the next level and automates responses with AI. Essentially, XDR platforms take in more signals than EDR and apply AI to take automated actions, making it a whole lot easier for security teams to respond to attacks.

EDR (Endpoint detection and response)

- Endpoint security only
- Siloed endpoint alerts
- Helpful against endpoint-specific cyberattacks

XDR (Extended detection and response)

- Holistic security and signal correlation across multiple domains
- Incident-based investigation and response across the environment
- Protects against advanced cyberattacks such as ransomware, BEC, and adversary-in-the-middle (AiTM)

Why Microsoft Defender XDR?

Enable rapid response with XDR-prioritized incidents. Remediate threats quickly with a complete view of the cyberattack chain and prioritized investigation and response at the incident level.

Disrupt advanced cyberattacks at machine speed. Stop lateral movement of advanced cyberattacks with advanced AI capabilities that automatically isolate compromised devices and user accounts.

Transform SOC productivity with the generative AI of Copilot. Respond to cyberthreats faster with step-by-step guidance, empower any analyst to build queries in natural language, and reverse-engineer adversarial scripts in seconds.

Unify security and IAM. Protect your hybrid identities and identity infrastructure from credential theft and other threats with seamless integration of Microsoft Entra ID and XDR.

Defender XDR has built-in AI, global threat intelligence, and advanced analytics to collect, correlate, and analyze security alerts at machine speed. That's something it does across entire digital estates, including endpoints, identities, email, cloud apps, data, and cloud infrastructure. It's unique among XDR solutions in that it's the first to deliver a unified security operations experience. It's also the first solution on the market to offer the built-in generative AI assistance of Copilot.

With these converged capabilities, Defender XDR provides improved threat detection, faster response times, and crucially, reclaimed time that SOC analysts can focus on proactive hunting, prevention, and reducing operational complexity and costs.

Defender XDR unifies a set of capabilities that will be critical for security teams going forward:

1. **Advanced cyberattack chain visibility.**
2. **Unified investigation and response.**
3. **Automation of data correlations, analysis, and response actions.**
4. **Broad intelligence and threat vector visibility.**
5. **Embedded generative AI with Copilot.**

3 Build a unified defense with Defender XDR

Defender XDR addresses the complexity of today's cyberthreats with simplicity and analytical acumen. Supported by AI and automation, it helps analysts make sense of alerts across endpoints, hybrid identities, email, collaboration tools, cloud applications, cloud workloads, and data. Then it automatically disrupts cyberattacks in progress.

By unifying a powerhouse of threat protection capabilities into a unified security operations platform, SOC teams gain a key advantage over bad actors: speed. In fact, Defender XDR comprises not only AI-enriched XDR, but also security and information event management (SIEM), threat intelligence, and a generative AI copilot, helping the SOC stay a step ahead.

Defender XDR gives organizations a superior set of protections that integrates with email security and identify and access management (IAM) as a critical preventative solution. It also gives SOC teams scalability with features that reduce the need for manual intervention, such as auto-healing capabilities for common issues and XDR-automated disruption to protect against ransomware and other advanced cyberattacks.

AI: AI-powered security operations enhanced with Copilot

XDR: Protect and defend across workloads

SIEM: Flexible detection across digital estate

Threat intelligence: Comprehensive cyberthreat insights

Efficiency that spans the entire cyberattack chain

Defender XDR is the only XDR solution that offers native, platform-level protection across every layer of the cyberattack chain. With capabilities such as proactively preventing malware and malicious links in Microsoft Teams, quarantining phishing emails, and safeguarding identities with conditional access, the platform ensures advanced prevention across the organization, allowing your team to:

- Reduce cyberattack surfaces with threat-based configuration recommendations and built-in vulnerability management.
- Automatically contain and remediate compromised assets.
- Use incidents to respond to cross-workload threats from a single portal.
- Speed up response with an experience designed for SOC efficiency.
- Integrate the security ecosystem via unified APIs and connectors.
- Protect seamlessly across first-party and third-party endpoints, identity, email, documents, cloud apps, data, and cloud workloads.
- Shift from detection to automatic disruption and containment of threats.

In the sections that follow, you'll delve into several ways that Defender XDR uniquely empowers SOC teams to be proactive against cyberattacks.

4 Respond rapidly with XDR-prioritized incidents

One important way that Defender XDR makes security operations more efficient is by automatically aggregating alerts and the associated context into incidents.

Incidents dramatically reduce the need for SOC teams to sift through random pieces of information and allow them to investigate and stop cyberattacks more efficiently. With an incident-based approach, they can bring the pieces of the puzzle together much more quickly.

Why are incidents important?

Incidents **run across all data sources** and correlate all alerts and signals associated with the same cyberattack.

The **incidents queue** is a central location for SOC teams to triage and prioritize cross-domain incidents.

The **incident graph** visualizes the cyberattack story, including impacted assets and associated evidence artifacts.

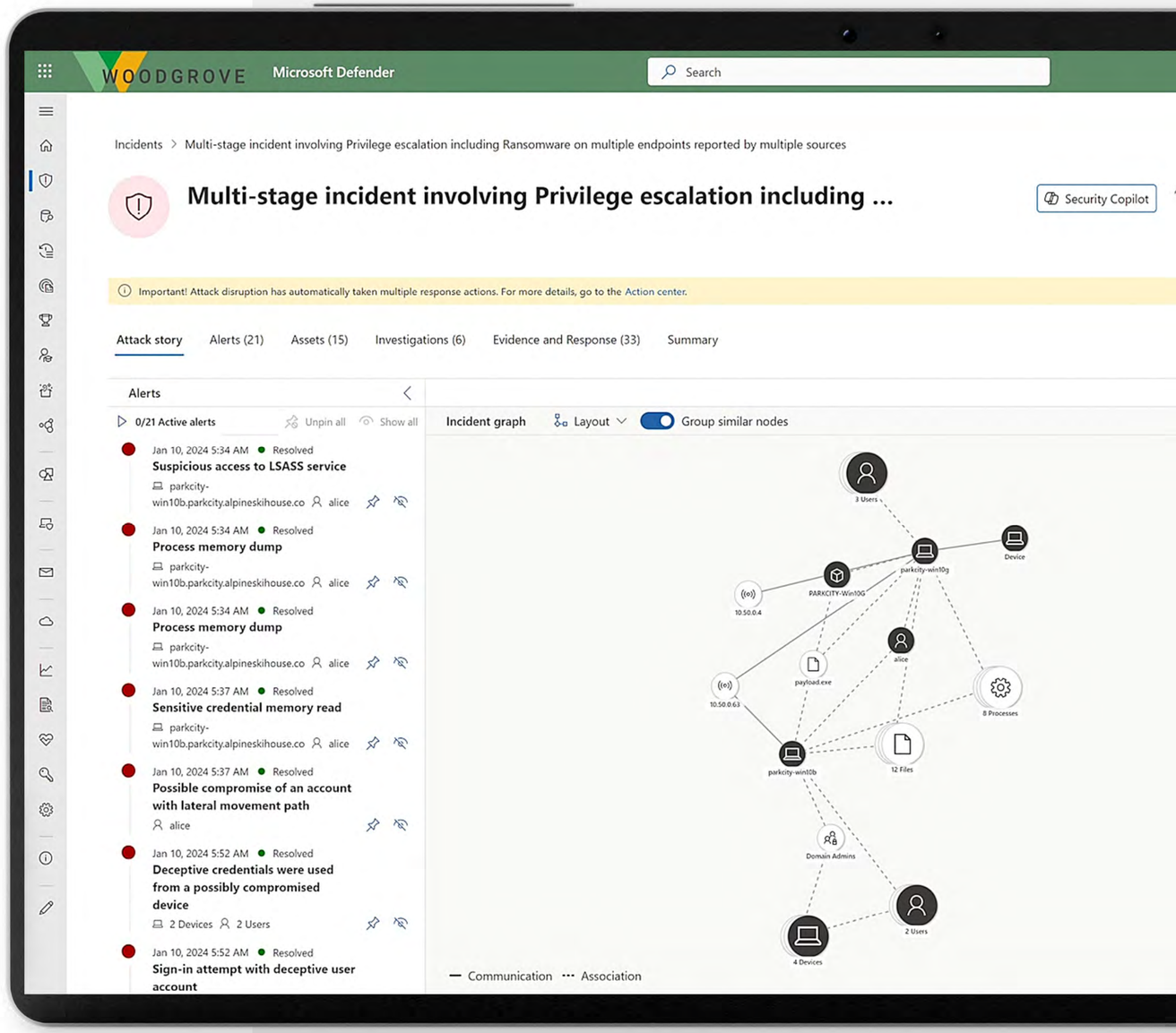
In the Microsoft Defender portal, analysts can work on entire incidents rather than individual alerts across all threats. From the incident queue, they can initially triage and prioritize incidents using details like incident severity, descriptive title, number of alerts, and affected assets.

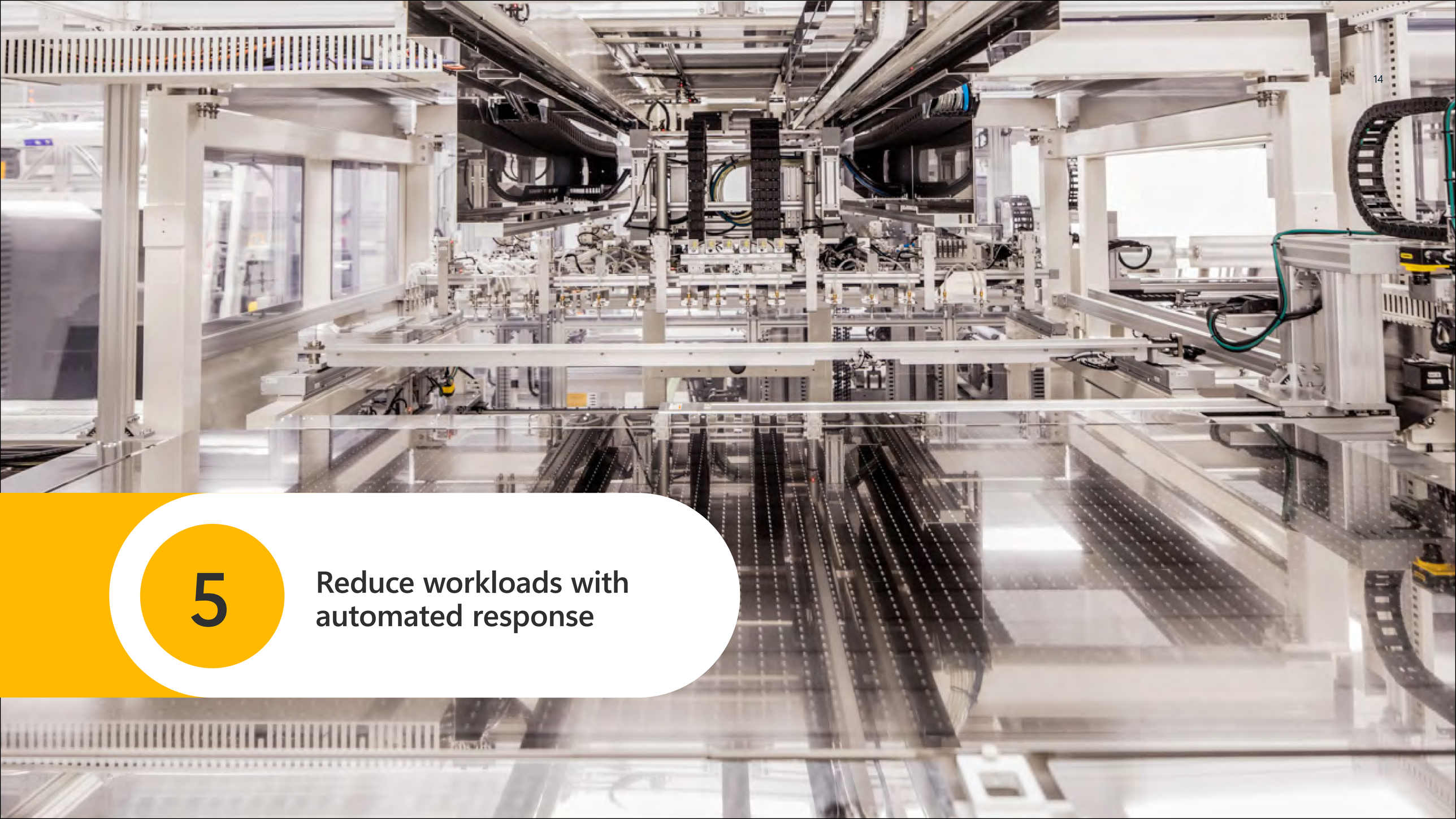
Special tags also provide critical context, like an incident category and potential threat attribution. For example, a ransomware incident with high severity should be addressed first. Looking into an incident, analysts can see an automatically generated incident graph telling them the full cyberattack story, including the impacted assets across devices and identities, as well as all evidence artifacts on each of them.

These features allow analysts to:

- Investigate and respond effectively with **incidents automatically correlated from alerts** and their associated information.
- Gain a **full picture of a cyberattack quickly** with an **incident graph** visualizing the progression of the cyberattack and all the entities involved.
- Understand the comprehensive incident scope easily and with **unified entity pages** for **easy entity inspection and pivoting**.

The **incidents queue** is a central location for SOC teams to triage and prioritize cross-domain incidents using details like incident severity, descriptive title, number of alerts, and affected assets.





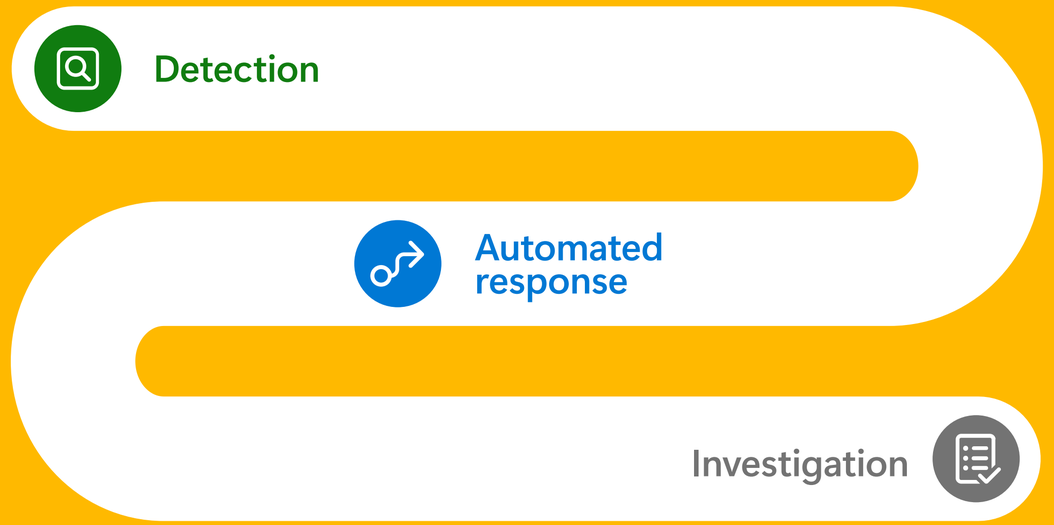
5 Reduce workloads with automated response

Defender XDR uses automated self-healing to investigate and remediate alerts across domains. As a result, 75% of alerts are automatically remediated. In the grand scheme of things, this means your team can focus on more complex cyberthreats. In addition, automatic responses are customizable. You can build automated responses to recurring alerts in your environment using custom detection in combination with Kusto Query Language queries.

Consider a scenario where a cyberattacker has compromised a single device using a weaponized Word document, implanting a backdoor. The Microsoft Defender portal provides a comprehensive view of the cyberattack story, revealing activity in Word followed by a PowerShell script that dropped a file and established persistence in the registry. These cases, though prevalent, demand significant time and effort when repeatedly dealt with.

Fortunately, Defender XDR automates self-healing for many such cyberthreats, triggering a fully automatic investigation and remediation flow as soon as the incident is created. The platform ensures that all incident history remains accessible for review if needed, saving valuable time and resources.

Automated response flow:



Detection

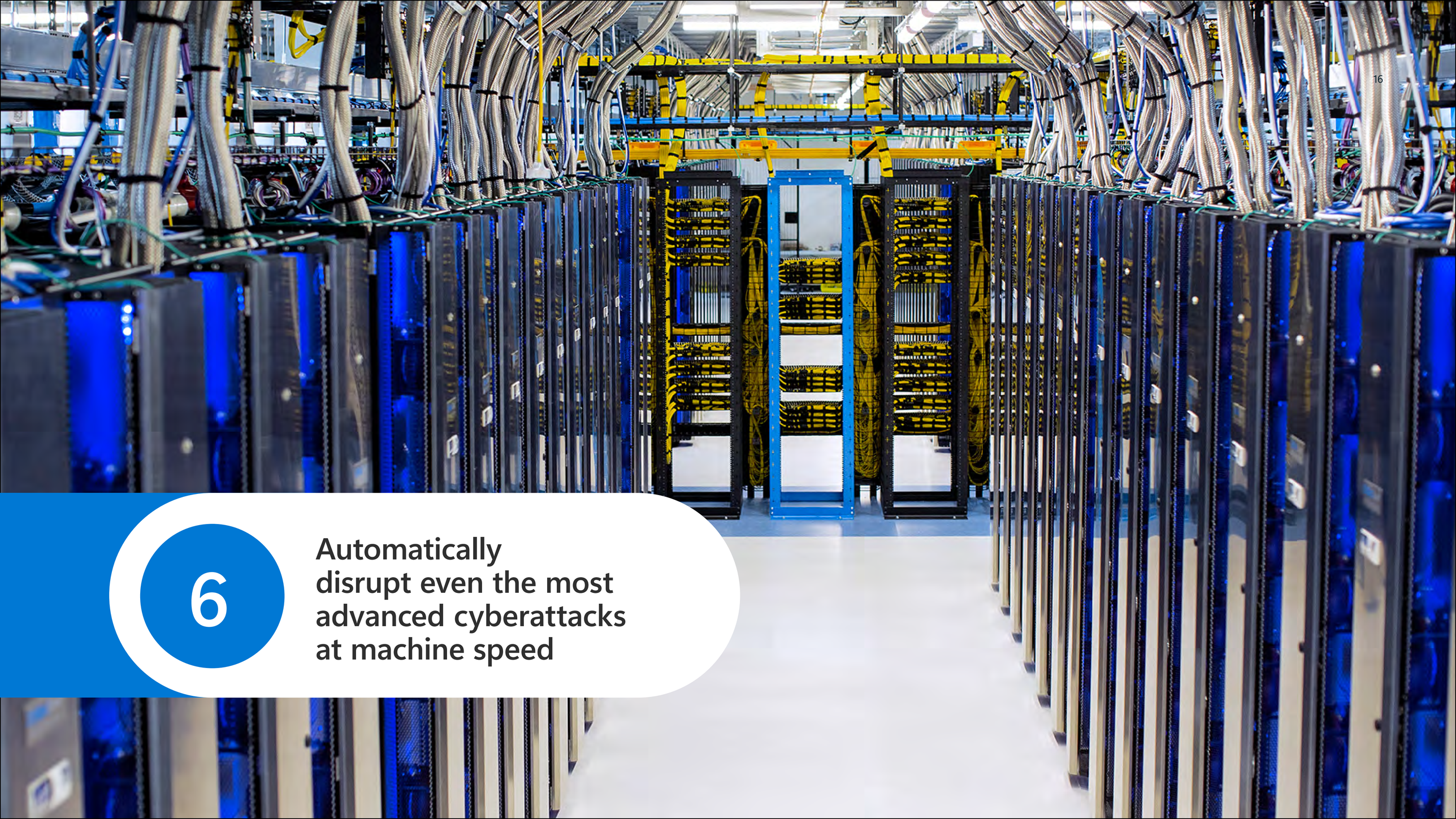
- A cyberattacker compromises a device using a weaponized document to install a backdoor
- An incident is created

Automated response

- Built-in self-healing removes malware and returns the environment to a healthy state

Investigation

- The incident is automatically resolved and removed from the queue
- All history is maintained for the analyst's review



6

Automatically disrupt even the most advanced cyberattacks at machine speed

3 minutes

is the average amount of time it takes to disrupt ransomware attacks with Defender XDR.

Automatic attack disruption is a powerful, out-of-the-box capability that can automatically stop the progression of some of the most sophisticated attacks early on. This is a technology that you won't find anywhere else. Defender XDR correlates a wide breadth of signals to gain insights and effectively detect in-progress cyberattacks. If an ongoing cyberattack such as ransomware or financial fraud is detected with a very high degree of confidence, the system instantly disrupts it by containing the affected assets. That can mean suspending an identity or isolating a device from connecting to any other resource on the network.

Automating this process changes the speed of response for most organizations, and therefore helps reduce the total cost of a cyberattack by limiting compromise and reducing the level of productivity that is impacted.

Automatic disruption in action

Here's an example of how automatic disruption works:

- **Detection**. XDR correlates signals from multiple sources into a single, high-confidence incident.
- **Classification**. The scenario is automatically classified, and assets controlled by the cyberattacker are identified.
- **Cyberattack disruption**. AI-powered automation isolates infected devices and suspends compromised accounts in real time.
- **Remediation**. XDR prevents lateral movement across the digital estate. The SOC team is in full control of investigating and remediating throughout.

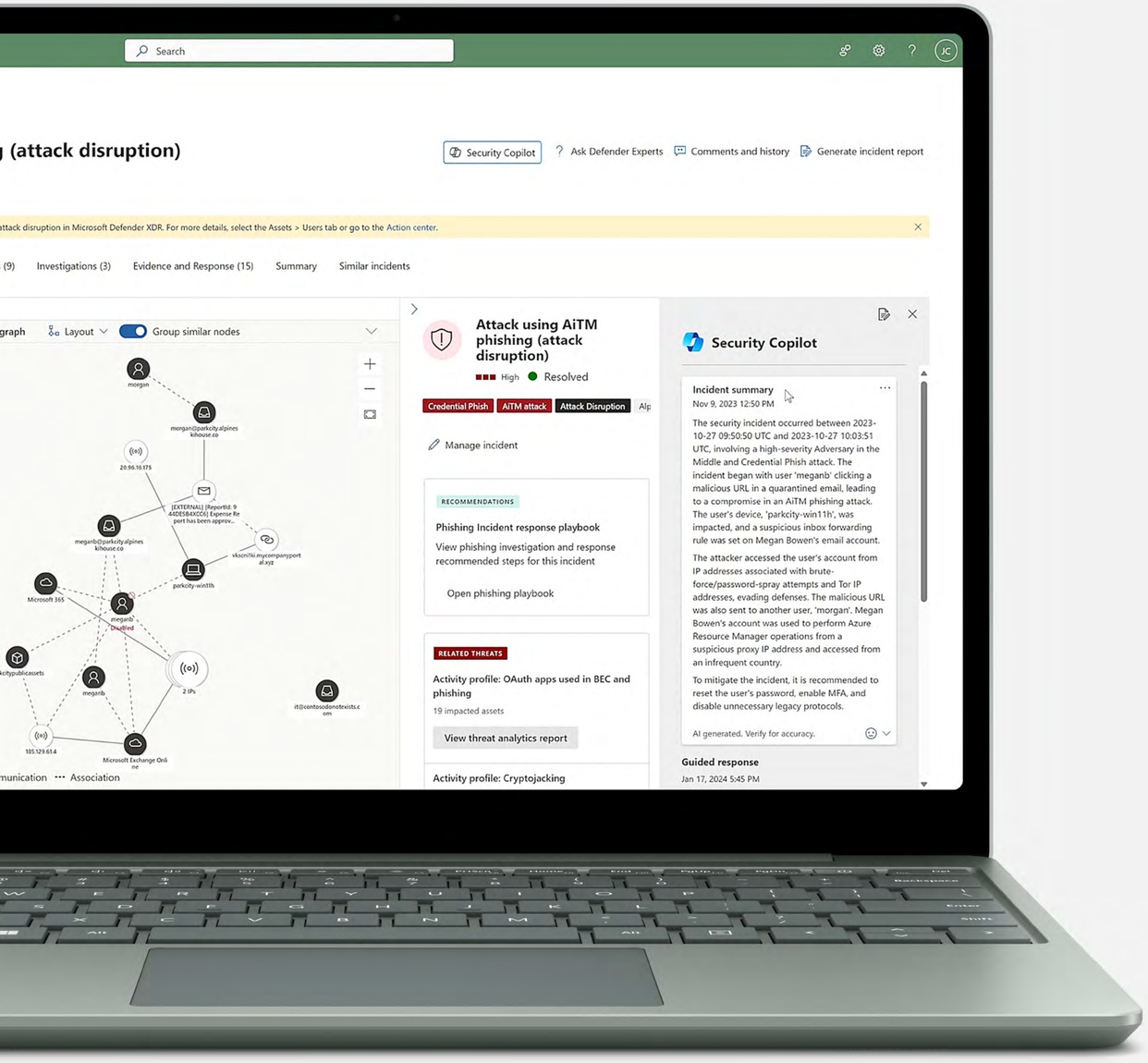
Scenario 2: Human-operated ransomware

Human-operated ransomware is an even more sophisticated example of a cyberattack Defender XDR can automatically disrupt. Here's how a human-operated ransomware attempt could play out:

1. **Initial access.** A bad actor steals credentials on the dark web, by phishing, or by other means.
2. **Credential theft—10 minutes in.** The criminal targets the local security subsystem service to do a credential dump.
3. **Reconnaissance—the first hour.** The cyberattacker searches the network topology to gain access to high-value devices.
4. **Lateral movement—1 to 1.5 hours.** The cyberattacker gains access to additional devices via remote desktop protocol (RDP), copying payloads with Server Message Block (SMB) and PSExec.
5. **Impact.** The cyberattacker deletes file backups and shadow copies and conducts mass file encryption.

XDR can automatically detect cyberattack behaviors such as lateral movement and credential harvesting, generate alerts for the security team, and take automatic response actions before step 5 ever materializes. For example, you might see the following:

7 Generative AI meets XDR: Copilot



Copilot is the first generative AI security product to help defend organizations at machine speed and scale. It comes embedded with Defender XDR and works seamlessly with the Microsoft Security suite, combining the most advanced GPT-4 model from OpenAI with a Microsoft-developed, security-specific model.

Copilot allows security professionals at all skill levels to easily avail themselves of global threat intelligence and be effective and fast at their job. It helps experienced and junior analysts alike enhance and grow their capabilities and skills while supporting efficient workflows and collaboration on security challenges.

Copilot offers step-by-step guidance tailored to the incident an analyst is working on, directing them on triage, investigation, containment, and remediation steps so they can save precious time and focus on the highest risks. It can also help security teams prepare customizable, ready-to-share reports that capture all the activities related to the incident.

Here are just some of the things security teams can do with Copilot:

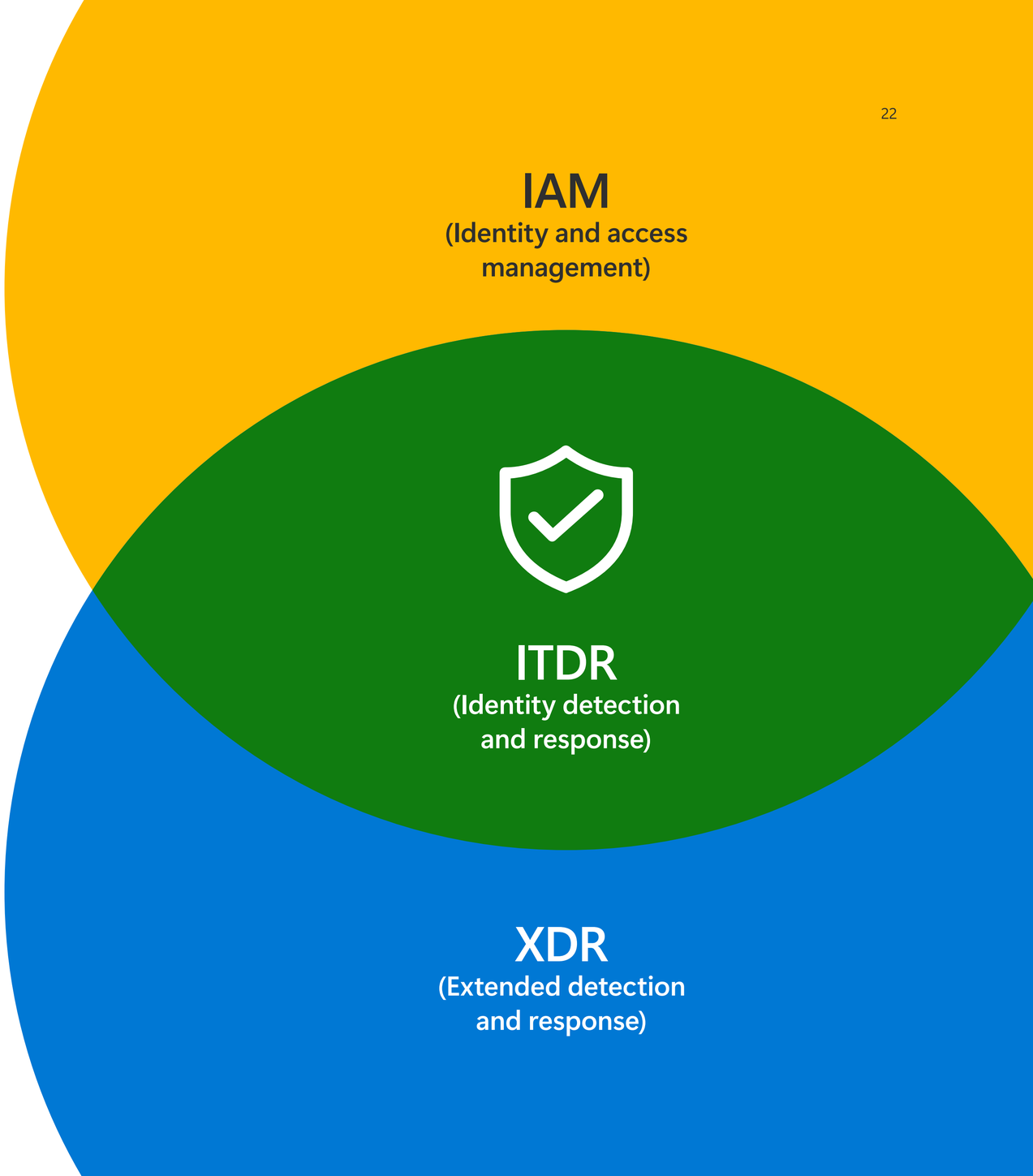
- **Investigate and respond to cyberthreats in a guided experience.** Summarize an incident, analyze the impact it can have, get guided recommendations, and generate reports for faster investigation and remediation.
- **Upskill security talent.** Give every team member access to new skills to complete complex tasks like threat hunting and reverse-engineering of malware.
- **Assess risks with AI-enriched threat intelligence.** Inquire in natural language about emerging cyberthreats and gain contextualized insights for rapid response to new and evolving cyberthreats.

8 Unify security and IAM with ITDR

Security professionals know that a single compromised user can lead to business shutdown—and the time when controlling digital access was as simple as setting up a perimeter has passed. Identity cyberattacks are intensifying, and it's virtually impossible to anticipate and address the unlimited number of access scenarios that can occur across an organization and its supply chain. This is especially true when it includes third-party systems, platforms, applications, and devices outside the organization's control, or when the organization has a hybrid operational model.

Broader solutions that encompass identity can help bring your cyberdefenses in line with modern security needs. To operate safely, you must secure access for every one of your customers, partners, and employees—and for every microservice, sensor, network, device, and database.

Identity detection and response (ITDR) is another critical component of modern cybersecurity. Bringing together elements of XDR and identity and access management (IAM), ITDR encompasses the solutions and strategies for protecting, detecting, and responding to identity-based threats. As a leader in both security and identity, Microsoft is uniquely positioned to help customers achieve more comprehensive identity protection both pre and post-breach.



9 Elevate your security with Defender XDR

Amplify your security team's efforts with the speed and simplicity of Defender XDR.

Defender XDR is the culmination of years of Microsoft innovation aimed at giving security teams an edge against cyberattackers. As part of the only unified security operations platform on the market that combines the capabilities of XDR, AI, SIEM, and IAM, and as the first XDR with built-in AI assistance, Defender XDR is designed to help your organization withstand the security challenges of the future. In a landscape rife with skilled bad actors possessing ample resources and relentless determination, a unified defense will continue to be the only defense.

Learn more about Defender XDR or start a free trial

Get more resources about making XDR part of your SOC

Additional resources:

Learn about the Microsoft unified security platform

Discover more about Copilot

Sources

[1] Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider

[2] February 2022 survey of 200 US compliance decision-makers (n=100 599- 999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research.