Microsoft Security

Supercharge your security operations with XDR

Improve your SOC efficiency with unrivaled threat intelligence and automated attack disruption of sophisticated attacks like ransomware with Microsoft 365 Defender



The current state of security operations

Growing frequency, speed, and sophistication of threats

Today's cybersecurity landscape continues to see an increase in attacks across all categories – more phishing, more ransomware campaigns, more identity-centric threats, while also growing in velocity. Attackers, on average, begin moving laterally only 72 minutes after a link is clicked in a phishing email. With the ransomware as a service (RaaS) gig economy on the rise, anybody can now get their hands on tooling developed by the cyberworld's most prolific nation-state attackers, increasing their success rates and ability to scale.



Attackers begin moving **72 minutes** after a link is clicked in a phishing email

Siloed solutions are slowing response

It's no longer enough to protect your endpoints and have an entirely separate email security strategy. Attacks are targeting the gaps between these siloed point solutions and crossing multiple domains, leaving defenders to have to manually correlate individual alerts together to detect a broader attack. Sophisticated attacks are moving across email and endpoints, all the way to user identities, cloud applications and your data. A point solution strategy leaves security analysts to manually correlate alerts together to identify attacks because they never see the big picture. This not only slows down detection, but investigation and remediation as well.

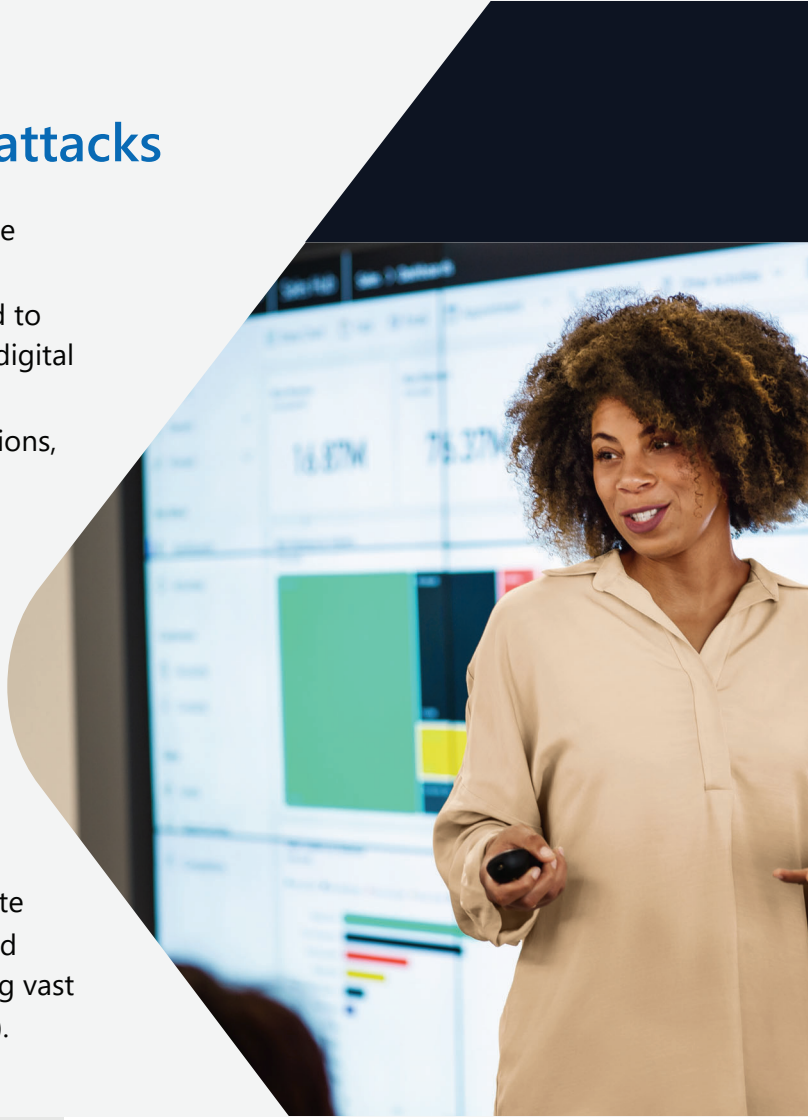
According to a Gartner study[3], security decision makers are becoming more dissatisfied with the operational inefficiencies and lack of integration that come with using a diverse range of traditional security tools and are instead seeking more effective and integrated solutions.



[3] Gartner: Top 5 Trends in Security Vendor Consolidation, 2022

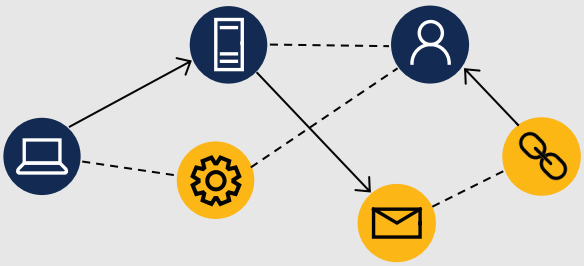
XDR—the answer to modern attacks

To tackle the nature of modern attacks crossing multiple domains and close security gaps, security teams need a unified solution that allows them to detect and respond to threats more efficiently across an organization's entire digital estate. Using powerful intelligence that automates the correlation and analysis of data, as well as response actions, XDR can help the Security Operations Center (SOC) transition from a reactive approach to a proactive defense strategy, while improving threat detection, response times, and most importantly freeing up time for the SOC analysts to focus on proactive hunting and prevention.

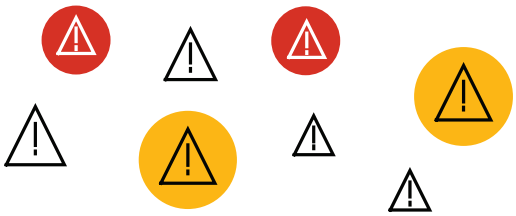


Extended Detection and Response (XDR)

solutions are designed to deliver a holistic, simplified, and efficient approach to protect organizations against advanced attacks. They give SOC teams a more complete view of the kill chain for more effective investigation and provide auto remediation across multiple domains using vast sets of intelligence and built-in artificial intelligence (AI).



VS.



XDR

- Holistic security and signal correlation across identity, email, endpoint, cloud app, data loss prevention (DLP) security, and more
- Incident-based investigation and response experience
- Protects against advanced attacks such as ransomware and business email compromise (BEC)

EDR

- Endpoint security only
- Siloed endpoint alerts
- Can only help fend off endpoint-specific attacks and lacks the big picture to help with advanced attacks

XDR gives security teams a new way to drive process and cost efficiency across their operations. As you consider an XDR solution for your organization, look for this critical set of capabilities:

01.

Advanced kill chain visibility and protection

To protect against advanced attacks, XDR solutions need to cover different asset types and unify security for critical threat entry points like email and identity, but also protect attack points further down in the kill chain including endpoints, cloud apps, and DLP data. By consolidating these data sources, XDR solutions correlate low level alerts into a single incident and help uncover the full kill chain of a sophisticated attack that would be overlooked by point security solutions.

02.

Unified investigation and response

Effective XDR solutions are designed to enable security analysts to be more effective. Incident-based investigation showing the end-to-end view of attack, contextual deep dives, and response playbooks with best practices, are all critical in making it easier for SOC teams to investigate and respond to attacks more efficiently.

03.

Automation

The increasing volume and speed of advanced attacks challenge the capacity of most security teams. XDR solutions provide automation in two ways. They use the breadth of their underlying signal and AI to provide built-in automation to respond to advanced attacks, but also provide options for companies to create custom automations. Both help scale the SOC scale.

04.

Broad intelligence and threat vector visibility

An XDR solution should incorporate intelligence. It should draw insights from a broad set of sources to analyze signals and better understand the threat landscape, as well as first-party research that informs prevention, detection, and protection mechanisms. A greater number and diversity of signals enhance the ability to see and understand more threat vectors, allowing the XDR solution to quickly identify an attack at an earlier stage, reduce the amounts of alerts and incidents, and enable the SOC team to respond to the latest threats more effectively.

05.

Optimized total cost of ownership

XDR enables vendor consolidation for organizations by integrating multiple, siloed security tools purchased into a unified solution. It removes the need to purchase from various vendors and the manual work needed to correlate signals. Instead, XDR provides a comprehensive solution for detection, response, and remediation, reducing acquisition costs and process overhead.

Supercharge your SOC experience with Microsoft XDR

Recognized as a leading[2] XDR solution, Microsoft 365 Defender delivers a unified investigation and response experience and provides native protection across endpoints, hybrid identities, email, collaboration tools, and cloud applications with centralized visibility, powerful analytics, and automatic attack disruption. With Microsoft 365 Defender, organizations can gain a broader set of protections including email security and identify and access management as critical preventative solutions, benefit from auto-healing capabilities for common issues, and scale SOC teams with XDR-automated disruption to protect against ransomware and other advanced attacks more effectively while safeguarding organizations' business continuity.

Microsoft 365 Defender provides defenders with a host of key capabilities to stay ahead of attackers, including:

1. Enable rapid response with XDR-prioritized incidents

Microsoft 365 Defender correlates native signals across multi-platform endpoints, hybrid identities, email, and collaboration tools, as well as SaaS apps and DLP insights to provide a complete view of the kill chain. This deep context allows SOC teams to investigate and respond at the incident level, making prioritization easy and remediation faster.



[2] Forrester New Wave™: Extended Detection and Response (XDR) Providers, Q4 2021.

Stay ahead of advanced attacks

Speed matters in a security analyst's daily operations. That's why Microsoft 365 Defender provides unified investigation and response designed to deliver the most efficient experience for SOC teams for faster response times.

For a streamlined investigation, Microsoft 365 Defender provides a visual graph of the attack, showing all impacted entities to help the SOC easily understand how the attacker went from compromise to target.

You can investigate alerts in the context of the entire incident and use in-product remediation playbooks to respond quickly—all as a connected experience without context switching. You can even dive deep with a single language for advanced hunting across all services. Additionally, to make sure automations help you respond even faster Microsoft 365 Defender supports real-time custom detections.



Enabling a data-centric SOC with DLP signal

Data loss prevention (DLP) is crucial for organizations to protect sensitive information and mitigate the risk of data loss or leakage. Integrating DLP alerts into the incident investigation experience gives SOC analysts an entirely new way to prioritize, based on the sensitivity of affected data.



Microsoft 365 Defender gives you the ability to understand the impact of a data breach quickly by correlating DLP alerts into the XDR incident view, the ability to conduct advanced hunting, as well as take remediation actions directly from the Microsoft 365 Defender portal. Adding data-centricity into your SOC experience will simplify the correlation of an attack to the detection of data leaks to understand the impact end-to-end faster and more effectively.

2. Disrupt advanced attacks at machine speed

Microsoft 365 Defender leverages the breadth of our XDR signal and our research-informed, AI-driven detection capabilities to identify advanced attacks like ransomware and it acts at the incident level with automatic attack disruption. Attack disruption contains in-progress attacks by automatically disabling or restricting devices and user accounts used in an attack—stopping progression and limiting the impact.

» Scale your SOC team with automatic containment of affected assets

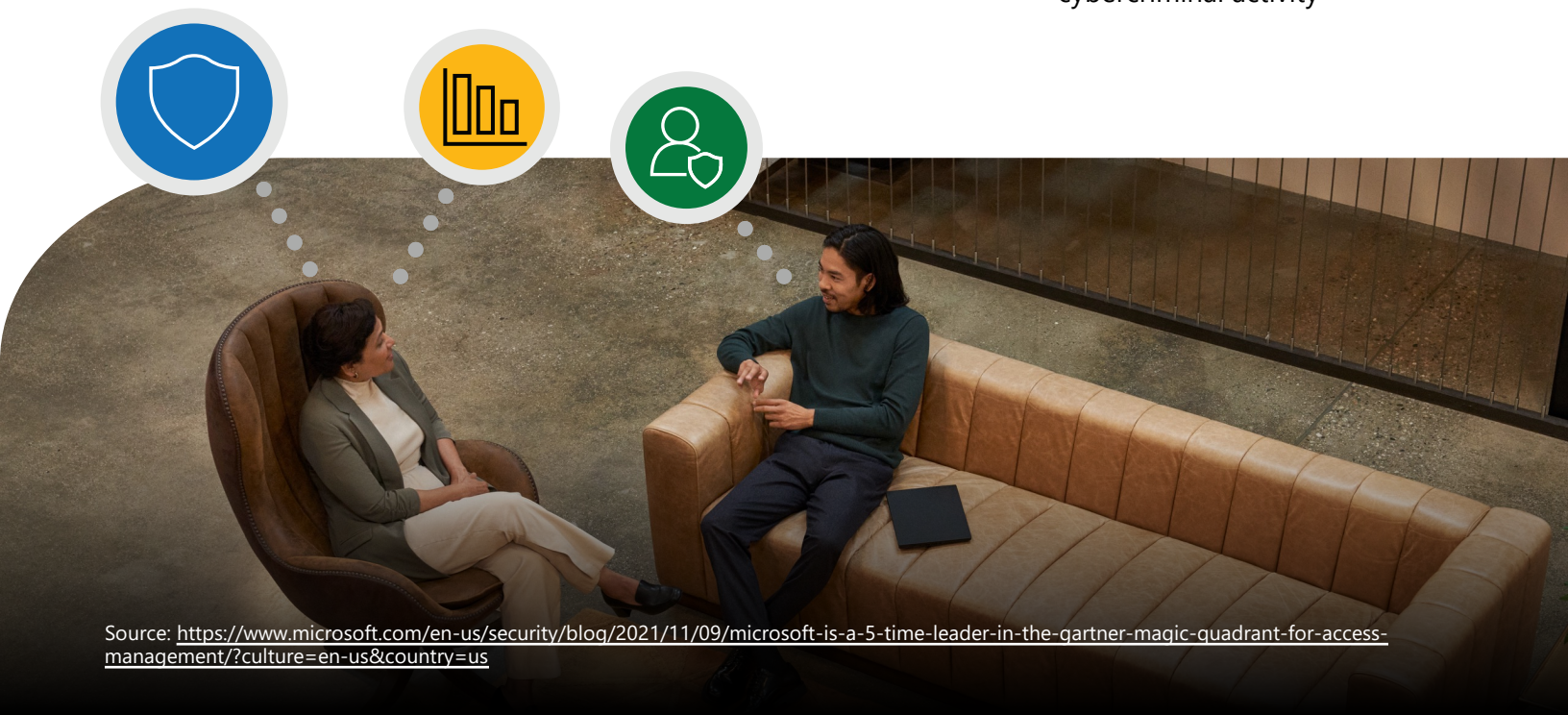
Automatic attack disruption is designed to contain attacks in progress by automatically disabling or restricting compromised devices and user accounts—stopping progression and limiting the impact to organizations. This is a big innovation; today most security teams can't respond fast enough to sophisticated attacks like ransomware or BEC campaigns and are typically reactive by cleaning up based on impact. With attack disruption, attacks are contained to a small number of assets, dramatically minimizing the impact and improving business continuity.

» Build efficiencies on the industry's widest insight into attack vectors

With 65 trillion daily signals and 8,500 security professionals, Microsoft security has visibility into more threat vectors than any other vendor. When paired with our natively integrated XDR platform, SOC teams have better real-time protection against sophisticated threats and can respond more quickly.

65 trillion signals

Analyzed daily by Microsoft to better understand and protect against digital threats and cybercriminal activity



Source: https://www.microsoft.com/en-us/security/blog/2021/11/09/microsoft-is-a-5-time-leader-in-the-gartner-magic-quadrant-for-access-management/?culture=en-us&country=us

3. Unify XDR security and identity access management

Identities are a critical threat vector because most attacks include compromised identities to move laterally. Microsoft combines the identity protection capabilities from our industry-leading[5] identity access and management platform with our XDR solution, providing a single integrated experience for protecting identities and defending against threats. This powerful combination offers preventative capabilities such as Conditional Access, that are built directly into the identity platform Azure AD, while providing the full breadth of threat protection capabilities of Microsoft's XDR. This gives you a unified solution protecting hybrid user and workload identities, as well as the underlying identity infrastructure.

» Create operational efficiencies and reduce cost

Microsoft 365 Defender provides a unified experience for protecting identities on-premises and in the cloud and combines those signals with all the other sources for the full XDR view of the attack kill chain, creating significant efficiencies for the SOC. In addition, buying Microsoft E5 Security is a cost-effective approach to consolidating vendors getting both industry leading identity and industry leading XDR capabilities in a single package.

» Best of breed, unified into a leading XDR solution

In addition to being a leading identity solution provider, the other solutions unified within Microsoft's XDR are best of breed and an endpoint security solution is often the starting point for an XDR discussion. Gartner named **Microsoft a Leader in the 2022 Gartner® Magic Quadrant for Endpoint Protection Platforms with multi-platform protection** including Linux, macOS, iOS, and Android. [3]

How Microsoft 365 Defender improves the SOC's efficiency with a deeply integrated protection stack

>80%

alert reduction in the SOC queue [4]

>75%

of work items resolved with automation [4]

242%

return on investment [4]

[3] Source: https://www.microsoft.com/en-us/security/blog/2023/03/02/microsoft-is-named-a-leader-in-the-2022-gartner-magic-quadrant-for-endpoint-protection-platforms/

[4] Forrester: The Total Economic Impact™ of Microsoft 365 Defender

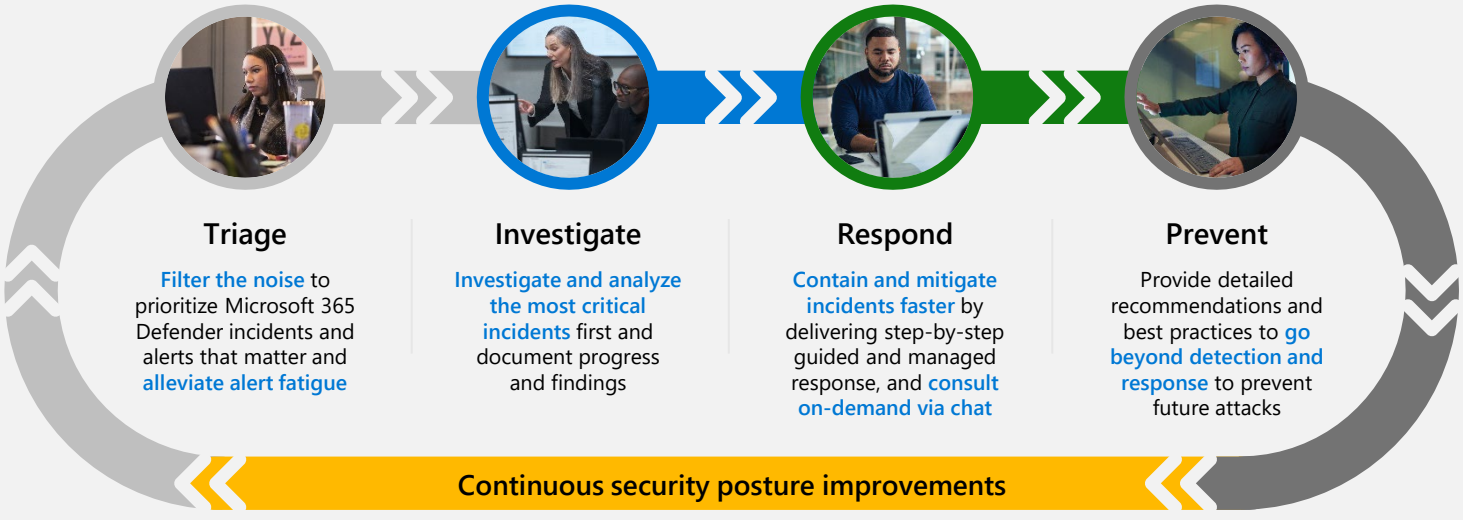
Microsoft Defender Experts for XDR

The cybersecurity industry is grappling with an ongoing shortage of skilled experts. Even when talent is available, access to highly skilled expertise remains a challenge. This predicament has made a robust, managed security service an essential consideration. **A managed extended detection and response (MXDR)** service provides a comprehensive solution to this problem by bridging the gaps in expertise, efficiency, and scope.

- **Expertise**: Organizations want to make their SOC teams operate better as fast as possible, however, their teams may lack the skill sets needed to thoroughly investigate incidents or support 24/7 coverage.
- **Efficiency:** Organizations strive for greater efficiency, but their teams face alert fatigue and the need to prioritize essential tasks. They seek assistance beyond resolving minor incidents and false positives and need to reduce the volume of alerts and incidents they see over time.
- **Scope:** Many organizations have adopted EDR but are not getting visibility beyond the endpoint. MXDR's advantage is the ability to visualize and correlate threat data across domains and deliver human-led expertise quickly to help organizations accelerate or augment their SOC capabilities.

Microsoft Defender Experts for XDR is our first-party MXDR service that extends beyond the endpoint to protect across Microsoft 365 Defender using leading end-to-end protection and expertise to help security teams triage, investigate, and respond to incidents to stop attackers and prevent future compromise.

How Defender Experts for XDR works



Defender Experts for XDR provides leading end-to-end protection and expertise to deliver:

- **Unrivaled coverage:** The broadest service coverage across our XDR solution.
- **Leading human and machine expertise:** Backed by AI-powered Microsoft Threat Intelligence to catch threats others miss.
- **Unified industry-leading solution:** With a turnkey, seamless experience across industry-leading products and services.

Industry recognition

Forrester New Wave™: Extended Detection and Response (XDR)

Microsoft was named a Leader in the inaugural Forrester New Wave™: Extended Detection and Response (XDR), Q4, 2021,[5] receiving one of the highest scores in the strategy category. **Microsoft 365 Defender** was rated as "differentiated" in seven criteria including detection, investigation, and response, and remediation.

Figure 2
Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

MITRE Engenuity ATT&CK® Evaluations

For the fourth consecutive year, Microsoft 365 Defender demonstrated its industry-leading protection in MITRE Engenuity's independent ATT&CK® Enterprise Evaluations[6], showcasing the value of an integrated XDR-based defense. Microsoft demonstrated complete visibility and analytics across all stages of the attack chain.

Gartner

Microsoft is named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms and was rated highest on the ability to execute.[7,8] The Microsoft 365 Defender portal unifies best-of-breed security for endpoints, email, identities, and SaaS applications into a comprehensive XDR experience.

[5] The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

[6] MITRE Engenuity ATT&CK® Evaluations, Wizard Spider + Sandworm Enterprise Evaluation 2022, The MITRE Corporation and MITRE Engenuity.

[7] 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, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. Gartner is a registered trademark and service mark and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

[8] Gartner Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Chris Silva. 31 December 2022.

What customers are saying



ING takes advantage of the full scope of Microsoft 365 Defender to reimagine banking for a digital audience. The IT team can now better recognize phishing attempts and block them right from the start, building on its own intelligence by using query data to identify additional risks.

> "A single layer of detection isn't strong enough and is prone to some level of false positive… On the other hand, Microsoft 365 Defender correlates signals across endpoints, email, documents, identity, apps, and more."

> "We consider it a game-changer that Microsoft 365 Defender combines signals for threat hunting because it connects data from the identity and endpoint perspectives to pinpoint truly malicious events."

—Krzysztof Kuźnik, Product Owner at ING

G&J Pepsi-Cola Bottlers had deployed and benefited from Microsoft 365 Defender, which was the base G&J Pepsi needed to expand security over after recovering from the ransomware attack. Microsoft 365 Defender is uniquely able to help detect and respond to ransomware threats like the one G&J Pepsi experienced in 2021.



> "Having a strong security posture focused on protecting physical security and the security of devices, identities, and data is critical to company stability and were key components to a successful defense against cyberattacks."

—Eric McKinney, Enterprise Infrastructure Director at G&J Pepsi-Cola Bottlers

Summary

XDR emerges as a revolutionary approach to combat cyber threats and empowering SecOps to do more with a unified detection and response experience. Advanced attacks such as ransomware are pushing the boundaries and highlighting the shortcomings of siloed security solutions. The need for a more comprehensive and integrated solution has never been more apparent, and XDR provides exactly that.

Microsoft 365 Defender is recognized as a leading XDR solution and defined by its unified protection across endpoints, hybrid identities, email, collaboration tools, and cloud applications. Beyond incident-based investigation and response, it offers centralized visibility, powerful analytics, and automatic attack disruption, to drive SOC efficiencies and ensure that organizations have access to the latest intelligence and research-based protections.

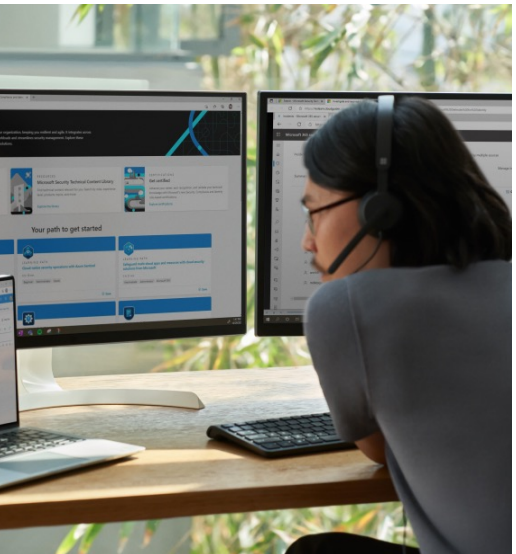
Lastly, Microsoft 365 Defender is the only XDR that combines a leading identity and access and management platform with its XDR solution, for a single, integrated experience to protect identities and defend against threats, creating significant total cost of ownership benefits across process efficiencies, as well as consolidating costs with a single vendor.

XDR is a must-have for any modern security strategy, so SOC teams are well positioned to keep up with the evolving attack landscape and aided by an intelligence-driven and unified approach to threat protection.











Get started today



Visit our website to learn more about Microsoft 365 Defender



Ready to get started?
Sign up for a free trial



Documentation for a step-by-step guide on how to work with Microsoft 365 Defender



Stay up-to-date with our latest innovations, features updates, and best practices and subscribe to the Microsoft 365 Defender Blog



Do you love learning videos? Head to the Microsoft 365 Defender Virtual Ninja Show for deep dives with our product teams

© Microsoft Corporation. All rights reserved. This material is provided for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED.