Seeing the Whole Picture:
How XDR Unifies Detection and Response

proarch Microsoft

The current state of security operations

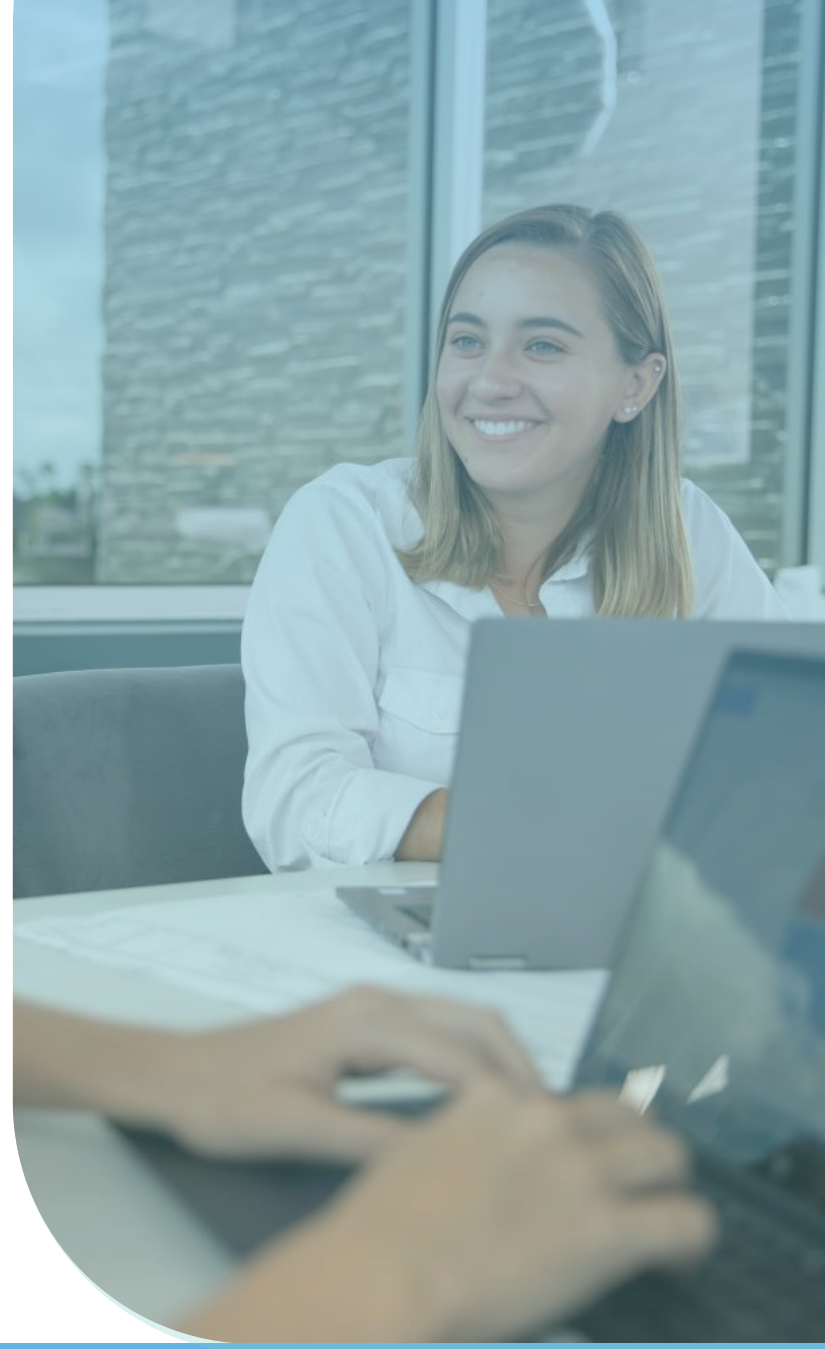
Growing frequency, speed, and sophistication of threats

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. 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.

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, 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.[1]



[1]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, 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).

Endpoint detection and response (EDR) solutions are not enough

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)

vs.

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

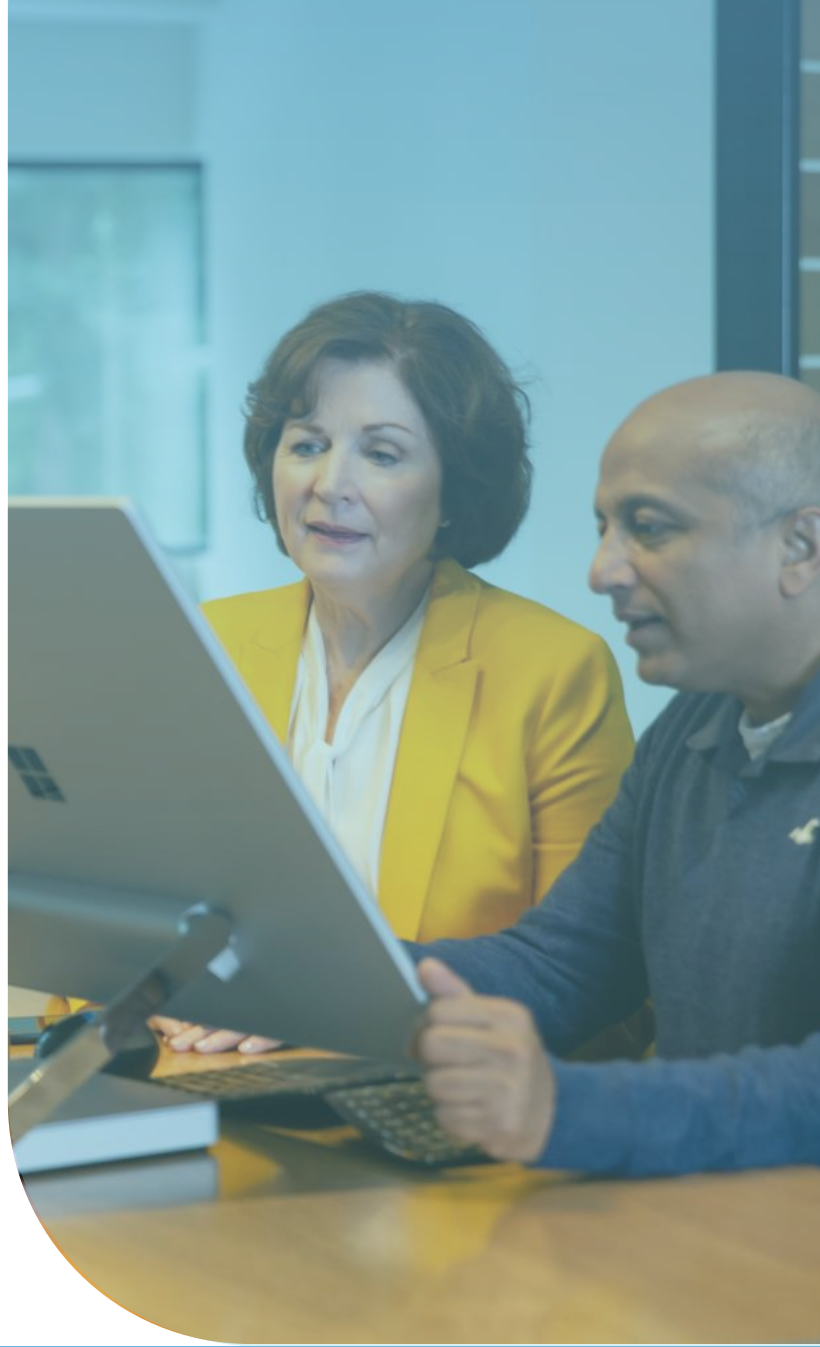
As you consider an XDR solution for your organization, our security experts can provide an assessment of your current environment and give you a new way to drive process and cost-efficiency across your operations. We focus on the following critical set of capabilities.

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 otherwise 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

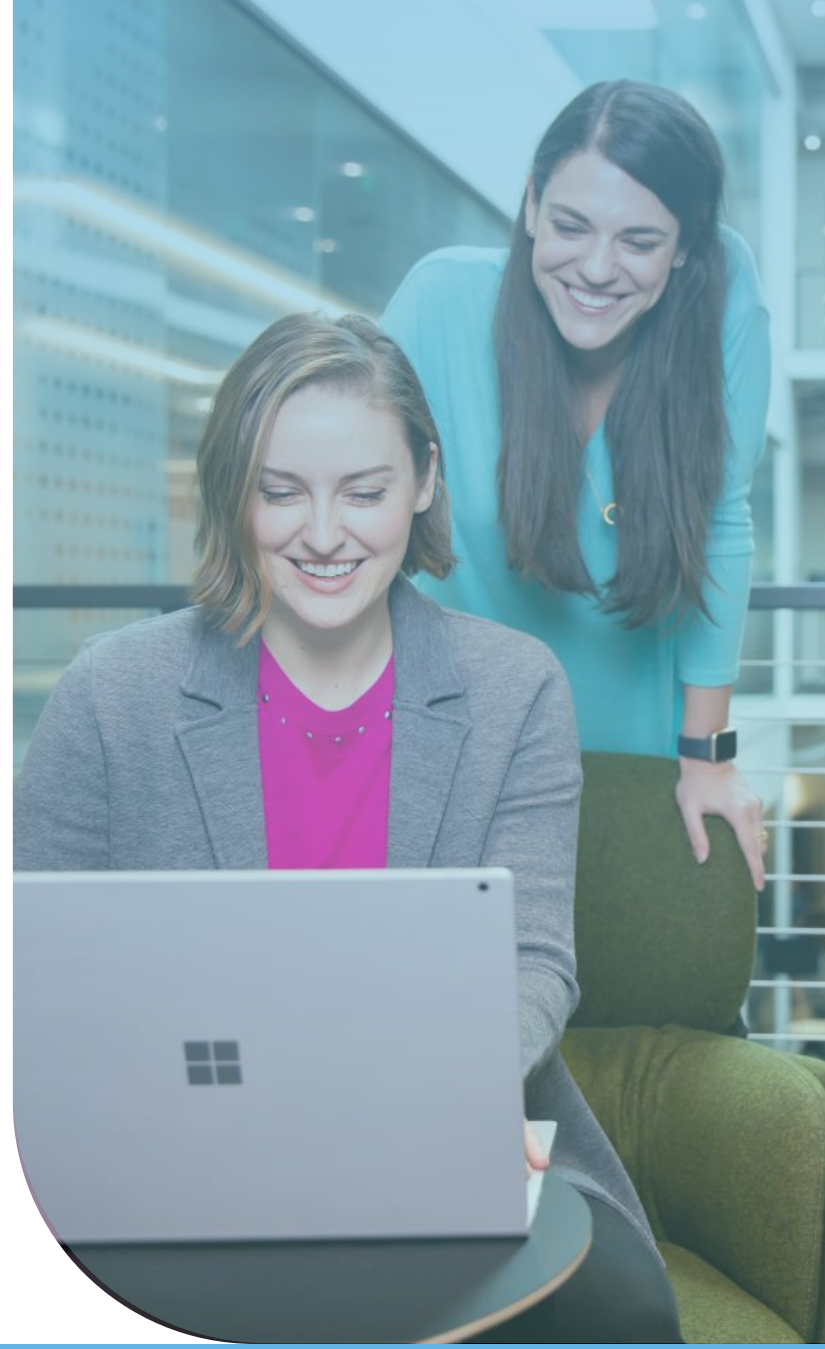
The increasing volume and speed of advanced attacks challenge the capacity of most security teams. XDR solutions provide automation in two ways. They use the breadth of their underlying signal and AI to provide built-in automation to respond to advanced attacks, but also provide options for companies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

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. Improved 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 365 Defender, the Microsoft XDR solution

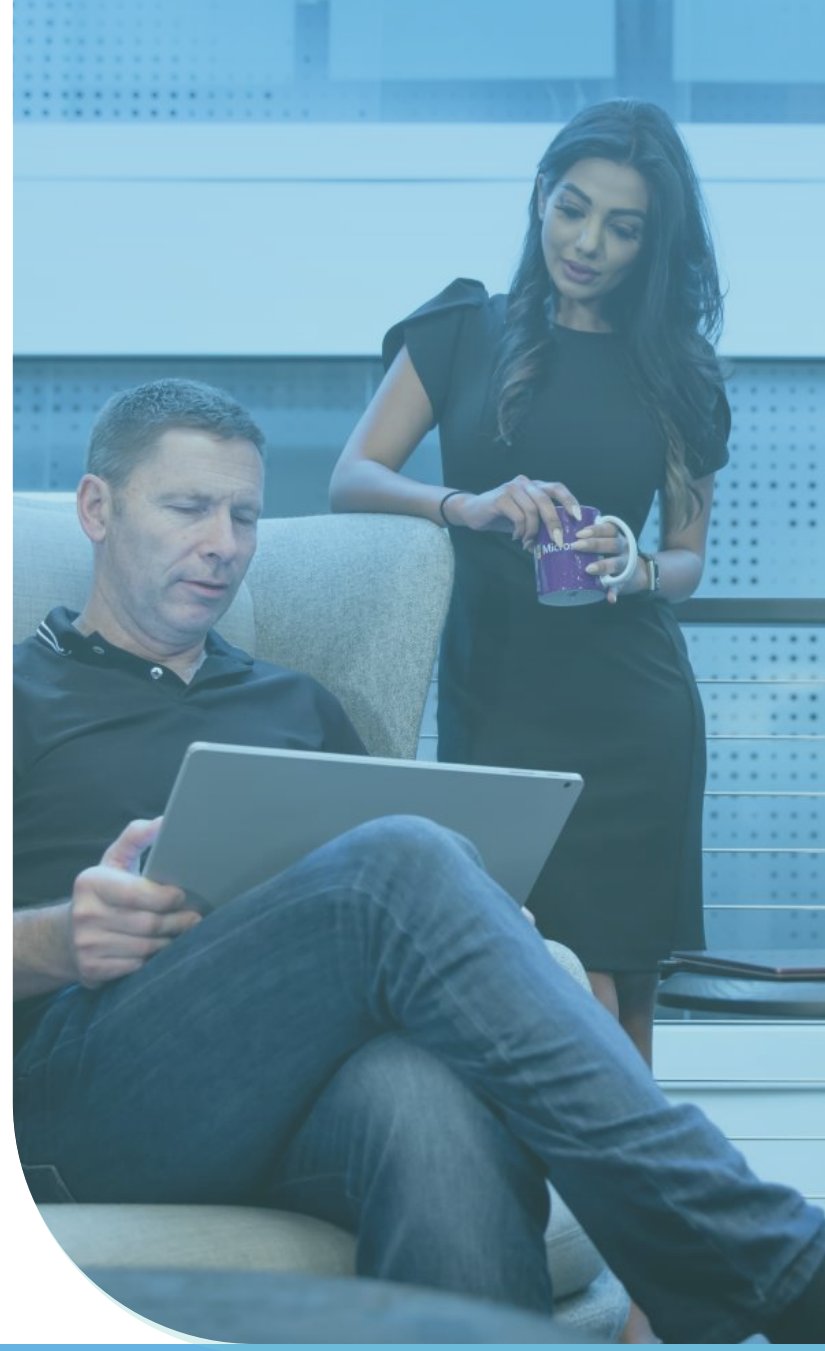
As a security advisor to businesses like yours, we recommend Microsoft 365 Defender. It delivers a unified investigation and response experience and provides native protection across endpoints, hybrid identities, email, collaboration tools, and cloud applications with centralized visibility, powerful analytics, and automatic attack disruption. With Microsoft 365 Defender, you gain a broader set of protections including email security and identify and access management as critical preventive solutions. You'll also 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, so you can:

Enable rapid response with XDR-prioritized incidents

1

Microsoft 365 Defender correlates native signals across multiplatform 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.



Stay ahead of advanced attacks

The ability to correlate alerts efficiently is central to 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 having to switch context. 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.

Enable 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, and the ability to 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 so you can understand the end-to-end impact faster and respond more effectively.

Disrupt advanced attacks at machine speed

2

Microsoft 365 Defender leverages the breadth of the Microsoft XDR signal and research-informed, AI-driven detection capabilities to identify advanced attacks like ransomware and provides automatic response 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 8,000+ security professionals,[3] Microsoft security has visibility into more threat vectors than any other vendor. When paired with Microsoft's natively integrated XDR platform, SOC teams have better real-time protection against sophisticated threats and can respond more quickly.

65 trillion signals

synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity[3]

3. Plan for the future with Microsoft Security | Microsoft Security Blog

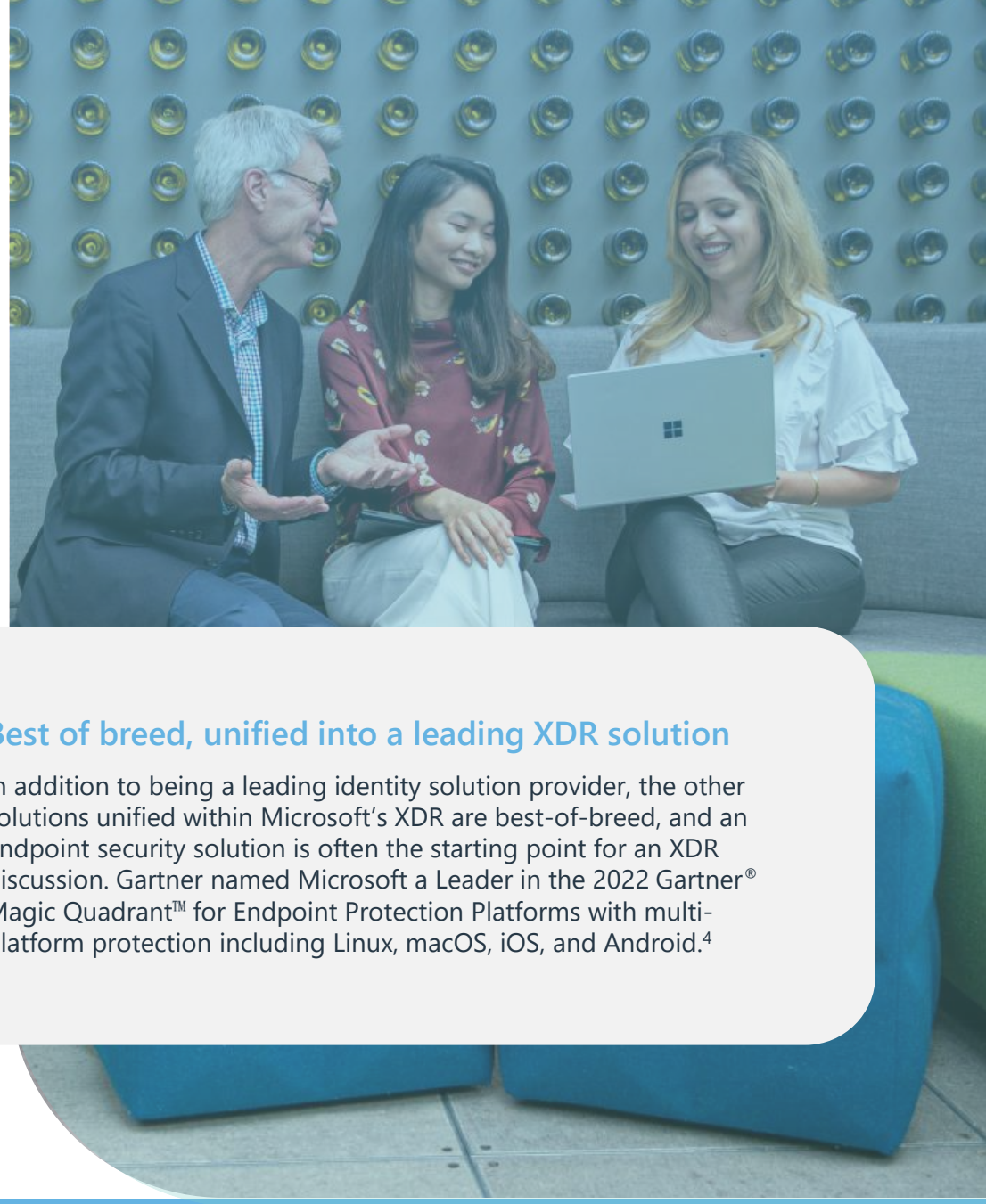
Unify XDR security and identity access management

3

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[4] 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 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 that protects 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 365 Defender is a cost-effective approach to consolidating vendors, delivering 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.[4]

4. Microsoft, "Microsoft is named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms," March 2, 2023

What businesses are saying

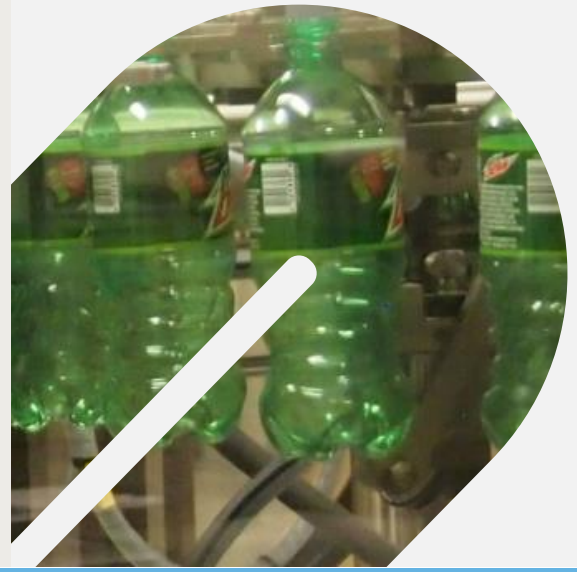
ING takes advantage of the full scope of Microsoft 365 Defender to reimagine banking for a digital audience. The IT team can now better recognize phishing attempts and block them right from the start, building on its own intelligence by using query data to identify additional risks.

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 deployed 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 has emerged as a revolutionary approach to combating 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 is 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, all while 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, aided by an intelligence-driven and unified approach to threat protection.

Get the threat protection you need today

ProArch is a trusted Microsoft Solutions Partner helping businesses protect their IT and OT systems with top-notch Managed Detection and Response (MDR) services.

Powered by Microsoft Defender and Sentinel, our solution monitors your environment 24/7, quickly detects and resolves threats, and cuts down alert noise by up to 99%, so you can focus on what really matters.

What sets us apart is our commitment to long-term security—offering not just immediate protection but ongoing guidance, strategic improvements, and access to senior security experts to keep your entire attack surface secure.

Ready to get started?

Contact us today