Supercharge your security with Managed EDR

Improve your Security efficiency with unrivaled endpoint protection, threat intelligence and automated disruption of sophisticated attacks like ransomware with Managed Microsoft 365 Defender for Endpoint from Ekco.

The current state of security operations

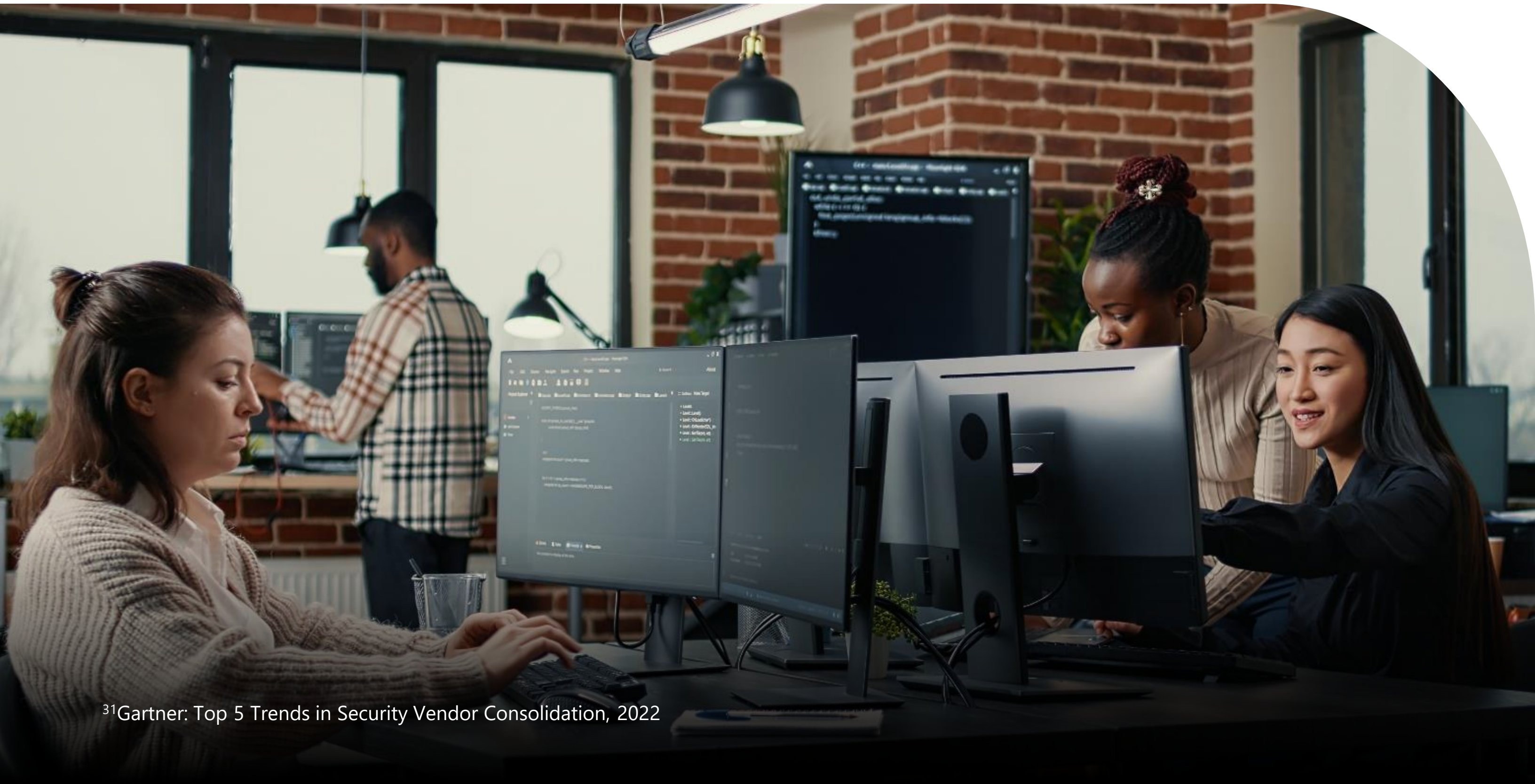
Growing frequency, speed, and sophistication of threats

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

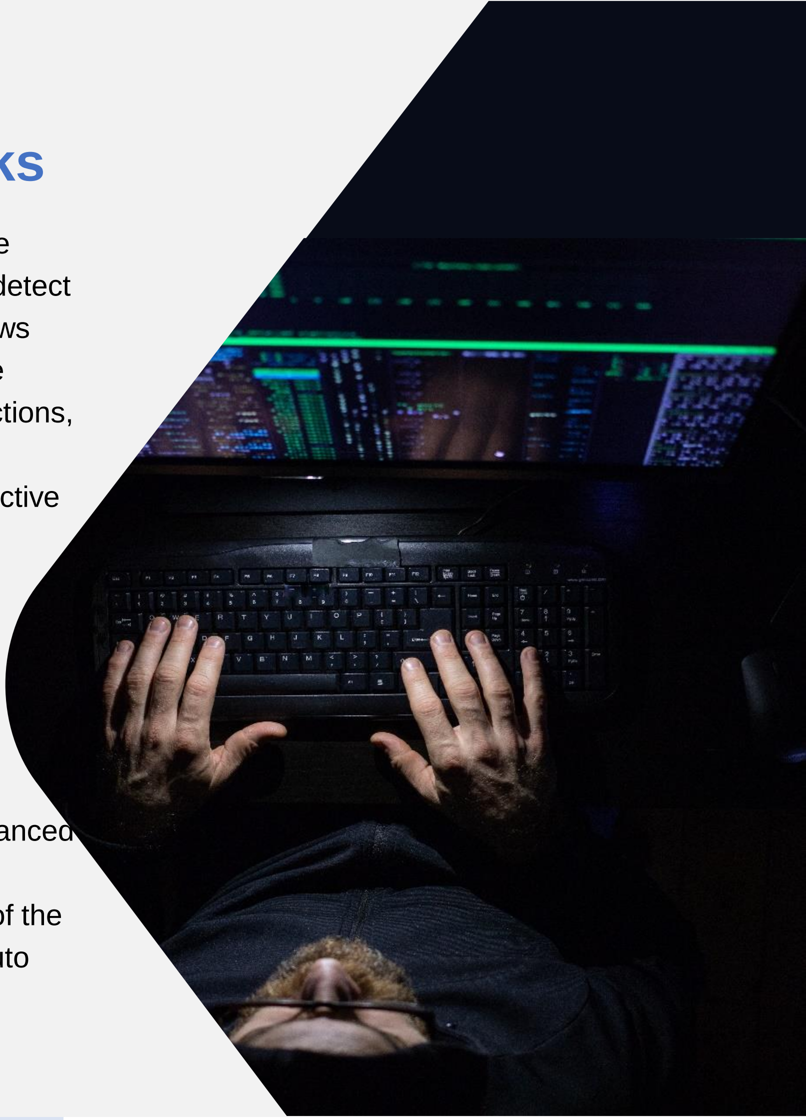
It's no longer enough to protect your endpoints. Attacks are targeting the gaps between these siloed point solutions and crossing multiple domains. Sophisticated attacks are moving across email and endpoints, all the way to user identities, cloud applications and your data. A basic endpoint protection strategy leaves gaps in your defences that attackers can and do slip through. This not only leaves your company exposed, but unless you have threat detection, investigation and remediation available to you, can be difficult to stop.

According to a Gartner study, IT 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 managed solutions.[1]



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

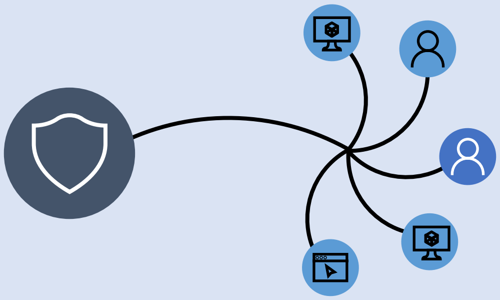
Managed EDR
The answer to modern attacks



To tackle the nature of modern attacks crossing multiple domains, IT teams need a solution that allows them to detect and respond to threats. Working with a partner that allows them to access powerful intelligence that automates the correlation and analysis of data, as well as response actions, XDR can help them transition from
a traditional protection-only reactive approach to a proactive defense strategy, with the addition of threat detection, incident response times, and most importantly freeing up time for the in-house IT team to focus on driving their business forward.

Endpoint Detection and Response (EDR)

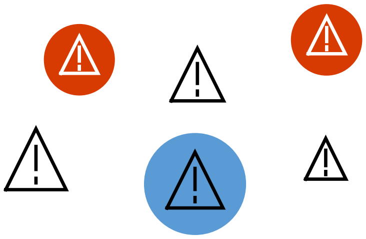
solutions are designed to deliver a holistic, simplified, and efficient approach to protect endpoints against advanced attacks. Linking EDR with threat detection and hunting capabilities gives organisations a more complete view of the kill chain for more effective investigation and provide auto remediation across multiple domains using vast sets of intelligence and built-in artificial intelligence (AI).



Managed EDR

- Access to a 24/t Security Operations Centre (SOC) staffed by experts
- Incident-based investigation and response experience
- Protects against advanced attacks such as ransomware and business email compromise (BEC)

VS.



Endpoint Detection and Response (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

Managed EDR gives IT teams a new way to drive process and cost efficiency across their operations. As you consider an managed security solution for your organisation, look for this critical set of additional capabilities you gain access to:

01.

Attack Surface Reduction

The attack surface reduction set of capabilities provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs.

02.

Next Generation Protection

To further reinforce the security perimeter of your network, Microsoft Defender for Endpoint uses next-generation protection designed to catch all types of emerging threats.

03.

Core Defender Vulnerability Management

Built-in core vulnerability management capabilities use a modern risk-based approach to the discovery, assessment, prioritization, and remediation of endpoint vulnerabilities and misconfigurations.

To further enhance your ability to assess your security posture and reduce risk, a new Defender Vulnerability Management add-on for Plan 2 is available

04.

Endpoint Detection and Response

Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars. Advanced hunting provides a query-based threat-hunting tool that lets you proactively find breaches and create custom detections.

05.

Auto-Investigation and Remediation

In conjunction with being able to quickly respond to advanced attacks, Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

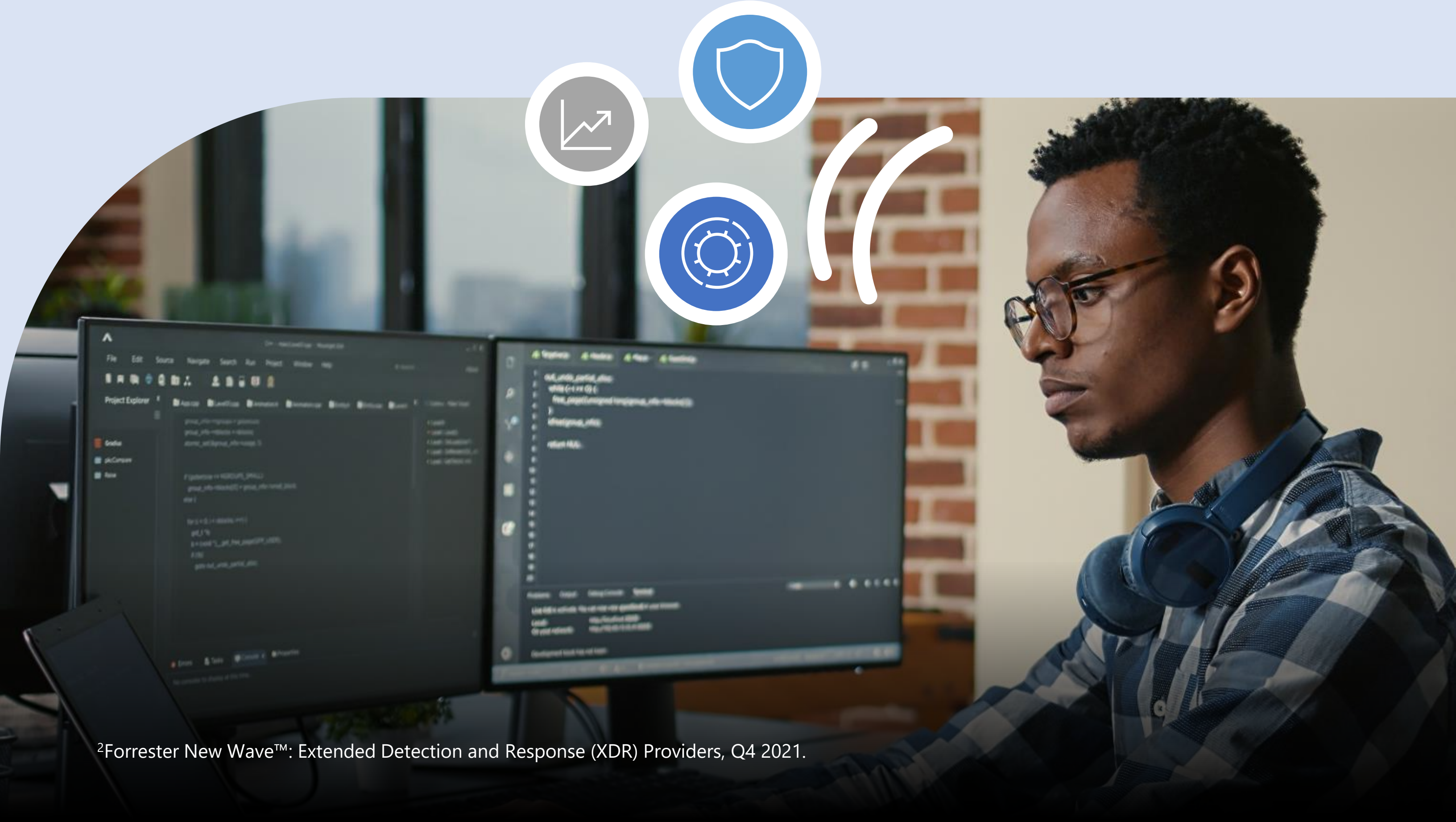
Supercharge your Security experience with Microsoft 365 Defender, the Microsoft EDR solution

Recognized as a leading[2] EDR 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, managed by an expert security provider, organisations can gain a broader set of protections as critical preventative solutions, benefit from auto-healing capabilities for common issues, and scale their operations to protect against ransomware and other advanced attacks more effectively while safeguarding business continuity.

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

1. Enable rapid response with prioritized incidents.

Microsoft 365 Defender can correlate 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 Ekco to investigate and respond at the incident level, making prioritisation 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 Ekco with unified investigation and response designed to deliver the most efficient experience for faster response times.

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

We can investigate alerts on your behalf in the context of the entire incident and useremediation playbooks to respond quickly. We can even dive deep with a single language for advanced hunting across. Additionally, to make sure automations help us respond even faster Microsoft 365 Defender supports real-time custom detections.

Microsoft 365 Defender gives you the ability to understand the impact of a data breach quickly by correlating alerts into our incident view, giving us the ability to conduct advanced hunting, as well as take remediation actions across your estate directly from the Microsoft 365 Defender portal. Adding data-centricity simplifies 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 allows the analysts in the Ekco SOC to leverage the breadth of 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 can contain in-progress attacks by automatically disabling or restricting devices and user accounts used in an attack—stopping progression and limiting the impact.

Scale your security operation 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 anyone else. Pairing the power of the platform with the decades of experience in our SOC , you have better real-time protection against sophisticated threats and we can respond more quickly on your behalf.

43 trillion signals

synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.[4]

[4] Microsoft, "Microsoft Digital Defense Report," November 2022

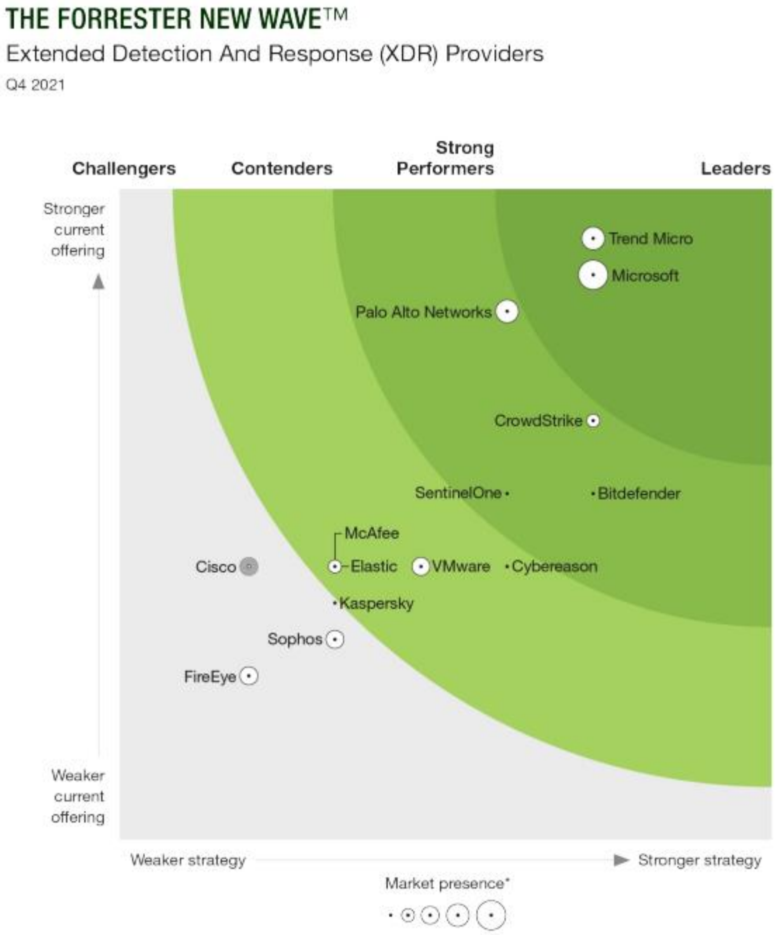
Industry recognition

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,[6] 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



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[7], 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.[8, 9] The Microsoft 365 Defender portal unifies best-of-breed security for endpoints, email, identities, and SaaS applications into a comprehensive XDR experience.

[6] 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.

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

[8] 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.

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

Summary

Managed EDR emerges as a revolutionary approach to help organisations combat cyber threats. The managed solution that Ekco offers arms you 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 Managed EDR from Ekco provides exactly that for your business.

Microsoft 365 Defender is recognized as a leading EDR solution. Beyond the endpoint protection, the managed solution from Ekco provides incident-based investigation and response, it offers centralized visibility, powerful analytics, and automatic attack disruption.

A Managed EDR solution is a must-have for any modern company looking to elevate their security strategy to the next level. Move beyond traditional protection measures and future-proof your organization's security with the addition of threat detection and incident response. Get access to a range of skills and services that were previously beyond your reach.

EKCO

Contact us today.
info@ek.co