Managed Detection and Response (MDR)
Microsoft Defender for Endpoint

Endpoint security is a critical tool for businesses that want to gain centralised protection for all network endpoints, such as laptops and mobile devices, against malware, hacking attempts, and data breaches.

By working with a trusted security specialist, businesses can benefit from 24/7 monitoring and rapid incident response, ensuring threats are neutralised before they can cause significant damage. This enhances your organisation's security posture and also allows internal IT teams to focus on core business tasks, improving overall operational efficiency.

Three Major Challenges of Endpoint Security

Changing Threat Landscape

- The nature of work has changed, and Endpoints represent a significant attack surface. Most breaches are due to existing vulnerabilities or misconfigurations.
- The volume of attacks and threat actors continues to grow. Added to that, the costs of data breaches and regulation are increasing.
- Many organisations struggle to meet conditions to get cyber insurance.

Legacy Approaches

- Most organisations have basic endpoint protection in place, but it is not enough.
- Organisations need detection and response capabilities, as well as vulnerability management, to extend endpoint protection.

Skills Shortage

- 100% protection is impossible; incidents happen so you need an incident response capability that detects and responds.
- Most organisations lack the expertise to manage this 24x7x365.
- Access to Incident Response Specialists is essential in a modern enterprise.

Ekco Managed Detection and Response Service

Attack Surface Reduction
Minimise risks by reducing the surface area of attack, resisting attacks and exploitations

Auto Investigation & Remediation
Automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

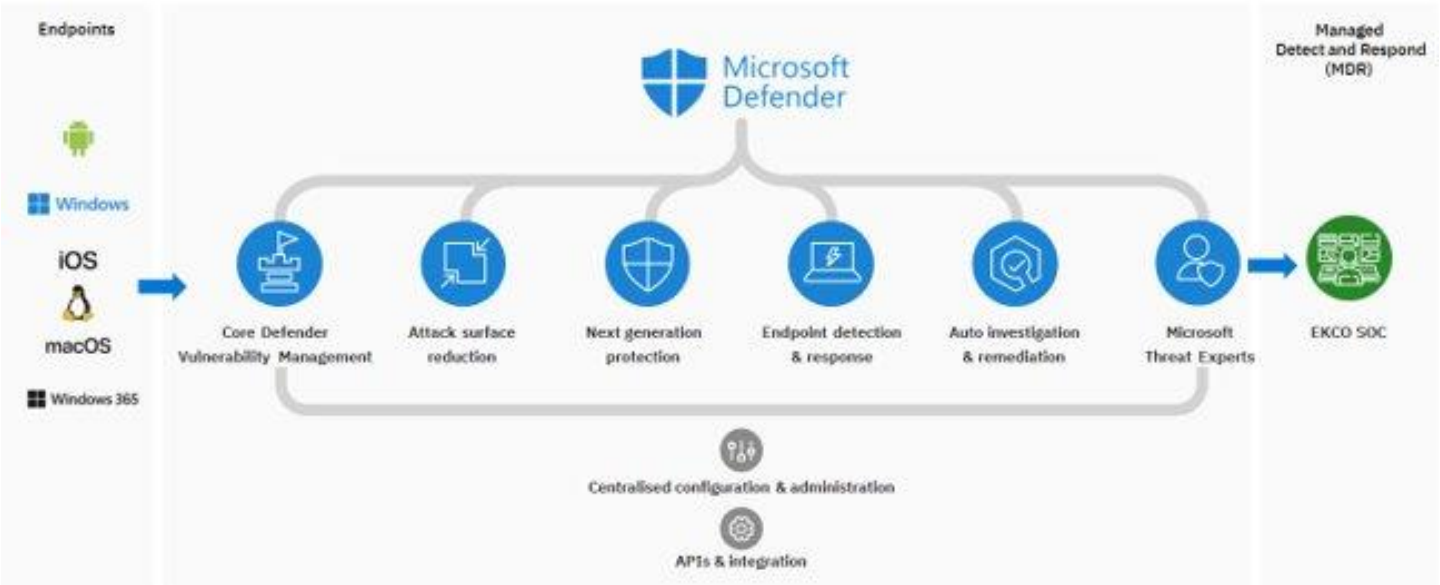
Next Generation Protection
Block sophisticated threats and malware with machine learning and behavioural-based, real-time protection.

24x7x365
Around-the-clock detection and response from experienced threat experts.

Threat Hunting
Experts proactively hunt to spot anomalies or known malicious behavior.

Endpoint Detection & Response
Rapidly detect, investigate, and respond to advanced threats.

Threat and Vulnerability Management
Discovery, assessment, prioritisation, and remediation of endpoint vulnerabilities and misconfigurations



Why Ekco for MDR?

Security Focused
Our security team supports clients ranging from individual financial institutions to Fortune 500 organisations. We deliver the highest calibre of information and cyber security, risk management and governance. Our analysts are all trained to industry standards and for the specific technologies in use in each client SOC.

Quality and Commitment
Our certifications in ISO9001, ISO27001, and CREST demonstrate our dedication to quality and information security, enabling us to consistently meet customer and regulatory requirements.

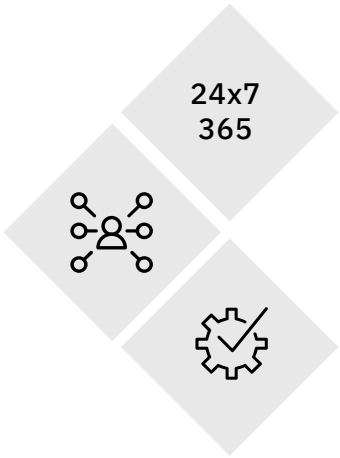
Global Experience
Our team has a wealth of experience founded on advising, implementing, and embedding industry security frameworks and principles into organisations. As a result, we have formed a leading Security Operations capability for multiple large customers.

Service Description	Essentials	Advanced
Microsoft Defender for Endpoint Deployment and onboarding	✓	✓
Next Generation Protection: Blocks sophisticated threats & malware	✓	✓
Attack Surface Reduction	✓	✓
Managed Incident & Alert Monitoring and Triage – Incident Response	✓	✓
24x7 Security Operations Centre	✓	✓
Incident Response Retainer	✓	✓
Endpoint Detection & Response		✓
Automatic Investigation and Remediation (AIR)		✓
Threat and Vulnerability Management		✓
Advanced Threat Hunting		✓
Microsoft Secure Score for Devices		✓

Monitoring of Microsoft Defender for Office 365 / Data Loss Prevention / Cloud & Identity is available as an add-on.

Solution & Benefits

- A Detection and Response service leveraging Microsoft Defender for Endpoint
- Optimised configuration of Defender for enhanced protection.
- Managed Vulnerability Management
- Additional context and guidance on alert handling
- Next generation protection & Attack surface reduction
- Incident Response Retainer
- Automatic investigation and remediation



- Round-the-clock incident response (24x7 SOC X 365)
- **Security Threat Focused -** Advanced analytics to detect complex threats
- Incident Containment & Triage
- Automate containment response to block threats
- Improved speed of detection & response
- **Security Provider First -** Expert level threat monitoring & analysis
- Reduced Cost & Complexity
- Simple pricing structure

Why Ekco?

Ekco is one of Europe's leading managed cloud and security service providers. We make it easier for you to innovate, scale, manage, troubleshoot and secure. With a network of over 200 dedicated security specialists, we have the skills and experience to support your entire cyber security lifecycle. Our experts know the tools and methods used by the criminal underworld to successfully attack organisations across the globe.

www.ek.co info@ek.co

Microsoft Solutions Partner
Security

Microsoft Partner
Microsoft

Microsoft Ireland
Partner of the Year 2023 Winner
A Rising Star
Security