

Managed Security Services

Advanced Managed Detection & Response (MDR) and Managed Extended Detection & Response (MXDR) services, delivered via the Chorus **24x7x365 Cyber Security Operations Centre (CSOC)** and powered by Microsoft Defender XDR and Microsoft Sentinel.



Staying ahead of evolving cyber threats

Cyber security attacks are increasing in frequency and sophistication, which is why cyber security is a key business priority. Today, organizations need to reduce the likelihood of an attack, proactively detect threats, and rapidly respond to reduce potential business impact. To achieve this, organizations need the right processes and technology in place with a team of highly skilled security experts, however for many, this is uneconomical to build and maintain internally.

Delivered via our 24x7x365 CSOC, our managed security services help organizations stay protected in today's rapidly evolving threat landscape. Through our highly qualified SecOps team, advanced automation and processes and underpinned by powerful Microsoft security technologies, we bring affordable enterprise-level security to organizations of any size.



Microsoft MDR & MXDR Services

Our managed security services leverage Microsoft technologies to help organizations detect, investigate, hunt and respond to cyber security threats. We provide flexible managed security services, allowing organizations to choose the right level of protection to meet their security requirements.

MDR Endpoints

Advanced Managed threat detection and containment service for endpoint protection with Microsoft Defender for Endpoints.



MXDR Advanced

Extended threat detection and containment across identity, network, email, infrastructure, data and applications using Microsoft security tooling.



MXDR Premium

Extended threat detection & containment across identity, network, email, infrastructure, data and applications using Microsoft security and third party tooling.



Microsoft MDR & MXDR Security Services

Service Benefits

24x7x365 Advanced CSOC – Our 24x7 CSOC makes best use of technical innovations and cutting-edge security technologies to deliver an advanced service. Underpinned by our team of highly skilled and experienced CSOC analysts, our team protect your organization around-the-clock.

Leading technical architecture – Built on Microsoft Defender XDR and Microsoft Sentinel, our CSOC architecture is built to best-practice benefiting from advanced automation, machine learning and AI to reduce alert noise and accelerate threat detection and response speed and accuracy.

Rapid threat detection and response – Through our skilled SecOps team and use of automation, we ensure cyber threats are quickly identified, investigated and remediated – reducing the likelihood and potential impact of successful attacks, to keep your organization ahead of evolving threats.

Maximise the value of your Microsoft licensing – With most organizations already using Microsoft 365, we use the powerful security features available to maximise the value of your licensing, removing third party costs and consolidating technologies to reduce complexity.

Proactive and preventative protection – We take our managed security services a step further by building in pre-emptive protection through advanced threat hunting and cyber threat intelligence to proactively block emerging and unknown threats before they occur.

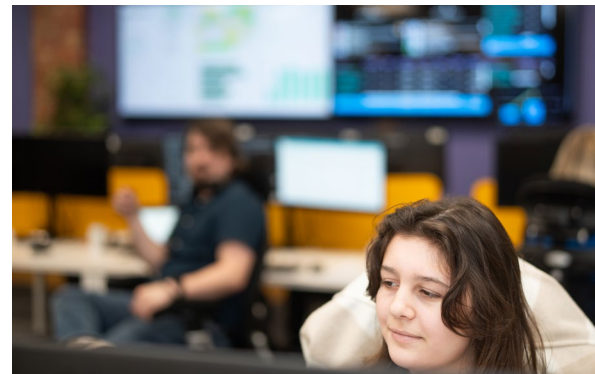
Cyber risk reduction – With proactive threat detection, investigation, hunting and response, your organization is better protected and cyber risk is greatly reduced. This helps you to reduce cyber insurance premiums, meet compliance regulations and benefit from peace of mind against increasingly costly attacks.

Our CSOC Metrics

<5 mins Mean Time to Acknowledge (MTTA)

<15 mins Mean Time to Close (MTTC)

50% Incidents closed by automation



WHAT'S INCLUDED?

24x7x365 CSOC

Flexible Coverage

24x7 Monitoring

Proactive Cyber Threat Intelligence (CTI)

Threat Detection

Threat Triage & Investigation

Rapid Threat Response & Containment

Proactive Threat Hunting




Service Governance & Reporting

Security Reviews & Recommendations

Streamlined Service Transition

Microsoft Security Guidance

Microsoft MDR & MXDR Services Compared

SERVICE COMPARISON		 MDR Endpoints	 MXDR Advanced	 MXDR Premium
24x7x365 UK-based CSOC		✓	✓	✓
Analysts available by phone 24x7		✓	✓	✓
30 minute high severity SLA		✓	✓	✓
Containment and response actions		✓	✓	✓
Chorus proprietary analytic rules		✓	✓	✓
Microsoft Security suite coverage	Defender for Endpoint	✓	✓	✓
	Defender for Identity		✓	✓
	Defender for Cloud Apps		✓	✓
	Defender for Office		✓	✓
	Defender for Cloud		✓	✓
Azure services			✓	✓
Microsoft Sentinel custom integration				✓
Threat Detection & Response Coverage	Endpoints	✓	✓	✓
	Entra ID Identities	✓	✓	✓
	Servers	✓	✓	✓
	Active Directory Identities		✓	✓
	Non-Azure cloud services			✓
	Networking log sources (Firewalls/Switching/APs)			✓
3rd Party APIs/Logs				✓
Weekly security service reports		✓	✓	✓
Cyber Essentials aligned TVM report		✓	✓	✓
Endpoint threat hunting		✓	✓	✓
Cyber Threat Intelligence		✓	✓	✓
Standard security playbooks		✓	✓	✓
Security recommendations & guidance		✓	✓	✓
Service governance		✓	✓	✓
MITRE ATT&CK framework mapping		✓	✓	✓
Custom security playbooks			✓	✓
Extended threat hunting			✓	✓
External attack surface monitoring				✓

Lite MDR & MXDR

Lite version of all three services available that only covers alerts classified as Medium or High in Microsoft Sentinel.

Microsoft-verified MXDR

Our MDR & MXDR services are delivered through our partner, Chorus and their 24x7x365 CSOC. Chorus are members of the Microsoft Security Intelligent Association (MISA) and awarded Microsoft-verified MXDR solution status.

Microsoft Intelligent Security Association

 Microsoft Security

 Microsoft Verified Managed XDR Solution

What next?

For more information on our cybersecurity services or to book a demo, please contact our sales team.



WEBSITE



EMAIL



PHONE