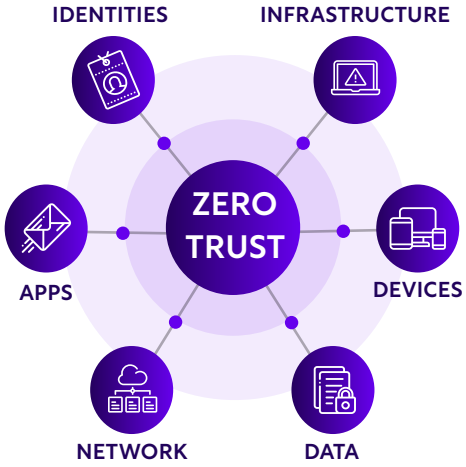
Microsoft SOC Services

Advanced Managed Detection & Response (MDR) and Managed Extended Detection & Response (MXDR) services, delivered via the Chorus Cyber **24×7×365 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, organisations need to reduce the likelihood of an attack, proactively detect threats, and rapidly respond to reduce potential business impact. To achieve this, organisations 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 the Chorus Cyber 24×7×365 CSOC, our managed security services help organisations stay protected in today's rapidly evolving threat landscape. Combining a highly qualified SecOps team, advanced automation and processes and underpinned by powerful Microsoft security technologies, we bring affordable enterprise-level security to organisations of any size.



Microsoft MDR & MXDR Services

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

MDR

Advanced threat detection and containment services to protect all of your identities and endpoints including 1x firewall.

(Defender for Endpoints & Sentinel)

MXDR

Extended threat detection and containment across your entire Microsoft E5 security tooling + various third party sources.

(Defender Stack & Sentinel)

Microsoft MDR & MXDR Security Services

Service Benefits

24×7×365 Advanced CSOC – Our 24×7 CSOC makes best use of technical innovations and cutting-edge security technologies to deliver an advanced service. Underpinned by a team of highly skilled and experienced CSOC analysts, we will protect your organisation 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 organisation ahead of evolving threats.

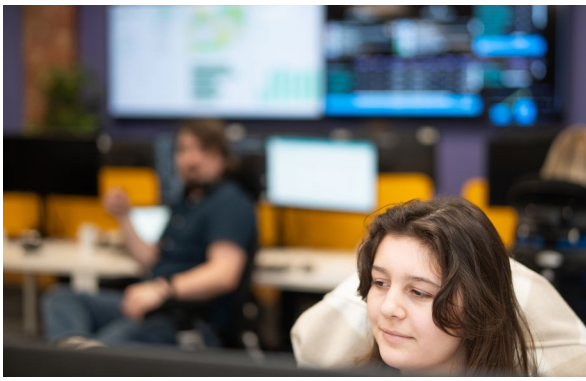
Maximise the value of your Microsoft licensing - With most organisations already using Microsoft 365, we use the powerful security features available to maximise the value of your licensing, removing third party costs and consolidating technologies to reduce complexity.

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 organisation 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.

CSOC Metrics

<5 mins	Mean Time to Acknowledge (MTTA)
<20 mins	Mean Time to Close (MTTC)
50%	Incidents closed by automation



WHAT'S INCLUDED?

- 24×7×365 CSOC
- Flexible Coverage
- 24×7 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	MXDR
24×7×365 CSOC		✓	✓
Analysts available by phone 24×7		✓	✓
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			✓

MDR & MXDR

Two flexible 24×7 managed security services, allowing organisations to choose the right level of protection.

Microsoft-verified MXDR

Our MDR & MXDR services are delivered through our partner, Chorus Cyber and their 24×7×365 CSOC. Chorus are members of the Microsoft Security Intelligent Association (MISA) and awarded Microsoft-verified MXDR solution status.

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Contact us

partners@choruscyber.com | www.choruscyber.com

chorus cyber