CyberOne

MDR as a Service

Stop Threats. Reduce Risk. Prove Resilience.

Powered by Microsoft Sentinel. Realised by CyberOne.

Security You Own. Outcomes You Can Prove.

CyberOne delivers AI-assisted Managed Detection and Response (MDR) that runs in your Microsoft tenant. Our 24x7 CREST-accredited Global SOC monitors, investigates and responds while you retain full control of your data. Optional NCSC-accredited Cyber Incident Response is on call for assured escalation. You get board-ready ROI and evidence every month.

Part of CyberOne's Assure365 suite, our Managed Microsoft Security solution offers modular cyber security services tailored to your needs. It delivers comprehensive, scalable protection to strengthen resilience and free your teams to focus on core business objectives.

CyberOne's MDR as a Service

CyberOne delivers an MDR as a Service with outcomes you can prove to the board. Here's what you can expect:

Stop Threats.

Prevent Breaches 24×7
Continuous monitoring, investigation and response to contain threats before they spread.

Protected From Day One
Automated onboarding gets baselines, detections and playbooks, accelerating time to value.

Protect Critical Assets. Assured by CREST.
Pre-approved containment with named owners and audit-ready evidence, delivered by CREST-accredited SOC.

AI That Speeds Decisions
CyberOne AI enriches and prioritises alerts so analysts act faster and noise stays low.

MITRE ATT&CK-Aligned Detections. Fast.
Deploy an extensive, tuned ruleset quickly to close gaps and surface threats sooner.

Escalate Fast With NCSC Accredited Response.
NCSC Cyber Incident Response available via retainer or call-off Statement of Work for assured escalation when it counts.

Reduce Risk.

Your Data. Full Control.
Keep your data sovereign, no third-party data storage, we only view your Microsoft log ingestion, giving you total control of your data.

20 Years of Deep Industry Expertise. Delivered
demonstrable cyber experience across finance, business services, healthcare, manufacturing and retail, aligned to regulatory needs.

Maximise Microsoft Investments
Get solid ROI from Microsoft 365. We lift utilisation now and bring new security features online fast to widen coverage and cut effort.

Modular By Design. That's Assure365.
Add Incident Response, Dark Web Monitoring and Cyber Tabletop Exercises when needed to match coverage, budget and timeline.

Prove Resilience.

One Portal. Total Clarity.
Live incidents, insights and board-ready reports in one place. No chasing. No guesswork.

Faster Together. With Microsoft Teams.
Live alerts, updates, approvals and incidents handled in Microsoft Teams, speeding decisions and capturing an audit trail you can share.

Focus On Growth. Unlock Innovation.
We free up your technical talent so they can concentrate on innovation and growth initiatives with measurable business impact.

Board-Ready. Proven Value.
Monthly reports with actions, trends and ROI metrics tied to business priorities and risk.

Audit-Ready Reporting & Compliance.
Timelines, approvals and artefacts captured in your portal with control mappings you can lift into audits and board packs.

Supporting Certification. Driving Customer Trust.
Operating controls, continuous monitoring and reporting align to Cyber Essentials requirements supporting certification and strengthening trust.

MDR AUTO

Switch On & See Value. Fast. From Day One.

Microsoft-first monitoring with AI-assisted triage and board-ready reporting in your environment, ideal to prove value quickly & clearly.

Benefits Include:

- **Response:** Automated containment, where pre-approved.
- **Investigation:** AI-assisted triage and investigation.
- **Signals:** Devices and identity only.
- **Automation:** Pre-built automations.
- **Threat Intelligence:** Core integrations.
- **Reporting:** Automated monthly summary.
- **People:** Account Manager.
- **Portal & Communications:** Live incidents, Microsoft Teams alerts.
- **Content:** Focused CyberOne rules and playbooks.

Additional Options:

- **Cyber Incident Tabletop Exercising**
- **NCSC-Backed Cyber Incident Response** via Retainer or Call-Off SoW
- **Dark Web Monitoring + Takedown Service**
- **Penetration Testing** (Red & Purple Teaming)

How We Deliver Your MDR Service

Clear steps with minimal disruption and measurable outcomes from day one. We set up, run 24x7 and continually improve your Microsoft-first MDR with your team.

Connect

Align on outcomes, scope and risk. We confirm data sources, access, approvals and the RACI between your team and ours. Escalation paths and reporting cadence are agreed upon, so decisions are fast and clear.

Enable

Platform Engineers and SOC Analysts deploy tuned content and safe automation in your environment. We baseline noise, map coverage to your risks, set and agree clear KPIs.

Review

An Customer Success Account Manager walks through Monthly Reviews and agree next steps, including board summary: actions taken, trends and KPIs highlight cost-control, opportunities and capture decisions and owners.

Operate 24x7

Our Global SOC is human-led, with our Certified Experts as the decision makers; we augment monitoring, detection, investigation and response with AI. If an incident escalates, the path to our NCSC-accredited Cyber Incident Response team is ready.

Optimise

The SOC continually tunes and refines to expand coverage, reduce noise and build operational maturity. Prioritising highest risks, we share impact through ongoing reports; new Microsoft features are implemented maximising protection and utilisation.

One Team. One Plan. Faster Response.

If an incident needs hands-on support, utilise our optional NCSC-accredited Cyber Incident Response via retainer or call-off Statement of Work. The same team that monitors your environment coordinates response, so decisions are quicker, handoffs are minimal and it's easier to manage end-to-end.

One Escalation Path

On-call 24x7 with Microsoft Teams war room supporting clear communications and approvals.

Faster Containment

Pre-agreed playbooks, defined roles and named owners accelerate containment.

Clearer Communication

Analysts, Engineers and Incident Response leads work to one plan, reducing handoffs and delays.

Stronger After Every Event

Post-incident reviews tune detections and playbooks, improving maturity and resilience over time.

Complete Incident Audit Trail

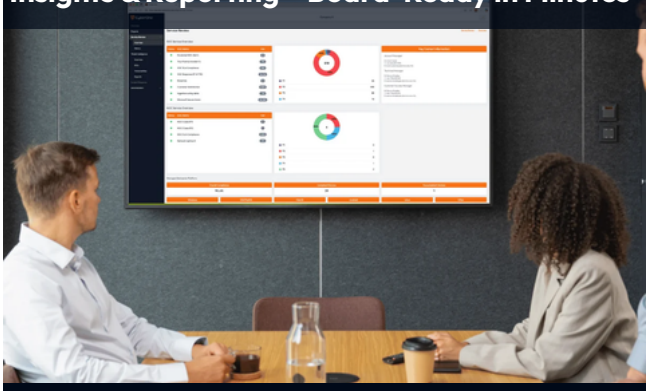
Timelines, decision logs and artefacts are captured in your portal for audit and compliance reviews.

Incident Exercising & Preparedness

Scenario-based exercises and tabletops validate plans, roles and approvals, so you are response-ready.

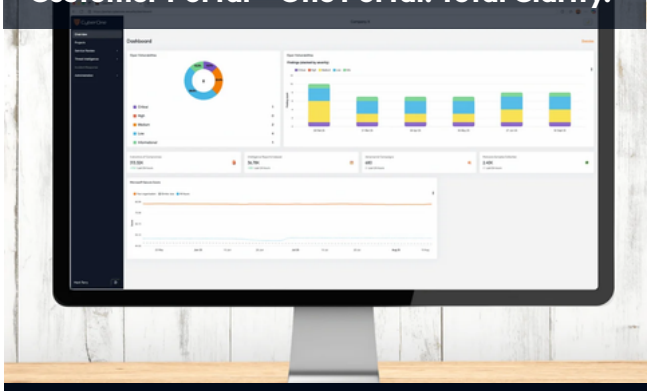
The CyberOne Difference: Key Features & Add-Ons

Insights & Reporting – Board-Ready in Minutes



Operational reports, KPIs and trends you can lift straight into packs; everything auditable.

Customer Portal – One Portal. Total Clarity.

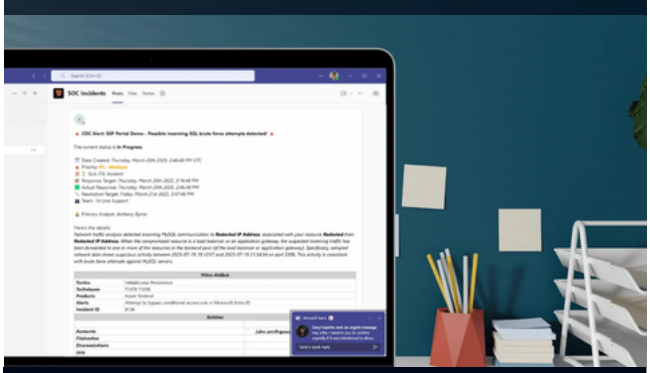


Live incidents, reports, evidence and roadmap in one place so everyone sees the same picture.

Threat Intelligence That Matters

Curated intelligence applied to detections and playbooks so risks show first, not more noise.

Microsoft Teams Integration



Real-time alerts, context and approvals in Microsoft Teams with our SOC for faster decisions.

MXDR as a Service - When You Are Ready To Scale

Step up from MDR Auto when you want broader coverage, proactive hunting and hands-on response across your Microsoft estate. MXDR combines Microsoft Defender XDR, Microsoft Sentinel and advanced automation with CyberOne runbooks to close gaps faster.

Enhancements

Wider Signals
Email and collaboration, SaaS and cloud workloads, data and compliance signals, on-prem and hybrid infrastructure.

Proactive Operations
24x7 threat hunting, deception and continuous purple teaming to validate and improve detections.

Hands-On Response
Managed containment and remediation for high-severity incidents, coordinated with your IT and cloud teams.

Higher Automation
Safe auto-isolation and access revocation with in-Teams approvals to speed decisions without losing control.

Executive Reporting
Risk KPIs, control coverage mapping and quarterly strategy reviews tied to business objectives.

Trusted By Leading UK & Global Businesses

From public sector and government bodies to healthcare, finance, retail, manufacturing and professional services, these organisations rely on CyberOne for proactive detection, rapid response and continuous risk reduction with compliance, helping them thrive in a world of constant change.

FirstBank Since 1894 · Elysium Healthcare · BARRICK · Rodda's · HODGE · Mulberry · Graphnet Transforming Care · Cygnet Health Care · healix INTERNATIONAL · International IDEA · Thai Union · Pell Frischmann · RICS · ALYSIAN DIGITAL BUSINESS TRANSFORMATION · Eden Futures · 10 DOWNING STREET · bre

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft Verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

CyberOne | +44 (0) 3452 757575 | hello@cyberone.security | cyberone.security

Assured Service Provider – in association with National Cyber Security Centre · Assured Service Provider – in association with National Cyber Security Centre – Cyber Incident Response: Standard Level · CREST · CREST Security Operations Centre · CREST Incident Response · CREST Penetration Testing · Member of Microsoft Intelligent Security Association – Microsoft Verified Managed XDR Solution · Microsoft Solutions Partner – Security, Specialist – Cloud Security, Identity and Access Management, Threat Protection · Microsoft Solutions Partner – Modern Work · Microsoft Solutions Partner – Infrastructure Azure · Microsoft Solutions Partner – Data & AI Azure