CNS

at Six Degrees

MANAGED EXTENDED DETECTION AND RESPONSE

Actively protect and defend your organisation against cyber-attacks and vulnerability exploits, 24x7.

> **Imagine knowing what an attacker will do next, and being able to protect your organisation before the attack even starts. That's the power of CNS at Six Degrees' Managed Extended Detection and Response service.**

Today's Cyber Security Challenges

When your organisation is diverse and leverages multiple clouds, solutions and applications, your exposure to data breach increases:

- Larger attack surface as your organisation leverages more interconnected technologies and services
- Non-managed corporate devices reduce cyber security best practices
- Increased targeting from highly motivated and increasingly sophisticated hackers bypassing traditional antivirus software and security controls

Proactive Protection in a Hostile Digital Landscape

Six Degrees' Managed Extended Detection and Response (MXDR) service provides a combination of best practice configurations to protect and defend your environment actively against cyber-attacks and vulnerability exploits, along with 24x7 monitoring and detection of attacks against your on-premises SaaS, PaaS, public and private cloud, and hybrid-based environments.

The service leverages key defence capabilities and attack risk reduction methods and monitors for security incidents occurring within your environment, while reviewing and reporting on attacks that the service components are actively blocking and protecting your organisation from.

Our MXDR service provides alerts and analysis of attempted attacks, along with intelligence into these attempts that assists with threat hunting and pre-emptive guidance to continue to defend against advanced and persistent adversaries.

How Managed Extended Detection and Response Works

The service is delivered by highly trained cyber security professionals operating from our 24x7 Security Operations Centre (SOC).

We deliver cyber incident management, incident response, breach prevention, and incident analysis, all while assuring we are detecting breach attempts proactively based on the very latest cyber security intelligence and threat indicators.

- Proactive defence across your environment, protecting your organisation from attack
- Automated and analyst-led response actions to contain and stop threats and attacks
- Intelligence-led threat hunting to inform your organisation of potential attack techniques and threat actor activity
- Unified cyber security service providing rapid analysis, investigation, and contextualisation of threats
- Reduce hackers' ability to expand cyber-attacks across your infrastructure
- Minimise the risk of data breach resulting in financial, operational and reputational damage
- Maintain operational resiliency, backed up by an industry-leading fully managed service

Managed Extended Detection and Response

Managed Extended Detection and Response is a fully managed service powered by the Microsoft 365 Defender suite and Microsoft Defender for Cloud, providing a unified cyber security service with rapid analysis, investigation and contextualisation of threats.

- 24×7 real-time alert management, advanced and extended detection and rapid response
- Comprehensive protection throughout your infrastructure – across multi-cloud, hybrid environments, and through to your endpoints and users
- Trended reporting to quantify the risks that have been contained
- Bespoke deployment, configuration and management to maximise your protection
- Industry-specific expertise that elevates your cyber security to the next level

Managed Extended Detection and Response Features

What It Does	Why This Matters	What It Means
Proactive and managed defence against attack and vulnerability exploits.	Prevents threats before they even become an incident.	Security assurance and less time spent dealing with security incidents.
Analysis of attacks and attempted attacks to enable threat investigation and threat hunting.	Identifies possible advanced persistent threats and attack techniques.	Greater insight into possible attack techniques and tools allows preemptive measures to be taken to assure your security.
Actioned response to attacks through pre-approved actions.	Stops attackers that infiltrate your defences, protecting your organisation from wider security incidents.	Automated isolation, restriction or containment of endpoints, servers and services, disablement or restriction of users, blocking, restriction, or containment of suspicious code and programs, malware and payload blocking, and URL blocking.
Extended security monitoring across your entire infrastructure, services and applications.	Looking across your wider estate allows better security insights and provides better detection capability.	Creates less chance of a successful attack and provides the ability to better understand attack techniques and respond appropriately.
Provides threat intelligence and insight extended across your infrastructure.	Allows intelligent proactive measures to be taken to disrupt adversaries across multiple platforms.	Provides greater assurance that your organisation is being kept secure.
True 24x7 service managed by security professionals working from a SOC.	Being able to see and respond to a cyber incident as it happens greatly reduces the potential damage it can cause.	Complete oversight and analysis so all threats are identified and remediated.
Full incident analysis with actionable remediation guidance.	Alert investigation is time consuming and requires the necessary expertise to truly understand.	Concise contextualised prioritisation of threats and relevant communications based on business asset classification.
Regular review and recommendations of security insights.	As attacks become more complex and multi-staged, it's difficult to make sense of the threats detected.	Board level security key performance indicators that allow your organisation to visualise the value generated from the service. Outcome-focused actions to improve your cyber security posture and combat against new threats.
Bridging the gap between IT operational teams and cyber security.	Provides the correct levels of insight and advice for IT operational teams to provide a secure and stable IT environment.	Ensures the correct levels of controls are in place to protect the needs of the organisation and assets.
Feature rich and fully integrated cyber security ecosystem.	Analysing interactions between users, devices, applications and locations ensures any hostile threat is seen and stopped.	Continuous assessment coupled with cyber security expertise gives you the who, what, how and when.
Ongoing cyber security trend analysis.	As your digital estate changes and threat actors adapt their tools and tactics, regular trend reviews provide insight into what is changing and how that can impact your environment.	Our cyber security experts will be able to advise on how attacks are changing and how your defences should adapt to provide the necessary levels of protection.

Recorded Future

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Six Degrees' Managed Extended Detection and Response service features tooling from the world's largest threat intelligence company, Recorded Future, integrated with Microsoft Sentinel, along with Microsoft 365 Defender suite and Microsoft Defender for Cloud. Leveraging leading security technologies in this way extends our capabilities to take proactive measures to disrupt adversaries across your infrastructure.

Our Credentials

Microsoft Partner Microsoft | Azure Expert MSP

Member of
Microsoft Intelligent Security Association
Microsoft

Microsoft Solutions Partner
Infrastructure
Azure
Specialist
Infra and Database Migration

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

Microsoft Solutions Partner
Data & AI
Azure
Specialist
Infra and Database Migration

Microsoft Solutions Partner
Modern Work
Specialist
Calling for Microsoft Teams

Microsoft Solutions Partner
Digital & App Innovation
Azure

CERTIFICATION BODY
CYBER ESSENTIALS PLUS

ISO
27001

CNS
at Six Degrees

To learn more about Managed Extended Detection and Response, please contact sales@6dg.co.uk or call 0800 012 8060.