wavenet

EBOOK

MXDR

Managed Extended Detection & Response

Safeguard your IT infrastructure with enhanced visibility and threat intelligence from multiple data sources, for quick threat analysis and faster incident response.

Introduction

Managed extended detection and response (MXDR) is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response with the goal of rapidly identifying and limiting the impact of threats.

Wavenet CyberGuard's solution is designed to collect, monitor, and analyse information presented by the subscribed services in real-time, and then apply advanced threat intelligence and correlation techniques, to try and identify suspicious activity, for which alerts will be generated for further investigation by our Cyber Security Analysts.

In today's dynamic and evolving threat environment, we understand that busy IT teams don't have the time or resources to do threat analysis of emerging threats on their own. This is where our specialist team can help with continuous threat modelling, detection development, and response services.

Our dedicated team spends countless hours analysing the different types of attacks, emerging threats, suspicious behaviour, vulnerabilities, and exploits that they uncover across the entire threat landscape, to better enable us to defend against them.

Once an alarm is triggered it is vital to be able to access all information as quickly as possible, which allows our Security Analysts to make informed decisions quickly, based on our mature Incident Response playbooks.

CyberGuard's Managed XDR service is built upon Microsoft's leading XDR and SIEM solutions (Microsoft 365 Defender and Microsoft Sentinel) to provide integrated protection across your endpoints, identities, Microsoft 365, Cloud applications and email environments.

The core services include

- **Defender for Endpoint (EDR):** Discover and secure endpoint and network devices across multiple platforms
- **Defender for Identity:** Manage and secure hybrid identities and simplify employee, partner, and customer access
- **Defender for Cloud Apps:** Get visibility, control data, and detect threats across cloud services and apps
- **Defender for Office 365:** Protect your email and collaboration tools from advanced threats, such as phishing and business email compromise
- **Sentinel:** Centralised platform for the correlation, enrichment and aggregation of security incidents and events (SIEM)

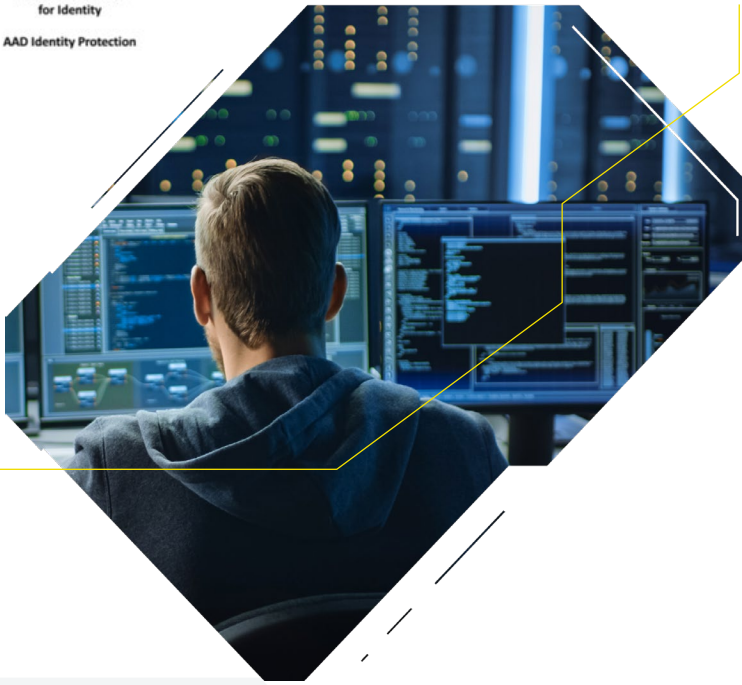
The Solution

With an integrated Microsoft Defender XDR solution, security professionals can stitch together the threat signals received and determine the full scope and impact of the threat; How it entered the environment, what it's affected, and how it's currently impacting the organisation. Microsoft Defender takes automatic action to prevent or stop the attack, and self-heal affected mailboxes, endpoints, and user identities.

Microsoft 365 Defender (XDR)

Microsoft 365 Defender is a unified pre and post-breach enterprise defence suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

With the integrated Microsoft 365 Defender XDR solution, security professionals can analyse and correlate the security data that each of the core Defender products receive and determine the full scope and impact of the threat; how it entered the environment, what it has affected, and how it is currently impacting the organisation. Microsoft 365 Defender takes automatic action to prevent or stop the attack and self-heal affected mailboxes, endpoints, and user identities.



Microsoft 365 Defender

Defender for Endpoint (EDR)

Defender for Endpoint (EDR) is an advanced endpoint protection platform. It provides real-time protection against cyber threats on endpoints, servers, and mobile devices, leveraging behavioural analysis, machine learning, and threat intelligence.

The platform enables proactive monitoring, detection, and response to suspicious activities and attacks on desktops, laptops, and servers. It offers features like automated investigation and remediation, advanced analytics, and attack surface reduction.

Defender for Identity

Defender for Identity is a cloud-based security solution that focuses on detecting and protecting against advanced threats targeting an organisation's identities and user accounts. By analysing user behaviours and security signals, it identifies suspicious activities and potential attacks, providing real-time threat detection and security insights.

The platform leverages machine learning algorithms, user, and entity behavioural analytics (UEBA), and integrates with other Microsoft security solutions to deliver comprehensive protection against identity-related threats and attacks on both on-premises and cloud environments.

Defender for Cloud Apps

Defender for Cloud Apps is a security solution designed to protect cloud-based applications, with a focus on platforms like Microsoft 365, SharePoint Online, OneDrive for Business, and Teams, however integration with other popular 3rd party solutions are also available. It uses advanced threat detection, real-time monitoring, and behavioural analytics to identify and mitigate risks such as malware, phishing, data breaches, and unauthorised access.

The solution enforces security policies, offers data loss prevention capabilities, and provides insights into emerging threats and vulnerabilities. By utilising Defender for Cloud Apps, organisations can enhance the security and compliance of their cloud environments and proactively protect against potential security incidents.

Defender for Office 365

Microsoft Defender for Office 365 is a comprehensive security solution designed to protect organisations using Office 365. It offers advanced threat protection against phishing emails, malware attachments, malicious links, and insider threats.

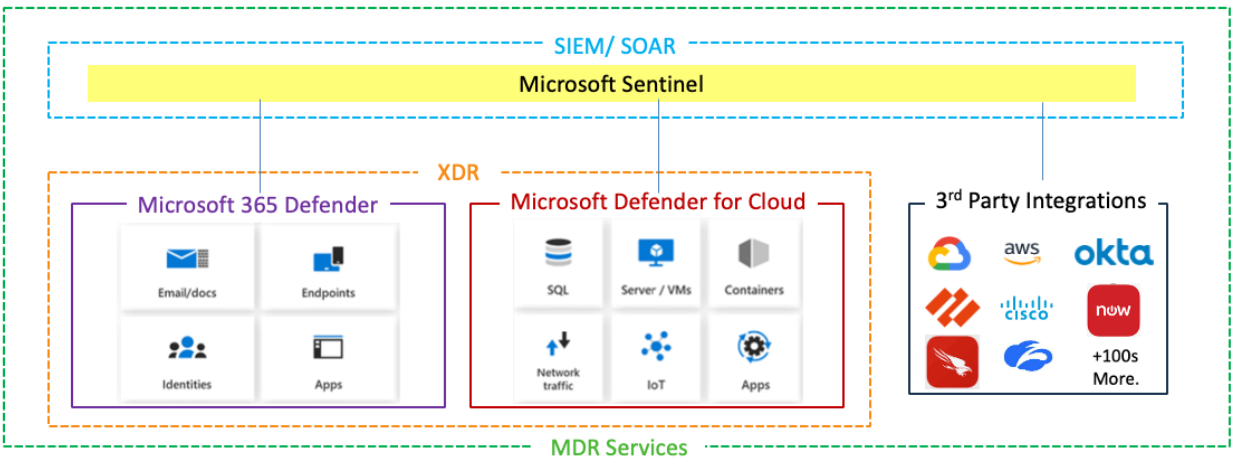
The solution integrates with Exchange Online, SharePoint Online, OneDrive for Business, and Teams, providing real-time scanning, safe attachments, safe links, and anti-phishing capabilities. It leverages machine learning, threat intelligence, and security insights to detect and mitigate emerging threats, enhancing the overall security and protection of Office 365 environments.

Microsoft Sentinel

Microsoft Sentinel is a Cloud-native SIEM platform that helps organisations detect, analyse, and respond to security threats before they impact and harm business operations by providing security teams with visibility into activity within their environments so they can response swiftly to potential cyberattacks and meet compliance requirements. The following core features of the Microsoft Sentinel platform enable the collection and analysis of data at cloud scale, leveraging advanced detection analytics, enhanced with machine learning and artificial intelligence to hunt suspicious activities at scale across multiple data sources and respond to them swiftly to minimise impact.

An Integrated Approach

By leveraging the strengths of both Microsoft 365 Defender and Microsoft Sentinel, organisations can achieve a more robust and proactive security posture, benefiting from enhanced visibility, advanced threat detection, streamlined incident response, and centralised security management, as well having a leading platform to scale out an integrated threat detection and response solution, leveraging data from many other sources from across your organisations infrastructure, networking, cloud and business applications to provide total visibility.



CyberGuard Monitoring & Support

Some businesses will have a dedicated security team devoted to keeping their business safe. Unfortunately, many companies cannot afford to employ a specialised team, so the responsibility of protecting you against a cyber-attack is left to the IT or Office Manager. Even the most skilled IT Manager may not have time to investigate all the alerts, along with keeping pace with the ever-evolving threat landscape.

CyberGuard's specialised team will work to keep your business safe and to protect you against a cyber-attack, keeping pace with the ever-evolving threat landscape.

Key service features include:

- Support and development of the security platforms
- Management and development of detection analytics against the latest and emerging threats
- Integration of both in-house and commercial threat intelligence data.
- Support from Crest accredited Cyber Incident Response Team (CSIRT)

Following the onboarding period and transition into BAU (business as usual) operations, our 24/7 UK based SOC team will actively monitor and analyse and triage security alarms and incidents received in line with CyberGuard's incident handling playbooks, which we have spent hundreds of hours developing and refining. Our SOC Analysts are trained to execute the playbooks to ensure high integrity and that a consistent conclusion is reached as quickly as possible.

Our SOC Analysts have access to advanced tools, for example, advanced malware analysis engines & sandboxing, and commercial threat intelligence platforms including dark web, to help to identify the legitimacy of a threat as quickly as possible so that CyberGuard's Security team can take the appropriate measures to make sure your business is protected.

SLA's

All alerts and incidents ingested into the CyberGuard SOC are subject to a priority-based SLA system as follows.

Priority	Time to First Response	Time to Resolution Plan
Critical	15 minutes	1 hour
High	30 minutes	2 hours
Medium	1 hour	4 hours
Low	4 hours	24 hours

Threat Hunting & Intelligence

Our highly skilled team of security analysts operate from CyberGuard's dedicated Security Operations Centre (SOC), taking responsibility for monitoring, detecting, and investigating potential incidents and ensuring prompt and efficient escalation of potential issues to key stakeholders both within the CyberGuard team and our customers.

Threat Hunting

CyberGuard's threat hunters take an intelligence led approach to proactive threat hunting, understanding both the current global and organisational threat landscape in relation to your environment.

Example threat hunting scenario

A new vulnerability, exploit or malware campaign is reported. CyberGuard will create hunting rules to detect the associated TTPs (Tactics Techniques & Procedures) and hunt retrospectively across the data collected within the platform looking for any evidence of them being used previously to compromise or attempt to compromise your environment. The hunting rules derived from this process are then tuned and implemented as detection analytics moving forward.

Threat Intelligence

CyberGuard works with a number of security businesses, both private and public, to share and expand cyber threat intelligence. Gathering and using Threat Intelligence gives CyberGuard an insight into attackers, their motives and their capabilities providing invaluable information to enhance security and reduce time to detection.

CyberGuard's SOC team use this intelligence to help them identify who is attacking, why are they doing it, what are they after, how are they doing it, where they come from, how we recognise them, and how can we mitigate against them.

CyberGuard have access to many sources of threat intelligence, for example

- **CyberGuard's Curated Intelligence:** CyberGuard gathers intelligence from various sources, including our existing customer base, so an attack seen against one customer is analysed, and the intelligence gained from this is shared amongst all others.
- **Commercial Threat Intelligence:** A tier 1 security partner provides us with a vast amount of reporting around the latest threats, vulnerabilities, and exploits, but also the associated threat actors and their tactics, techniques and procedures to power detection development.
- **Commercial Threat data:** CyberGuard integrates commercial threat data feeds collected from the trillions of signals processed by our security partners into the technologies of our MDR customers.
- **High fidelity Open-source feeds:** Cyber Security has a real strong community for information sharing which CyberGuard team members take an active role in, as such we review selected high-fidelity threat data feeds to complement our commercial data for integration into customers platforms.
- **National Cyber Security Centre (NCSC):** To identify Advanced Persistent Threat (APT) groups and add these IOCs (Indicators of Compromise) to our combined threat intelligence feeds.

The MDR Team

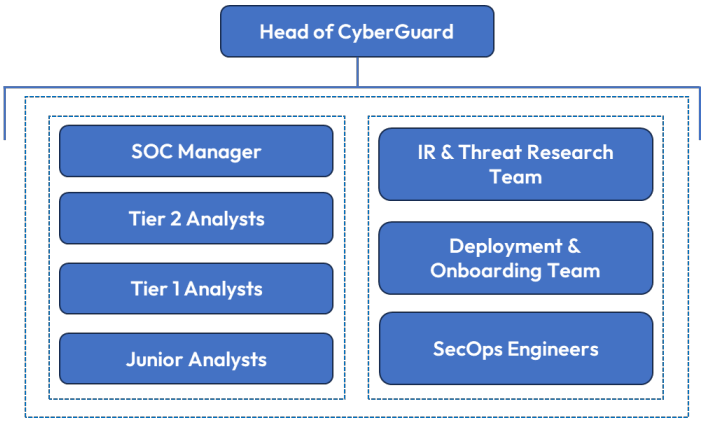
Junior & Tier 1 Security Analysts: Responsible for the triage of alerts and handling of customer services requests. Incidents are escalated to senior resources within the CyberGuard SOC team and stakeholders within the customer organisation in-line with defined SLA's**.** Note: Junior Analysts have their work peer reviewed by a Tier 1 Analyst.

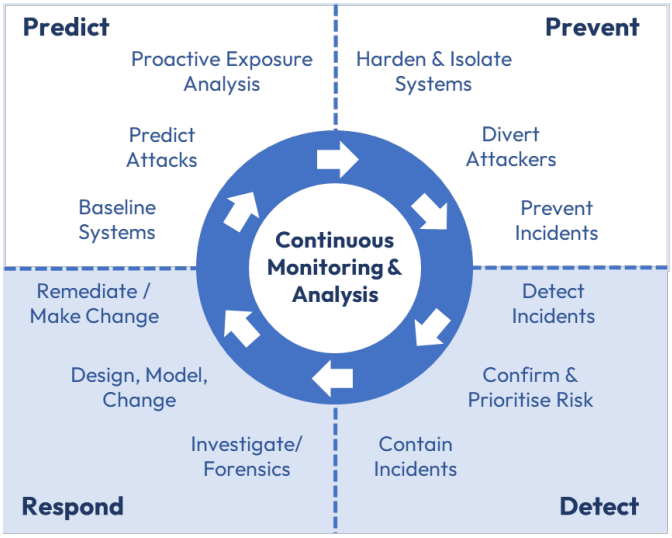
Tier 2 Security Analysts: Experienced staff who ensure incidents are detected, tracked and investigated with full adherence to all procedures and reporting requirements within the SOC. Provide mentoring to Tier 1 Analysts. Gather intelligence reports and interact with other security and network groups as necessary. Co-ordinate with the SecOps team to continually tune alerts and events and automation process automation.

Threat Research & Incident Response Team: Responsible for the research, development and maturity of the forensic and investigations program within CyberGuard. They will examine threat intelligence, malicious code (malware), attack vectors, network communication methods, and analyse outcomes against target systems and networks, and produce technical post-action reports.

Deployment & Onboarding Team: Subject matter experts in the deployment of new services including EDR/XDR Solutions, Azure Cloud security technologies and SIEM platforms. They perform SIEM deployments into customer environments, drive process improvements, develop new SIEM use cases and drive the implementation and adoption of new capabilities.

SecOps Engineers: Responsible for the administration and development of the SIEM platform including, playbooks, Azure functions, workbooks & dashboards, and architecture, configuration, testing and analytic (KQL) performance within Azure Sentinel. The SecOps engineers work closely with the Head of CyberGuard, Blue Team Leaders, and Analysts to optimise technologies, processes, and detections.





Service Deployment

Onboarding to the Microsoft 365 Defender XDR (Extended Detection and Response) platform is a crucial step to ensuring effective threat detection and response across your organisation's Microsoft 365 environment. Here's a brief overview of the onboarding process:

Preparation

- Ensure that you have the necessary licenses and subscriptions for Microsoft 365 Defender.
- Identify key stakeholders and team members who will be involved in the onboarding process.

Planning

- Create an onboarding plan that outlines the goals, timelines, and milestones for the onboarding process.
- Define roles and responsibilities for team members involved in the onboarding process.
- Determine which Microsoft 365 services and components will be integrated with Microsoft 365 Defender XDR.

Technical Configuration

- Set up the required prerequisites, such as Azure Active Directory (AAD) and Microsoft 365 services.
- Configure Microsoft 365 Defender XDR settings and policies based on your organisation's security requirements.
- Ensure that necessary permissions and access controls are in place for the platform.

Data Integration

- Connect Microsoft 365 Defender XDR to relevant data sources within your organisation, including email, endpoints, and cloud services.
- Configure data connectors to collect logs and telemetry data for analysis.

Alerts and Incident Handling

- Configure alert policies to define which events should trigger alerts.
- Establish integration into the Wavenet CyberGuard SOC & Threat Intelligence platform.

BAU Processes

- Continuously monitor the platform for alerts and incidents.
- Analyse and fine-tune detection rules and policies to reduce false positives and improve detection accuracy.

WAVENET.CO.UK

0333 234 0011

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG

cyberguard@wavenet.co.uk

wavenet

Networking
& Connectivity

Unified
Communications
& Voice

Contact Centres

Mobile Solutions
& IoT

IT, Cloud
& Technology

Network
Intelligence

CyberGuard