



Service Description

G-Cloud 14 - Managed Security Service

Version 1.0



Azure
Expert
MSP

Windows and SQL Server Migration Advanced Specialisation
Teamwork Deployment Advanced Specialisation
Calling for Microsoft Teams Advanced Specialisation
Meeting and Meeting Rooms Advanced Specialisation
Adoption and Change Management Advanced Specialisation
Threat Protection Advanced Specialisation
Identity and Access Management Advanced Specialisation
Information Protection and Governance Advanced Specialisation
Cloud Security Advanced Specialisation
Azure Virtual Desktop Advanced Specialisation

transparency
transformation • partnership • clarity

Contents

Contents	2
Managed Security Service Introduction	3
Benefits of Microsoft Security	3
Full Managed Security Service	4
Managed Detection & Response	5
Managed Security Products.....	5
Overview.....	5
Managed Microsoft Sentinel.....	5
Managed Defender for Endpoint	6
Managed Defender for Cloud.....	6
Managed Defender for Office 365.....	6
Firewall Perimeter Defense.....	7
24/7 Incident Response Service	7
Business Premium Security Support	7
Threat & Vulnerability Management.....	8
Security Awareness Training.....	8



Managed Security Service Introduction

Whether you're looking to fully outsource your security needs or give your in-house team a helping hand keeping your environment secure, our managed services are just what you need. With expert deployment, management and ongoing configuration to keep your security tooling at the cutting edge of threat intelligence, our services take the pressure off your team.

From our Microsoft XDR verified fully managed security service, which offers end-to-end protection 24x7, to our individual managed services for specific security tooling and threat and vulnerability management, through to our complete Managed Security Service. Our highly experienced and accredited Microsoft Security experts will work in partnership with you, to achieve your goals.

With our cutting edge threat intelligence and Secure by Design blueprint, we'll configure your tooling to defend you against the latest threats.

Benefits of Microsoft Security

- **Expertise and specialisation:** At Transparency we've been providing XDR verified services for years across multiple sectors
- **Continuous Monitoring:** We monitor your IT environment constantly to ensure no threats or data breaches occur
- **Proactive approach:** Our managed services ensure a proactive approach to security, stopping problems before they happen
- **Cost-Effective Solutions:** Reduce upfront costs in implementing and maintaining a secure IT solution
- **Scalable:** Our Microsoft Security Managed Services are scalable, meaning they can grow as your business does



Explicit verification
(never trust,
always verify)



Least Privilege
(provide only the access required, and only for
the duration needed)



Assume Breach
(always assume users
or systems will fail)

Full Managed Security Service





Our end-to-end managed security service is like no other, helping protect your systems and data with cutting edge technology and threat intelligence. With proactive threat hunting and vulnerability management you're protected from day one while we strengthen and develop your security posture over time.

Our team are experts in all things Microsoft, so you can be confident that we not only use best-of-breed tooling but that we have the experience to secure the full Microsoft technology stack.

Your security posture will be enhanced continuously, configured to our cutting-edge Secure by Design blueprint so your security infrastructure is protected against both new and existing threats. It's a full SOC and security team on your side, day and night.

Service highlights:

- Microsoft Sentinel (SIEM) implementation, tuning, and maintenance.
- All-inclusive Security Operations Centre (SOC) 1st- 3rd Line telephone, email, and remote support for Security related incidents.
- Post-breach remediation planning
- Execution of the recovery plan, up to 5 days per annum
- 24x7 incident management and response.
- Remote Service Delivery Management.
- Bi-annual end user security education and awareness training.
- Monthly external vulnerability scans and remediation activity.
- Internal vulnerability scans (optional, additional charge applies)
- Security posture maintenance / improvement through monthly assessment and remediation activity.
- Monthly Managed Security Service report.

 Proactive protection around the clock Cybercriminals don't take a day off, so neither do we. Our Security Incident and Response Team monitor your environment armed with the latest threat intelligence to keep you protected every minute of every day.	 Security posture stronger by the day A 'set and forget' approach isn't good enough. The world of security threats moves quickly, and your security posture needs to stay steps ahead.	 Leading edge technology We use the best security technology on the market. We use Microsoft's extensive security suite supplemented with third-party technology as needed for a market leading solution.	 Stay in control with transparent reporting We'll never keep you in the dark about your security. We'll keep you informed about any threats or incidents detected and any actions taken.
---	--	---	--





Managed Detection & Response

Detect and respond to security incidents day and night.

When it comes to security, there's no one size fits all. Our Managed Detection and Response (MDR) service is designed to provide expert cyber security, with flexibility built in. Stackable, scalable modules allow you to take what you need and leave what you don't.

Built in response to customer challenges, on a foundation of decades of expertise and industry best-practice – our MDR service has been crafted for you.

Whether you're looking to extend your IT team's capabilities, maintain compliance with your cyber insurance or you're after cost-effective cyber security – our MDR service ticks all the boxes.

 <p>Extend your cyber security coverage 24x7. There's no need to get out of bed at 3am or expand your IT team, our experts are already on it.</p>	 <p>Assist your cyber insurance strategy. Whether you're in a highly regulated industry or not, take the headache out of insurance.</p>	 <p>Get expert support as an extension of your team. Keep your internal team focused, with our SOC on hand when you need them.</p>	 <p>A cost effective solution for organisations of all sizes. A scalable solution for just what you need that works with what you've got.</p>
--	--	---	--

Managed Security Products

Overview

Our Managed Security Products provide the very best reactive support and ongoing proactive management of your security tooling to provide tactical enhancement of your security posture. Delivered in isolation or as a bespoke collection of services, Transparency can support you in the adoption and management of point solutions from Microsoft and existing services to ensure you continue to get the most out of your security tooling investments.

Our available services at the time of writing include:

- Managed Microsoft Sentinel
- Managed Microsoft Defender for Endpoint
- Managed Defender for Cloud
- Managed Defender for Office 365
- Firewall Perimeter Defense
- Threat & Vulnerability Management (including Threat Intelligence)
- Managed Secure Score
- Security Awareness Training

Managed Microsoft Sentinel

As Microsoft's best-in-class cloud-native Security Information and Event Management (SIEM) platform, Microsoft Sentinel delivers an overview of your security posture using enriched signalling and telemetry data from relevant IT resources across your technology estate.

By applying Machine Learning and Artificial Intelligence to this information, it compares and correlates security events and alerts from these various sources and products to create an accurate summary of all incidents across your IT infrastructure.

However, Microsoft Sentinel isn't just an activate and forget service. It requires a tremendous amount of configuration and ongoing tuning to get the best out of it. This often requires in-depth technical and security knowledge.

As part of Transparency's Managed Microsoft Sentinel service, we solve these issues by performing first time configuration and continuous optimisation thereafter. We'll then monitor your Microsoft Sentinel environment on an ongoing basis and resolve issues with the platform. Through guided remediation with pre-allocated resolution time, we provide the detail on what needs to be done to resolve security alerts and can help with those most critical to your organisation.

Managed Defender for Endpoint

Microsoft Defender for Endpoint (MDE) provides advanced endpoint security that helps organisations detect, prevent and respond to sophisticated threats, including "living off the land" attacks. Using a series of behavioural sensors embedded in the operating system, it collects and processes signals to check and assess your security status – and alert you when something isn't right.

Microsoft protects endpoints through a combination of prevention, detection, and auto-remediation and has been named a security leader in [The Forrester Wave 2022 Enterprise Detection and Response report](#).

By taking advantage of big-data, device-learning, and unique Microsoft optics, cloud products like Microsoft 365, Azure and other online services, MDE provides accurate behavioural insights and clear recommendations for how you should manage threats – before they disrupt your operations.

Transparency's managed MDE service makes it easier and less time-consuming for you to stay on top of your cloud security. By aligning with our Secure by Design Blueprint, we ensure consistent best practices and protection throughout the configuration, maintenance, and ongoing operation of Defender for Endpoint.

We automatically send any 'high severity' security alerts to our Transparency Security Operations Centre for immediate triage, assessment, and guided remediation. All other 'less severe' alerts are shared with your own internal IT Operations team.

Managed Defender for Cloud

Microsoft's impressive Defender for Cloud solution simultaneously manages your existing cloud security posture, while also providing effective protection from threats. As a result, you benefit from more secure cloud resources and more resilient workloads running across your Azure, hybrid and other cloud platforms, such as GCP and AWS.

Transparency's managed Microsoft Defender for Cloud service makes it easier and less time-consuming for you to stay on top of your cloud security. By aligning with our Secure by Design Blueprint, we ensure consistent best practices and protection throughout the configuration, maintenance, and ongoing operation of Defender for Cloud.

We automatically send any 'high severity' security alerts to our Transparency Security Operations Centre for immediate triage, assessment, and guided remediation. All other 'less severe' alerts are shared with your own internal IT Operations team.

Managed Defender for Office 365

Microsoft Defender for Office 365 protects your organisation and employees against various threats to their email messages, URL links and collaboration tools. Because every business uses Microsoft 365 in different ways and to satisfy different needs, you can also define your own policies and processes for threat protection. Everything is reviewed and updated regularly to stay up to date with new threats as they emerge.

Transparency's managed Microsoft Defender for Office 365 service makes it easier and less time-consuming for you to stay on top of your cloud security. By aligning with our Secure by Design Blueprint, we ensure consistent best practices and protection throughout the configuration, maintenance, and ongoing operation of Defender for Office 365.

We automatically send any 'high severity' security alerts to our Transparency Security Operations Centre for immediate triage, assessment, and guided remediation. All other 'less severe' alerts are shared with your own internal IT Operations team.

Firewall Perimeter Defense

Firewalls play a critical role in protecting organisations from cyberattacks. However, if they are not properly configured or maintained, they may be left vulnerable to breaches.

Transparency Cyber's Managed Firewall Service prevents this risk by taking a holistic approach to your firewall security strategy – both on-premises and in a hosted environment.

We start by ensuring your firewall is correctly configured, end to end, and offer recommendations for any improvements we feel are necessary or useful. We also ensure that your firewall configuration can be successfully recovered in the event of an unexpected major incident.

Because every organisation has different priorities and needs, we offer a cost-effective solution to meet yours. Once agreed, Transparency Cyber will take full responsibility for managing your firewall and routing available alert information to our dedicated Service Desk so we can resolve any issues quickly for you.

24/7 Incident Response Service

If the worst happens, we've got you.

In the event of a cyber attack, you need to know you've got the right people on your side. Our 24/7 Incident Response Service is designed to identify, contain and eject attackers quickly, to get you back on your feet

To contain the scope of an attack, your response needs to be fast with the best tools and expertise at your disposal. But what if your internal team can't cope in the event of a breach?

With our 24/7 Incident Response Service you will have our team here on standby to help with around the clock response, and the expertise you need to get back online securely.

Incident Response Service	Incident Recovery Service
<ul style="list-style-type: none">✓ Managed Investigations✓ Triage✓ Confirm Breach✓ Analyse✓ Containment	<ul style="list-style-type: none">✓ Guided Remediation✓ Root Cause Analysis✓ Bi-Annual Vulnerability Assessment✓ Detailed Incident Reports

Business Premium Security Support

Stay secure and productive with Microsoft 365 Business Premium

Microsoft 365 Business Premium delivers a range of enterprise class features to manage your security and enable your workforce to stay productive in the new hybrid world of work. With the recent introduction of Defender for Business to the suite you now have the tools you need to strengthen your endpoints and run your business securely from anywhere. Business Premium also includes enterprise-grade Endpoint Detection and Response (EDR), Automated Investigation and Response (AIR) and Threat and Vulnerability Management (TVM) tools.

But, to get the full ROI on your investment in Business Premium it needs regular configuration, maintenance and management, and teams need ongoing support. Our Business Premium Security Support service was created to support our customers in response to Microsoft's expansion of Business Premium to include Defender for Business.

The service is designed to give you access to the support you need from our dedicated SOC and support desk team, so you can get the most out of the tools at your disposal. Do more and stay secure, without the headache of maintenance.

Threat & Vulnerability Management

With cybercriminals constantly looking for weaknesses to exploit in your organisations' IT systems, it's essential that you are confident you will be able to quickly identify and mitigate any potential security risks before they take advantage.

Threat and Vulnerability Management (TVM) plays a vital role in helping you stay ahead of cyber-attacks. Using the best-of-breed Tenable Nessus vulnerability scanner, Transparency Cyber will scan your public-facing IT infrastructure to check for any potential risks and vulnerabilities that can be used as entry points to gain a foothold in your organisation. Then, our experts will analyse any identified issues and provide guided remediation to mitigate them. As a result, we will help to reduce your attack surface, improving your security posture.

Meanwhile, our proactive Threat Intelligence provides you with the insights and information you need to stay one step ahead of zero-day and other emerging threats. When a potential risk is identified, our specialist security team will immediately provide you with best practices guided remediation.

Security Awareness Training

A productive, efficient organisation demands a robust security strategy – as well as a competent IT team to maintain and update it. But employees themselves also have a critical role to play. So much so, that they can make or break their company's security based on the way they behave at work.

One of the best ways to promote employee best practice in this area, is by sharing regular, relevant security training and awareness programmes. Not only will this encourage good habits, but it will also make everyone appreciate their responsibilities and improve their vigilance when it comes to protecting valuable technology assets.

As dedicated IT security experts, Transparency can provide the insights and advice your workforce needs to improve its approach to protecting your business.

Our training syllabus includes a high-level overview of the most common security threats an employee may encounter during their working lives. It is delivered biannually as standard, or more frequently if required, and supported by a detailed document that can be distributed or hosted on your company intranet.

All training is continually reviewed and updated by our internal security researchers as new threats are found, to ensure you always receive the very latest knowledge and innovation. We can also focus on specific topics or provide more in-depth training by request.



Explicit verification

(never trust,
always verify)



Least Privilege

(provide only the access required, and only for
the duration needed)



Assume Breach

(always assume users
or systems will fail)