wavenet

EBOOK

CyberGuard Assurance

Comprehensively enhance your security posture.

Introduction

In the ever-evolving landscape of cybersecurity, companies who perhaps do not benefit from extensive organisational structures, or subject matter experts, often find it challenging to navigate the complexities of procuring and managing essential security services. The disjointed nature of traditional, one- off services can lead to fragmented security postures and unexpected costs, making it difficult for smaller businesses to maintain robust protection against cyber threats.

Understanding these challenges, CyberGuard have developed a comprehensive package of services that consolidates essential cybersecurity activities into a streamlined monthly subscription. This innovative approach simplifies the procurement process, providing continuous access to a broad range of services that cover several critical aspects of a company's cybersecurity journey. By transitioning from ad-hoc purchases to a predictable, recurring monthly model, we make cybersecurity both accessible and affordable.

The packages include key services such as Cyber Essentials Plus certification, regular external and internal vulnerability scans, dedicated cybersecurity consulting, and an incident response retainer. Each service is designed to comprehensively enhance your security posture, ensuring that all potential vulnerabilities are addressed proactively.

CyberGuard Assurance packaged services are delivered with a hands-on account management approach, ensuring that you seamlessly utilise these services and have the support and expertise needed to navigate the complexities of cybersecurity with confidence.

What's Included

CyberGuard Assurance package options are designed with specific components to ensure that each aspect of your cyber security strategy aligns seamlessly with your organisational goals and evolving threat landscape.

Internal & External Vulnerability Scans

Stay ahead of potential threats with our vulnerability scans. These regular assessments help identify and fix vulnerabilities in your network and systems, ensuring your defences are always up-to-date against the latest cyber threats. With the ever-changing landscape of cybersecurity, having regular scans allows your team to make informed decisions to secure your estate.

Incident Response Retainer

In today's digital landscape, it's a matter of "when," not "if," a cyber incident will occur. Being prepared for that moment is crucial. Our Incident Response Retainer service provides initial triage when an incident is discovered, including recovery planning, damage containment, investigation, and remediation. We act as a calming and goal-oriented presence to minimise the impact on your operations. Gain peace of mind knowing that expert help is just a call away when you need it most.

Cyber Essentials Plus

Achieving Cyber Essentials signifies that your organisation has undergone a rigorous assessment to verify the effectiveness of your cybersecurity measures and controls. It shows your commitment to protecting sensitive information and fostering trust with your customers and partners. Whether you are looking to gain a spot on a public sector framework or demonstrating good cyber hygiene, Cyber Essentials is considered a significant benchmark in securing your business.

Cyber Security Consulting

Our expert cyber consultants will provide guidance, tailored advice and actionable recommendations to enhance your organisation's security posture. Whether you need strategic planning for a new service, risk assessment for a new product, specific security solutions, or a tailored action plan based on the scanning results, these consulting days are designed to augment your cyber efforts and provide real value towards securing your company.

Cloud Configuration Security Assessment

Cloud services and in particular the Microsoft 365 platform provide attackers with a large attack vector which has typically fallen outside of the traditional security controls and testing schedules. It is unlikely that the security controls you have relied upon in the past will fully protect your environment The risk of not securing such a critical area of the business is extremely high.

Copilot AI Readiness Assessment

Discover if you are ready for Copilot. Microsoft 365 Copilot AI technology is on the verge of revolutionising the way businesses operate. Preparation is vital to avoid major issues, such as privacy concerns, data exfiltration, or a data breach. Understand & ensure your security posture and data protection policies are ready for AI adoption, considering aspects such as education, skills, governance, risk and compliance management.

CyberGuard Assurance Packages

Our goal is to provide you with a robust, easily manageable cybersecurity solution that grows with your business and adapts to evolving threats. By opting for our monthly subscription model, you can:

- Gain the peace of mind that comes from working with a strategic partner in your cybersecurity efforts, to protect and mitigate against the many cyber security threats that are present.
- Gain access to an extensive range of services without the complexity and high costs typically associated with one-off purchases.

	CyberGuard Assurance Core	CyberGuard Assurance Plus	CyberGuard Assurance Elite
Bi-Annual Internal Vulnerability Scan	✓	✓	✓
Monthly External Vulnerability Scan	✓	✓	✓
CE Assessment & Certification	✓	✓	✓
CE Plus Audit & Certification		✓	✓
Incident Response Retainer		✓	✓
Cyber Security Consultancy		✓	✓
vCISO Consultancy			✓
Cloud Configuration Assessment			✓
Copilot AI Readiness Assessment			✓
Security Awareness & Phishing Training	Optional Add-on	Optional Add-on	Optional Add-on

Vulnerability Scanning

As part of CyberGuard Assurance, our penetration testers will attempt to gain access to your computer systems and networks, potentially without the knowledge of usernames, passwords or any other normal means of access, ultimately, to find any vulnerabilities that a hacker could exploit. Our testers will never scan or test any computer or server that has not been agreed within the scope, and at no point will any form of backdoor be introduced into your systems.

- **Vulnerability Analysis:** The attack surface (in scope) will be subject to a vulnerability assessment using industry standard tools and techniques. The tester will review the results to understand what, if any, vulnerabilities exist and the potential risk they provide to your business.
- **Exploitation and Post-Exploitation:** The tester will look to exploit any vulnerabilities discovered on the attack surface using various exploit frameworks and toolkits, to attempt to gain access to a system or information over and above what is publicly available. If the exploitation is successful, it will be used to escalate privileges and/ or enable lateral movement within the environment to gain the highest level of access possible, within the testing timescales.
- **Issue Notification:** If any critical vulnerabilities are discovered and exploited as part of the testing engagement, you will be notified immediately, prior to the formal report, so appropriate remediation can be prioritised.
- **Reporting:** The report will include including an executive summary, technical details associated with techniques used and details of potential issues.

Bi-annual Internal Infrastructure Scans

Internal infrastructure testing will target your endpoint devices, computers, laptops, servers and networking equipment. The objective is to find out how far an attacker could get and therefore what they could access if they gained access via internal infrastructure. The tester will try to exploit any vulnerabilities found to gain access to the company's data.

Monthly External Infrastructure Scans

External Penetration testing will target your externally facing IP addresses (within agreed scope) which could be hosting servers and devices such as email servers, web servers or firewalls. Cloud-based services such as Office 365 are included in this scope. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access. If vulnerabilities are found, then the tester will attempt to exploit the weakness to gain access to the network.

Cyber Essentials

Cyber Essentials Accreditation & Certification

The UK Government believes that being Cyber Essentials accredited could prevent "around 80% of cyber-attacks" and is crucial in improving a company's cyber security. Our CyberGuard team can guide you through the steps towards achieving Cyber Essentials accreditation with the minimum of fuss, assisting with the whole process and to help you with any questions along the way. CyberGuard's consultants will determine if the Cyber Essentials guidelines are being followed by checking parts of the network and running several scans. CyberGuard can offer both an assessment and the actual audit.

Cyber Essentials: A self-assessed basic level of certification based on a questionnaire which is then verified and awarded by CyberGuard.

Cyber Essentials Plus: An audited service to provide higher level of assurance whereby CyberGuard test that the five key security controls are working in practice by simulating basic hacking and phishing attacks.

Wavenet is accredited and approved by IASME to perform assessments and audits for Cyber Essentials. IASME are the National Cyber Security Centre's sole Cyber Essentials Partner, responsible for the delivery of the Cyber Essentials accreditation and certification scheme. As a certification body, Wavenet can conduct the audit and award the certificate if you meet all the criteria. One of our Cyber Assessors will link to you remotely to conduct an audit against the criteria specified for Cyber Essentials Plus.

Cyber Essentials Plus

Cyber Essentials Plus is an audited accreditation framework that enables you to assure and demonstrate to your customers, investors, insurers, and others, that you have properly implemented the essential security precautions within the following key security controls, to better protect your businesses from internet-based attacks.

- **Boundary firewalls and internet gateway:** Devices are configured to prevent unauthorised access, from inside or outside the network, to company data and systems, while still allowing secure access to people who are allowed access.
- **Secure configuration:** Devices and software settings are as secure as possible.
- **Access control:** Only authorised personnel to have access and suitable permissions to their accounts.
- **Malware protection:** Protection is installed and up to date to prevent system penetration.
- **Patch management:** All software and applications are licenced, supported with up to date patches.
- **Cloud services:** All cloud services are included in the scope of the assessment.

Incident Response Retainer

Expert support at the ready in the event of a major security incident

In the event of a cyber-crisis, the Incident Response Retainer provides you with immediate access to CyberGuard resources with a guaranteed response and priority response times, consequently minimising the overall impact of the security event. The Incident Response Retainer is a pre-arranged block of Incident Response hours, at a discounted rate, with the ability to use the hours on a variety of technical or strategic services within the year.

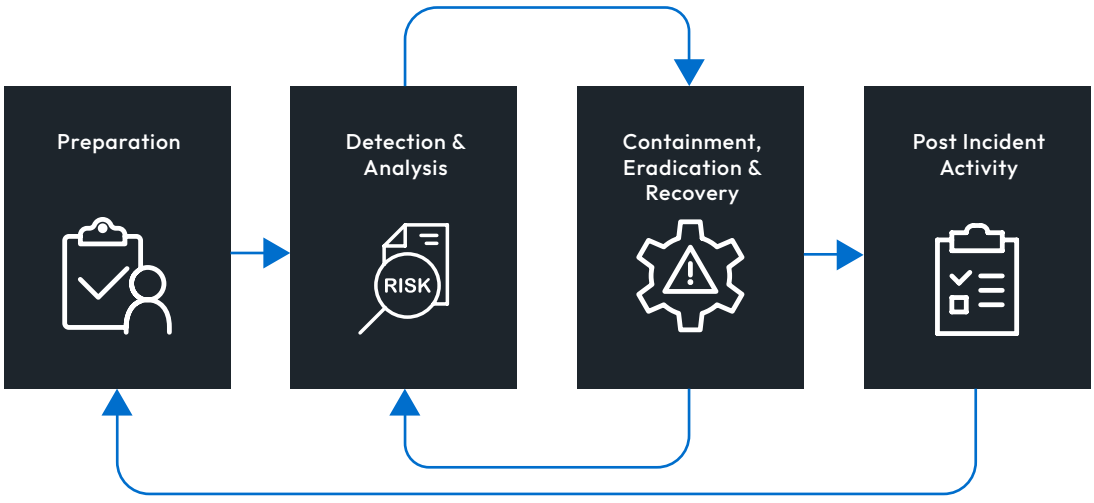
The Incident Response team will be engaged for initial discovery and information gathering about the potential incident and guide you through the entire cyber event lifecycle, from initial incident identification through to lessons learnt, supporting you with the decision-making processes experienced during an incident to help limit the chance of reputation damage and restore service as quickly as possible.

Technical & strategic services that can be used with the IR Retainer

Advisory Services including IR planning & Tabletop exercises • Compromise Assessments • Threat Hunting • System Hardening

What is classed as a cyber-incident?

Website attack • Data compromise • Business Email Compromise • Malware infection • Ransomware • Insider threat • Denial of Service (DOS/DDOS)



Whilst the vast majority of incidents can be handled remotely, should a site visit be required (for example where remote access to data is not possible) then we can dispatch one of our Incident Response resources.

CyberGuard Assurance includes 2 days for Incident Response. The incident team leader will estimate if additional time is required beyond the initial 2 days, during an active incident, on the basis of a preferential hourly rate going forward.

Cloud Configuration Security Assessment

The world of cyber security is constantly changing as new vulnerabilities are found, and new attack vehicles are created to exploit these. As organisations adopt cloud-based solutions such as Microsoft 365 it is unlikely that the security controls you have relied upon in the past will fully protect your environment. The use of cloud-based solutions for collaboration and information sharing has created new opportunities for exploitation. It is highly recommended that your security posture is tested regularly to make sure that holes are identified and fixed before cyber criminals have a chance to exploit them.

Microsoft 365 includes a suite of security features to address these risks. However, for these features to work, they must be properly deployed and understood. The often-complicated modifications necessary to maintain appropriate security must be carefully considered alongside an impact assessment. CyberGuard Assurance can optionally include cloud assessment services that can:

- Help you to make the best use of Microsoft 365 security features, to enhance your security, availability, and service uptime, balanced with an improved user experience
- Help you to understand the key risks and dependencies for your workplace
- Receive a report with recommendations on how you can strengthen your Microsoft 365 security posture from your current position

Microsoft Office 365

Microsoft cloud services and in particular the Microsoft 365 platform provides attackers with a large attack vector which has typically fallen outside of the traditional security controls and testing schedules.

The risk of not securing Microsoft 365 as a critical area of the business is extremely high. Our team of highly skilled security experts have developed an understanding of the common attack TTPs (Tactics, Techniques and Procedures) used by attackers, the areas of the platform which are commonly exploited due to weak or incorrect configurations and the options available both out of the box and/or as an add-on to help you to secure this environment.

Technical & strategic services that can be used with the IR Retainer

- **A security and breach assessment, to investigate and identify the current status and any possible breach that may have already taken place.**
  - **Configuration and protection policy audit**
  - **MFA and MDM configuration**
  - **Admin users / permissions and conditional access**
- **Secure configuration recommendations and changes in the form of a report**

If we jointly agree subsequent requirements to be completed by Wavenet outside of this, an estimate will be provided based on an additional day rate.

Copilot AI Readiness Assessment

Microsoft Copilot AI technology is on the verge of revolutionising the way businesses operate

Copilot for Microsoft 365 is an AI-powered assistant that helps users to create, communicate, and collaborate more effectively, promising to revolutionise how you and your colleagues use tools such as Word, Outlook, and Excel, to name a few.

Discover if you're ready for Copilot with our readiness assessment, preparing your organisation for AI while helping you remediate risk, optimise efficiency, and implement user-centric improvements. You will receive tailored recommendations, actionable next steps, and a clear view to overcoming any obstacles to adoption.

The CyberGuard consultant will conduct an assessment focusing on Co-Pilot readiness, Identity and Access Management (IAM), Information Protection & Data Loss Prevention (DLP), and data protection processes. This will include an introductory session outlining the objectives and methodology of our assessment.

Assessment Process

The assessment focus will be on understanding your organisation's readiness for Co-Pilot, evaluating key aspects such as knowledge, skills, and competencies, essential for effective governance, risk management, and compliance (GRC).

Specific attention will be given to Identity and Access Management, examining processes such as user provisioning, authentication mechanisms, and access controls. Strengths and areas for improvement will be identified to enhance overall security posture in readiness for AI adoption.

An assessment of the effectiveness of your organisation's Information Protection & Data Loss Prevention strategies will be conducted to review data classification policies, data loss prevention measures and data protection processes. The assessment will aim to identify vulnerabilities and propose strategies to mitigate risks and protect sensitive data from potential breaches.

Deliverable

At the conclusion of the assessment, the results will be presented to key stakeholders. This will include a detailed report summarising the results, along with actionable recommendations for improvement. We will highlight areas for enhancement and provide guidance on implementing best practices to strengthen Co-Pilot readiness, bolster GRC practices, and enhance data protection processes across your organisation.

If we jointly agree subsequent requirements to be completed by Wavenet outside of this, an estimate will be provided based on an additional day rate.

Security Awareness Phishing Training

Users can be either your weakest link or your best asset in defence against a cyber-attack

Cyber security awareness training for staff is a critical (but often overlooked) part of protecting a business.

CyberGuard Assurance can optionally include an awareness programme as an add-on service, to educate employees about keeping security in the forefront of their minds and driving home the importance that due diligence is imperative.

Having a team of staff that understand the risks and are encouraged to report potential issues will greatly enhance your chances of protecting your business. It's a fact that your end-users are often the weakest link in your network security.

CyberGuard's extensive security and awareness training helps users identify potential risks and provides mechanisms for validating and reporting suspicious emails. The most common ways employees are targeted by cyber criminals are:

- Ransomware
- Malware
- CEO fraud
- Compliance failure
- Phishing attacks
- Spear phishing attacks
- Executive whaling
- Social engineering

91% of all successful data breaches start with an email

Security and awareness training helps users identify potential risks, and provides mechanisms for validating and reporting suspicious emails. The service optionally included as an add-on with CyberGuard Assurance can include the following activities.

- **Phishing attacks:** We'll attempt to compromise the users' accounts and identify employees who are not working with cyber security in mind and who have weak passwords and network security. Month-on-month, an improvement in employee cyber behaviour is expected.
- **Video training:** Engaging video content on the issues around cyber security is made to all staff, or selected staff with specific learning requirements.
- **Password check:** We'll run our state-of-the-art password checker, bi-annually, to pinpoint domain passwords that do not adhere to password protocols. We'll inform employees of the need to change their password and offer advice on how to set a secure but memorable password.
- **Reporting and validation service:** With a simple click, emails can be sent to the security team at CyberGuard who will forensically analyse the email to check if it is genuine and return to it to the user if it is safe.
- **Quarterly cyber security newsletter:** Delivered every quarter by email to all employees with useful hints, tips and ideas for working securely.

How to get started

1 Schedule a consultation

2 A customised proposal

3 Quick and easy setup

4 Ongoing support

Step 1:

To begin, schedule a brief consultation with our team. This initial discussion helps us understand your current cybersecurity state and specific needs. We will ask a few essential questions about:

- The number of users in your organisation
- The number of IP addresses that need scanning
- Any particular cybersecurity challenges or priorities you have

Step 2:

Based on the consultation, we will provide a tailored proposal outlining the services that best meet your requirements. This proposal will detail the monthly subscription cost and the specific services included, ensuring complete transparency.

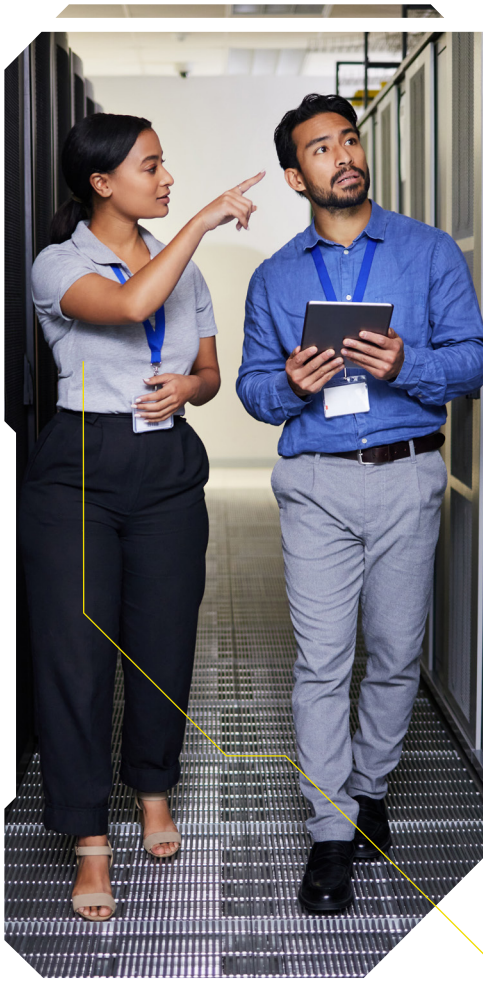
Step 3:

Once you approve the proposal, we move quickly to set up your services. Our process is designed to be as streamlined as possible, minimising disruption to your daily operations. We handle all the technical details and heavy lifting, ensuring a smooth integration with your existing systems.

Step 4:

After setup, you'll have continuous access to our comprehensive suite of cybersecurity services. Our dedicated account managers will provide ongoing support and ensure that all services are running optimally.

We believe in a hands-on approach, making sure you always have the assistance you need to navigate any cybersecurity challenges.



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