vivo comms

EBOOK

Secure your business with CyberGuard

Cybersecurity services to protect your networks and data around the clock.

EBOOK

Secure your business with CyberGuard

Contents

Introduction 3

Challenges to overcome 4

The solution 5

Our services 6

Managed security operation centre 6

Incident response 8

Penetration testing services 9

Who we work with 10

Customer quotes 11

Who are VivoComms 12

Introduction

In recent years, where technology permeates almost every aspect of a business's operations, it is more crucial than ever to protect company data and assets from cyber crime. From data breaches to ransomware attacks, hackers are constantly devising new ways to exploit vulnerabilities and compromise sensitive information.

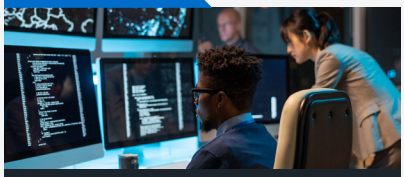
As the frequency and sophistication of attacks continue to evolve, organisations face the complex challenge of keeping up. Cyber security services need to become more advanced to meet the evolving threats that continue to be a business risk.

The cyber Security mix

A good security offering now needs to contain a mixture of the following services to be complete:

Managed Detection & Response

Pen-testing



Incident Response

Training & Certification

Security Posture Review

Managed Firewall

The challenge is to continually monitor your security posture and act quickly when a problem is found.

CyberGuard Professional Services

CyberGuard's professional services have been developed to defend your business operations from ever-evolving cyber threats.

We can provide a complete suite of cyber security services supported by a dedicated team of certified experts utilising the latest tools and methodologies. Services include comprehensive intrusion testing and in depth incident response, strategic security planning and road maps, risk assessment, vCISO, security awareness training, certifications and accreditations.

Challenges to overcome

Sophisticated infrastructures require sophisticated security

The adoption of mobility, IoT and cloud-based services has introduced additional potential entry points for would-be hackers to gain access to the network.

As infrastructure becomes more distributed, it places a greater burden on organisations to effectively manage, monitor and secure their systems. Businesses now realise that they need robust, manageable and cost-effective security processes across an extended network, without inhibiting a great user experience.

Multiple companies – too many choices

Diversifying your cybersecurity strategy with multiple providers can sometimes introduce unexpected challenges. Juggling different platforms might raise integration questions and can, at times, complicate centralised oversight. This potentially impacts the efficiency of monitoring and incident responses Furthermore, harmonising communications, maintaining uniform accountability, and standardising compliance and reporting can be intricate with varied formats and metrics.

However, a collaborative approach can be the key By partnering with a primary cybersecurity provider, businesses can benefit from tailored recommendations and best-practice advice specific to their unique needs. This central point of contact can liaise and collaborate effectively with other providers, ensuring that security measures are harmoniously deployed and configured. Embracing collaboration, while having a focal point of guidance, can offer both diversity and cohesion in cybersecurity.

A managed SOC assumes the pivotal role of overseeing your security landscape. It's at the forefront, persistently monitoring for threats and ensuring prompt actions against cyber-attacks

Real-time monitoring for real-time risks

In the digital landscape, vulnerabilities and weak configurations can be the Achilles' heel of any network. The moment they emerge, cyber criminals, ever-vigilant, are ready to working to exploit them. These threat actors relentlessly probe systems, hunting for any chink in the armour. For businesses, this necessitates not just periodic check-ins, but continuous, 24/7 surveillance.

Real-time dashboards have become essential tools, offering instant visibility into pressing events within their infrastructure that demand swift action. Coupled with expert recommendations, they pave the way for swift remediation. With unyielding 24/7 oversight and timely reporting, businesses can confidently navigate the cyber realm, assured of their fortifications.

The solution

VivoComms CyberGuard solution provides the very latest in cybersecurity services. With so many variations of threats and the potential of multiple security gaps within organisations, CyberGuard gives peace of mind that your security is in good, experienced hands.

Don't let the threat of cyber crime get the better of you. With the right experts at hand, and with proper preparation, you can mitigate risk. And, if the worst does happen, you can recover. We offer a range of services to help you strengthen your security from all angles.

We protect our customers from end-to-end through: Security Testing, Managed Detect & Respond Services, Security Awareness Training and Cyber Certification, and provide reassurance in the event of an attack through fast and effective Cyber Incident Response, built upon sound threat intelligence gathered by our own team of cyber analysts coupled with intel from various global sources.

Our cybersecurity services give you:

- Peace of mind with UK-based, 24/7 monitoring and response
- Intelligence-based analysis for better visibility of threats
- A proactive approach to security
- Help from trusted CREST and CHECK-accredited professionals

Benefits:

- Improve visibility with our Threat Intelligence
- Proactively monitor your infrastructure
- 24/7 UK Security Operations Centre (SOC)
- Support from a cyber security incident response team (CSIRT)

We work with leading technology providers in the cybersecurity sector, including:

Microsoft Security · paloalto NETWORKS · Qualys. · KnowBe4 Human error. Conquered. · CROWDSTRIKE

Our services

Managed Security Operation Centre

At the heart of our cybersecurity efforts lies our UK-based Security Operations Centre (SOC), operational 24/7. This dedicated team comprises seasoned and accredited cybersecurity experts, diligently sifting through a multitude of alerts from various sources.

Choosing our SOC brings many advantages. Foremost among them is the capability to detect and counteract security threats in real-time, curtailing their potential to inflict substantive damage or result in financial losses. With vigilant eyes on networks, systems, and applications, our SOC ensures that deviations and questionable activities are swiftly detected and addressed.

Features and benefits:

- Threat Detection and Response
- Incident Management
- Proactive Threat Hunting
- Enhanced Incident Response Time
- Better visibility
- Reduced costs

Our SOC delivers the following MDR services

Managed SIEM

Our state-of-the-art SIEM solutions, powered by Microsoft Sentinel, ensures a comprehensive view of your security landscape. Through intelligent log analysis and event correlation, we spotlight unusual patterns and behaviours, facilitating quicker incident response and better threat visibility.

Managed EDR

We recognise the need for a layered defence strategy. By integrating industry leaders such as Microsoft Defender and CrowdStrike, our Endpoint Detection and Response (EDR) service offers unmatched precision in pinpointing and neutralising threats at the endpoint level, well before they can proliferate.

Managed XDR

Extended Detection and Response (XDR) is a unified defence against incidents that span endpoints, identities, email, collaboration tools and cloud applications. By monitoring diverse attack surfaces and analysing the overall threat landscape, XDR provides a higher level of protection against emerging and sophisticated threats.

Managed NDR

Network Detection and Response (NDR) platforms capture network metadata, enriches it with machine learning derived security intelligence, and applies it to your detection and response use-cases. NDR continuously analyses network traffic and behaviour, enabling security teams to respond quickly and prevent potential breaches or damage.

Managed Firewalls

A robust perimeter is fundamental to cybersecurity. Our managed firewalls not only act as your organisation's first line of defence against intruders but are also continually updated and fine-tuned to adapt to evolving threat patterns, ensuring that your network boundaries remain impregnable.

Managed Vulnerability Scanning

To be forewarned is to be forearmed. Our proactive vulnerability scanning solution delves into your systems, networks, and applications, identifying potential weak points. This ensures you can act pre-emptively, fortifying vulnerabilities before they can be exploited.

Incident response

When faced with a cyber incident,time is of the essence. VivoComms Cyber Security Incident Response (CSIR) service is CREST-approved, a testament to our unparalleled expertise in the field. In the aftermath of a cyber attack, our primary focus is on swift containment, recovery, and ensuring minimal business disruption.

Our CSIR service encompasses:

- Rapid Response: Efficiently addressing security incidents to prevent further damage.
- Expert Analysis: Identifying the nature and scope of the breach, ensuring informed decisions at every step.
- Recovery and Restoration: Re-establishing the integrity of your systems and getting your operations back on track.
- Post-Incident Review: Analysing the incident to provide actionable insights, bolstering your defences for the future.

IR retainer services

For organisations seeking added peace of mind, we offer our IR Retainer Services. With this, you're not only prepared for potential incidents but also assured of priority response, ensuring even swifter action and mitigation in the event of an unforeseen breach.

Features and benefits:

- Crest Accredited
- Incident Management
- Proactive Threat Hunting
- Enhanced Incident Response Time
- Service Excellence

Penetration testing services

Penetration Testing, also known as “Pen Testing”, is a simulated cyber-attack carried out by in-house experts to assess the security of a computer system.

By simulating real-world attack scenarios, our Crest-accredited team can identify weaknesses in the system’s defences, such as misconfiguration, outdated software or insecure network settings.

They can then create an efficient defence plan against hacking attempts.

Our pen testing services include:

- Infrastructure Assessment
- Mobile and Web Application Security
- Red Team Assessment
- PCI DSS Assessment
- Stolen Device Assessment
- Physical Security Assessment
- GDPR Assessments

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CREST

Features and benefits:

- Identify Potential Vulnerabilities
- Proactive Security
- Risk Mitigation
- Compliance and Regulations
- Incident Response Planning
- Stakeholder Confidence

Who we work with

Enterprises: Large corporations in sectors such as finance, technology, manufacturing and retail

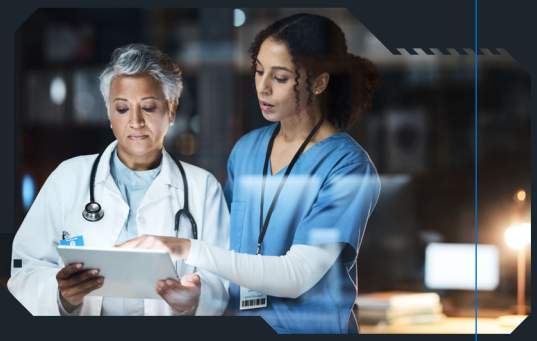
Helping to protect their sensitive data, networks and systems.

Small and Medium-sized Businesses (SMBs)

Working to provide cost-effective solutions tailored to their specific needs.

Healthcare Providers: Hospitals, clinics and healthcare organisations

Helping to secure patient information, comply with data protection regulations and ensure the continuity of critical healthcare services.



Educational Institutions: Schools, universities and educational institutions

Helping to protect student data, research and intellectual property, as well as secure their network infrastructure.

Customer quotes

The proof of concept went as well as it possibly could have, the process of integrating new systems and protocols was managed seamlessly.

Birmingham Community Healthcare NHS Foundation Trust

The cybersecurity services provided have given us, as a business and as individual users, the confidence to resume normal working practices after the 2019 cyber-attack.

Balfours

The stable infrastructure and support they provide for us allow us to keep doing what we do with new and exciting ways to enhance the patient experience that we feel sets us apart in our industry.

MYA Clinics Ltd

We can always rely on VivoComms to be ahead of the curve in providing new and innovative technologies to the marketplace and by doing so they have helped keep our business ahead of the competition.

Berry Palmer and Lyle Global

GET STARTED

Build business resilience and improve your security strategy with Wavenet.

CyberGuard Technologies is the security division of Wavenet. We provide a suite of fully managed end-to-end security services from a 24/7 UK security operations centre. Our cyber defences protect against the potential devastation of an attack from cyber-criminals including defending your finances, identity, reputation, data and your customers' confidential information.

We provide cybersecurity, communications and technology-managed services that grow with your business – no matter what the future holds.

We focus on finding the right cybersecurity solutions so you can focus on what matters most to your business – for today and tomorrow. Always thinking ahead, we give you the confidence that when you work with us, we'll future proof your business.

Talk to us

WWW.VIVOCOMMS.CO.UK

02476 620 250

Vivo Telecommunications Ltd
Friars House
Manor House Drive
Coventry
CV1 2TE

contact@vivotelecommunications.co.uk

vivo comms

Networking & Connectivity

Unified Communications & Voice

Contact Centres

Mobile Solutions & IoT

IT, Cloud & Technology

Network Intelligence

Cyberguard