CYBERHUB

LAYERED CYBER SECURITY SOLUTIONS TO PROTECT YOUR CUSTOMERS INFRASTRUCTURE

www.cyberhub.biz

Why is there a need for Email Security?

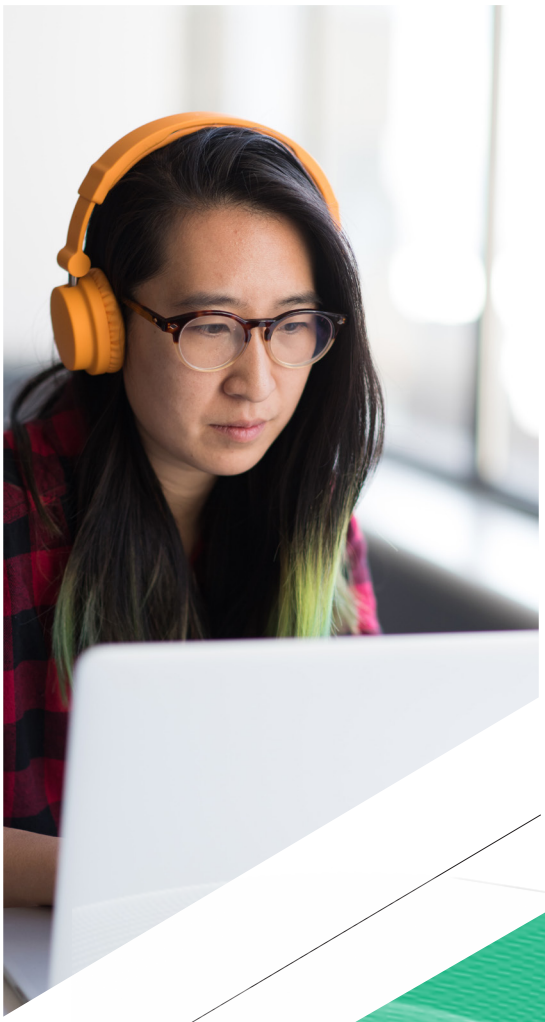
91% OF CYBER ATTACKS START WITH A PHISHING EMAIL

Introduction

CyberHub are a distributor focused on layered cyber security solutions, specifically tailored towards Managed Service Providers and Value-Added Resellers looking to adapt their business model to an ever-changing IT landscape which requires end-to-end cyber security services that protects organisations from threats.

CyberHub's partnership with their vendors is cultivated to bring growth to their channel partners both in terms of reoccurring revenue and a relevant set of products that meets the modern threat landscape.

Our vendors share one characteristic, best of breed cybersecurity products tailored for MSPs.



Channel Partner

We help to meet the demand for cybersecurity by discovering innovative, emerging cybersecurity solutions. We support and empower our partners to stay competitive, protecting themselves and their clients through relevant, scalable, multi-vendor technology partners.

Vender

Looking to expand your footprint into Africa? We understand the threat landscape and what a solid security stack should entail. With cybersecurity growing, offering the right cybersecurity solutions to support our channel partners to stay ahead of cyberthreats is key, enabling channel partners to be the most helpful to the SMB market.

Business

South Africa has the third highest number of cybercrime victims worldwide. Cyberattacks can threaten businesses of any size, small businesses are particularly more vulnerable to cyber threats because cyber criminals know they have fewer resources to defend themselves against cyber-attacks.

Cyber Security Layers

We live in a world where cyber-attacks are coming from multiple vectors (email, end point, network, and more). And one-layer traditional Anti-virus approach no longer enough to keep your business safe

A mindset shift to a more proactive multi layered cyber security approach is required.

A layered security approach is about having different security controls, at different levels that factor in different types of threats to protect assets to help ensure that each defence component covers its threat vector, strengthening your overall security posture. Making it more challenging to find ways to infiltrate the system. Lowering your risk of a breach.

It is recommended that all businesses have multiple layers of security to protection their business not matter the size.

Cyber Security Layers

Human Element

Cyber criminals rely heavily on user interaction and behaviours. For this reason, educating and training end-user's is key in helping them identify socially engineered attacks be they in the form of phishing emails, impersonating websites & attempts via internet messaging to get users to open malicious links.

Cloud

Cloud security needs to be a layer in your cybersecurity infrastructure if you have migrated all or some of your IT systems and operations to the cloud.

Network

Preventing unauthorised people or programs from accessing your networks and the devices connected to them. Keeping email and web gateways protected is the only way to ensure you aren't bombarded with malicious attacks, as well as stopping data loss that could damage a business and put you in breach of compliance.

Endpoint

An endpoint is a device such as Laptops, desktops, mobile phones, tablets, printers, or other wireless devices, servers, and virtual environments. The Problem is that all these endpoints are vulnerable to a cyberattack and could easily serve as an entry point for unauthorised users. Cybercriminals are constantly devising new ways to take advantage of employees, infiltrate networks, and steal private information.

Data

Data security is not just important for organizations. Data protection comes into play on the personal computers, tablets, and mobile devices as it has moved to the cloud and accessed through the internet. Hackers know the importance of your information and they want to exploit this, stealing it by any means.

Solutions

Bob's Business
Cyber Security Awareness Training

Bob's Business makes cyber security courses fun, engaging and approachable for employees at all levels of your organisation.

Human error accounts for 4 out of the top 5 causes of data breaches (ICO). Technology alone cannot protect the modern organisation, which is why Bob's Business created Cyber Security Awareness Culture to raise staff awareness, reduce organisational risk of breaches, positively change cultures, and ensure compliance for organisations large and small.

Bob's Business's unique, jargon-free, animated cyber security training courses are tailored to transform the cyber awareness culture of your workforce and with engagement rates of over 90%, there is no better way to strengthen your human firewall.

Combining their engaging cyber security courses with a brand-new Employee Vulnerability Assessment and their award-winning phishing simulation, Think Before You Click, it's a truly unique approach.

CELERIUM

Businesses are under attack, small businesses are easy targets.

While traditional cyber security companies focus on developing complex, expensive products designed for large organizations with dedicated cyber security analysts and experts, small businesses are watching their spends, and without the resources to invest in even basic levels of protection, small businesses are particularly vulnerable to cyber-attacks.

Celerium (formally known as Dark Cubed) offers a smarter cyber security solution built from the ground up for small and medium sized organizations that focuses on identifying malicious IP addresses from where threat actors operate and blocking them automatically before they can secure a foothold on your network.

Designed to be lightweight, affordable, autonomous, and easily deployed in ten minutes, it requires no in-house security expertise to operate. And, because it focuses on the root cause of all cyber-attacks, Celerium can materially reduce the risk of a successful breach of your network.

Easy NAC

What is Easy NAC?

Easy NAC is a powerful Network Access Control solution designed to streamline and enhance network security. It provides organisations with a simplified approach to managing and controlling access to their network resources.

Key Features and Benefits

- Seamless Integration: Easy NAC seamlessly integrates with existing network infrastruc ture, making deployment quick and hassle-free.
- Comprehensive Access Control: It allows administrators to define and enforce granular access policies, ensuring only authorised devices and users can connect to the network.
- Endpoint Compliance: Easy NAC verifies the compliance status of endpoints, such as anti virus software, operating system updates, and firewall settings, before granting network access.
- Guest Access Management: Administrators can easily create and manage guest accounts with customised access permissions, ensuring secure and controlled guest connectivity.
- Real-time Monitoring and Alerts: Easy NAC provides real-time visibility into network ac cess attempts and sends alerts for any suspicious activities, enabling swift response to potential threats.
- Reporting and Analytics: It offers comprehensive reporting and analytics capabilities, al lowing organizations to gain insights into network usage, security incidents, and compli ance posture.

How Does Easy NAC Work?

Easy NAC operates on the principle of endpoint authentication and authorization. When a device attempts to connect to the network, Easy NAC verifies its identity, checks for compliance with security policies, and grants or denies access based on predefined rules. It supports various authentication methods, including 802.1X, MAC address, and web-based login.

Deployment and Management

Easy NAC is designed to be user-friendly, with an intuitive interface that simplifies configuration and management tasks. It supports both on-premises and cloud-based deployments, providing flexibility to suit different organisational needs.

For more information and a detailed demonstration of Easy NAC, please visit our website or contact our sales team.

Solutions

Improve your client's end-user awareness and their ability to recognise phishing attempts with confidence. This is your client's opportunity to test their users with real-time, realistic phishing emails. Will they spot something 'phishy' going on?

Online training portal - Users access their own portal to take online courses at times convenient to them, anywhere at any time, on any device.

Executive training modules - Our executive training modules explain cyber risk in a business con-text. Building company culture starts at the top.

Knowledge assessments - All security awareness modules include short knowledge assessments to rein-force training, ensuring understanding of key subjects.

Multi-client monitoring – Simplify client management with a centralised multi-tenant dashboard. Sit back and monitor client progress or take charge and provide them the managed service they need.

White labelling to hero your brand – We're not precious on branding, use your own on a 100% white-la-bel platform… go be the Hero.

Simple licensing and competitive pricing – Generate attractive margins and a recurring revenue stream with the most competitive pricing on the market and no business overhead.

- No setup fees.
- No minimum order or term.
- No required revenue targets

Solutions

mailprotector

Mailprotector is a cloud-based email security and management platform that offers a comprehensive suite of solutions to protect businesses of all sizes from cyber threats. Founded in 2000, Mailprotector has estab-lished itself as a leading provider of email security solutions, with a mission to make email safer and more efficient for businesses around the world.

The Mailprotector platform provides a range of email security solutions including inbound and outbound email filtering, email encryption, email archiving, and email continuity. These solutions are designed to pro-tect businesses from phishing attacks, malware, ransomware, and other cyber threats that can compromise sensitive data and disrupt operations.

With a commitment to simplicity, reliability, and ease-of-use, Mailprotector offers an intuitive platform that is easy to deploy and manage. The company's solutions are compatible with most email services and plat-forms, including Office 365, Exchange, G Suite, and more.

At Mailprotector, the team is dedicated to providing outstanding customer support and ensuring that businesses are protected from email-based threats. Their team of experts are available 24/7 to provide support and guidance, and the company offers a range of training resources to help businesses make the most of their email security solutions.

Mailprotector is trusted by thousands of businesses around the world, including healthcare providers, financial institutions, legal firms, and government agencies. With a focus on innovation, customer satisfac-tion, and industry-leading email security solutions, Mailprotector is committed to helping businesses thrive in a world where email threats are becoming increasingly sophisticated and dangerous.

Solutions

Remediant

Privileged Access Management (PAM) is a solution that helps organisations restrict privileged access within an existing Active Directory environment A PAM solution such as Remediant offers a secure, streamlined way to authorise and monitor all privileged users for all relevant systems ticking compliance boxes.

The Remediant approach is built upon the principle of Zero Standing Privilege, Remediant's award-winning SecureONE PAM software delivers just enough, just in time privileged access and continuous discovery with agentless, vault-less simplicity – unlike bloated, complex legacy PAM solutions that leave unprotected attack surfaces and are difficult to deploy. SecureONE protects millions of endpoints and has been adopted by major enterprises across a number of industries.

SOFTACTIVITY

Problems at the office? Employees shopping on eBay or wasting time on Facebook? Doing everything but working? Or worse, stealing company intellectual property?

The workplace is changing rapidly. More companies are rolling out remote work programs. With remote workers, user activity monitoring is far more critical. This is because, with any remote employee, you are limited in the ways that you can observe and control their work-related activity.

Remotely monitor employee computers on your network in real time. Monitor users on: Workstations, Laptops, Desktop Computers in a private network, and VM or VDI environment or choose to monitor Remote Workers on: Terminal Servers, Windows Server, Citrix Virtual Apps/XenApp, RDP/RDS server farms.

Trusted by 10,000+ organizations in 150+ countries, serving customers in a variety of industries: financial, IT services & MSP, manufacturing & industrial, wholesale & retail, insurance, healthcare, education, government and law enforcement, and more.

Solutions

SPECOPS
AN OUTPOST24 COMPANY

IT security starts with strengthening the weakest link – passwords. Specops Software is a leading password management and authentication solution vendor.

Create and manage an AD password policy. Simplify passwords for users and place the burden on au-then-tication systems. A third-party password policy solution can help users create stronger passwords.

Enterprise Password Management. Your clients are likely using dozens of logins during their working day. Bring the same level of protections you want on an Activity Directory password to the rest of the passwords in use in their organisations.

Password reset best practices. Security is key when evaluating a self-service password reset tool. When a user can't remember their password, they must establish their identity with another secure factor.

Active Directory Password Screening. Stop the ripple effect of breaches with a user-friendly authentication system that automatically blocks breached passwords from being used in Active Directory.

WEBROOT®
an opentext company

Webroot Endpoint Protection (Global Site Manager)

Purpose-built to save MSPs time and money, stop sophisticated attacks, streamline management and much more. The Global Site Manager is designed for service providers with complex, multi-site, multi-administered deployments. And with it's new Evasion Shield can protect against file-based and fileless script attacks, block malicious JavaScript, VBScript, PowerShell, macros, and more. Enables admins to detect scripts running in their environments and allows whitelisting for legitimate scripts.

Webroot DNS Protection

Webroot's DNS Protection is purpose-built to help MSPs solve the need for better internet security. By providing cloud-based, domain layer security that protects users externally, rather than relying entirely on the endpoint, providers can ensure that most internet threats are contained before they even reach the customer's network.

Webroot Security Awareness Training

End-users are your clients' first line of cyber defence and their weakest link. Webroot's security awareness training offers comprehensive cyber security education that MSPs can deliver to their clients, building revenue whilst enhance clients' security by educating users.

Contact Details

Botswana: +267 71 803 747
South Africa: +27 (0)10 822 7392

info@cyberhub.biz
www.cyberhub.biz

CYBERHUB