CYBERHUB

LAYERED CYBER SECURITY SOLUTIONS TO PROTECT YOUR CUSTOMERS INFRASTRUCTURE

www.cyberhub.biz

Why is there a need for Email Security?

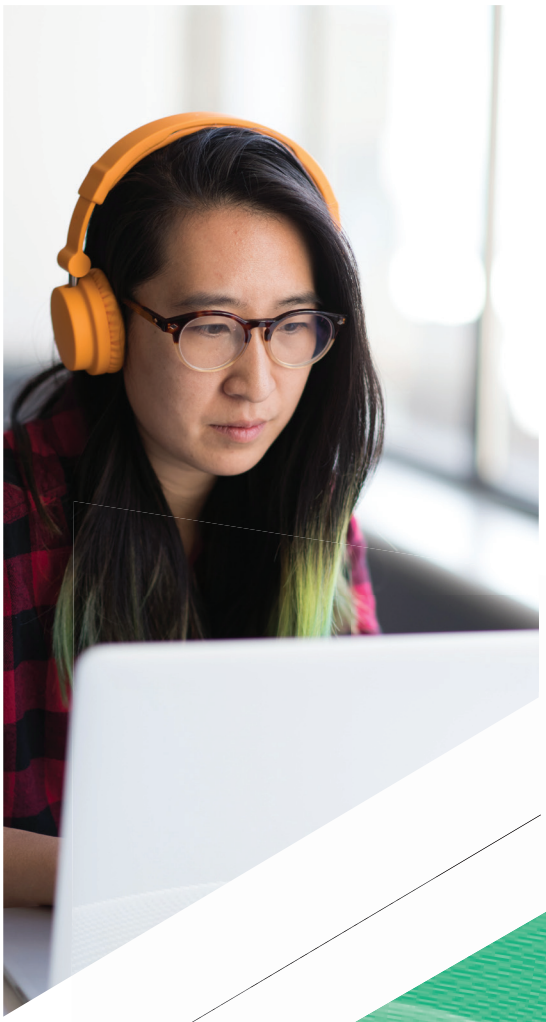
91% OF CYBER ATTACKS START WITH A PHISHING EMAIL

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

Blackpoint offers it's Gartner-recognised 24/7 Managed Detection and Response service using its patented SNAPDEfense platform, NICOS network tap, and 3rd party integrations.

Cyber threats are constantly evolving and SMBs are looking to their Managed Service Providers for a cyber security solution. Blackpoint's Security Operations Centres (SOC) is well-versed in the constantly changing threat landscape and will provide absolute and unified security for you and your clients network infrastructures – giving you peace of mind that you are secure.

Let Blackpoint's experienced MDR ream monitor, actively hunt, and respond to real-time threats using its patented SNAP-Defence platform.

SNAP-Defense Live Network Mapping & Asset Visibility

In order to best protect an organisation's infrastructure, the organisation must first know what is connect to it. With increase of smartphones, IP-enabled devices, and the Internet-of-Things (IoT), organisations need to know what devices are connected to their infrastructure, where they are, and what they are doing at all times. Blackpoint's Network Mapping + Asset Visibility feature allows you to do exactly that, obtain a bird's eye view of your network and see threat alerts fire in real-time giving you the ability to detain infected devices immediately.

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.

Solutions

CARBONITE®
an opentext™ company

From long-term backup to rapid recovery, data migration and endpoint protection, Carbonite's comprehensive platform provides a complete data protection strategy for today's growing businesses.

Carbonite Endpoint

Data created on desktops and laptops is vulnerable to ransomware, human error, hardware failures, loss, and theft. Carbonite Endpoint protects against these common data loss scenarios.
With features like geo-tracking and remote wipe, Carbonite Endpoint provides all-around endpoint data protection. So, you can take control of your critical business data–no matter where it's stored.
Carbonite Backup for Office 365
To prevent data loss in Office 365 applications, organizations need a purpose-built backup solution that ensures IT administrators can recover as much — or as little — data, as necessary. Carbonite Backup for Office 365 offers multiple options for recovering data in Office 365 applications. So, no matter the cause or extent of data loss, an IT administrator can use purpose-built tools to recover what they need and ensure users have access to their Office 365 data.

Carbonite Server

All businesses need a straightforward, complete backup and recovery solution that keeps data secure, minimizes downtime and protects company operations. Carbonite Server backup offers complete protection for physical, virtual, and legacy systems. Flexible recovery options and optional onsite hardware allow you to hit your RTO and RPO targets.

Carbonite Migrate

Carbonite Migrate quickly and easily migrates physical, virtual and cloud workloads with minimal risk and near zero downtime. The simple, automated solution allows you to avoid lock-in to a specific hypervisor, cloud vendor or piece of hardware. The streamlined process automates and consolidates numerous steps into just a few simple tasks, reducing the amount of work necessary to reach your migration goals. Once the replication is complete, you can test the target environment before cutover without impacting production workloads or users.

Carbonite Availability

Carbonite Availability enables IT organizations to maintain the highest availability of their Windows and Linux servers by using continuous replication that maintains a secondary copy without taxing the primary system or network bandwidth. With support for physical, virtual or cloud source systems or target environments, Carbonite Availability is a comprehensive option for organizations with mixed IT environments.

.

Solutions

COMODO

Activate breach protection for your business with the Dragon Platform. Their complete cloud-native frameworkdelivers zero trust architecture to protect & defend your endpoints.

Comodo's Advanced Endpoint Protection is a game-changing, validated approach that ensures that malicious software will not harm your business. Today everyone is focused on trying to stop malware. Only Comodo is focusing on stopping malware damage.

Comodo's Managed Detection & Response (MDR) Protect

Pair Managed Detection & Response with Advanced Endpoint Protection to outsource the management of your networks and endpoints to Comodo to prevent breaches.

Comodo Endpoint Manager – Standard Editions

The World's Only Centralized IT Management Platform that is Powerful, Efficient and Quick to Implement and includes features such as Remote Monitoring and Management | Service Desk | Patch Management, customized scripts, etc.

Comodo Endpoint Manager – Standard Edition – Mobile

Comodo Mobile Device Management (MDM) capabilities allow you to deploy or retire, secure, monitor and manage Android or iOS mobile devices with GPS location, wipe, and device encryption. Distribute applications, manage data and configuration settings and patching with the complete visibility and controls you need to manage any mobile device that accesses business-critical data.

Comodo MDR Force Detect Network Cloud

Comodo MDR is a 24/7 Security Operations Centre delivers as a Service (SOCaaS). Their service provides a team of security researchers who extend your IT team to safeguard your IT systems and infrastructure. Using Comodo SIEM and endpoint management technologies along with threat intelligence from the Comodo Threat Lab, their security experts hunt for vulnerabilities, continuously monitor your IT systems for indications of compromise, and contain advanced threats. They work closely with your IT team to prioritize and fix security flaws and remediate issues.

Comodo's Secure Internet Gateway

There are links to malicious websites everywhere and hackers are using sophisticated tactics to lure users into clicking them. Employees are smart, but they're not all cybersecurity experts. In under two minutes, you can deploy Secure Internet Gateway and protect your network against internet-based threats, while simultaneously preventing unproductive web browsing.

Comodo Secure Internet Gateway protects your network against all web-borne threats and enforces productive user web browsing in minutes.

Comodo's sophisticated filtering system and containment solution is designed to keep unwanted email from ever entering your network.

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

WEBROOT®

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