brigantia

What is Brigantia?

Brigantia is a value-added managed services distributor providing a comprehensive range of cyber-security solutions complemented by our secure, enterprise-class data communications and cloud services.

Brigantia has three distinct business areas designed to add maximum value to its reseller, MSP, MSSP and consultant partners' businesses:

Brigantia Distribution

Providing innovative and best-of-breed IT managed services enabling Brigantia partners to offer their end-user clients comprehensive, cost-effective IT solutions with key focuses being on the security and availability of systems, data and communications.

Brigantia Consulting

Offering GDPR and InfoSec consultancy services providing a three-stage process towards GDPR compliance as well as assistance with Cyber Essentials, Cyber Essentials Plus and ISO27001.

Brigantia Enhance

Comprising "Business Enhance" which delivers regular events, training, cost savings and rebates and "Personal Enhance" which delivers discounts and savings to our partners' owners, management and staff.

Brigantia exists to add value to all its partners' businesses

HEIMDAL™ SECURITY

The only unified cybersecurity suite

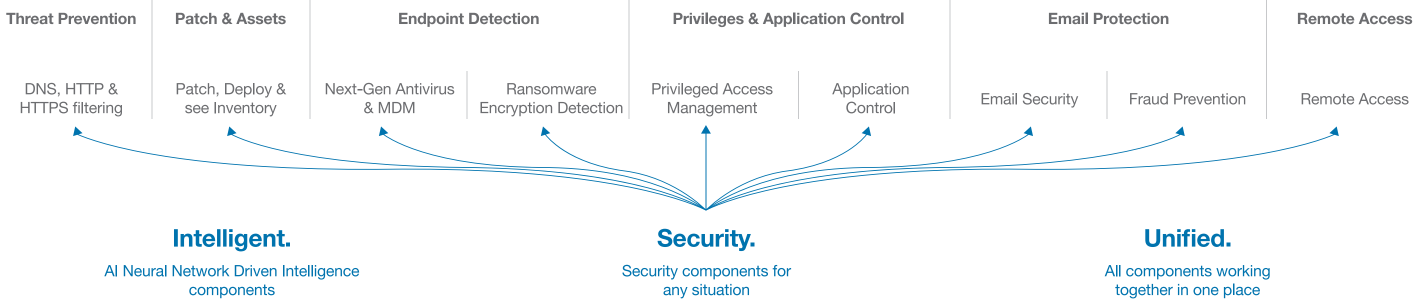
Cybersecurity solutions made simple

Heimdal Security has a fully integrated network & endpoint protection suite with ground-breaking live threat intelligence, appraised by the FBI, and with products recommended by the RBS Banking Group.

- Worked with the FBI to track and bring down the original Cryptolocker domains
- Originated from two-time winners of the Defcon CTF World Championships
- HQ in Copenhagen with two UK Offices

The only vendor in the market to have an offering to combine: next generation anti-virus, traffic filtering down to DNS level on the endpoint, and silent, automated third-party patch management.

- Multiple layers of protection to defend both corporate networks and endpoints
- Scalable solutions from one endpoint through to corporate environments
- Multiple products run through one endpoint client giving exceptional management capabilities through a single admin portal
- A recommended add-on by Microsoft



Threat Prevention: DNS, HTTP & HTTPS filtering

Patch & Assets: Patch, Deploy & see Inventory

Endpoint Detection: Next-Gen Antivirus & MDM; Ransomware Encryption Detection

Privileges & Application Control: Privileged Access Management; Application Control

Email Protection: Email Security; Fraud Prevention

Remote Access: Remote Access

Intelligent.
AI Neural Network Driven Intelligence components

Security.
Security components for any situation

Unified.
All components working together in one place

2020 Computing Security Awards WINNER

Anti APT Solution of the Year

Some of Heimdal's UK customers

Royal Bank of Scotland

twm solicitors

Brentwood School

HEIMDAL™ SECURITY

Get a grip on your Vulnerability and Patch Management and strengthen your security

Heimdal Security Patch & Asset Management

Deployment, Vulnerability and Asset Management.

Vulnerability management should be proactive and not reactive, it should not be a constant drain on time and resources, with Heimdal Security these problems are solved.

Heimdal's Patch & Asset Management features provide:

- Pre-emptive vulnerability management for both Windows and third-party applications
- Patching of third-party applications on-the-fly, anywhere in the world and according to any schedule, silently and automatically
- The ability to view and manage software inventories
- Full visibility and management via one centralised admin console, including being provided with all the tools needed for your patching / vulnerability management compliance requirements

True cyber resilience and security starts with efficient vulnerability management. It is critical for all organisations to be able to demonstrate compliance with the DPA 2018, the GDPR and the UK PSN software patching regulation.

Heimdal's Patch & Asset Management also provides a Full Software Asset Management giving the ability to:

- See any software assets in inventory, alongside their version and installed volume
- Report and demonstrate compliance
- Update or roll-back software or OS
- Un-install any software
- Allow users to install "approved" software themselves
- Set the time you wish updates to happen

The Infinity Management add-on module will allow you to deploy any software, at any location, at any time.

- Encrypted packages stored on Heimdal servers
- HTTPS transfers from Heimdal servers
- Available anywhere in the world with no need for additional infrastructure
- Ability to offer an installation catalogue set by the system administrator
- Accepts any MSI/EXE installer and offers command lines for scripting

HEIMDAL™ SECURITY

Hunt, Prevent, Detect and Respond

Heimdal Security Threat Prevention

Hunt, Prevent, Detect and Respond to Endpoint Threats.

- Working in tandem, DarkLayer Guard and VectorN Detection are the proactive, code-autonomous tools fine-tuned to layer on top of any existing security solutions.
- Threat intelligence is live from the malware infrastructure to provide a unique level of protection.
- Enhanced with TTPC (Threat To Process Correlation), clients gain the essential threat hunting tools to map out the security-critical points in their environment
- Complete with market-leading Predictive DNS (AI & ML algorithm that is capable of predicting a domain is malicious before it even hosts any malicious content)

DARKLAYER GUARD™

DarkLayer Guard is the essential Host-Based Intrusion Prevention System (HIPS).

- Unique 2-way traffic filtering engine
- Supports fully customisable category-based content filtering
- Block network communication to mitigate Zero Hour exploits, ransomware and data leaks
- Using Heimdal's ground-breaking Threat To Process Correlation technology, an organisation can identify attacking processes and provide HIPS capabilities for endpoints

10,975
MALICIOUS DOMAINS

The number of malicious domains removed monthly in the UK, by one agency alone.

– NCSC.gov.uk

1,783
RANSOMWARE COMPLAINTS

The number of complaints filed to The Internet Crime Complaint Center (IC3), with an average of 5 victims daily.

– FBI

VECTOR^N DETECTION™

VectorN Detection leads the way with code-autonomous detection to find threats unseen by next-generation anti-virus and code scanners.

- Tracks device-to-infrastructure communication to detect second generation malware strains that no other product can spot
- Uses machine learning to establish compromise patterns and offer indicators of compromise/attack
- Complements and boosts any other endpoint security

By leveraging the unique intelligence gained through blocking threats at the DNS, HTTP and HTTPS level, DarkLayer Guard and VectorN Detection not only give the power to stop active attacks, but they also accelerate the investigation process.

Traditionally, deploying a new security solution has been daunting with potentially a high cost! With Heimdal's Threat Prevention this is not the case.

Heimdal's Threat Prevention is compatible with any existing endpoint security solutions or other Heimdal Security modules.

Available on

3,785
CORPORATE DATA BREACHES

In 2017, as recorded in The Internet Crime Complaint Center (IC3). On average, 10 data breaches happen daily.

- FBI

79%
DNS ATTACKS IN 2020

Nearly 4 out of 5 organisations (79%) have experienced a DNS attack in 2020.

– IDC 2020 Global DNS Threat Report

HEIMDAL™ SECURITY

Next-gen Antivirus With Market-leading Mitigation for Stronger Endpoint Security

Heimdal Security Next-Generation Endpoint Antivirus

Antivirus remains an integral part of protecting any network.

In an ever-changing threat landscape, impeccable detection and powerful mitigation is a fundamental security layer.

Heimdal's Next-Generation Endpoint Antivirus combines the techniques known by both traditional and next-gen Antivirus to detect and remediate viruses, APTs, financial fraud, ransomware and data leaks.

Heimdal's Next-Generation Endpoint Antivirus Provides

- Impeccable detection and market leading mitigation
- Low impact local file/signature scanning
- Active registry change scanning
- Real-time cloud scanning with detection through machine learning
- Sandbox and backdoor inspection capability

Heimdal's Next-Generation Endpoint Antivirus leads the field in malware testing on its own. When supplied with Heimdal's Threat Prevention, thus gaining Heimdal's live intelligence feed, it gains the ability to mitigate otherwise hidden threats and provides essential EDR (Endpoint Detection and Response).

MDM is included free of charge and includes:
Heimdal's MDM solution is offered directly as part of the APP that also offers Threat Prevention and Next-Gen AV for mobile.

It will offer you the ability to remotely track and manage devices:

- Can remote Locate devices
- Can remote Wipe devices
- Can remote Lock devices

*IOS does not support Threat Prevention DNS Filtering or Next-Gen AV

Available on

Firewall
Incoming attack prevention

Using connection and login activity scanning our firewall offers all the traditional firewall features, such as port and application management, as well as unique features such as **Brute Force Ransomware** prevention and device **Isolation**.

AV - Stage 1:
Local File/Signature & Registry scanning

Our Next-Gen AV uses real-time **low impact** in-memory and oil and signature scanning, combined with active registry change scanning to provide leading edge traditional type Antivirus detection and mitigation.

AV - Stage 2:
Real-Time Cloud Scanning

All files not known to the local database are sent to our cloud for scanning. Using 1000 CPU cores topped with **Machine Learning Detection** algorithms, we add another dimension to detection.

AV - Stage 3:
Sandbox and backdoor inspection

Files that still do not show as malware, enter our **sandbox** to see if they act as malware. This is done by also checking the file communication to see if it tries to contact **Command and Control servers**.

AV - Stage 4:
Process Behaviour based scanning

When files start to execute our Next-Gen AV continues to monitor precesses and process changes with Heuristic, **Behaviour engines** to give our X-Gen Antivirus the ability to detect code changes at all levels.

Tested by VB100 - with 100% detection!
3 times in a row

Independent Tests of
Anti-Virus Software

OPSWAT
CERTIFIED

MailSentry™
E-MAIL SECURITY

No more doubt, no more dangerous emails

Heimdal Thor MailSentry

Keep the spam and email malware problem under control effortlessly, with minimal time investment for your sys-admins.

Over 55% of all incoming emails are spam, seeping your attention away from the legitimate ones. But beyond the wasted time, spam emails are also dangerous.

MailSentry Email Security will keep your inboxes clean and lean.

Eliminate the hassle and danger of churning out spam emails and allow your employees to just focus on the work that matters.

MailSentry Email Security is the professional spam and email malware filter solution that corporate environments can now rely on. The multiple analysis vectors apply technological expertise to scan for all possible cues and seamlessly filter spam out of your organisation's inboxes.

Step up now and stop spam and email malware. We're here to help.

MailSentry Email Security uses an entire array of technologies to detect and block spam, malware and ransomware threats before they compromise your IT system through malicious emails.

Compatible with our advanced technology for combating fraud. The advanced spam and malware filter MailSentry Email Security is also compatible with MailSentry Fraud Prevention, a module especially designed to combat the growing threat of Business Email Compromise (BEC) attacks.

Your business and employees will be spared from:

- The pervasive, evolving threat of phishing
- The again-growing threat of ransomware
- Malicious links and attachments
- Email exploits and botnet attacks
- The frustration of having to click away through never-ending spam emails
- Emails coming from infected IPs and / or domains
- Unwanted content
- Botnet attacks through email
- Advanced spam

Spam emails are today a growing threat

They flood inboxes, diminish productivity and bring a host of cybersecurity dangers like malware, ransomware or phishing.

A professional spam and malware filter keeps all that safely away.

brigantia

Brigantia Distribution - Email Security

MailSentry Email Security will keep guard, so you don't have to.

Benefits	MailSentry Email Security Standard Version	MailSentry Email Security Advanced Version	MailSentry Fraud Prevention (our add-on for fighting BEC attacks)	Manually Checking and Sorting Emails	Regular Spam Filters
MX Record based setup	✓	✓	✗	✗	✗
Anti-Spam	✓	✓	✗	✗	✓
Botnet protection	✓	✓	✗	✗	✗
Highly accurate spam-filter	✓	✓	✗	✗	✗
DKIM/SPF & DMARC sender check	✓	✓	✓	✗	✗
Advanced malware filtering	✓	✓	✗	✗	✗
Protection against ransomware	✓	✓	✗	✗	✗
Phishing protection	✓	✓	✓	✗	✗
Threat tracing	✓	✓	✗	✗	✗
Full audit log	✓	✓	✗	✗	✗
Web-based administration	✓	✓	✓	✗	✗
Office 365 integration	✓	✓	✓	✗	✓
Personal quarantine email	✓	✓	✗	✗	✗
ISO27001 Certified Hosting	✓	✓	✓	✗	✗
SOC2 Certified Hosting	✓	✓	✓	✗	✗
ISAE 3000 Certified Email Service	✓	✓	✓	✗	✗
90 Days email relay included	✓	✓	✗	✗	✗
Real-Time formatting check of attachments	✗	✓	✓	✗	✗
Deep attachment scanner	✗	✓	✓	✗	✗
Deep content inspection	✗	✓	✓	✗	✗
Protection against advanced email threats	✗	✓	✓	✗	✗
Full forensic data logging of the email	✗	✓	✗	✗	✗
Customisable threat alerts	✗	✓	✗	✗	✗
Fast detection of fraud attempts	✗	✗	✓	✗	✗
Fast detection of spoofed emails	✗	✗	✓	✗	✗
Fast detection of CEO fraud	✗	✗	✓	✗	✗
Fast detection of imposter threat	✗	✗	✓	✗	✗
Fast detection of man-in-the-email attacks	✗	✗	✓	✗	✗
Saved time from manual background checks	✓	✓	✓	✗	✗
Professional 24/7 support	✓	✓	✓	✗	✗
Detection of modified invoices	✗	✗	✓	✗	✗

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

MailSentry™ FRAUD-PROTECTION

Adds a new layer of security to any existing email filtering solution

Heimdal Thor MailSentry

MailSentry uses more than 125 vectors of analysis, together with advanced threat intelligence, to detect and prevent Business Email Compromise (BEC), CEO Fraud, phishing and complex malware before they reach the user. MailSentry adds a new layer of security to any existing email filtering solutions.

The global cost of email fraud according to the FBI

$12.5 billion per year

Eliminate imposter and insider threat due to BEC scams

The average number of BEC attacks per month has risen by 120% between 2016 and 2018.

BEC attacks are a form of social engineering. They prey on people's trusting and cooperating nature in order to cause damage. Thor MailSentry™ utilises unique technology to scan for all possible cues and to detect BEC attempts.

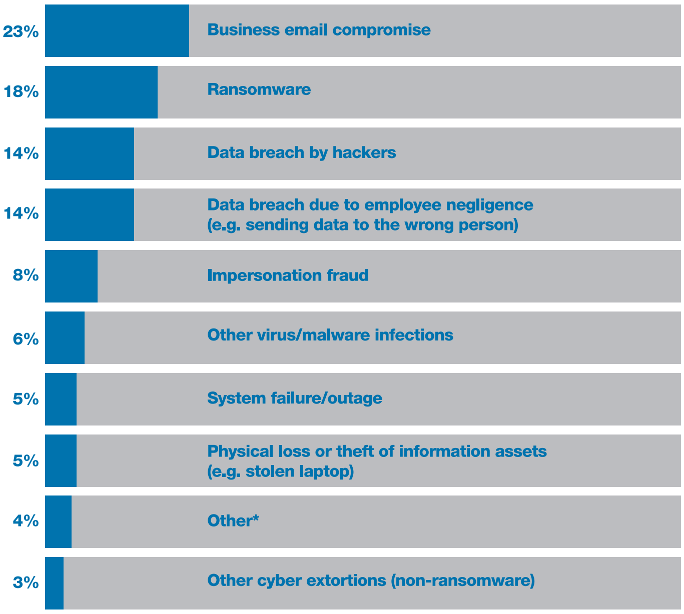
Product features

- Monitoring of all emails alongside existing email filtering solutions
- Detection of BEC, CEO Fraud, Phishing and advanced malware
- Find Imposter Threats (Modified PDFs such as invoices)
- Live monitoring and alerting 24/7 by a specialist fraud team
- Scans content of attachments in-depth wording, IBAN, SWIFT, Account numbers etc and checks bank details against known fraudulent lists to detect attacks
- Can be connected to external invoice approval systems using APIs
- Alerts you if historic emails are detected as malicious

Benefits

- Directly reduces monetary loss as a result of fraudulent invoices
- Reduce mail fraud as a result of CEO imposters and negative brand impact

Cyber Claims received by AIG EMEA (2018) - By reported incident



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations.

FORSETI

Unparalleled DNS security, threat prevention and HIPS to your network

Forseti

Forseti brings you Unparalleled DNS security, threat prevention and HIPS to your network.

This helps by greatly enhancing your protection against APTs, data leaks, ransomware and network malware.

Forseti uses Machine Learning on device-to-infrastructure communication to spot and stop attacks that firewalls can't see, offering you an essential threat hunting tool to prevent attacks on your network.

Protect your perimeter with a truly unique approach to DNS security

With Forseti, your network is protected against:

- RANSOMWARE
- DATA EXFILTRATION
- APTs
- MALWARE

Block malicious web content

Over 22% of all new domains are created for illegal purposes. And it would be impossible for your users to know exactly which websites are completely safe.

For instance, malicious code can be often found in banners on entirely legitimate websites.

But Forseti blocks access to websites containing malicious code and to servers controlled by cybercriminals. Every day, we evaluate over 300,000 domains.

Prevent data leakage

Forseti also stops communications from any existing malware intrusions, avoiding data leaks by detecting and blocking malicious traffic initiated by threats such as APTs and ransomware.

Detect advanced malware

If Forseti ever identifies an infection, we send you alerts for every type of device that's been infected, including PCs, Macs, Androids and iOS devices.

Add an extra layer of protection through advanced Machine Learning and strong, actionable intelligence

Instantly trace infections to specific users and entry points.

- Significantly raise your overall security
- Minimise your costs
- Protect your infrastructure
- Don't lose your revenue, intellectual property or productivity
- Free up your internal resources
- Access a real-time overview of your current security status

CyberSmart

Automated compliance for Cyber Essentials

CyberSmart

What is Cyber Essentials?

The government's Cyber Essentials scheme ensures basic cyber-security measures are in place, preventing approximately 80% of cyber attacks. The scheme is based on 5 controls and ensures that most vulnerabilities are secured.

Why just 5 controls?

The 5 specific controls give an organisation a high-level of cyber security without an enterprise-level cost.

- 5 basic controls provide a simplified framework, unlike ISO27001
- Despite its simplicity, Cyber Essentials prevents or mitigates as much as 99.3% of attacks (University of Lancaster study)

Times are changing, attacks are changing

- Cyber attacks are evolving constantly
- Traditional endpoint security is not enough
- Cyber Essentials gives organisations a layered approach to security

Benefits of Cyber Essentials

Cyber Essentials helps prevent the majority of cyber attacks. Even a simple virus or piece of malware could result in the loss of company and client data, disrupt cash flow, and waste time. Never mind the reputational damage a data breach can cause. Loss of data could also breach the Data Protection Act and lead to fines or prosecution.

Since October 2014, it has been mandatory to have a Cyber Essentials certification if you have any public sector or local authority contracts. Holding a Cyber Essentials badge also enables you to bid for these contracts.

Cyber Essentials covers the technical baseline for devices for GDPR, PCI-DSS, HIPPA, ISO27001 and others.

What is CyberSmart?

CyberSmart is an automated platform that allows your clients to achieve Cyber Essentials certification and maintain their compliance, easily and automatically.

The CyberSmart platform consists of two parts: a cloud-based dashboard and a device based application, that anyone, regardless of technical expertise or compliance fluency, can operate via the platform.

The cloud-based dashboard

The cloud-based dashboard is used to manage the compliance process; it allows the partner to add new organisations, check the compliance status of individual devices and allows organisations to obtain Cyber Essentials certification.

Tooltips, guides and live support ensure that anyone, regardless of technical expertise or compliance fluency, can operate the platform.

Device-based app

The CyberSmart app is deployed to all devices in the organisation. These apps periodically check and report on the compliance status of the device and give visibility on the level of compliance within the organisation.

Continuous compliance

Once certified, CyberSmart ensures you maintain compliance with ongoing monitoring and regular reporting for you and your clients; thus moving from point-in-time to ongoing protection.

The Process

The platform is designed to assist organisations in achieving Cyber Essentials certification in the easiest and shortest time possible. The entire process can be divided into four parts:

Step 1: Identify

Scanning for vulnerabilities provides the capability to identify all Cyber Essentials weaknesses. The CyberSmart app automates the search for weaknesses in the organisation's system, no prior technical knowledge is required.

Step 2: Fix

CyberSmart gives visibility of all compliance issues on devices so, armed with this information, remediation is simplified. CyberSmart is written in plain English, using smart questions and offers step-by-step guides and live online support. The technology ensures good security practices stay in place after certification.

Step 3: Certify

Security is only one part of being compliant, it is equally important for organisations to demonstrate that cyber security is taken seriously and that their data is in safe hands, which builds trust. and can limit liability in the event of a data breach. Once Cyber Essentials is achieved, the official Cyber Essentials badge is provided for use as well as a physical certificate.

Step 4: Protect

Compliance is not a once-in-a-while exercise but an ongoing process. CyberSmart quietly monitors and reports on organisational compliance allowing for the provision of real-time threat information and security updates. Annual ongoing technical support and £25K of cyber-security insurance is also included free of charge.

CyberSmart is supported on Windows, Mac OS, iOS and Android.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

islonline

Connect to a computer or remote device in seconds

Support your clients remotely

Using ISL Online you can view the screen and control the desktop to provide fast remote support for your clients.

Licensing

All in one - One ISL Online license includes remote support, remote access, live chat and web conferencing software, as well as the mobile app versions of all products.

Unlimited installations - You may run ISL Online software on an unlimited number of computers or mobile devices.

Unlimited workstations - You may connect to an unlimited number of computers.

Unlimited operators - You may create an unlimited number of operators that can host a session.

Unlimited clients - You may connect to an unlimited number of clients. The number of purchased licenses defines the number of simultaneous sessions.

Security	Remote Support	Remote Access	Live Chat	Web Conference
AES 256-Bit End-to-End	✓	✓	✓	✓
Encryption	✓	✓	✓	
Passess Firewalls	✓	✓	✓	✓
User Authentication	✓	✓	✓	✓
Unique Session Codes	✓	✓		✓
Code Signing Certificate	✓	✓	✓	✓
Personal Access Password	✓	✓	✓	✓
One-Time Access		✓		
Password		✓		

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

Features	Remote Support	Remote Access	Live Chat	Web Conference
Screen Sharing	✓	✓	✓	✓
File Transfer	✓	✓	✓	✓
Chat	✓	✓	✓	✓
VoIP & Video	✓	✓		✓
Unattended Remote Access		✓		
Multi-Monitor Support	✓	✓		
Remote Reboot and Reconnect	✓	✓		
Wake on LAN		✓		
Session Transfer	✓	✓	✓	✓
Session Recording (Export to AVI)	✓	✓		✓
Remote Printingt	✓	✓		
Unlimited File Sharing		✓		
Administrator Rights	✓	✓		
Remote System Information	✓	✓		✓
Real-Time Customer Support	✓	✓	✓	✓
Whiteboard Annotations	✓	✓		✓
Enterprise Instant Messaging			✓	
HTML/AJAX Client			✓	
IP Geolocation			✓	
Canned Responses			✓	
Online Meetings				✓
Webinar for Large Audience				✓
Import & Export Powerpoint				✓

brigantia

Brigantia Distribution - Security Training

KnowBe4
Human error. Conquered.

Manage the ongoing problem of social engineering

KnowBe4 Security Awareness Training

More than ever, employees are the weak link in an organisation's network security. They are frequently exposed to sophisticated phishing and ransomware attacks. Employees need to be trained and remain on their toes with security top of mind.

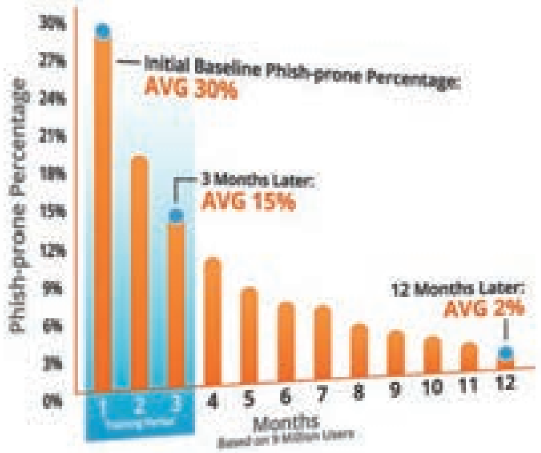
Did you know?

- 91% of successful data breaches start with a spear phishing attack
- 10-15% of phishing attacks are making it through your filters
- Ransomware has increased by 229% since 2017 with nearly 100K attacks daily
- About 30% of data breaches are caused by repeat offenders. This highlights a continued problem: Risk accumulates over time when proper education and reporting do not happen.

KnowBe4 enables employees to make smarter security decisions by training them to understand the mechanisms of spam, phishing, spear phishing, malware, ransomware, and social engineering, and then applying this knowledge in their day-to-day job. Simply put, KnowBe4 helps you build a human firewall as your last line of defence. You need this because between 10-15% of phishing attacks do make it through your filters.

In a study of more than 9 million users across nearly 30000 organisations over a 12-month period, KnowBe4 found an initial baseline Phish-prone percentage of 27% across all industries. After only 90 days of training and simulated phishing, the Phish-prone percentage dropped over half to 13%, and after 12 months, it was minimised to only 2.17% – an astounding 94% improvement in one year after using the KnowBe4 platform.

Forrester Research assessed the performance of the KnowBe4 platform in their Total Economic Impact (TEI™) Study and found a 127% return-on-investment with a one-month payback.

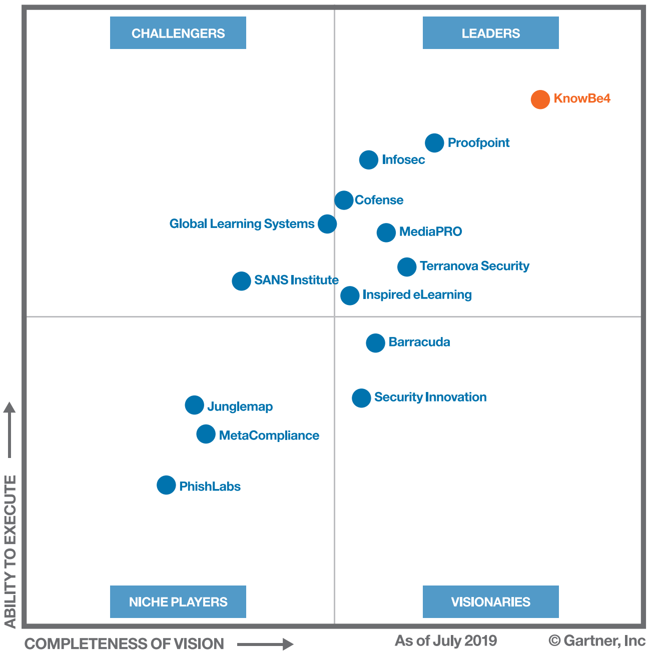


Did you know that 91% of successful data breaches started with a spear phishing attack?

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com



As of July 2019

© Gartner, Inc

Introducing KnowBe4 as a Managed Service (KaaMS) from Brigantia

Available as a full whitelabel service.

Available	KaaMS	KnowBe4 Licence Only
Access to KnowBe4 training	✓	✓
Access to KnowBe4 phishing simulations	✓	✓
Professional client consultation	✓	✗
Professional guidance & advice	✓	✗
Relevant phishing simulations	✓	✗
Custom spear-phishing campaigns	✓	✗
Appropriate training per department	✓	✗
Training fully managed and reported upon	✓	✗
Phishing fully managed and reported upon	✓	✗
Vishing fully managed and reported upon	✓	✗
USB drive tests fully managed and reported upon	✓	✗
Immediate training provided to staff who fail phishing emails	✓	✗
Monthly reporting	✓	✗
Close to zero ongoing overhead for reseller	✓	✗

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

GDPR365

The tools to demonstrate GDPR compliance

GDPR compliance management

GDPR365 is a GDPR compliance management service with powerful workflows and collaboration tools.

The suite of tools from GDPR365 enables organisations to assess, implement and monitor their data-security practices and demonstrate their compliance with data-protection regulations, thereby reducing the risks associated with non-compliance.

The platform stores all audit trails and documentation in one place, making it the perfect centre for managing compliance efforts. All the workflows and tools necessary for ensuring ongoing compliance are built into GDPR365, so it is quick and easy to demonstrate compliance to suppliers, clients, regulators and data subjects.

With everything in one place, the effort required to be compliant and the risks of non-compliance are reduced whilst also gaining valuable insights into personal data usage by the organisation.

Assess

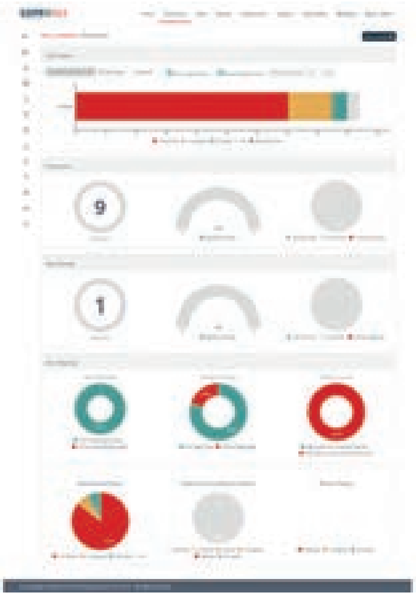
Understand the GDPR and compliance checklists so the initial review of current data protection practices is started.

Implement

Define policies and Implement processes that are needed in place to ensure compliance.

Monitor

Maintain and build on the policies and processes that are in place to ensure your GDPR compliance programme stays current as the organisation evolves.



Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

brigantia

Brigantia Distribution - Automated Compliance

Benefits for management

- Reduced risk and global oversight
- See an end-to-end picture of your GDPR compliance efforts throughout the process
- A complete overview of the organisation’s inbound and outbound personal data flows and data processing activities
- Provides an overview of volume and status of subject access requests

Reduce non-compliance risks

- Compliance checklists
- Gap and assessment readiness reports
- Records of processing activities
- Data Protection Impact Assessments

Data Subject Consent
Direct Electronic Marketing & Profiling
HR Practices
Information Use & Security
Add New

Make data security a key brand value

- Employee training on data protection
- Privacy notices and internal policies
- Data subject access request management

Understand personal data use/security

- Data mapping
- Breach management
- Processors and data sharing

Checkbox consent mechanism and privacy notices

Data protection policies and other governance documents

Data mapping workflow

Customised compliance assessment checklists

Employee training documents and training programme management

Data breach incident management

Subject access request management

Record of processors and data sharing management

Progress visibility and accountability reports

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

Managed detection and response services

bluedog

bluedog's full suite of Managed Detection and Response services provide businesses with a level of network protection typically only afforded by large corporations. bluedog brings high quality technology, support and service to the small to medium business, helping protect their business from cyber threats.

This allows you to focus on your core business, while bluedog handles your security headaches.

Voted one of the Top 10 Cyber Security Start-Ups of 2019 by Enterprise Security Magazine.

bluedog vs Traditional SOC

The significant difference with bluedog and traditional SOC, is that bluedog completely manage the monitoring, detection and response lifecycle, taking control of your cyber security and dramatically reducing the mean time to discover an incident, recover from the incident and lower the risk and total cost of the attack.

Built in at a defensive layer with an offensive angle to detect cybercrime at the earliest possible stage, bluedog can help you minimise 'the window-of opportunity for these criminals.

Managed Detection

bluedog's 24/7/365 managed monitoring provides ongoing network traffic analysis and feedback regarding your business security.

Monitoring is the window into a network's security; carried out in real time, as it changes in the face of new attacks, new threats, software updates, and reconfigurations.

Monitor

Provides valuable insight into what is going on within your network, offering visibility into your security management with assessments of your sensitive data, critical infrastructures and applications.

- IP traffic raw data
- Traffic flow and file transfer
- http and DNS queries
- Emerging threat policies
- Malware, adware
- iPhones, iPads, PC's and other devices

Analysis

Provides regular tailored reports at the frequency of your choice, which can be sent to your own IT services provider to manage, or bluedog can do that for you. The bluedog security services centre can monitor your network 24/7, providing immediate actionable recommendations and respond accordingly.

- SOC level analysis and reporting
- Global traffic and event monitoring
- Real-time data flow and analysis
- Unusual network activity

Detect

The bluedog Security Operations Centre monitors your network 24/7, providing immediate actionable recommendations.

- The qualified team of security analysts watch over your assets, making sure bad actors are not reading along with you.
- Anomalies are constantly analysed, identifying attack types and new ways attackers try to break into your company.
- The moment a problem has been detected, the bluedog incident responders kick in to fight together with you!

Respond

Whether it is general network security, through to penetration testing, anti-phishing or emergency support, bluedog have got you covered.

- Threat hunting and reporting
- Flag unusual activity (software and file transfer)
- Incident response
- Expedite network forensic investigations

bluedog features

Multi-tenancy - Monitor and manage all your customers installations through one online console

Cloud-based console - From a single console in the cloud, you can manage, monitor and report on your customer instances with no downtime

Dedicated support - Allow bluedog to manage, monitor and report on your customer’ network activity, or DIY

Compliant - No data transferred through you, or bluedog

Recurring revenue - bluedog’s low entry price point allows you to earn a higher monthly recurring fee from your customers and differentiate from the competition

Secure - VPN protected from the moment your box is plugged into your network

bluedog
SECURITY MONITORING

Provides your organisation with threat hunting services

What is MDR and why is it important?

MDR (Managed Detection & Response) is an outsourced solution that provides organisations with threat hunting services and then responds once they are discovered.

There are many MDR solutions out there but here's why we believe bluedog shines above the rest.

How do you really know what is happening in your network? You have firewall, great! You have endpoint protection, Fantastic! These are a great way of defending your network and all the data accessible upon it. However, no security system is perfect so what you have so far, think of it as a starting point.

Now is the time that you need to consider a monitoring solution for your network: This is for you to see if anything is getting through your first line of protection. Most businesses at this point look towards a SIEM (System Incident & Event Management) tool to check activity in the network. If you have several security experts monitoring the traffic and events 24/7 and knowing what they're looking for then this is a great way to maintain your network. If, however, you don't have a SOC (Security Operation Centre) in house, having a SIEM tool is next to useless…

There are thousands of events that happen in the network every day, getting through them all and identifying which ones are bad is a lot of work and could prove to be an expensive tool that you don't see much value in at all.

bluedog works differently, it provides you with a SIEM tool that you can plug in and leave, knowing that if there is ever an issue, you will be alerted to the fact straight away. bluedog has a team of qualified people watching your valuable assets 24/7, allowing you to focus on your core business. By only alerting you to only the things that matter, you're not seeing all the noise of the false positives that would otherwise waste your time.

bluedog will be alerting and reporting to you on all the below as standard:

Managed Detection

Your internal network will be monitored for malicious activity 24/7. An alert will be sent immediately when suspicious activity has been identified.

Rogue device detection

Continuously probing the network to find devices that shouldn't be there, reporting on new and re-appearing devices. Data gathered from this will help to enhance the managed detection service.

Weekly vulnerability scan on all internal IPs

Vulnerability scans help look at where the weaknesses are in the network. This way you can pay more attention to possible attacks at the most vulnerable points. Weekly reports help you to determine where the vulnerabilities are within your network, allowing you to act before the attackers have a chance to get in.

All these extra services allow you to stay in control of your network meaning that you are proactively able to shut down ways for attackers to get in. With a team of qualified people watching over all this 24/7, it means you can relax and leave the security of your business to the experts.

bluedog
SECURITY MONITORING

Strengthen your organisation with bluedog

bluedog's Microsoft 365 security & operational monitoring

Many businesses are now using Microsoft 365 to work collaboratively from anywhere. Would you know if a user has been compromised? A hacker will not usually attempt an attack until they educate themselves on user behaviour, giving a much better chance of a successful attack. This is the point you generally find out an account has been compromised but unfortunately, this is too late.

With bluedog Microsoft 365 security monitoring, bluedog can track the way an attacker navigates through the network: picking up on unusual location of login, network lateral movement and data exfiltration. By correlating this data and more, the patterns of attackers are easily spotted. As soon as an incident is identified, you will be alerted by the security team allowing action to be taken before damage is done.

As well as managed Microsoft 365 security monitoring, bluedog's brand new dashboard shows all the productivity info you need for your auditing requirements. The dashboard has been created in view of offering an in depth look at operational activity within Microsoft 365 which gives you an understanding who is doing what.The new and improved dashboard allows you to gain insights for all the following in an easily digestible way.

Exchange activity

Login Locations	Successful or failed login attempts
Inbound and Outbound email traffic	Deleted email
Exchange activity	Email attachments

SharePoint and OneDrive activity

Files accessed	Files previewed
Files modified	Files uploaded
Files moved	Files Deleted
Files downloaded	

Teams

Teams meetings	Files shared over Teams
Teams activity	

With the bluedog Microsoft 365 monitoring detailed dashboard, you can search per user or perform a search on several users at one time to see activity throughout a chosen time period, whether that be throughout the day, week or month, with the ability to input dates from start date to end date, you are easily able to pull off audit reports to suit your specific requirements.

Frequently Asked Questions

Can we trace if someone extracted information from the network when they for example put in their resignation, to validate they didn’t breach any of the non-competition clauses in a contract?

Yes, this capability is certainly present inside the bluedog Microsoft 365 monitoring solution. It is possible to have a full overview of what actors have been doing. The ability to review files, folders and emails that have been accessed, downloaded, deleted, etc, gives this overview in time and place. This is a great benefit to identify any data that may have been stolen or leaked, drilling down to the user and IP address.
Important note The contents of files or emails themselves are not visible to bluedog, only the filenames and locations of files inside SharePoint/ OneDrive and the subject of email or filename of the attachment.

Can we find out if someone is in a different location than where they claim they are?

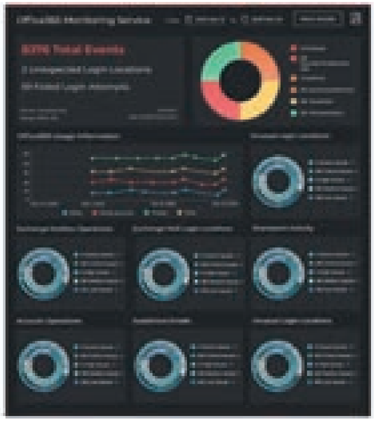
Yes, this is possible as the IP address of user activity is stored with the location at the time of the activity. This allows the bluedog team to determine where actors are located while performing their activities.

Can we see if a certain office location is working more proactive than other locations are?

Yes, the capability of grouping data sets based on geolocation, country and city are present in the bluedog Microsoft 365 monitoring solution. This gives the ability to check on performance or make other geographical correlations from the data.

Would this offering be able to provide a report to show the number of external (only) emails sent by each user over a period, i.e. seven days?

Yes, this is possible. The Exchange dashboard provides insights into email behavior from within the company. It also shows how email is treated, showing the types of email a user sends and receives. This provides great insights on any targeted attacks on the company. Identifying which users are receiving most phishing attacks and looking at the kind of malware. With this information, bluedog can provide recommendations on what action to take that will improve security measures for the business.



bluedog
SECURITY MONITORING

How bluedog strengthens your organisation with

Penetration testing

The bluedog pen test approach

- Security is about people, not technology
- Assessments should be business risk driven
- If nobody understands a report, you've failed...

There are so many providers out there that claim to provide the best possible penetration testing services. How do you know who you should pick?

First things first, you have to know the scope of testing. Penetration testing is a widely used term and can mean many different things: Is it a web application only? Does it include a source code review? Is infrastructure involved? A cloud application with Azure or AWS? Trying to get a complete overview of issues or is there a goal driven approach, where the assessment tries to actually break into an organisation and steal crown jewels? All these examples can fall under the term penetration testing.

One of the core missions of bluedog is to help you identify exactly what it is your client is asking for. We are here to help you, each step of the way. Using a unique approach to prepare, execute and deliver on promise is what makes bluedog unique. The entire process is closely governed and controlled by skilled professionals with dozens of years of experience in the field.

The bluedog professionals are trusted to train employees of major companies like Accenture and Petronas in fields of penetration testing, code review and forensics.

Testing web apps is done with tooling, is it?

No, it isn't. We no longer live in the zero's where applications were written in a straight request/response manner. We live in a mobile world now, where responsive, single page application with front and backends are flourishing. Tooling doesn't work anymore on these types of applications. It's all about business logic bypasses and authorisation or authentication flaws inside applications.

Can you do something with a backend API that you are not supposed to, building a malicious app around that API? This is the kind of stuff that requires human intelligence and not a tool. Sure, tooling helps with the easy stuff. But do you really want to settle for a C when you can get an A+ instead? This is where bluedog comes in to help. With subject matter experts in the cyber security work field, all trained within the bluedog Academy to ensure that all types of assessments are performed methodically and in accordance with the OWASP ASVS testing guidelines. This assures that each test undergoes the same set of quality controls!

The report is about the business risk!

Security testing is done by technical experts, who know how to break into an application or network with ease. But the result for all these assessments still is a report that is used within organisations to assess and mitigate risks identified during these assessments.

So, would you rather have a brilliant tester with an unreadable technical report, a sloppy tester with a brilliant report that management also understands or a brilliant tester with a brilliant report? We hope that we can guess that answer for you.

What we do at bluedog when it comes to writing reports, is to look as the business risk and impact for the issues that have been identified. Not only on an individual basis, but more so what will happen if individual issues are combined into a chained attack.

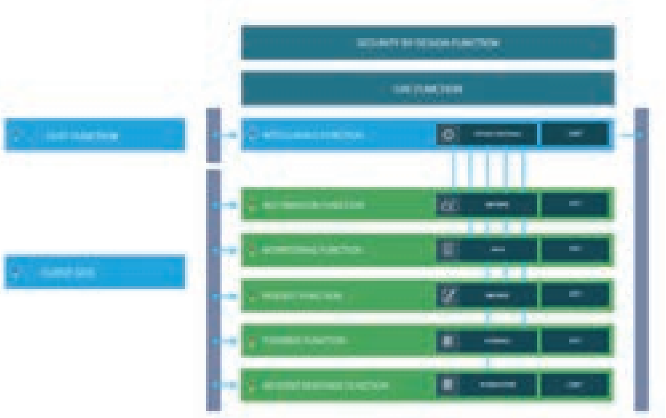
bluedog helps you getting the best results!

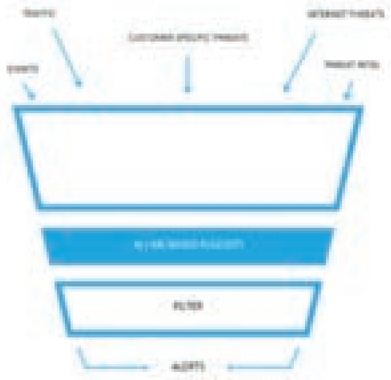
The approach bluedog takes remains the same as regards the type of test: preparation, assessment, QA, reporting. Governed and controlled by skilled subject matter experts with dozens of years of experience.

It’s vitally important to assure that penetration tests are performed and reported in a way that takes business risk into account. No plain technical risk reporting but rather placed into real world context that is easy to understand for management and the risk/compliance departments.

bluedog helps with this and offers the unique capability of integrating the results of all types of security assessments into the SOC design.

The pen test function provides information for the intelligence function to become better. This way, evidence-based compliance management can be achieved in a strong way, as the virtual CISO teams from bluedog in the GRC Function can work with all the data and aid in the continuous compliance frameworks for any company.





bluedog
SECURITY MONITORING

Strengthen your organisation with bluedog

Pen test vs Vulnerability scan

With cyber-attacks now the norm and becoming more advanced, it is important now, more than ever, to undertake regular vulnerability scans and penetration testing to identify vulnerabilities in your network and ensure that your cyber-controls are working.

Identify the difference

Vulnerability scanning - an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Penetration testing (which is often shortened to simply "pen testing") is when a simulated cyber-attack on a computer system or network is performed to evaluate how secure it is. Think of it as a computer hacker who is on your side and trying to break into your systems to find the vulnerabilities before the criminal hackers do. Pen Tests involve a variety of methods to examine a network to find potential vulnerabilities and then test to check that the vulnerabilities are real. This is all done to improve computer and network security so that the correct protection can be applied to safeguard against future attacks.

To summarise, A vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities. A penetration test is a detailed hands-on examination by a real person that tries to detect and exploit weaknesses in your system.

How often?

The internet has made it easy for attackers to engage with companies around the world. A cyberattack can damage a company in many ways, it is vital that they are always appropriately protected.

Vulnerability scans are conducted weekly with bluedog and reported back on a clear report showing all findings. However small a company's budget is, regular vulnerability scans should be seen as a necessity and priced in as part of their IT budget.

Pen testing should be at least annually. That being said however, the recommended frequency changes depending upon the assessed risks involved.

Pen testing should be undertaken after deployment of new infrastructure and applications as well as after major changes to infrastructure and applications (e.g. changes to firewall rules, updating of firmware, patches and upgrades to software).

The ICO says that "the GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place"

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

	Vulnerability Scanning	Pen Test
What's covered?	Detects and classifies system weaknesses in computers, networks and predicts the effectiveness of countermeasures	A simulated cyber-attack on a computer system or network is performed to evaluate how secure it is and reduces weaknesses.
How often?	bluedog offers this weekly as standard within subscription. Recommendation is at least once per quarter.	At least once a year. It is recommended that a pen test is conducted whenever internet facing equipment undergoes significant changes.
What does it focus on?	Typically looks for any known software vulnerabilities that could be exploited.	Discovers unknown weaknesses and looks to exploit them showing a more accurate report.
What's on the report?	Provide information on what ongoing vulnerabilities exist, showing areas that need attention.	Contains analysis and recommendations to improve the security of the examined application. Several diagrams will be added based on the results obtained during the study.
By Whom?	Automated report from scanning the network with bluedog.	Manually through a trained and governed specialist.
Who should need this?	Every business should be scanning their network regularly for vulnerabilities.	The ICO says that "the GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place". In practice this will mean undertaking vulnerability scanning AND penetration testing – at least once a year, probably once a quarter and depending on your 'risk appetite' weekly or even daily. PCI-DSS are required to have a pen test every 180 days.

Speak with your customer and consider the following:

- **Company size**. It’s no secret that bigger companies with a greater online presence might also have more urgency to test their systems, since they would have more attack vectors and might be juicier targets for threat actors.
- **Budget**. Pen tests can be expensive, so an organisation with a smaller budget might be less able to conduct them. A lack of funds might restrict pen testing to once every two years.
- **Regulations, laws and compliance**. Depending on the industry, various laws and regulations might require organisations to perform certain security tasks, including pen testing.
- **Infrastructure**: if your customer is on a cloud environment, they may not be allowed to test the cloud provider’s infrastructure. The provider may already conduct pen tests internally.

Why choose bluedog for Pen testing?

The high-level approach bluedog takes remains the same regardless of the type of test: preparation, assessment, QA and reporting. bluedog is governed and controlled by skilled subject matter experts with dozens of years of experience. It’s vitally important to assure that penetration tests are performed and reported in a way that takes your organisational risks into account. No plain technical risk reporting, but rather, placed into real world context that is easy to understand for management and the risk / compliance departments.

The resultant report shows the vulnerabilities in a straightforward way, making it easy to see which issues need addressing the most.

This way, evidence-based compliance management can be achieved in a strong way, allowing bluedog’s virtual Chief Information Security Officer (CISO) team working in the Governance Risk Assessment and Compliance function to work with all the data and aid in the continuous compliance frameworks for any organisation.

Why choose bluedog for Vulnerability scanning?

Vulnerability management can be a nightmare at times: Individual scans lacking visibility on network scanning coverage and persistent issues over time, is an issue of the past. The bluedog solution combines accurate and detailed vulnerability management with actual business context, all included in the service modules offered. No more manual correlations, no more difficult talks with auditors on why you’ve changed risk ratings and no more frustration at having to sift through dozens of reports.

bluedog has more data and insights than the standard vulnerability management scanners. This allows us to look at and interpret your network data and make business correlations with the vulnerability scanning results we gather for you. We will remove or alter issues that we believe have no impact on your network. This gives you a trusted third-party report that you cannot change yourself, but will have the contents that you need.

Video-based training

Mi Crow

Mi Crow's video-based training lets your customers learn what they want, when they want, in just 3 minutes.

Mi Crow is simply the coolest, quickest smartest way for your customers to learn new skills and make their lives easier without you having to do very much because it has been done all for you.

Mi Crow's on-demand video library consists of over 500 Mi Crow Courses for:

- Microsoft Office 365
- Microsoft Teams
- Gmail
- Mental Health in the Workplace
- Leadership & Management
- Customer Service
- Selling Skills
- How to be Successful

Together with Mi Crow's '60 Seconds of Genius' an extensive library of video-based tips, tricks and hacks that your customers will crave.

The Mi Crow portal

- Your own branded online hub with your logo, your strapline and your colours
- Populated with a library of online videos that your customers will love
- Total flexibility in how you charge, use and deploy your content.

Mi Crow courses can be used to provide on-demand Training and Support or simply as a marketing tool to keep in touch with your customers.

Mi Crow's benefits

- More revenue from your existing and new customers
- Significantly strengthened customer relationships
- A unique competitive advantage.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

redstor™

Disrupting the norm and changing everything you know about data management

Redstor

Redstor is disrupting the norm and changing everything you know about data management. Backup and recovery, archiving, disaster recovery, search and insight, Office365 backups and data migration can now all be managed through a single control centre, on any device.

Backup and Recovery

Whether your data is on-premise, hybrid or in the cloud, Redstor's pioneering InstantData™ provides on-demand access, allowing you to stream it in real time to any device, making downtime a thing of the past. With their unique, user-driven streaming technology, you don't need to wait for a full recovery. At the click of a button, your data is restored within seconds, not days.

Features:

- Unthrottled recovery, eradicate downtime with instant access to all your data.
- Deployment your way, implemented in minutes as SaaS, on-site or as a hybrid solution.
- Centralised control, borderless visibility of all your critical data, from a single control centre.
- Radically reduce costs, no capex outlay, no surprises. Only pay for what you use with fixed costs.
- Liberate the IT team, powerful automation, reporting and monitoring.
- Built to scale, seamless SaaS solution effortlessly scales as your business grows.

Archiving

Offload data to our highly secure cloud platform to manage and automate all your archiving requirements through a single interface. Eliminate delays in accessing archived data, whilst dramatically reducing primary storage costs and improving the ROI of existing assets.

Disaster Recovery

The survival of your business could depend on how quickly you respond and recover from a disaster. Redstor can help you meet your recovery targets with instant recovery. Traditional backup and recovery methods could take days or even weeks to get your data back. Redstor gives you the tools to get your users up and running instantly, while your data restores in the background.

Search and Insight

Discover, search and action the entirety of your data. Redstor enables you to identify and mitigate data risks and reduce data storage costs by easily moving data to Redstor's cloud archiving platform, which importantly has no impact on data accessibility.

Redstor's InstantData™ ensures all data can be streamed instantly on demand. Compliance with legislation and regulation, including the requirement to securely erase files from within backup and archive environments, is made simple and auditable.

Office 365

Protect all the Office 365 data within your organisation, directly from Microsoft's cloud to the Redstor cloud, all through an intuitive web interface.

Simplify and automate your data management and assign consistent protection policies across your entire data estate with one central, easy-to- use system.

Redstor allows you to:

- Establish a consistent data protection policy across your whole estate, viewing cloud and onsite data in one place through a central management console.
- Address e-discovery requirements and comply with General Data Protection Regulation by searching and actioning all data wherever it resides.
- Define Office 365 retention periods and ensure they are aligned to your business requirements.
- Set up in minutes, and auto-scale the protection you need - without the need for capital expenditure.
- Avoid lock-in by migrating data easily.
- Deliver centralised management of data in Office 365 Exchange, Sharepoint and OneDrive without circumventing 0365 security and auditing.
- Retain full control of your data for business continuity by mitigating the risk of storing it with the cloud service provider.
- Benefit from faster, simpler recoveries with on-demand access to data in the event of accidental deletion or ransomware.

Single web-based control centre

Modern businesses need a unified view of all their data. Manage and protect your Office 365 data via a single control centre as part of a centralised data management solution. Gain borderless visibility of local and online data and set policies across your entire estate.

brigantia

Brigantia Distribution - Business Continuity

Plan 4 Continuity

Turning paper plans into automated, intelligent business continuity plans for all SMEs

Business Continuity Planning Tool for the Channel

Why you need to consider becoming a Plan4Continuity partner

Plan4Continuity is the channel's first cloud-based business continuity plan software-as-a-service that streamlines business process automation and creates an opportunity for multi-recurring revenue streams for MSPs servicing SMEs. A dynamic, intelligent cloud-based business continuity planning solution that can create, simulate and activate business continuity processes with the push of a button.

Creating an exceptional opportunity to upscale the quality and scope of services and products that can seamlessly integrate with Plan4Continuity including disaster recovery, cybersecurity, compliance, staff management, communication hardware and software.

How a partners' clients benefit

Plan4Continuity converts manual and outdated business continuity processes into intelligent, automated workflows that can accelerate business continuity planning and foster a culture of resilience within organisations and so create an improved understanding of processes. It allows MSPs to automate the complete process of creating, activating, reporting, and simulating business continuity plans.

Plan4Contiunity complies with ISO 22301 standards and best practices as well as regulatory requirements ensuring optimal recovery from a disruptive event, protection of revenue and profits and improved audit readiness.

- Takes care of all client's business processes
- Turns client's business continuity plan into a working document
- Provides preconfigured plans and templates so clients do not have to pay expensive external consultancy fees. Easily adapt the plans to fit client's business/ organisation's needs
- Reporting – easily inform all stake holders of after event status. Who did and said what. From employees to C-level to insurance provider

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

Activate with the Push of a Button

Convert manual business continuity processes into intelligent, automated workflows. Plan4Continuity combines the five most important elements of continuity planning – locations, people, services, assets and vendors. Streamline management and boost accountability and facilitates effortless reporting.

The reality is that there is no real advance notice that a disaster is ready to strike. Even with some lead time, things can go wrong as every incident is unique and unfolds in unexpected ways. That is why a business continuity planning is crucial to ensure your business continues operating during an unplanned event.

Plan4Continuity automates the whole process of creating, activating, reporting and simulating business continuity planning into a single cloud-based application.

Locations

Business continuity planning by location

You business may have different entities (or ‘locations’ as we refer to it) such as branches, regions, buildings, floors, departments, even home offices and temporary remote sites. Business continuity can be managed more effectively if you divide your business into locations.

People

People are a business’s most valuable assets

They are the ones who control the use of assets, deal with vendors, perform services, make decisions, pay wages and liaise with clients. People, from plan managers to action owners, need to be involved in your continuity planning.

Services

Without services, no business can function

Every company depends on external and internal services. Without electricity, internet connectivity, IT support and telephony a company would be unable to function. When these services are disrupted, the Disruptive Event Management need to provide alternative scenarios.

Assets

A business needs assets to provide services

An important part of business continuity is identifying the assets that are essential to business operations and to include these assets in business continuity plans. These can include basic service plans or schedules for when the services rendered by these assets become disrupted.

Vendors

Vendors need to be active participants

Vendors and suppliers of services play a critical role in the ongoing function of a business and therefore need to be active participants in your business continuity planning. They form an essential link in the supply and disaster recovery chain.

HORNETSECURITY

Making your emails safe

Email Security as a Service

Hornetsecurity is represented globally at 11 locations with around 200 employees and operates in more than 30 countries.

The premium services are used by approximately 40,000 customers including Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA and Claas and provides its services worldwide via nine redundant, secured data centres.

The product portfolio covers all important areas of email security, including spam and virus filters, legally compliant archiving and encryption, as well as defence against CEO fraud and ransomware.

Spam and Malware Protection

The extensive features and thorough filtering mechanisms of Hornetsecurity’ s Spam and Malware Protection module keep mailboxes free of annoying and harmful spam, with a guaranteed 99.9% spam detection rate and 99.99% virus detection.

- Email Live Tracking shows all processed emails in a single view
- Content Control blocks various file types on incoming and outbound email
- Compliance Filter adds additional filters to prevent data loss
- Threat Defence uses machine learning to prevent spam and viruses
- Black and Whitelisting via Outlook add-in

Advanced Threat Protection

Ransomware, spyware and viruses manipulate or damage operational and production processes, which can cause considerable operational and financial damage. The Advanced Threat Protection component of Hornetsecurity detects even the most sophisticated cyber-attacks.

- Targeted Fraud Forensic Analysis
- ATP Sandboxing with detailed reports (screenshots, signatures detected)
- URL Malware Control (with Realtime navigation protection)

Archiving

Email Archiving from Hornetsecurity is legally compliant, fully automated and audit-proof and is the ideal solution for long-term and secure storage of important company information, data and files.

- Fully automatic and secure archiving
- Legally compliant GDPR archive
- Variable retention periods with up to 10-year Email Retention

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

Signature and Disclaimer

Every outgoing email from a company contains both commercial and contact information: a uniform and legally compliant appearance is, therefore, a basic requirement.

Hornetsecurity's Signature and Disclaimer allows for the creation of consistent email signatures and disclaimers for your entire organisation quickly and easily.

Email Encryption

Encryption of data has become a priority because of compliance requirements as well as the enactment of the GDPR. In a business environment, the exchange of sensitive files and information takes place primarily via email communication. Email Encryption, from Hornetsecurity, ensures all-round encrypted exchange of emails for reliable, secure email communication.

- Global S/MIME & PGP Encryption
- Secure Cipher Policy Control
- Secure Websafe

Continuity Service

The failure of a mail server often leads to significant operational issues and even, possibly, financial losses. If Hornetsecurity's automated monitoring detects that the companies mail server has failed, the Email Continuity Service is immediately activated.

- Emails are delivered without interruption via POP3/IMAP mailbox or webmail access.
- Guarantee of 99.9% device availability for customers of Hornetsecurity's Email Continuity Service
- Industry-leading 90-day email availability

EXCYB
CYBER CRISIS EXERCISE

Helping leaders to understand the complexities and challenges of cybercrime

Delivering a real-life immersive scenario-based learning experience

Services

ExCyb is an exercise designed to develop SME board level executives and senior leadership teams in coping with a cybercrime attack. It is an event that will be used to test the leaders of an organisation in their management and leadership capability and capacity, through an appropriate highly cyber-focused scenario.

The exercise helps leaders understand the complexities and challenges of cybercrime. It will be a strategic exercise and will not require prior technical knowledge. However, it will test crisis command and control capabilities and skills.

ExCyb is a dynamic exercise that delivers a real-life immersive scenario-based learning. It will help leaders understand the challenges of managing a range of different crises. ExCyb will design and execute a series of short scenarios and help leaders to understand their roles and responsibilities in a safe environment.

The exercise will be managed by experienced and distinguished facilitators with specialist skills. The incident is developed in live time and is made realistic with bespoke video footage that raises the realism of what colleagues might face. It starts with a relatively minor issue that builds into a full crisis.

This includes many potential issues including public concern, media intrusion, stakeholder management, shareholder management, business continuity planning, preparedness, policies, procedures, resilience, team dynamics and tensions under pressure.

The exercise usually lasts for a day, although this is flexible and, at its conclusion, there is an action plan for the client to take forward. It is an ideal part of executive development and team building with business purpose.

Arm Against

Disruption

Most organisations are now heavily reliant on their own access to the internet, whether to trade, supply, communicate or for marketing. Keeping the digital pipeline working is a major responsibility and often the key ingredient in keeping organisations alive.

- What happens if that pipeline is damaged or blocked?
- What would your response be?
- The cause could be anything from a simple power cut to a catastrophic cyber-attack to internal negligence. But how would you cope?
- Who would be the key decision maker?
- Who would provide trusted information intelligence and data on which to make decisions?
- What would your communications strategy contain, and who would front it?

These are just some of the issues any organisation in crisis faces. Many practice for fire or power emergencies, but what effort is made to address digital disaster?

The aim of the ExCyb immersive training is to help the SME leadership team think beyond the status quo in an organisation and consider what could happen, using examples from others facing disruption, and to raise awareness of digital disruption and create a battle plan to arm the organisation in the event of a crisis.

Attack

The world is not just full of well-meaning people with good moral compasses. As crime statistics testify, there are many who would subvert, steal or attack irrespective of legal process and protection. In the digital world, there are many who would willingly spread malware, exploit weaknesses and disable an organisation's ability to operate.

Likewise, for profit or gain, they will remove data and use it as a commodity to sell or to further social engineering attacks.

Victims are sometimes specifically targeted by individuals, gangs or event states. Linked with an intelligence building campaign they will endeavour to disrupt or destroy while making a profit. An attack could also impact on an organisation randomly, only being successful because leaders have not prepared or taken their own cybersecurity seriously. Likewise, an organisation not protecting itself from an insider threat could also be subject to an attack.

ExCyb provides a considerable opportunity for leaders and decision-makers to explore what could go wrong and how to respond. Using immersive learning and latest scenarios, that are relevant and timely, the leadership team is led through a series of events which could impact on their organisation. Now is the time to prepare and arm for the inevitable attacks that could affect organisations. ExCyb offers an ideal experience to help SMEs in that task.

Failure

Losing access to the normal working tools in any organisation can be extremely frustrating. A power outage caused by roadworks, a storm, an outbreak of flu or a burglary can all disrupt operations and cause varying degrees of chaos that needs to be managed.

As organisations move to high dependency on their internet or cyber connectivity, the failure of access is now a major threat with a growing risk, that could jeopardise any operational function.

Failure of access could be as a consequence of software faults, ineffective legacy systems, Denial of Service attacks or any number of malware or ransomware attacks.

Having a plan to deal with digital failure should be as practiced as a fire drill. Knowing who does what, how to respond and most importantly how to return to normality are key questions to be addressed.

In doing so, the organisation needs to identify any weaknesses and ensure that they are addressed, exactly as would be done after a flood, power outage, a fire or a burglary. ExCyb offers the opportunity for SMEs to arm against many different forms of digital failure and to ensure that they understand their responsibilities in a safe environment. Hopefully, those extreme failures will not occur, but through ExCyb they will be better prepared and much more able to deal with any digital crisis in whatever format it occurs.

KEEPER

Top-rated password manager for protecting your business

Cybersecurity starts with password security

Individuals and businesses often deal with the password issue by using shortcuts.

For example, they choose simple passwords that are easy to guess, they use the same password for every online account, or they write those passwords on sticky notes stuck to the side of their monitor. Such methods may seem like an easy way to avoid the work of creating and using secure passwords, but they make it easy for cybercriminals to do their damage. People need a far more secure and convenient way to protect their online accounts and other online assets.

Save employees time, frustration and eliminate the need for them to reuse and remember passwords. Keeper will generate strong, random passwords and automatically fill them for users. The Keeper vault, with a responsive and intuitive user interface (UI), is available to employees from any device and location. Everything Keeper does is geared towards quick user adoption and security.

Keeper MSP includes

- An encrypted vault for every user, with folder and sub-folder functionality
- The ability to created shared team folders
- Allows access from unlimited devices
- A strong policy engine with enforcement
- Built-in, continuous security audit
- Advanced activity reporting and an alerts module
- Two-Factor Authentication (SMS, TOTP, smartwatch, DUO, RSA and FIDO U2F)
- Single Sign-On (SAML 2.0) authentication
- Active Directory and LDAP sync
- SCIM and Azure AD provisioning
- Email auto-provisioning and ability for command-line provisioning
- Developer APIs for password rotation and backend integration
- BreachWatch® by Keeper
- 1TB Secure Storage

Key features include

BreachWatch® by Keeper scans employees' Keeper vaults for passwords that have been exposed on the dark web from a public data breach and notifies the user to take action. It also informs the administrator whether that employee has resolved the exposed password or ignored it.

Security Audit Score and Reporting
KeeperMSP provides password security visibility with robust reporting and auditing tools to enforce internal controls and maintain compliance standards.

Admin Console
Distributes, manages and monitors KeeperMSP across the entire organisation and enforces password security, 2FA and other data security policies.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

cloud business comms

Powered by Konnectifi

Cloud Business WiFi

Konnectifi is a legally-compliant, guest WiFi solution, that can content filter and capture powerful data by using the existing wireless infrastructure. Guest WiFi should be a revenue generator, not just a cost centre. Konnectifi enables clients to capitalise on visitors' preferences for intelligent marketing activities, so helping to provide the right marketing messages, at the right time – increasing spend, repeat and referral business.

Partner Benefits

- Add more value to your clients by turning their Guest WiFi into a new revenue stream
- Partner margin control
- Marketing and technical support from Konnectifi, for you and your customers
- Free demo licence included

Data Capture

Customers who connect to your WiFi through their social profile or via an email based contact form, provide you with an insight into who your customers are. The data we capture means we collect their basic information such as age and gender, as well as further details including their interests.

Email your customers

Add newly captured data straight in to your email marketing platform to send highly targeted campaigns, split by user profiles.

More Facebook Likes

To access the WiFi through Facebook, people must ``like`` your page, giving you a powerful social media boost.

Seamless Guest Log In

Your guests only need to register once, as they will be automatically logged in on any return visits.

Analytics Reporting

We filter the data gathered by your system and convert it into easy-to-use customer insights and reports which you can access whenever, wherever.

Relevant Messages to your Customers

Our user-friendly, marketing tool-kit allows you to set-up vouchers to send to customers based on their birthday, visit frequency and other key dates and occasions.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

cloud
business
phones

Voice Communications without compromise

Cloud Business Phones

Brigantia's Cloud Business Phones provides a comprehensive range of features that allow businesses to link their fixed and mobile telephony easily and efficiently, helping them to improve their productivity and corporate image.

Flexibility, Scalability and Ownership

- Partner owns customer and contract
- Partner margin control
- Partner controls feature set
- Full whitelabel available
- Technical and sales training included as standard

Cost effective

Quick and easy to install, with no capital outlay, the Cloud Business Phones System provides all the functionality of a traditional telephone system with advanced features that make communicating with staff, customers and suppliers easy and efficient.

Flexible

Instant messaging, presence and click to call features enable you to instantly see who is available and connect with them, while hunt groups and wallboards help you manage and monitor your inbound calls and group communications.

Easy to use Management Portal

The easy to use portal enables company administrators and site administrators to view team activity and make real-time changes. Users can quickly and easily access standard features such as call forwarding, busy and much more.

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

cloud
business
IaaS

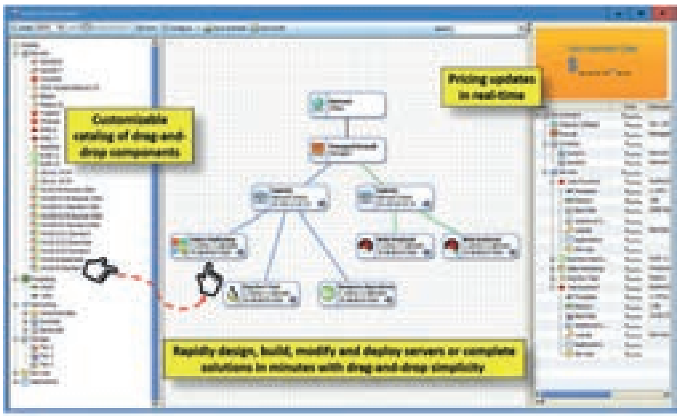
Powered by
xterity
cloud services
From Egenera

Managed Cloud Services

Cloud Business IaaS

Cloud Business IaaS provides advanced, easy-to-use and highly-available Cloud server infrastructure solutions with no upfront capital costs.

Cloud Business IaaS's Xterity platform is an enterprise-class, managed Cloud service specifically built for MSP and IT channel partners. Xterity enables partners to provide a branded, scalable and reliable platform that their customers can depend on for even the most critical and complex multi-tier applications.



Customizable catalog of drag-and-drop components

Pricing updates in real-time

Rapidly design, build, modify and deploy servers or complete solutions in minutes with drag-and-drop simplicity

The Xterity platform provides an intuitive, drag-and-drop cloud management solution that simplifies all cloud workflow processes including customised server/solution design, deployment, management, pricing, margin analysis, and billing.

Cloud Business IaaS's Xterity Platform delivers:

- Public Cloud
- Private Cloud
- Dedicated Compute Cloud
- Bare Metal Servers
- Disaster Recovery Solutions
- Cloud Backup as a Service

Why use Cloud Business IaaS Managed Cloud Services?

- Highly-available Private and Public Cloud IaaS services that are easy to deliver and manage
- Recurring revenues with margins of between 20% and 50%
- No upfront capital costs for hardware or software
- 24x7x365 level 2 and 3 partner support included
- Deliver high-value services without increasing in-house support costs
- Global presence in 8 x Tier III data centres
- Enterprise-class hardware platforms
- Compliance with ISO / SSAE / HIPAA and GxP for life sciences
- Full white label service with dedicated account management

Contact Brigantia

Unit 7, College Business Park, Kearsley Road, Ripon, North Yorkshire, HG4 2RN

Tel: 020 3358 0090 | Email: partnersupport@brigantia.com | Web: www.brigantia.com

cloud
business
EVS

POWERED BY bluedog SECURITY MONITORING

External Vulnerability Service

Cloud Business EVS

What is EVS?

The External Vulnerability Service (EVS) provides regular, scheduled scans of your perimeter. If a scan finds a problem then you get to find out before the bad guys do, this means that you can close potential "ways in" before they are exploited.

What is your perimeter and why does it matter?

In internet / digital terms, this is what is visible from the outside if someone is trying to break in.
Think of it as the equivalent of the security that you have on your office building: doors and windows with locks, an alarm, etc. This service provides the internet / digital equivalent of checking all of the entry points to your office on a scheduled basis.
It not only checks to see whether the defences that should be there, still are, but it also checks to see whether any newly discovered ways of breaking in are available. These "newly discovered ways of breaking in" occur a lot so this element is vital to your continued security.

What about your existing defences?

Most businesses have various defences in place such as antivirus programs and a firewall. If these are in place, then why would you need EVS? No protection is perfect, and this changes all the time; what was impenetrable yesterday may not be so tomorrow. EVS is a low-cost way of regularly checking that your defences are maintained at the level that you expect.

What can be tested?

Your business IP addresses are where the tests are pointed. This is not just your office external IP address but the others that you use too. This could be your website, your accountant's office, your home, the list goes on. When you sit down and really think about where you are exposed, you may be surprised.

What now?

Email partnersupport@brigantia.com or call Brigantia on 020 3358 0090 to discuss how you can resell this service to your clients.

cloud business comms

Broadband & Ethernet Communications Solutions

Cloud Business Connectivity

Brigantia's Cloud Business Connectivity services provide cost-effective and reliable internet connectivity for business users. The comprehensive range of services is designed to meet the needs of local offices, remote workers and larger offices needing efficient and effective, high-bandwidth connectivity.

Why fibre broadband?

- To improve in-house voice and data networks for improved information sharing
- To improve simultaneous access to online applications
- Home working

Why Ethernet?

- 99.99% uptime supported by industry-leading Service Level Agreements (SLAs)
- Enables the transfer of large amounts of data quickly and seamlessly
- Allows for and enhances high-quality voice, data, video and Cloud-based services
- Allows for data streaming and broadcasting services
- Facilitates the reliable extension of network infrastructures

Available Products

- ADSL (copper from the exchange to office) – the most cost-effective solution for low usage businesses
- FTTC (fibre from exchange to street cabinet, then copper to office) – around 10x faster than ADSL
- FTTP (fibre from exchange to office) – around 40x faster than ADSL. Not widely rolled out and available across the UK. Allows a choice of service packages to suit the client's budget
- EFM (ethernet over the first mile) and EoFTTC (ethernet over FTTC infrastructure) – provide high-speed internet connections, with service and bandwidth guarantees
- Leased lines – connect two or more locations with dedicated bandwidth

Information Security Management, Privacy, Governance and Compliance

Brigantia InfoSec Consultancy

Brigantia Consulting offers specialised data protection services to organisations: available at a variety of levels. This is delivered through a broad solution set to assist with Information Security Management, Privacy, Governance, Risk and Compliance.

Brigantia's InfoSec Consultancy services cover the following areas:

- Data Protection Act 2018 (DPA inc. GDPR) general consultancy
- DPA gap assessments
- DPA remediation consultancy
- Data Protection Officer as a Service (DPOaaS)
- ISO27001 Consultancy
- ISO27001 Implementation Consultancy
- Cyber Security Consultancy
- Data Protection and Security related policy and procedure preparation and provision
- Data Protection and Security Training Services
- InfoSec Consultancy
- Security Health Check
- Cyber Essentials certification
- Security Program Implementation & Management

For businesses and their employees

Brigantia Enhance Programme

Brigantia has been providing added value services, volume discounts and rebate programs to technology channel resellers, MSPs, MSSPs and consultants for many years. Brigantia Enhance is not about Brigantia’s core Distribution or Consultancy businesses, it is about the bits around the edges, the extra stuff, the enhanced services which are only for subscribing Brigantia partners.

Some examples of the Brigantia Enhance services:

Service	Description
Halfords Trade Card	Up to 50% discount at any Halfords store
Direct Debit	Low cost Direct Debit bureaux for collecting payments from your clients
Brigantia Partners Love2Shop Discount Card	Get 7% off at Shopping at over 50 major high street retailers
Petrol and diesel card	Discount fuel card
Free Legal and Business helplines *	Telephone advice and guidance for Health & Safety, Law, Tax, etc.
Kwik Fit	20% Off car servicing plus mobile tyre replacement discount
Supermarket discounts	4% Off at Sainsbury’s and Tesco
Cinema discounts	Save up to 40% on the cost of cinema tickets
Family days out discounts	Save up to 46% on costs at Alton Towers, Madame Tussauds, Thorpe Park, Legoland, the Dungeons and many other top UK attractions

Many other offers and services available

* 15% Brigantia Enhance Discount on all HR & H&S service agreements purchased from Croner.

Contact

Brigantia Partners Limited
Unit 7, College Business Park
Kearsley Road
Ripon
North Yorkshire
HG4 2RN

Telephone:
020 3358 0090

Email:
info@brigantia.com

Website:
www.brigantia.com

Contact Brigantia

Unit 7, College Business Park
Kearsley Road
Ripon
North Yorkshire
HG4 2RN

020 3358 0090

www.brigantia.com