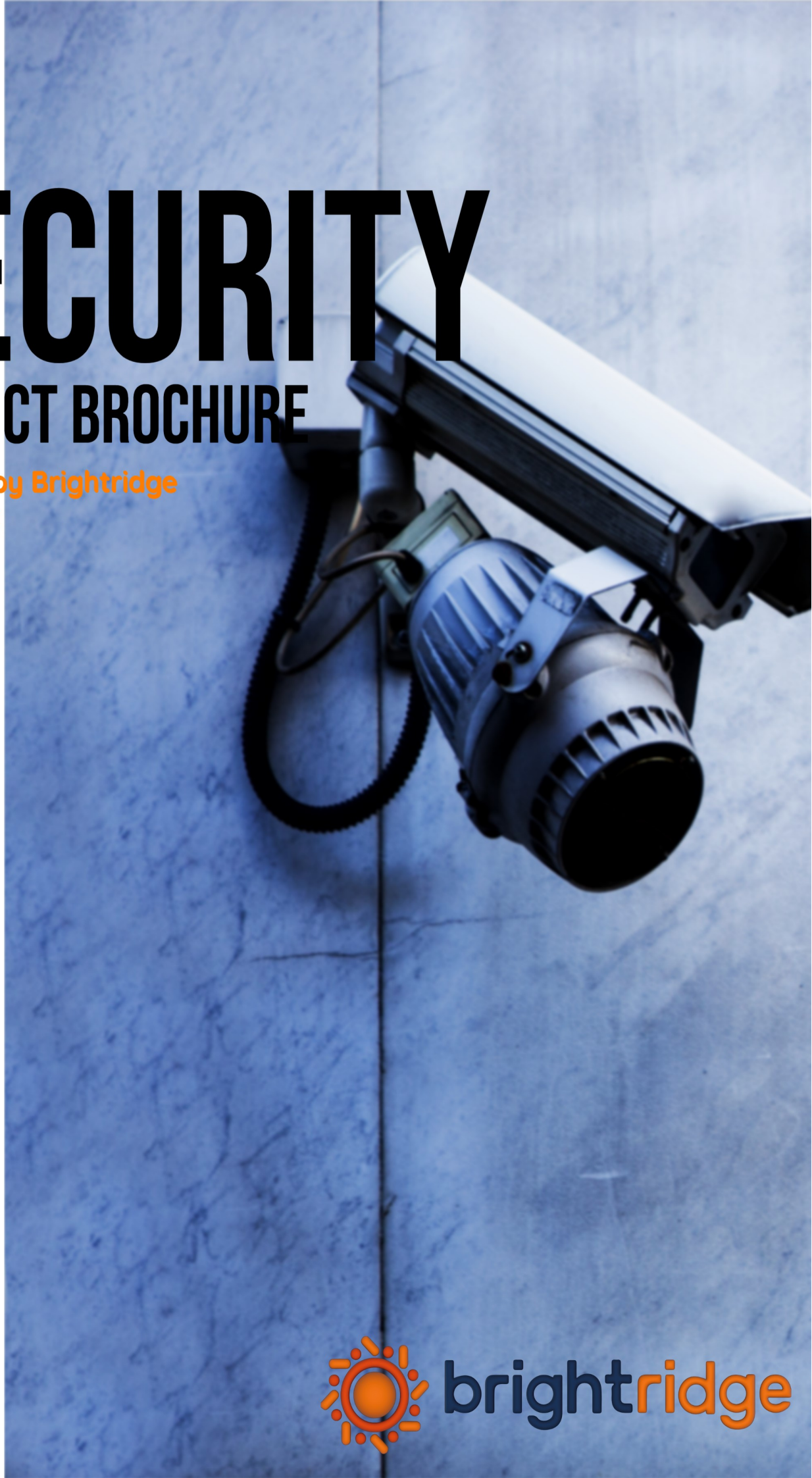
# SECURITY

## PRODUCT BROCHURE

Presented by Brightridge Technology



brightridge

# SECURITY SOLUTIONS & TECHNOLOGIES

Security risks pose a threat to many modern businesses and more than ever it is vital to be protected against various attacks that can compromise your data.

Brightridge have developed solutions to emerging threats in the technology landscape and worked with leading security providers using innovative technology that can ensure total business security for peace of mind and protection of data.

## PARTNERSHIPS

ID AGENT

LIBRAESVA

WEBROOT®

an opentext™ company

# DARK WEB ID

Dark Web ID combines human and machine intelligence with powerful search capabilities to scour the dark web to identify, analyze and proactively monitor for an organizatio's compromised credentials 24/7/365, alerting you to trouble fast

## HOW ARE CREDENTIALS COMPROMISED?

PHISHING 

WATERING HOLES 

MALVERTISING 

WEB ATTACKS 

## WHAT CAN AN ATTACKER DO WITH COMPROMISED DETAILS?

Send Span from Comromised Email Accounts

Deface Web Properties and Host Malicious Content

Install Malware on Compromised Systems

Compromise Other Accounts Using the Same Credentials

Exfiltrate Sensitive Data (Data Breach)

Identity Theft

# DARK WEB ID FEATURES

Our award-winning solution provides powerful intelligence and peace of mind at an excellent value. Always-on human and machine monitoring using real-time, analyst validated data goes to work immediately to protect your business from credential compromise risks

## COMPREHENSIVE, VALIDATED DATA

Get valuable intelligence you need to close security gaps with accurate data about your company's Dark Web credential compromise threats. Get additional protection from unpleasant surprises with credential monitoring for your supply chain and for the personal email addresses of your executive and administrative users, reducing the risk from cybercriminals gaining access to a privileged account.

Dark Web ID delves into every corner of the Dark Web, including:

Hidden Chat Rooms

Unindexed Sites

Private Websites

P2P (peer-to-peer) Networks

IRC (internet relay chat) Channels

Social Media Channels

Black Market Sites

## DEPLOY IN MINUTES

Dark Web ID takes just minutes to set up as SaaS or via an API and will start showing compromise results right away. You'll have a clearer picture of your security posture as well as a valuable early warning system for potential pitfalls for your business from credential compromise, giving you – an edge in securing your systems and data.

## EASILY INTEGRATES INTO TICKETING & CRM PLATFORMS

Enjoy seamless integration with popular PSA platforms including Kaseya BMS, Autotask, and ConnectWise. Reporting is flexible and can be integrated with your security operations center (SOC) and other alerting and remediation platforms with available APIs

# BULLPHISH ID

BullPhish ID transforms employees from security risks into security assets with security awareness training and phishing simulation campaigns using plug-and-play or customizable content. Video lessons and online quizzes are delivered via a personalized portal that make training painless for everyone.

## LEADING PHISHING SIMULATION PLATFORM

90% of data breaches start with a phishing email. Reduce your organization's chance of experiencing a cybersecurity disaster by up to 70% with security awareness training that includes phishing simulation using BullPhish ID.

Add every employee to your security team with security awareness training that empowers them to spot and stop phishing threats.

Automate training campaigns and reporting for stress-free, consistent training that gets results.

Choose from a rich set of plug-and-play phishing campaign kits and video lessons accompanied by short quizzes — or create your own phishing campaigns and training materials easily.

Effective, affordable one-stop phishing resistance training scales to fit any business and budget.

# BULLPHISH ID FEATURES

Effective, affordable one-stop phishing resistance training scales to fit any business and budget.

## RICH SET OF PHISHING SIMULATION KITS

Choose from a multitude of plug-and-play phishing simulation campaign kits with new content added every month to reflect the latest threats. Use preloaded kits or customize phishing emails, add attachments or create your own custom campaigns from blank templates.

## EASY CAMPAIGN MANAGEMENT

Utilize our automated tools to create, import and edit target employee groups to be included in your phishing simulation and training campaigns, run different campaigns for multiple groups, and schedule campaigns to be sent out at random times to prevent employees from warning each other.

## ENGAGING TRAINING

Deliver training that sticks featuring animated video lessons that meet employees where they are without boring tech speak to maximize retention. Each lesson comes with online quizzes to measure progress and see who needs extra help. Take advantage of the option to create and upload your own videos to meet your company's training needs.

## AFFORDABLE AND SCALABLE

Ideal for businesses of any size at a price that fits any budget. Pair this solution with Dark Web ID for detailed comprehensive credential alerts and reporting - giving you a clear picture of your vulnerabilities

# PASSLY

Passly provides must-have multifunctional protection against cybercrime that includes multifactor authentication, single sign-on, secure shared password vaults, automated password resets and simple remote management in one affordable secure identity and access management solution.

Secure identity and access management is a modern cybersecurity essential — but no one wants to shell out cash on multiple solutions. That's why Passly is a smart choice. We've included everything that businesses need to control access to their systems and data into one complete, affordable powerhouse.

## GET OUTSANDING FEATURES WITHOUT BREAKING THE BANK

### MULTIFACTOR-AUTHENTICATION

### SINGLE SIGN ON

### SECURE PASSWORD VAULTS

### BROWSER EXTENSION

### SIMPLE REMOTE MANAGEMENT

### EXCEPTIONAL VALUE

# EMAIL SECURITY

## UNMATCHED EMAIL PROTECTION

We deliver advanced security for cloud-based email platforms. Email Security Gateway protects Microsoft 365 and Google Workspace using multiple layers of protection, both at the Gateway and API layers, so multiple solutions are not needed. Email threats like phishing attacks, email fraud, and BEC are stopped before reaching their target.

Today's email threats move fast, and malicious files look more and more like ordinary files. Growing businesses need predictive email security to defeat today's threats with an eye on the future.

ESG filters all internal emails as well as inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. It provides both spam filtering and spam protection against advanced threats like phishing, malspam, business email compromise, and account takeover. We block over 99.9% of phishing and malspam attacks!

**SIMPLE AND EASY TO DEPLOY CONFIGURATIONS GUARANTEE THAT CUSTOMIZED EMAIL PROTECTION IS IN PLACE IN A MATTER OF MINUTES. DEPENDING ON YOUR NEEDS, YOU HAVE THE OPTION TO RUN IN THE CLOUD OR ON-PREMISE.**

# EMAIL SECURITY FEATURES

## SPOOFING PROTECTION

## PROTECTION AGAINST MALICIOUS FILES & URLS

## BEC & IMPERSONATION ATTACKS PROTECTION

## THREAT ANALYSIS PORTAL

## THREAT REMEDIATION

## EMAIL ENCRYPTION & CONTINUITY

# EMAIL ARCHIVER

## NEXT GENERATION EMAIL ARCHIVING

Archiver protects business critical information, simplifies compliance, improves employee efficiency!

Email Archiver is a powerful and simple solution for email Governance, Risk and Compliance; up and running in minutes creates 1:1 copies of all emails in a central email archive to ensure the security and availability of large amounts of data over a period of years.

No matter what email server you are using, either in the cloud or on premise: Email Archiver seamless integrates with any mail server, and offers native integration with Office 365 and Microsoft Exchange. Thanks to the exclusive Outlook Add-In, that supports both Windows and Mac, users can still access their archived email in the usual way.

## ON-PREMISE OR CLOUD

Available as on premise virtual appliance or as a private cloud service

## OFFICE 365 AND EXCHANGE NATIVE INTEGRATION

Native mailbox connectors for Microsoft Office 365 and Exchange

## GDPR COMPLIANT

Outstanding privacy management with privacy officer role and permission granularity

## OUTLOOK ADD-IN

Seamless access to archived emails with native Outlook Add-in and Web-App

## MULTIPLE STORAGE SUPPORT

Support a variety of storages: local disks, network disks and object storage (S3 compatible)

## FOLDER STRUCTURE REPRODUCTION

The folder structure of the archived mailboxes or PST files is applied to the archived email

# PHISH BRAIN

## PHISHING AWARENESS MADE EASY

PhishBrain analyzes each employee and organization, profiling each on an ongoing basis to determine their phishing risk profile. PhishBrain identifies the highest risk employees and tracks their progress over time, in order to become a truly security-conscious company.

## WHY DOES PHISHING WORK?

Phishing attacks are successful because they leverage the human factor, which is the weakest component of a company's security. People do not give sufficient attention to seemingly legitimate requests and end up erroneously sharing data

## WHY SHOULD YOU CARE?

25% of employees are quick to click on phishing email links and 50% of those submit information in web forms

## WHAT IS THE COST TO BUSINESS?

Breaches cost, on average, over $130,000, and can reach into the Millions, resulting in many companies going out of business

# TAILOR-MADE CYBERSECURITY FOR SMALL AND MEDIUM-SIZED BUSINESSES

Brightridge cybersecurity solutions were designed from the ground up to stop advanced threats and simplify your life as a business

## PRODUCT LINEUP

### BUSINESS ENDPOINT PROTECTION

Stop threats with next-gen threat intelligence
Protect your business from ransomware
Get full visibility and reporting
Set it and forget it

### DNS PROTECTION

Stop up to 88% of malware at the DNS layer
Get detailed reports on-demand
Enable policies by group, device, IP
Apply leading web classification

### SECURITY AWARENESS TRAINING

Reduce click-through on phishing by 70%*
Ensure compliance (SEC, FINRA, PCI, HIPAA, GDPR, etc.)
Educate users, protect data, and avoid fines
Schedule training and auto-run reports

# WHAT IS ENDPOINT PROTECTION?

Endpoint protection, or endpoint security, is a general term that describes cybersecurity services for network endpoints, like laptops, desktops, smartphones, tablets, servers, and virtual environments. These services may include antivirus and antimalware, web filtering, and more.
Endpoint protection helps businesses keep critical systems, intellectual property, customer data, employees, and guests safe from ransomware, phishing, malware, and other cyberattacks.

# WHY BUSINESS NEED ENDPOINT PROTECTION?

Criminals are constantly developing new ways to attack networks, take advantage of employee trust, and steal data. Smaller businesses may think they're not a target, but that couldn't be further from the truth. In fact, small businesses with 100 employees or fewer now face the same risk of attack as a 20,000-employee enterprise.
No matter their size, businesses need reliable endpoint security that can stop modern attacks. And since most companies are subject to some form of compliance and privacy regulations, protection for endpoints is 100% necessary to help businesses avoid hefty fines and damage to their reputation due to a security breach.

# WHAT IS DNS PROTECTION?

Before we talk about DNS security, you need to understand the DNS. The domain name system (DNS) works like a phone book for the internet. When a user enters text into a browser, DNS servers take that input and translate it into the unique internet protocol (IP) addresses that let the browser open the desired site. But DNS protocols were never designed with security in mind, and are highly vulnerable to cyberattacks, such as cache poisoning, DDoS, DNS hijacking, botnets, C&C, man-in-the-middle, and more.

By redirecting users' web traffic through a cloud-based, DNS security solution, businesses and MSPs can finely tune and enforce web access policies, ensure regulatory compliance, and stop 88% of threats at the network's edge—before they ever hit the network or endpoints.

# WHY BUSINESS NEED DNS PROTECTION?

Uncontrolled internet access is a high-risk activity for any business, regardless of size. Faced with today's sophisticated attacks, endpoint security alone is no longer enough to stay safe from modern cybercrime. In fact, a recent report from EfficientIP found that 77% of businesses around the world suffered at least one DNS cyberattack in 2018. What's even more worrying: on average, businesses got hit with as many as seven attacks throughout the year.

Per the report, the average cost of a single attack was $715,000 USD. When you do the math, it's clear how DNS Protection for servers, endpoints, and other networked devices could make all the difference to a business' success (and survival).

# WHAT IS SECURITY AWARENESS TRAINING?

Security awareness training is a proven educational approach for improving risky employee IT behaviors that can lead to security compromises. Through the efficient delivery of relevant information and knowledge verification on subjects including information security, social engineering, malware, and industry-specific compliance topics, security awareness training increases employee resilience to cyber attacks at home, on the move, and at the office.

By participating in security awareness training, employees learn to avoid phishing and other types of social engineering cyberattacks, spot potential malware behaviors, report possible security threats, follow company IT policies and best practices, and adhere to any applicable data privacy and compliance regulations (GDPR, PCI DSS, HIPAA, etc.)

# WHY BUSINESSES NEED SECURITY AWARENESS TRAINING?

As cyber security threats continue to evolve, security awareness training helps businesses decrease help desk costs, protect their reputation and secure their overall cybersecurity investment.

Brightridge makes it easy to implement an ongoing training program that significantly reduces the risk of security breaches through phishing simulations based on real-world attacks and training that covers relevant security and compliance topics.

# CONTACT BRIGHTRIDGE TODAY

## TO FIND OUT MORE ABOUT OUR SERVICES

SALES@BRIGHTRIDGE.CO.UK

0131 202 0777

WWW.BRIGHTRIDGE.CO.UK

brightridge

TAKE THE STRESS OUT OF IT. PARTNER WITH A LEADING MANAGED SERVICE PROVIDER


brightridge