bridgeall

Creating a secure and resilient business

A cyber security guide

bridgeall.com

Introduction

Cyber security is unfortunately a growing area of concern for many organisations. High profile breaches are becoming more and more common and the move to both home working and the cloud is creating new attack vectors that cyber criminals can use.

As cyber security threats evolve so does the way you should defend your organisation. From defence in depth to zero trust security, the cyber security game has completely changed over the last few years and staying up to date is key.

The good news is there is a wide range of technology solutions available to help you combat the rising threats and build a more secure and resilient workplace.

In this guide we will discuss the recent changes to cyber security and the practical steps you can take to defend your organisation.

Contents

Section 1

Cyber security trends

With the cyber security space constantly evolving, companies continue to add multiple layers to their IT networks that can create new vulnerabilities. Before we delve into these vulnerabilities and our approach to cyber security and the solutions available to help, we wanted to discuss the trends.

Growing cyber security threat

There is no getting away from the fact that cyber crime is on the rise. The COVID-19 pandemic has shown a significant rise in cyber crime and this unfortunate trend looks here to stay.

The attacks are getting more intelligent, varied and in some cases AI powered. Attacks are much more convincing, with impersonation of major brands with delivery updates, or your account being compromised with hackers gaining access to emails.

50%
Rise in security breaches in the last 12 months

As services have moved to the cloud, this has created a huge opportunity for cyber criminals to try to break passwords and access sensitive data. There are 579 password attacks every second—that's 18 billion every year.

The evolving workplace

As mentioned, the move to the cloud has been a significant opportunity for cyber criminals. Pair this with the move to hybrid working and this creates many opportunities.

Your organisation used to be secured by the network. Everyone worked with on-premise solutions within the network. Network is no longer the security perimeter however this is now identity. User names, passwords verified by admins or a single identity management solution is how you restrict and control access to your business areas.

Email continues to be the single biggest entry point for cyber criminals, and is worth a particular focus for your cyber security practices.

Everything is not all in the cyber criminals favour however. There has been huge steps forward in a number of areas that make cyber security easier. For example Multi Factor Authentication can remove the threat from 99% of password or phishing attacks. Combine this with AI powered threat protection, fraud protection and monitoring solutions now available and you can start to identify unusual behavior and stop it before it becomes a threat.

What do you do if you have a breach? You no longer have the ability to 100% secure your organisation, breaches can happen even to the best practitioners of cyber security good practice. The demand for cloud back up solutions is rising at a huge rate with a 17% growth expected each year until 2025.

Section 2

Different types of cyber security threats

Now that we have discussed the trends in cyber security we wanted to explain the different types of threats. Most of these terms you will be familiar with but we wanted to explain them just in case any were new.

Malware

Malware is a term used to describe malicious applications and code that can cause damage and disrupt normal use of devices. Malware can allow unauthorised access, use system resources, steal passwords, lock you out of your computer and ask for ransom, and more.

Cybercriminals that distribute malware are often motivated by money and will use infected computers to launch attacks, obtain banking credentials, collect information that can be sold, sell access to computing resources, or extort payment from victims.

Ransomware

Ransomware is a type of malware that holds computers or files for ransom by encrypting files or locking the desktop or browser on systems that are infected with it, then demanding a ransom in order to regain access. Ransomware attacks increased by 62% in 2021 compared to 2020, making up 10% of all data breaches. The average cost of a ransomware breach was $4.62 million in 2021 according to IBM.

Phishing

Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords - on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website.

- **Blanket phishing** – This is as discussed above, focused on mass emails impersonating big brands.
- **Spear Phishing** – Is more targeted than the blanket branded ones, where they will use your name, email, job title and other available information to make the email look more legitimate. For example, if you work in HR they could attach malicious software disguised as a CV or personnel file.
- **Whale Phishing** – Is a targeted phishing campaign, where the attackers have singled you out as a valuable victim, they know your information and will use this to try to manipulate you. For example, sending an email that looks like it comes from your boss asking for information or if you work in finance sending you a link to an invoice.

Section 3

Modern approaches to cyber security

With the evolution of the types and focus of cyber attacks the way we build cyber security approaches has also had to adapt. Below are 3 new approaches to better protect your organisation.

Defence in depth

Defence in depth comes from the military approach of securing something. Having different layers of warning, security and clearance needed to access different areas or move through your organisation.

Traditional cyber security approaches used to look to secure the network, all devices were within the outer firewall and so stopping anything coming in was a sure-fire way of securing your full infrastructure. Now with cloud services, hybrid working and multiple devices, you have hundreds if not thousands of different attack vectors you need to secure against.

Taking the principle of if there was a breach in one area how would I stop it spreading to other areas, allows you to build up a much stronger defence and reduce your risk.

Zero Trust Security

Today, organisations need a new security model that effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they are located.

This is the core of Zero Trust. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify."

Microsoft explains Zero Trust as, "Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to threats."

Shared responsibility model

The shared responsibility model is a key concept to understand when it comes to cloud. Cloud providers for any level of service only take on a certain level of responsibility. This will differ with the solution and whether it is IaaS, PaaS or SaaS. The idea behind it is to clearly showcase what a user of the platform is responsible for.

For example, in almost all cases the user is responsible for the data that sits within the platform. This could be CRM records, documents or SharePoint or code in a virtual server. In any of these scenarios if the data is deleted the cloud provider will regularly have some, normally limited, ability to recover this data, but that is not guaranteed and after a certain point this will get deleted too.

Section 4

Our approach to cyber security

When it comes to how best to approach your cyber security. We have outlined how we would approach it. We discuss a couple of different frameworks that you can use to build your cyber security strategy.

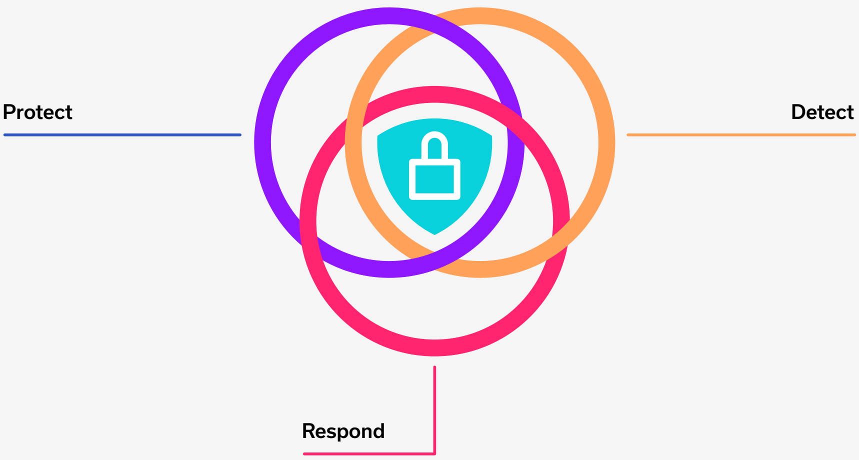
When looking to develop a cyber security strategy, it is important to properly assess your current set up and weaknesses. The below frameworks will help you categorise and analyse this in more detail.

The 3 principles of cyber security

One of the simple ways we like to approach cyber security is to develop improvements across the following three areas.

1. **Protect** – How well protected is your organisations data, apps, infrastructure? From better firewalls, email security, multi factor authentication etc. There are a wide range of things you can do to protect your organisation and understandably this is where the majority of your effort goes.
2. **Detect** – If a breach does happen how would you know. On average it takes 270 days to identify a breach. Ensuring you have monitoring and checks in place to be able to identify unusual behavior and stop it before it becomes a threat.
3. **Respond** – This is a key part, if you find a breach, what can you do about it? This is where your identity management and backup strategy come in. Do you have the ability to lock out the cyber criminals and then undo any damage they might have done.

The 3 principles of cyber security



3 key pillars of cyber security

Modern cyber security practice must focus across the following three areas. This ensures you follow the trends of defence in depth as effectively as possible.

Securing your data is critical. Where does your data reside, who has access to it and how secure are these systems. Ensuring you have sensitive data only accessible to key people. Does your systems support row, column or cell level security and security data policies can be a key step.

Identity is becoming a major pillar in cyber security and needs to be managed correctly. Having an identity management strategy and if possible a single solution that manages all identity in your organisation, can be extremely efficient to help manage access, leavers and breaches.

Devices is a newer attack vector driven by Bring Your Own Device (BYOD) and the move away from the office. Do you have anything in place to secure these devices if they are lost, stolen or compromised.

DATA

IDENTITY

DEVICES

3 KEY PILLARS OF
CYBER SECURITY

Section 5

Putting it into practice

Putting all of the above theory into practice can feel daunting, a key step can be to create a cyber security strategy that outlines the priorities and major threats, helping drive action. But this doesn't need to be intimidating, below we outline some of the simple solutions you can introduce to improve your cyber security.

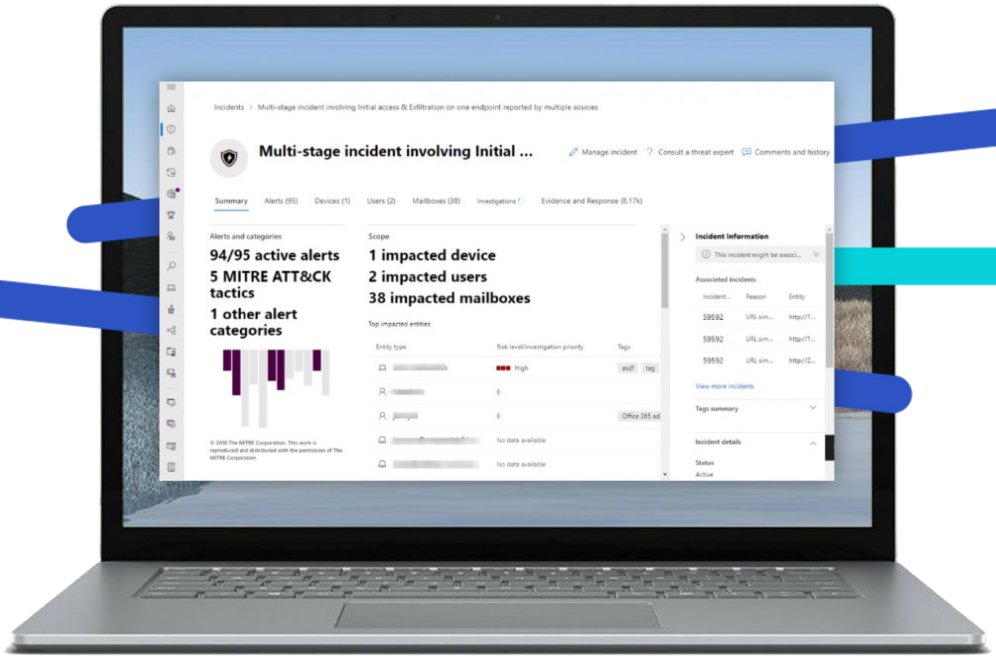
One of the first and easiest things organisations can do is move to one of the Microsoft 365 E3 or E5 bundles. This is the first thing we recommend to organisations as included in the bundle is a number of security solutions that can cover a wide range of bases. From multi factor authentication, threat protection, anti-phishing, identity management, device management and so much more.

Microsoft Security Centre

Microsoft security centre is the new and improved security hub within Microsoft 365. The idea behind the Microsoft 365 security centre is to create a central place where you can manage all of your security combining capability from Microsoft Defender centre and Office 365 security & compliance centre.

The improved Microsoft 365 security centre combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.

The new security centre enables your security and compliance teams to have centralised management across your Microsoft 365 services, bringing together Office 365, Windows 10, and Enterprise Mobility + Security (EMS), with several Azure capabilities.



Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources
Manage incident
Consult a threat expert
Comments and history
Summary
Alerts (95)
Devices (1)
Users (2)
Mailboxes (38)
Investigations
Evidence and Response (8.17k)

Multi-stage incident involving Initial ...

Alerts and categories

94/95 active alerts

5 MITRE ATT&CK tactics

1 other alert categories

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Scope

1 impacted device

2 impacted users

38 impacted mailboxes

Top impacted entities

Entity type	Risk level/investigation priority	Tags
[redacted]	■■■ High	asdf tag
[redacted]	0	
[redacted]	0	Office 365 ad
[redacted]	No data available	
[redacted]	No data available	

Incident Information

This incident might be associ...

Associated incidents

Incident...	Reason	Entity
59592	URL sim...	http://1...
59592	URL sim...	http://1...
59592	URL sim...	http://2...

View more incidents

Tags summary

Incident details

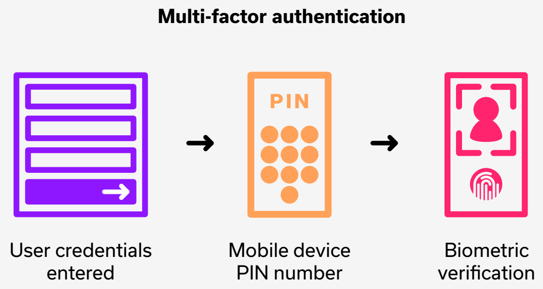
Status

Active

Multi Factor Authentication

Create barriers for cyber criminals by enabling multi factor authentication (MFA). MFA works by stopping an attacker from accessing protected accounts or resources. Thanks to the introduction of passwordless technology and architecture, it's much easier for employees and customers to use and also provides more security than traditional text (SMS) or voice approaches. Always authenticate and authorise based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Microsoft's Azure Active Directory (Azure AD) enterprise identity service provides SSO and multi-factor authentication to help protect your users from 99.9 per cent of cybersecurity attacks.



Email Security

As discussed previously email is the biggest attack vector for organisations, driven by phishing attacks. Securing email from attack can drastically improve your cyber security situation.

Microsoft Defender

Microsoft 365 Defender, part of Microsoft's security suite, leverages the Microsoft 365 security portfolio to automatically analyse threat data across domains, building a complete picture of each attack in a single dashboard.

Microsoft Defender prevents a wide variety of volume-based and targeted attacks including business email compromise, credential phishing, ransomware, and advanced malware with the help of a robust filtering stack.

Mimecast

Mimecast is a third-party application that protects your emails. Once set up, Mimecast scans and assesses every email that comes into your organisation. It also protects all links and attachments that come in. Via the Mimecast portal you can assess any withheld emails and release them if you are expecting them. Mimecast is one of the market leaders in this space and our recommended anti-phishing solution.

Backup and disaster recovery

Cloud backup and disaster recovery is a crucial fail safe for cyber security. If the rest of your security measures fail, the ability to restore your data and continue operating your business is a critical requirement. The key to this is ensuring you understand what you need to run your business.

Azure backup and disaster recovery

Azure Backup is Microsoft's answer to cloud backup. Like most services on Azure, it is a scalable storage solution based on your needs. It can all be managed through the easy backup Centre allowing you complete control of your backup policies.

Azure Backup can be used for a wide range of both Microsoft and non-Microsoft workloads.

Azure Disaster recovery allows you to always hold an instance of your services in another Azure data centre and have an almost instant failover should something go wrong. This is a more expensive approach but for business critical solutions can be extremely useful in minimising downtime.

Veeam Office 365 backup

Microsoft 365 provides powerful services within Office 365 – but a comprehensive backup of your Office 365 data is not one of them. Of over 1,000 IT Pros surveyed, 81% experienced data loss in Office 365 – from simple user error to major data security threats.

Veeam Backup for Microsoft Office 365 gives you the power to securely backup Office 365 to any location, including on premises, a hyperscale cloud, or a service provider. With Veeam you protect Office 365 data from security threats and retention policy gaps, quickly restore industry-leading recovery flexibility and meet legal requirements with efficient eDiscovery of Office 365 items.

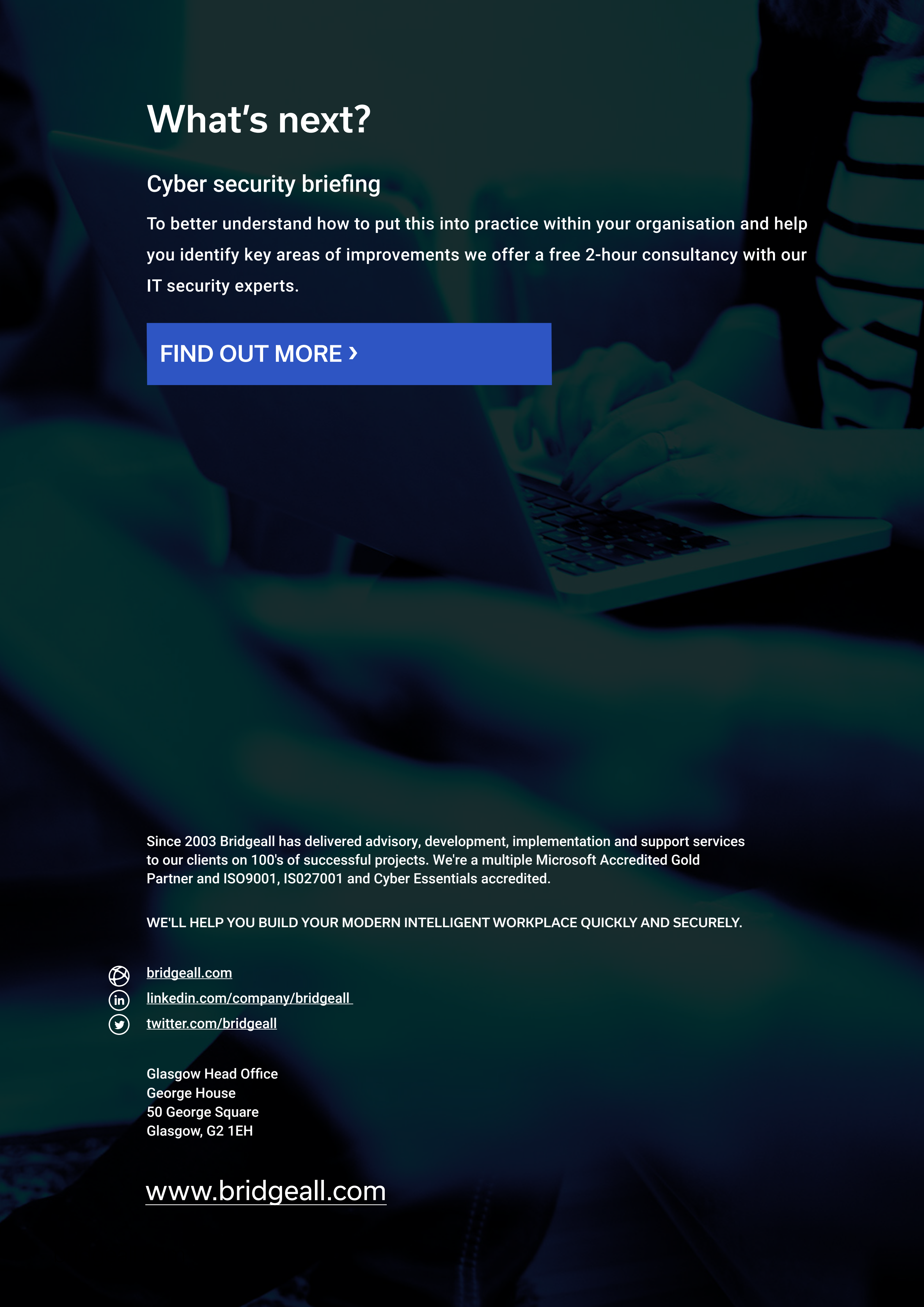
Securing your devices

With hybrid working and a wider range of work devices in your organisation, finding a solution to secure them is critical to your security strategy. Microsoft Endpoint Manager is our go-to solution.

Microsoft Endpoint Manager is a Microsoft Azure service that provides you with a wide range of features and services to manage and monitor a full range of devices including: mobile devices, desktop computers, virtual machines, embedded devices and servers.

Microsoft Endpoint Manager offers a seamless, end-to-end management solution without the complexity of a migration or disruption to productivity. It is perfect for organisations looking to provide greater security, monitoring and updates across a full range of devices.

Putting cyber security into practice is a complex and ever changing challenge. Our approach based on Microsoft technology allows companies to get the majority of the way there with a suite of solutions to secure different elements of your business. Keeping the principles at front of mind and continuing to evolve as the threats do.



What’s next?

Cyber security briefing

To better understand how to put this into practice within your organisation and help you identify key areas of improvements we offer a free 2-hour consultancy with our IT security experts.

FIND OUT MORE ›

Since 2003 Bridgeall has delivered advisory, development, implementation and support services to our clients on 100's of successful projects. We're a multiple Microsoft Accredited Gold Partner and ISO9001, IS027001 and Cyber Essentials accredited.

WE'LL HELP YOU BUILD YOUR MODERN INTELLIGENT WORKPLACE QUICKLY AND SECURELY.

bridgeall.com
linkedin.com/company/bridgeall
twitter.com/bridgeall

Glasgow Head Office
George House
50 George Square
Glasgow, G2 1EH

www.bridgeall.com