Defence in Depth

The 2022 Guide to Layered Security

Secure your systems and infrastructure to protect your business, no matter what the adversary

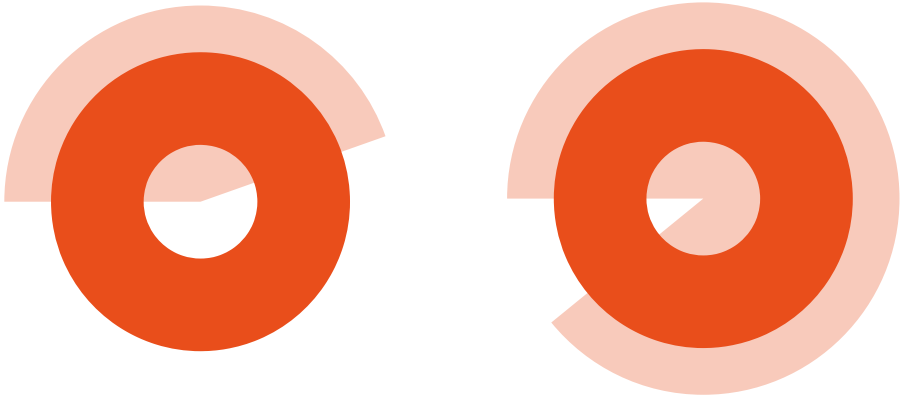
bluecar TECHNOLOGIES

Contents

The Current State of Security

In 2022, cybersecurity is more important than ever. Although the threat landscape is constantly evolving, the last three years have seen some major changes to the way that cybercriminals attack businesses, and there have been dire consequences. So far in 2022, 39% of all UK businesses have identified a cyberattack, with phishing attacks accounting for 83% of all attacks.

With cyberattacks becoming more advanced and prevalent, it is important that all businesses, regardless of size or industry, understand the common attack methods, and have systems and policies in place to reduce their cyber risk.

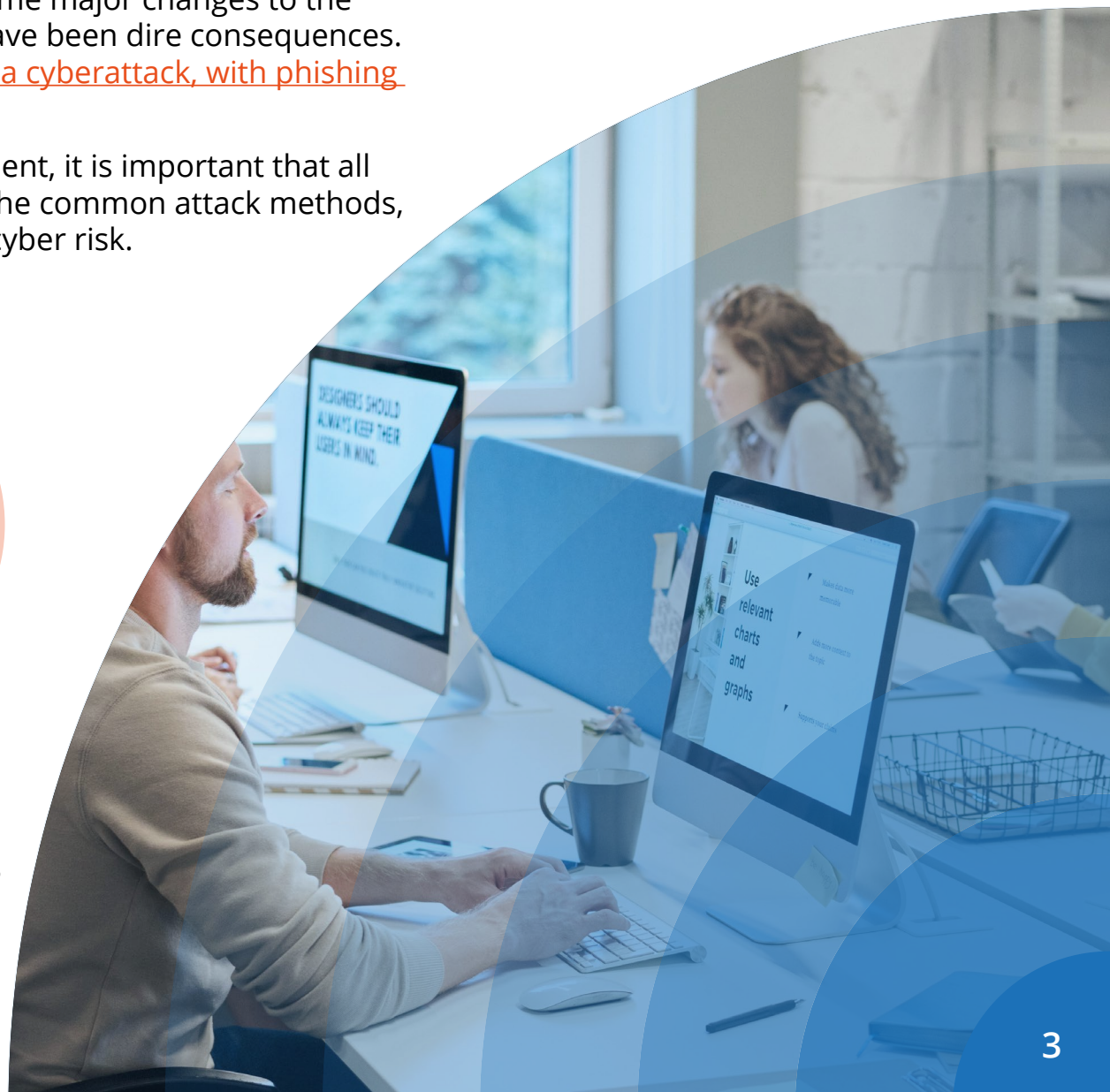


39%

of UK businesses have identified a cyberattack in 2022

83%

of these cyberattacks started with a phishing email



Common Attack Methods

In terms of news coverage, **ransomware** has been the number one cyberattack over the past 5 years. There have been some major ransomware attacks throughout the UK and the Republic of Ireland recently. Some of these include an attack on the Irish Health Service Executive, with recovery costing $442m, and an attack on the Hackney Borough Council costing approximately £10m to recover from. Whilst ransomware attacks have steadily increased in prevalence over the past 5 years, it is more concerning that from 2020 to 2021, ransomware related data leaks increased by 82%. This is due to double extortion, whereby if the company can recover from a ransomware attack through backups, without paying the ransom, the attackers will exfiltrate the data and either leak it online or sell it to the highest bidder.

Many of these ransomware attacks are initiated through **phishing** emails. Although in the past ransomware was typically a 'spray and pray' attack, now most attacks are instigated through highly targeted spear-phishing campaigns. These attacks are where the cybercriminal researches their target business and individuals, then tailors the phishing attack to them.

Another group of attack methods that are still plaguing businesses is a variety of **password attacks**. These attacks are typically initiated through credential stuffing, a form of cyberattack where the hacker collects stolen account credentials, typically usernames/emails and passwords, in order to gain access to other accounts. These credentials can be purchased on the dark web through previous data leaks, potentially due to other ransomware attacks. This is only effective if individuals reuse a password across different systems, however, this is a common practice. Some systems that are commonly targeted by credential stuffing include email clients, Remote Desktop Protocol (RDP), Virtual Private Networks (VPN), and Microsoft 365 accounts.

Looking Towards the Future

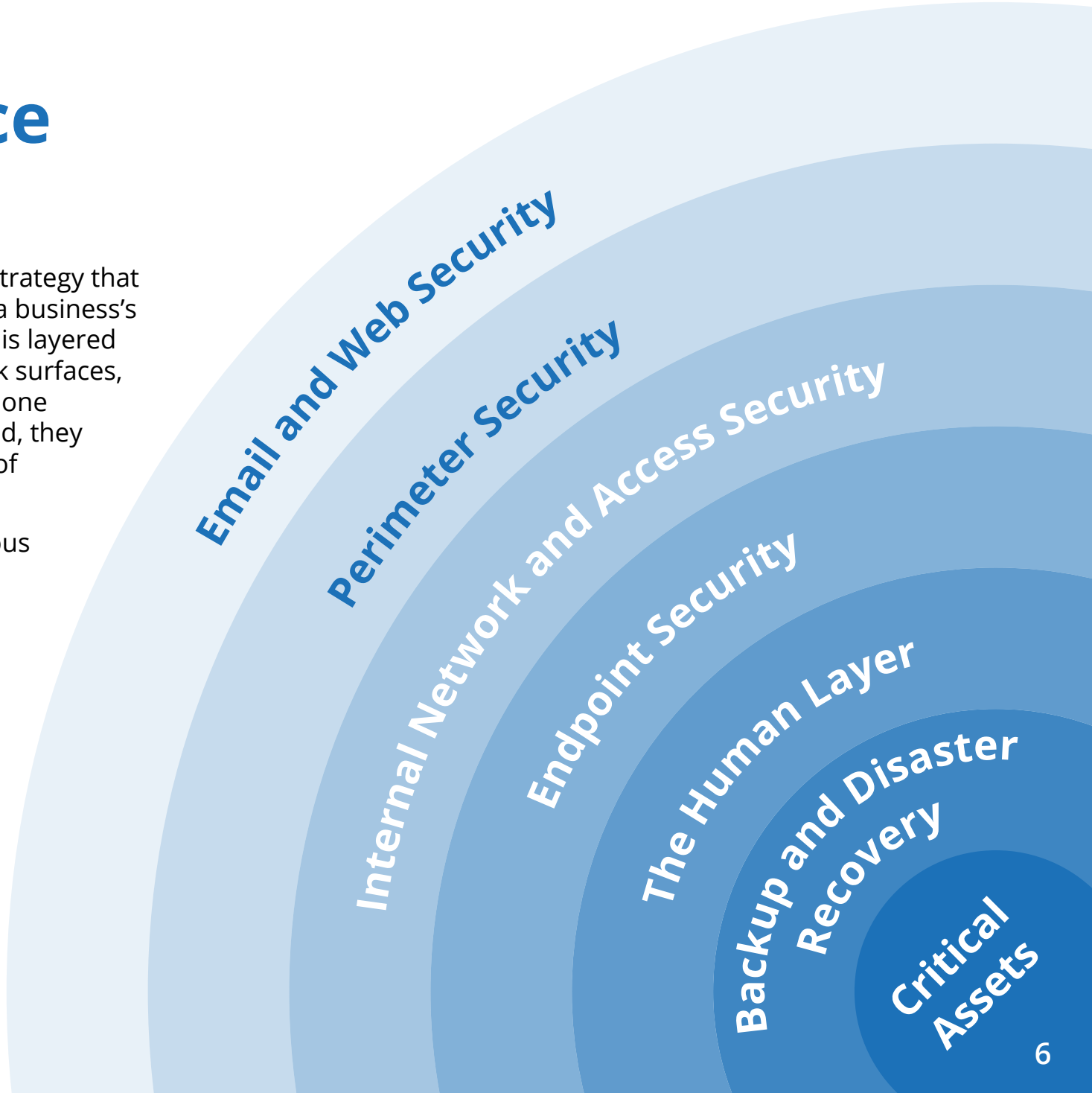
Whilst the previously mentioned attack methods have been around for quite some time, the ways in which cybercriminals target businesses is constantly changing. Alongside these attacks, there are also completely novel attack methods and malware types that are unknown to any business or security professional.

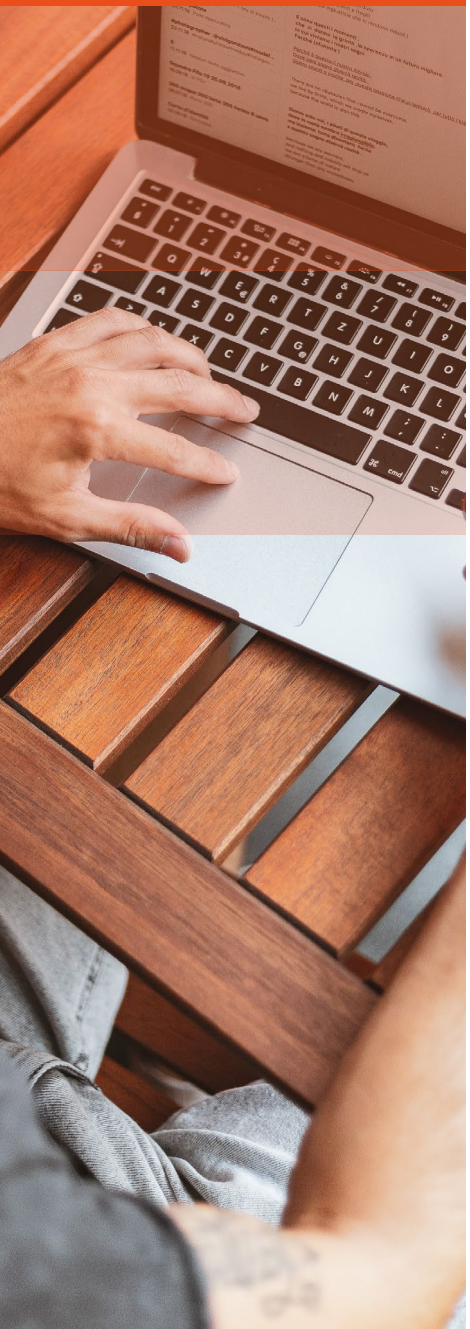
This creates a difficult situation for businesses as they must protect themselves against unknown threats that may not currently exist. As these new threats could be exploiting any attack surface, it is essential that businesses layer their defences to protect their critical assets.

What is Defence in Depth?

Defence in Depth (DiD) is a cybersecurity strategy that uses multiple layers of security to protect a business's critical assets and IT systems. Moving to this layered approach is effective as it secures all attack surfaces, and even if a malicious actor gets through one layer of defence with a novel attack method, they are likely to be stopped by a further layer of defence.

Each layer of security typically has numerous technologies working together, forming a security ecosystem, however, a number of technologies may be included within a single product, with many features being available as part of a Microsoft 365 subscription. Zero Trust also shares similarities with DiD, however, DiD is a more realistic strategy for most businesses, due to the complexity of Zero Trust.





Layer 1: Email & Web Security

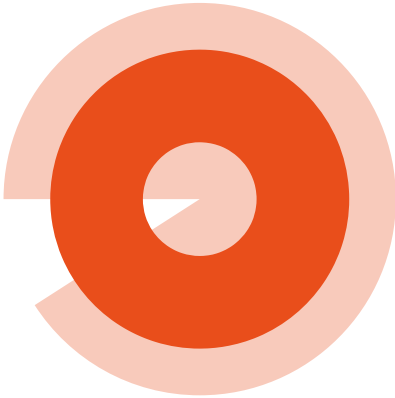
The first layer of defence is email and web security. This layer is extremely important with 90% of IT professionals stating phishing emails as their number one concern. Thankfully, if a business has a comprehensive email and web security solution, they significantly decrease their chance of having their data breached.

In regard to email security, all businesses should have their email set up correctly. This includes the use of authentication records, including **DMARC, DKIM and SPF**. Whilst these are simple controls, they can prevent the majority of low effort spray-and-pray phishing attacks, therefore there is no excuse why all businesses should not have them implemented.

Within this layer, businesses also need a dedicated **email security** solution. Most comprehensive email security solutions use AI to detect any potentially malicious emails and quarantine them before they even reach an employee's inbox. It is also important to have internal email protection, which can prevent the lateral spread of attacks if an account is compromised.

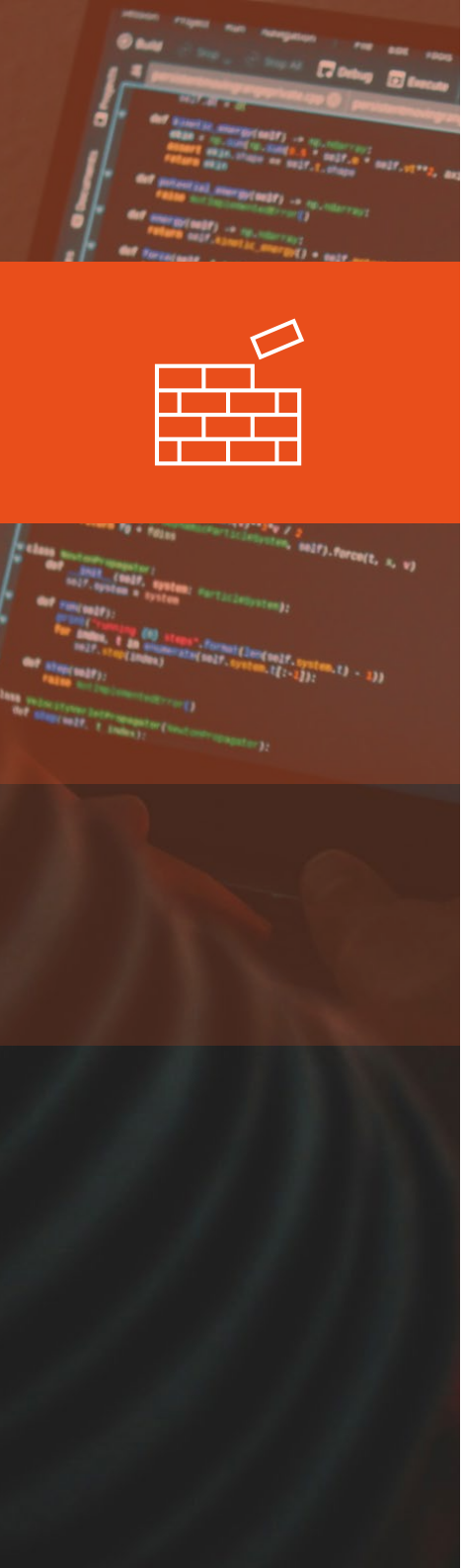
Closely related to email security in this layer is **web security**. A web security solution will not only protect against malicious URLs and websites but also enforce acceptable web use and mitigate shadow IT risks through uncontrolled cloud application risks, especially cloud storage.

This first layer will prevent most low-effort attacks, but if a threat does manage to penetrate this layer, there are 5 more to stop it from reaching a business's critical assets.



90%

of IT professionals state that phishing emails are their number one concern



Layer 2: Perimeter Security

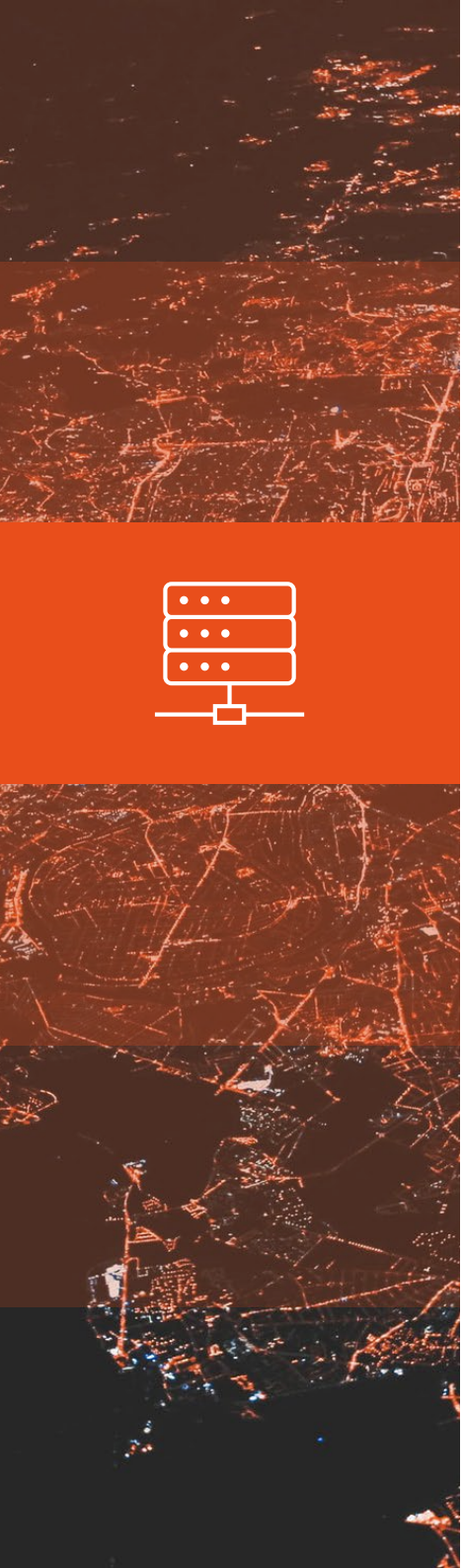
The second layer of defence is perimeter security. This layer includes technologies such as Next Generation Firewalls, Security Information and Event Monitoring and vulnerability management.

Next Generation Firewalls (NGFW) are the latest generation of firewall technology that provide features beyond a traditional firewall. For example, a NGFW includes additional features such as integrated intrusion prevention, application awareness and control, threat intelligence sources and the ability to address evolving security threats. A NGFW can block advanced malware, as well as provide greater visibility over the network, making it easier to defend against threats.

Security and Event Management (SIEM) provides businesses with next-generation detection, investigation and response to uncovered threats. The detection and investigation components use behaviour analytics, AI and threat intelligence to find any suspicious activities. A SIEM solution will respond to these incidents with built-in orchestration. This makes it easier for businesses to manage the massive amounts of security data that is being created at any point and prioritise the alerts and potential actions.

Vulnerability Management is the process of identifying, assessing, managing and remediating vulnerabilities across a business. Most vulnerability management solutions enable asset visibility and provide breach likelihood predictions to prioritise the most critical vulnerability on each asset, with recommendations on how to mitigate the associated risk. Vulnerability management makes it possible to defend against all known threats, but it is a cyclical process, that needs to be constantly managed.

With these technologies, many attacks will be stopped in their tracks before they get anywhere close to a business's data.



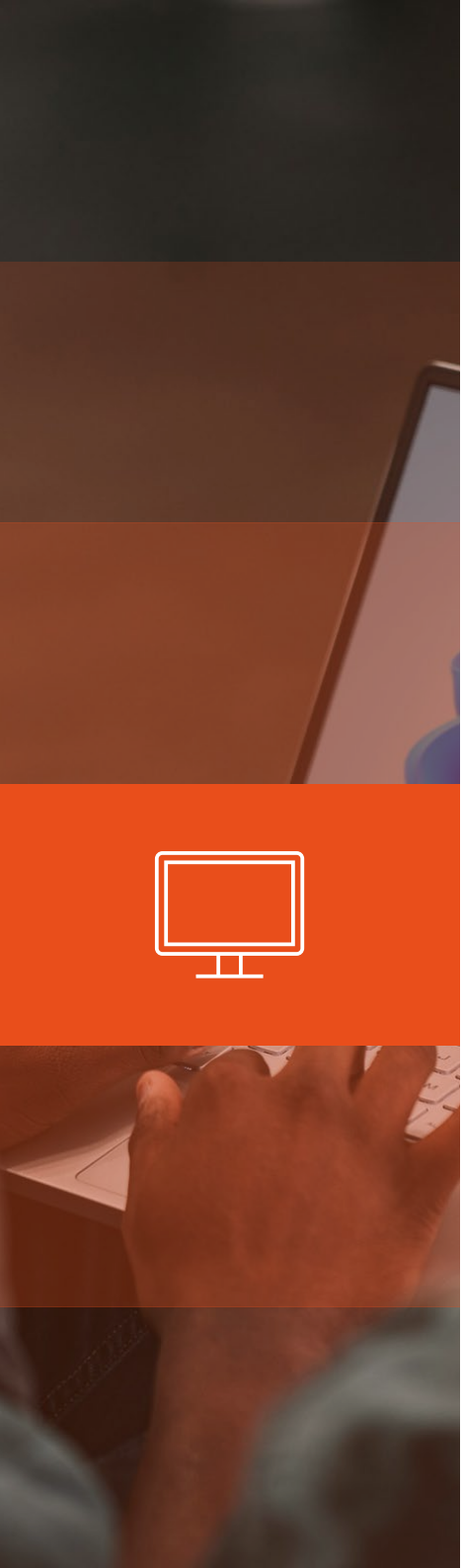
Layer 3: Internal Network and Access Security

If a cybercriminal successfully penetrates the first two layers of security, the next goal is to stop them from moving laterally across a network or accessing any additional data or IT systems. There are many technologies involved in this layer including Identity and Access Management (IAM), attack surface reduction and network segmentation.

Identity and Access Management (IAM) is a framework containing processes, policies and tools for defining and managing the roles and access rights of both users and devices for IT systems. The goal of IAM is to ensure that the correct users' identities are authenticated and that they can access the right tools and data necessary to do their jobs. Within IAM is an overlap between DiD and Zero Trust, which is the principle of least privilege. This concept states that users should ONLY have access rights to what is strictly required to do their job. With this principle, if a cybercriminal compromises a user's account, they do not have access to sensitive data. This framework also includes multi-factor authentication, which is another tool that all businesses should have enabled, as it is simple to set up and can prevent most account compromise attacks.

Network Segmentation is a technique where businesses divide their network into smaller sub-networks, with individual security controls and services on each sub-network. The goal of network segmentation is to ensure that if a cybercriminal intrudes on a business network, they cannot move laterally and uncover more data. There are also similar techniques that focus on segmenting cloud environments to bolster cloud security and compliance.

This layer plays an interesting role within Defence in Depth, as it does not necessarily prevent an attack, but rather ensures hackers can not get any closer to a business's critical assets. For this reason, the Internal Network and Access Security and layer 4 have some areas that overlap.



Layer 4: Endpoint Security

The next layer of protection is endpoint security. This layer is designed to secure any device connected to a network or IT system, including laptops, mobile phones, desktops, IoT devices, servers and virtual environments. This is achieved through an Endpoint Protection Platform (EPP), including Endpoint Detection and Response (EDR) and automated investigation and remediation.

Endpoint Detection and Response (EDR) is one of the key technologies within an endpoint protection solution. It works by detecting attacks based on endpoint behaviour, including process information, network activities, user login activities, file system changes and more. These abnormal behaviours can be detected in near real-time, allowing for either manual or automatic live response capabilities. As EDR uses behavioural-based classification, it is also possible for it to detect zero-day threats, before they cause greater issues.

Many EPPs can also complete **automated investigation and remediation**. Therefore, once a potential threat is found, the solution can perform automated remediation actions, such as sending a file to quarantine, stopping a service, removing a scheduled task and more. This greatly reduces the chance of a business falling victim to a cyberattack whilst there are no IT administrators actively checking the system.

The reason why this layer is relatively deep is due to the fact it does not prevent cyberattacks, but rather detects if there is a malicious actor or malware currently on a device.

65% of busiensses have seen a measurable increase in cyberattacks and attribute it to remote work

Source: Splunk

Layer 5: The Human Layer

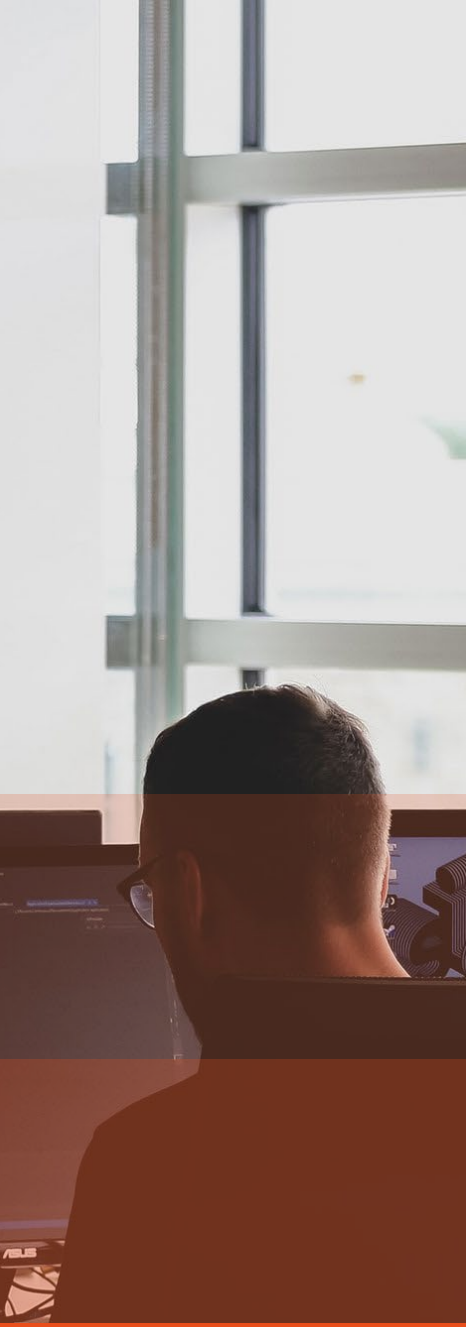
Although the previous four layers of security should prevent most cyberattacks, it is essential that employees have sufficient knowledge of cybersecurity to be able accurately identify and report any potential cyberattack or threat. The main concept within this layer is the human firewall.

A **human firewall** is similar to a traditional firewall, however rather than being an IT system, the employees within a business are given the tools and education to reduce cyber risk. In most businesses, all employees have access to sensitive company and customer data, and therefore everyone plays a role in securing the business.

Businesses can build the human firewall through regular training and education, and watertight policies and procedures that employees understand. The training and education program should give employees the skills to detect a potential cyberattack, and what actions to take to reduce the chance of falling victim to an attack. Common topics included phishing, social engineering, password hygiene, physical security, mobile device security, and threats specific to remote and hybrid work. The training should be interactive, specific to the business and industry, and employees should be given frequent 'refresher' courses to ensure the knowledge is retained.

43% of employees say they've made a mistake at work that compromised cybersecurity

Source: Tessian



Layer 6: Backup and Disaster Recovery

The final layer of security within Defence in Depth is backup and disaster recovery. If all else fails, businesses need to be able to recover their data so they can continue to function after a major cyberattack.

When businesses are considering **disaster recovery**, it is important to remember that it consists of both technology and processes. The same rings true for most layers of security, whilst technology is the backbone of each layer, it needs to be managed to ensure efficiency, either by an internal team member, or a trusted third party IT provider. The technology behind disaster recovery is a comprehensive backup solution. Thankfully, the proliferation of low-cost cloud storage has made it possible for all businesses to have regular offsite backups, greatly reducing the RTO and RPO, and making recovery as quick and easy as possible.

Although in the past, a comprehensive backup solution was the golden key when it came to ransomware, as it meant that businesses could restore to a previous backup and prevent any major data loss. Whilst this still works today, it does not prevent double extortion. This is why the previous 5 layers of security are even more important, as they should stop any ransomware attack significantly earlier than a business needs to resort to disaster recovery.

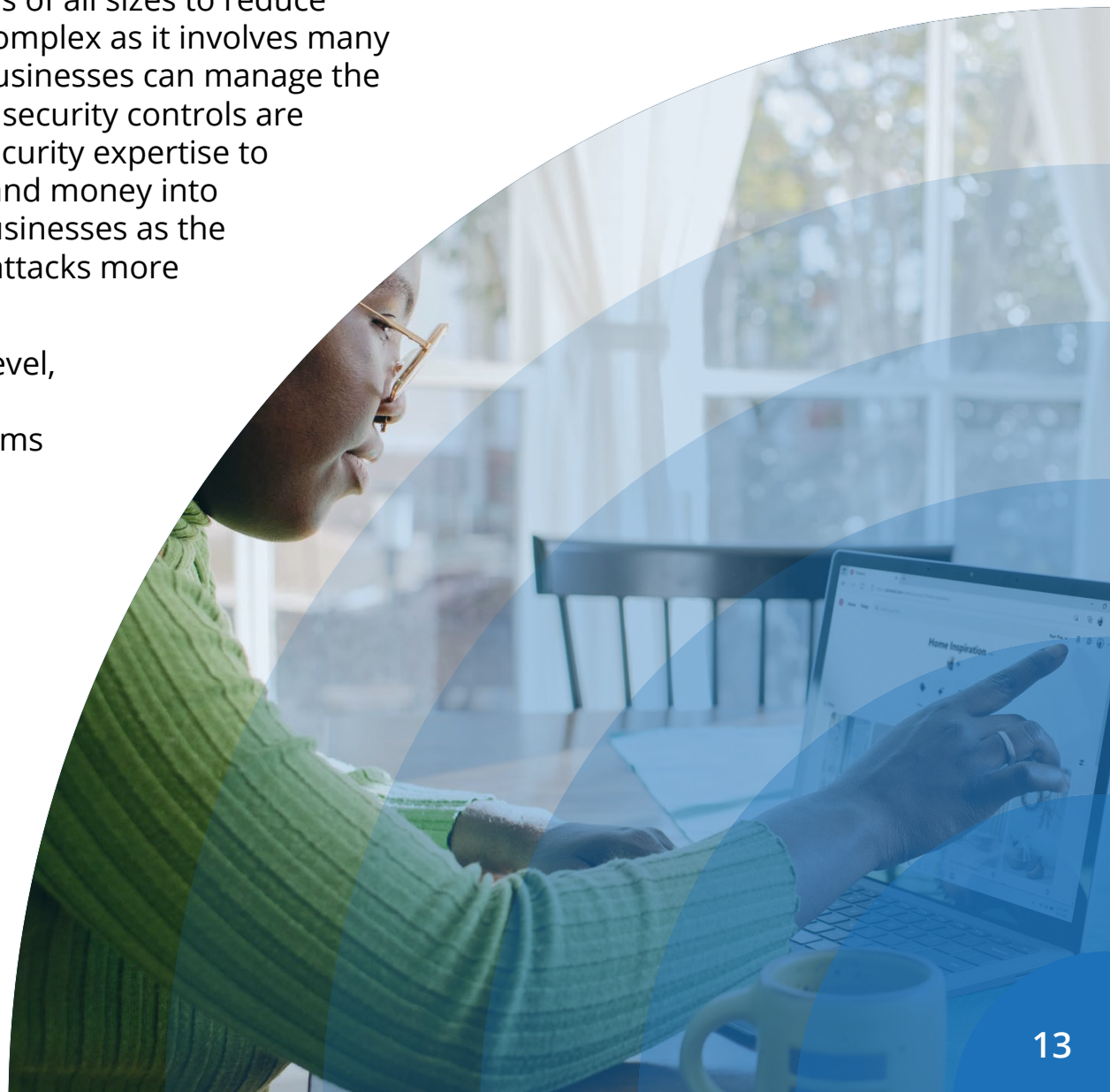
On average, businesses face 22 days of business interruption (less than 100% productivity) after a ransomware attack

Source: Coveware

How to Achieve Defence in Depth

Defence in Depth is a powerful strategy for businesses of all sizes to reduce their cyber risk. Although it may seem expensive or complex as it involves many technologies working together, there are ways that businesses can manage the complexity and cost. Many of these technologies and security controls are included within Microsoft 365, however, it requires security expertise to use them to their full ability. The investment of time and money into Defence in Depth is becoming an easy decision for businesses as the threat landscape becomes more complex, and cyberattacks more financially devastating.

If your business is ready to take security to the next level, contact us and we can support your business with a layered security strategy that will secure your IT systems against current and next generation cyber risks.



bluecar TECHNOLOGIES

www.bluecartechnologies.com

+441183 382 916

info@bluecartechnologies.co.uk