TRUSTMARQUE
Part of Capita plc

There are **No Perimeters** Anymore

Security for the Modern Datacentre

By Neel Dev, Cloud Practice Lead, Trustmarque

Contents

Introduction

In the era of Windows Virtual Desktop, Microsoft 365 and remote working, where does the security perimeter wrap around a business?

Ten to 12 years ago a common scenario was that most users worked on desktops in an office, and all applications were on servers in an organisation's own datacentres. Authentication was via Active Directory (or Novell E-Directory – remember that?). The perimeter was a group or layer of three or four firewalls.

Now, more and more organisations are adopting flexible and remote working. Also, applications are a mix of cloud-based and on-premises apps. So in that regard, there really are no clearly defined perimeters in 2020.

Neel Dev, Cloud Practice Lead, Trustmarque

> More and more organisations are embracing flexible and remote working.

Risks in the **“New World”**

Remote Working

As many workplaces closed because of COVID-19, it forced organisations to adopt remote working to allow business continuity. This meant less travel and a reduction in utility costs, which had many benefits (not least environmental). It also highlighted that the barriers to working from home in many cases was cultural rather than technical.

Businesses can see the advantage of reducing their own real estate by allowing home working, remote, virtual meetings and cloud-based datacentres.

Of course, this comes with some risk. For example, many companies have used Windows Virtual Desktop, Citrix or VMware Horizon View to enable workers to log on to corporate applications from personal devices such as tablets, phones and laptops. However, this introduces new attack points that are harder to protect.

Security questions arise: How can an organisation be sure what updates a user has carried out on a personal device? How secure is their home internet? What antivirus software have they got running on the device?

- **90%** of IT professionals believe **remote workers are not secure**
- Over **70%** think remote staff pose a **greater risk** than on site employees

Netwrix 2020 Data Risk and Security Report

Cloud Applications

We have seen many organisations adopt a small footprint in the cloud, most commonly by way of SaaS. For exmaple, Office 365, Salesforce, Dynamics CRM among many others. Many organisations are turning to PaaS services such as webapp-as-a-service or Azure SQL as a way of managing costs and also offloading security updates and patches, along with resilience and back-up to hyperscale cloud providers.

Again, as great as these services are and as easy as they may make the lives of administrators, this also means that the old world of perimeter security and Active Directory becomes even more irrelevant. That's because increasing numbers of apps are no longer housed in the corporate datacentre.

The top cloud security concern is **data loss and leakage: 64%**

2019 Cloud Security Report (ISC)

The ease of use of hyperscale cloud has also led to a new shadow IT problem as developers and users leverage tools and platforms like AWS, Azure, Google Drive and Dropbox. Without the knowledge of central IT, Data Loss Prevention, security and compliance becomes even harder to manage.

54%

of organisations are confident that their employees are not sharing data using any means of communication unknown to the IT team.

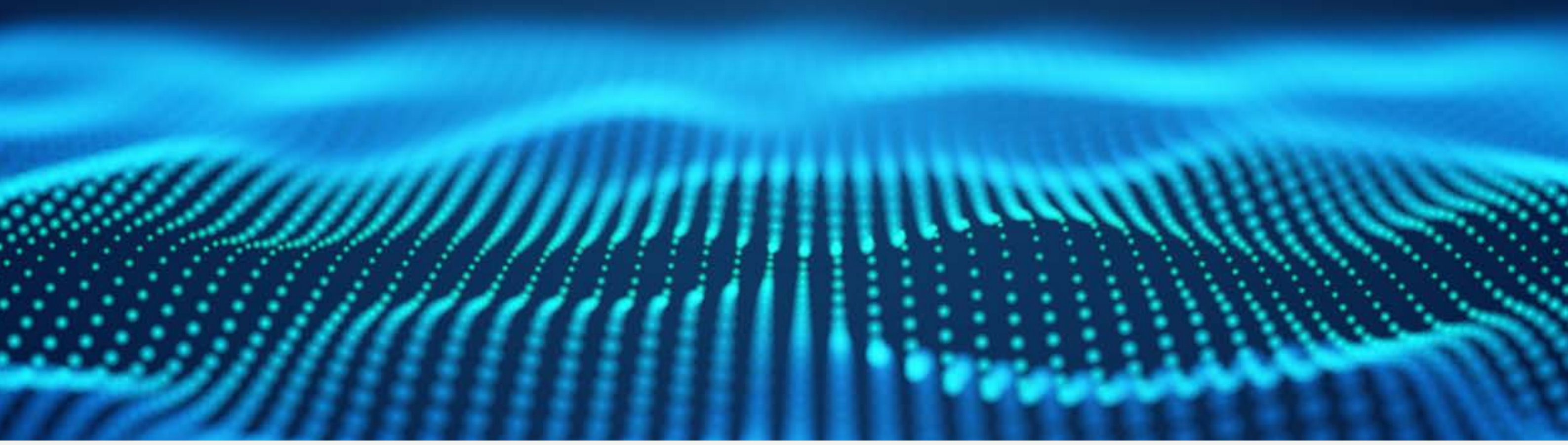
Netwrix 2020 Data Risk and Security Report

Two IT worlds: The interplay between legacy and cloud native applications

Customers often face difficulties when in a hybrid situation: backend applications or databases are often on-premise and front-end services are in hyperscale cloud.

Security can be a challenge when trying to use modern authentication or encryption technologies such as OpenID or SAML

Many organisations often have to manage the disparity between Windows Server-based applications that are hosted on a VM in a datacentre, and new cloud friendly applications that may be stateless, and support scale out, APIs and authentication via technologies such as OpenID or SAML. The interplay between these resources has been recognised by malicious players as a vulnerability and an attack vector which is something we are seeing across the market place.

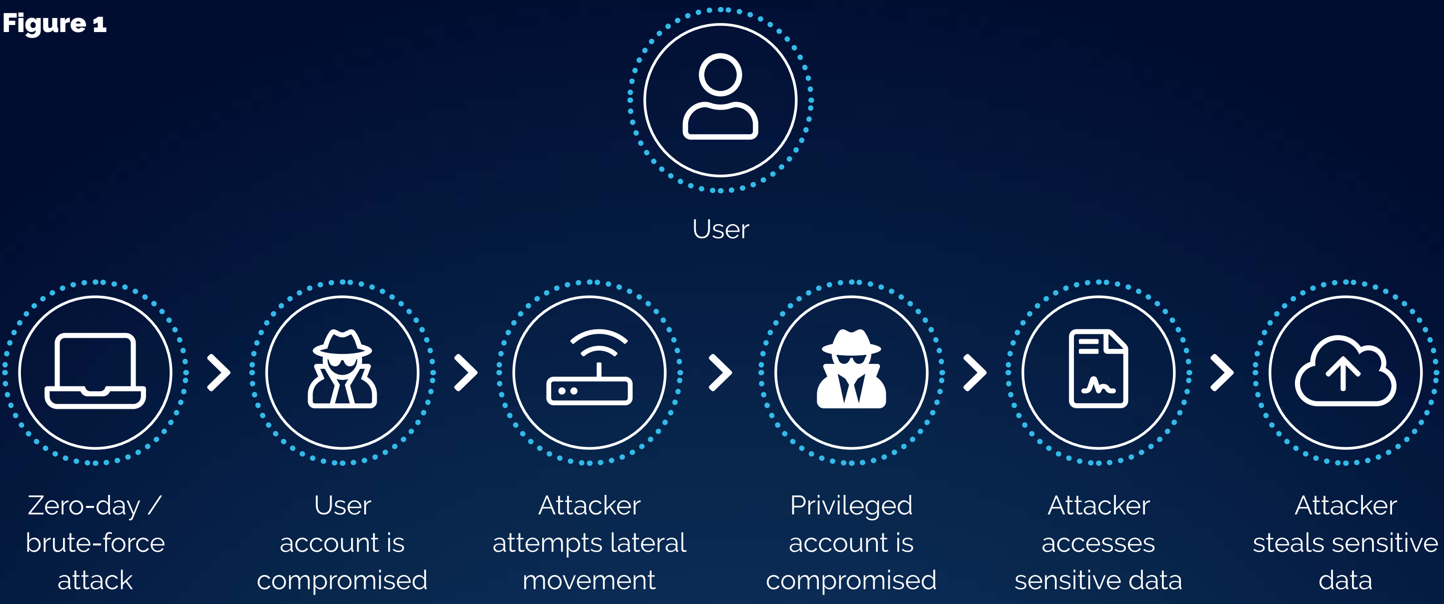


Current Attack Scenarios

A corporate network perimeter is no longer the most common attack point. This can be seen from the plethora of phishing attacks and password attacks.

As businesses and customers move more online, mobile app, websites, web facing applications and databases have become the next most common target. Below is an example of a common kill chain:

Figure 1


User
Zero-day / brute-force attack
User account is compromised
Attacker attempts lateral movement
Privileged account is compromised
Attacker accesses sensitive data
Attacker steals sensitive data

Apart from DDOS attacks the most common attacks seen in 2019 include:

- ⚠ Phishing attacks
- ⚠ Password attacks
- ⚠ SQL injection
- ⚠ Cross site scripting attacks
- ⚠ Drive by attacks

There are three common goals that cyber attacks are designed to gain access to:

- Corporate data
  (to steal or lock in a ransomware attack)
- Customer data
  (for malicious purposes or to sell on)
- Websites and applications
  (to attack and affect company brand or perception in the market)

> An organisation's data is its crown jewels and must be protected at all costs.

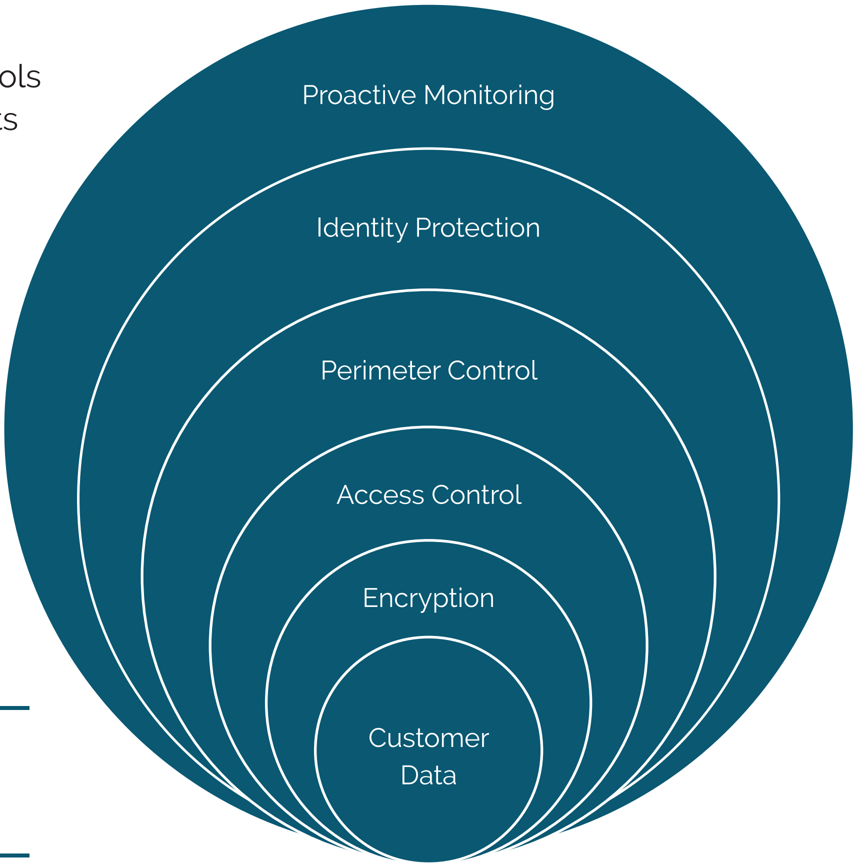
A Multipronged **Defence**

The best way to defend against increasingly sophisticated attacks is to recognise that at some point you will likely be attacked and compromised as an organisation. And prepare for that.

By having multiple layers of defence between an attacker and corporate data, we can stop the movement of a hacker or malicious code or software through the organisation at a particular layer, if others have been compromised. If we look at the previous example again (Figure 1), we see the following sequence:

- Company X had a legacy IT Administrator who is now Head of Information Systems
- One of the company's monitoring tools (Advanced Threat Protection) detects that the user's laptop, due to the nature of their current role, never accesses the domain controllers anymore - though they still have access to them. All of a sudden, the user's laptop is trying to gain access to the DCs.
- Investigation reveals that in spite of safeguards, their laptop has been compromised as has their identity.

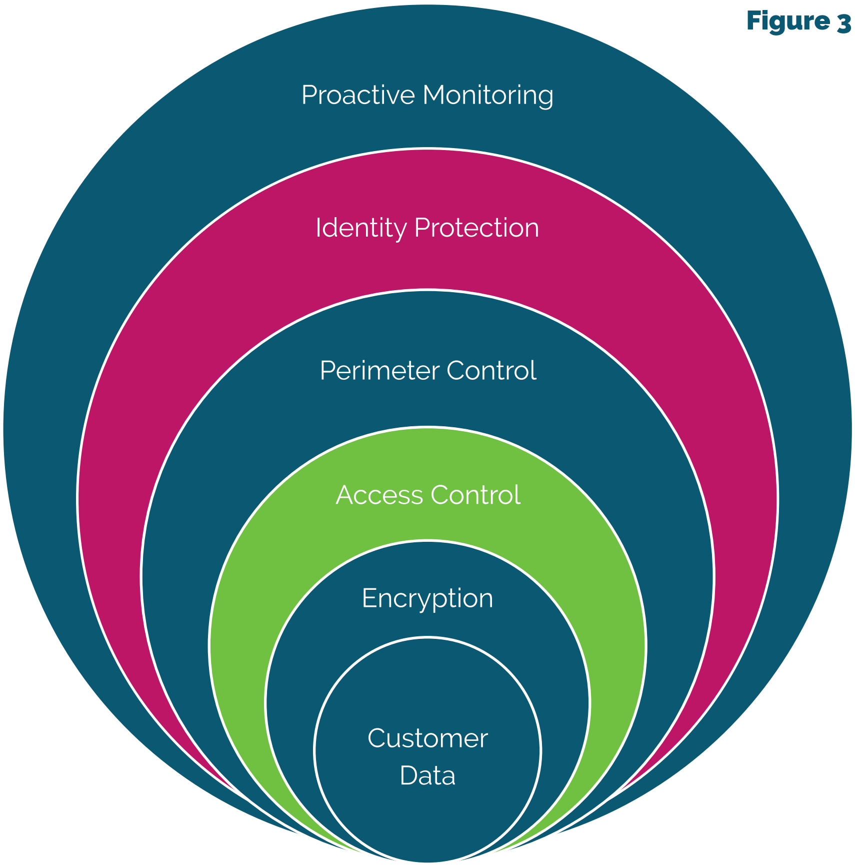
Figure 2 - The 'security onion'



- Thankfully, because the company invested in Azure Conditional Access (figure 4), the attacker could not get to the company data. As soon as the system picked up that the user's laptop was signing in from an unusual IP address, it asked for two factor authentication which the hacker was unable to provide.

- In our 'security onion' we can see that though the 'Identity Protection' layer has been compromised, the 'Access Control' layer came to the rescue.

Figure 3



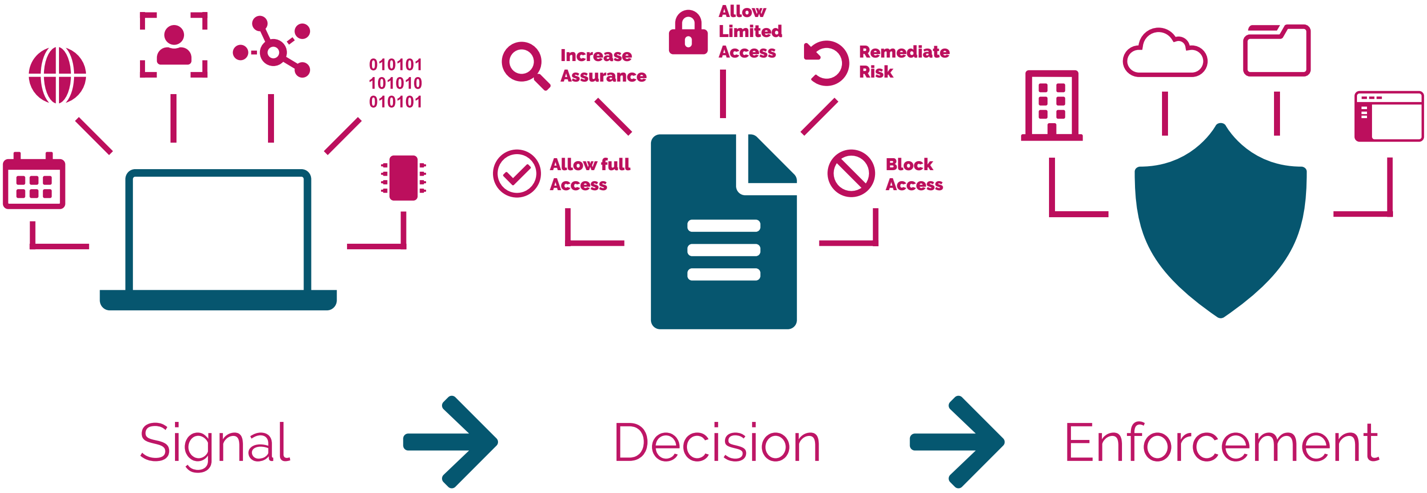
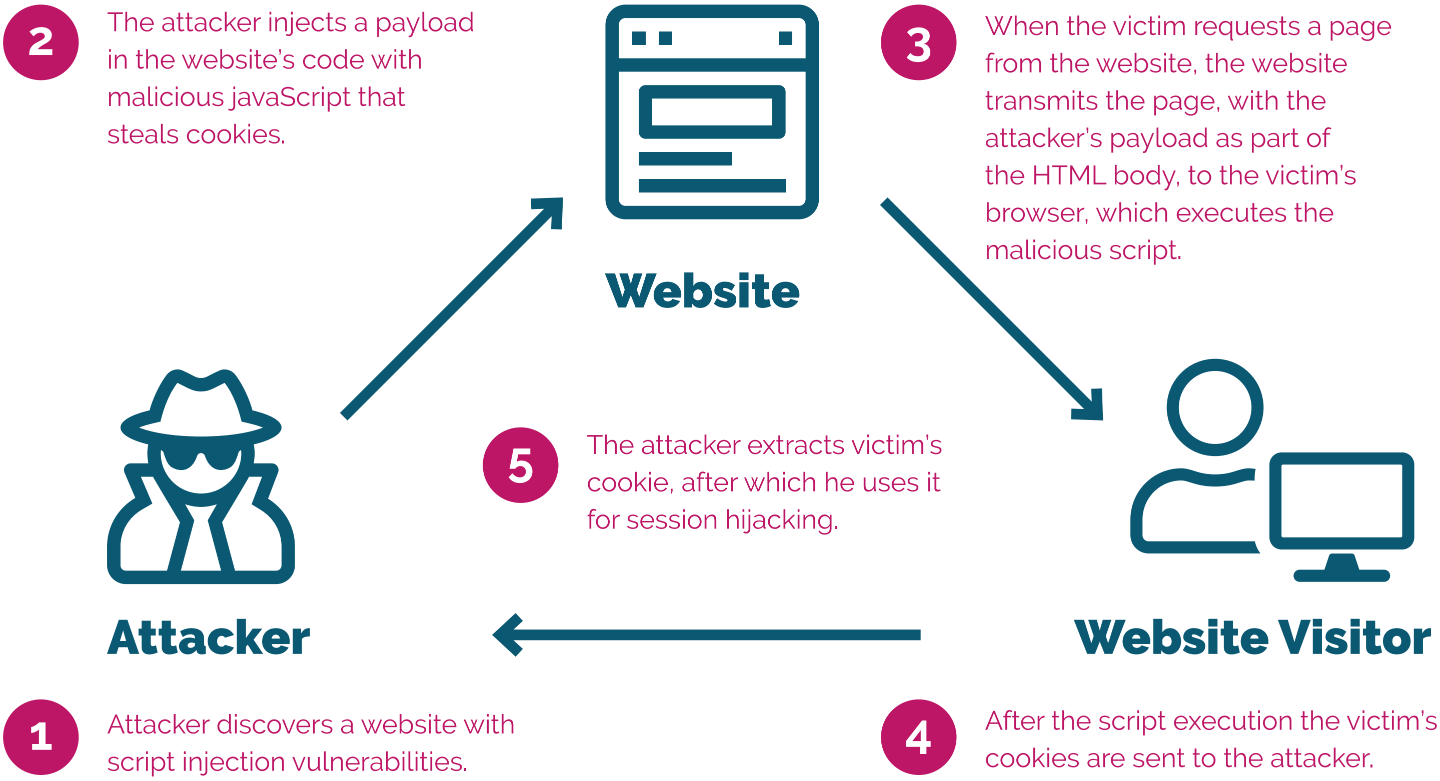


Figure 4

Below is an example of a website scripting attack

Figure 5



2 The attacker injects a payload in the website's code with malicious javaScript that steals cookies.

3 When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script.

5 The attacker extracts victim's cookie, after which he uses it for session hijacking.

1 Attacker discovers a website with script injection vulnerabilities.

4 After the script execution the victim's cookies are sent to the attacker.

In the case of these attacks, it is no longer the identity layer that is being attacked but the 'Perimeter Security' layer of the security onion. This is where a Layer 7 firewall, or a web application

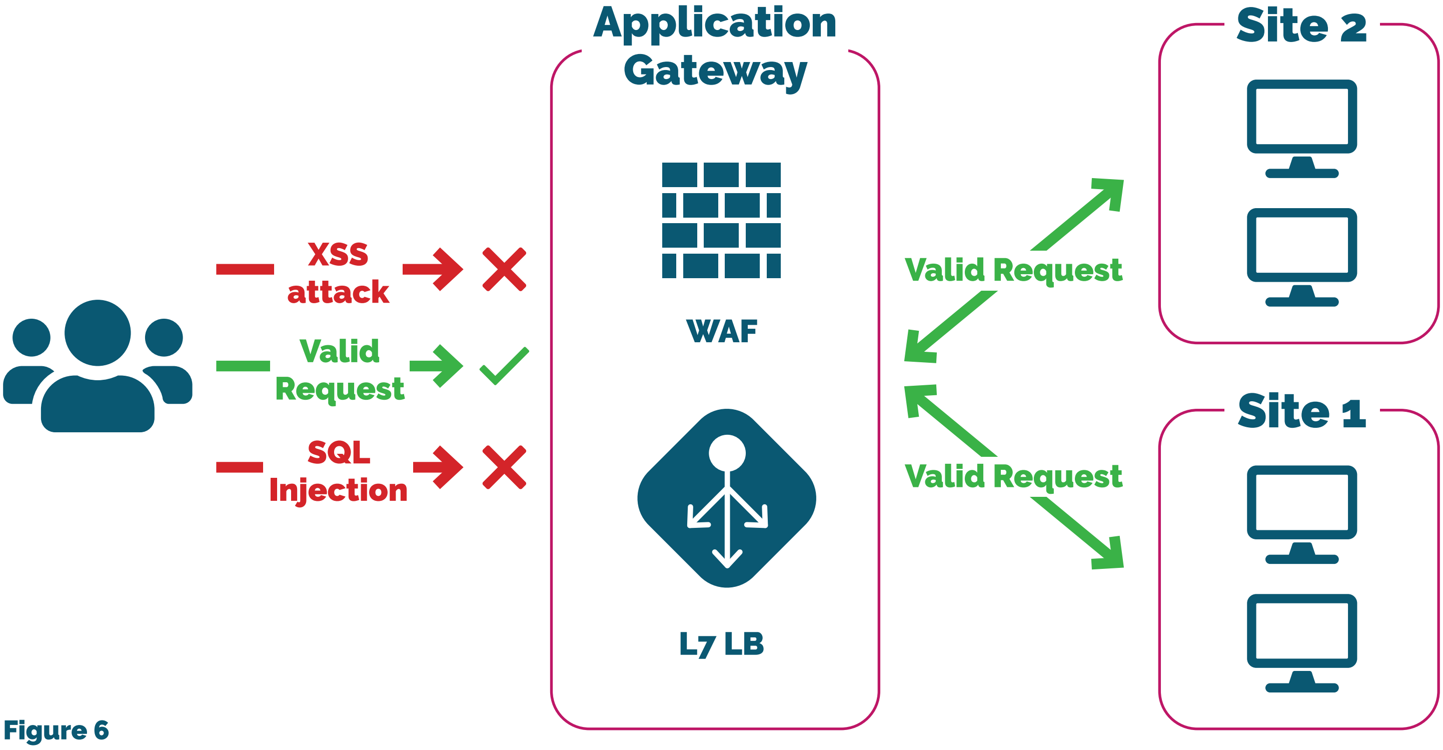
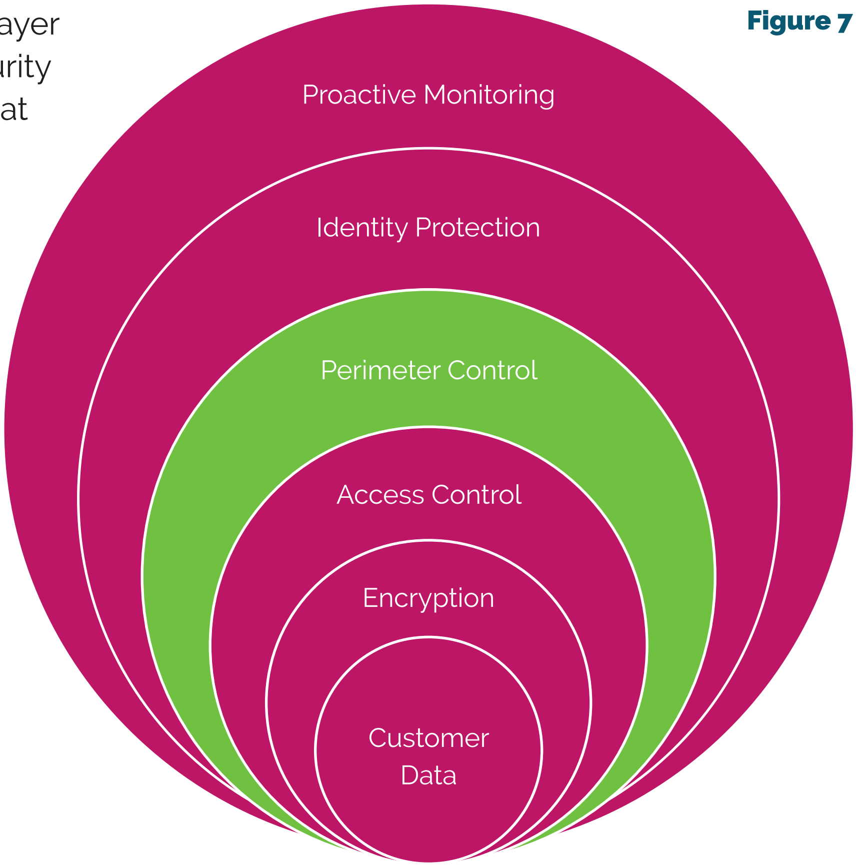


Figure 6

In this instance, the 'Perimeter Control' layer stops the attack. An added layer of security can be applied by using Advanced Threat Protection for Azure SQL and SQL Always Encrypted. It is worth noting that these are just some common attack scenarios. There are increasingly dynamic attacks arising – either brand new types of attack or sophistication brought to familiar attacks.

Figure 7



Macro Attacks

Macro Attacks - more sophisticated and malicious code continues to slip through defences.

Machine Learning Poisoning

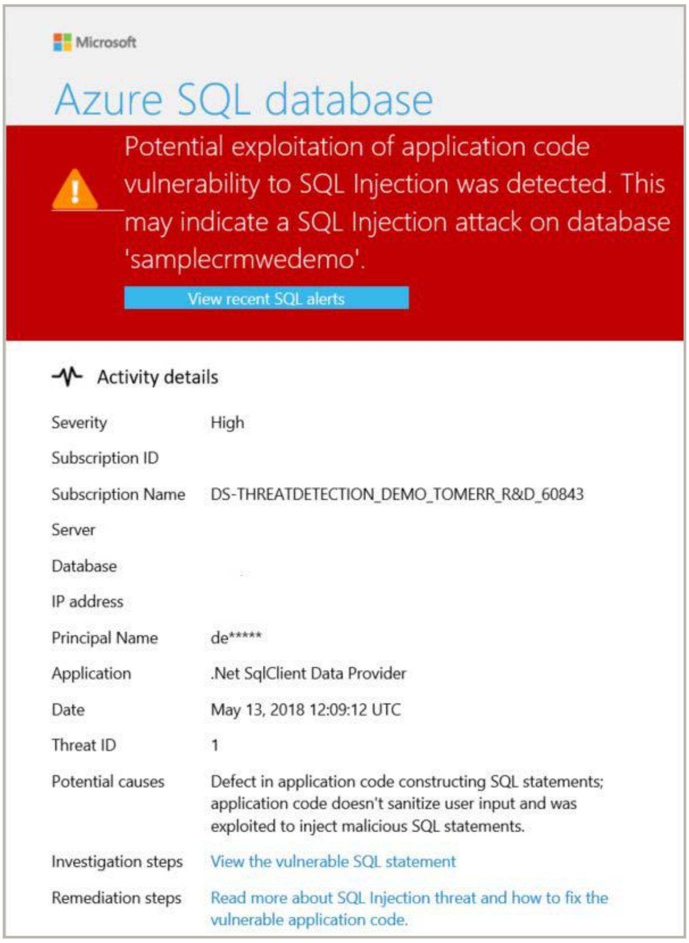
Machine Learning Poisoning is injection of malicious samples into ML algorithms and training sets to get information like buying patterns that are confidential.

AI Fuzzing

AI Fuzzing is the use of AI to find vulnerabilities and launch zero day attacks more frequently. AI Fuzzing is commonly used by security organisations to look for vulnerabilities in their own environments, but is also now being used by hackers. This is leading to more zero day attacks. Also hackers are attacking organisations before they have updated their software, which highlights the importance of quick updates.

Drive by Attacks

Drive by Attacks, where website visitor software and OS is quickly scanned for vulnerabilities and exploited, are getting more common with the advent of AI Fuzzing.



Azure SQL database

Potential exploitation of application code vulnerability to SQL Injection was detected. This may indicate a SQL Injection attack on database 'samplecrmwedemo'.

Activity details

Severity	High
Subscription ID	
Subscription Name	DS-THREATDETECTION_DEMO_TOMERR_R&D_60843
Server	
Database	
IP address	
Principal Name	de*****
Application	.Net SqlClient Data Provider
Date	May 13, 2018 12:09:12 UTC
Threat ID	1
Potential causes	Defect in application code constructing SQL statements; application code doesn't sanitize user input and was exploited to inject malicious SQL statements.
Investigation steps	View the vulnerable SQL statement
Remediation steps	Read more about SQL Injection threat and how to fix the vulnerable application code.

What Could a Potential **Defence Stack** Look Like?

It may seem like a daunting, complex and costly exercise to set up this multi-layered defence, but many of the technologies and products are already often incorporated into the infrastructure or are part of a suite.

We can simplify our security onion by segmenting under four broad categories:

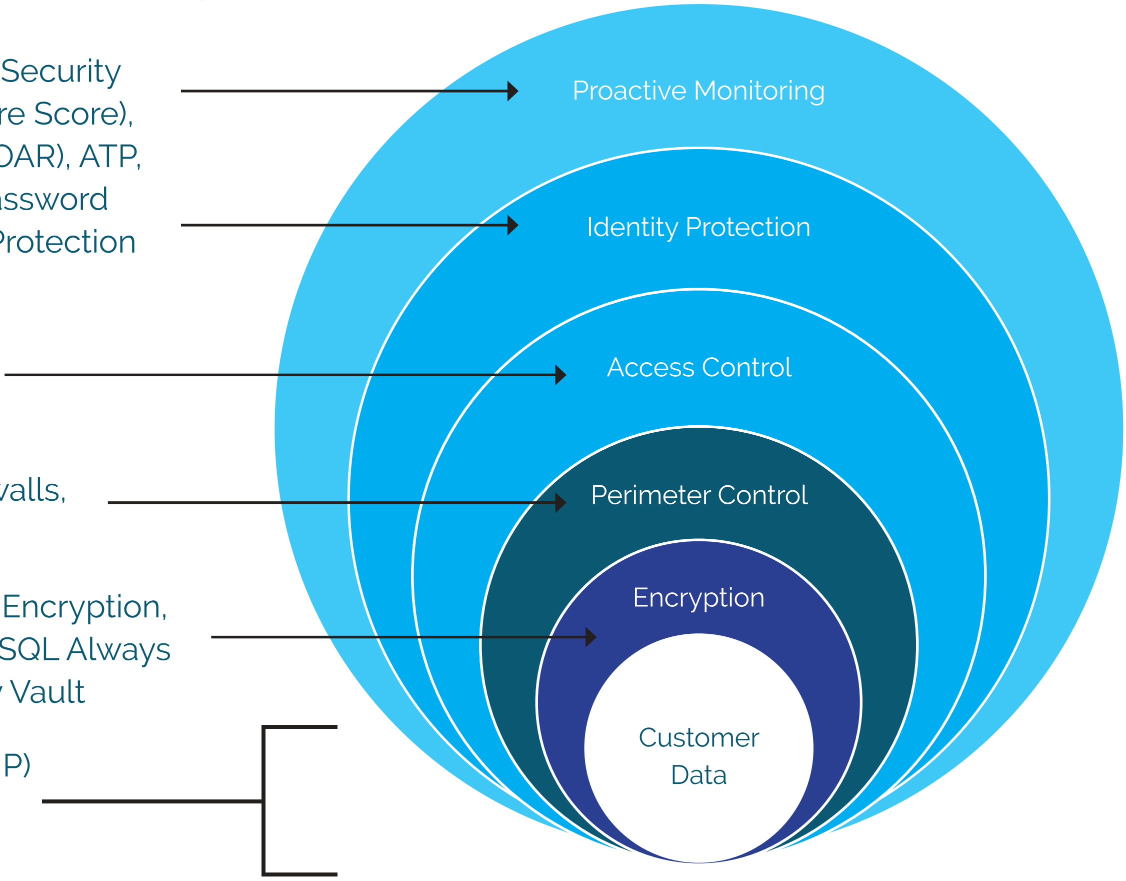
Azure Monitor, Azure Security Centre (CSPM - Secure Score), Sentinel (SIEM and SOAR), ATP, CASB (MCAS) PIM, Password Protection, Azure ID Protection

RBAC, Azure Policy

Azure Firewall, Azure WAF, CloudGen Firewalls, Azure Frontdoor

TLS, Storage Service Encryption, VM Encrypted, AzureSQL Always Encrypted, Azure Key Vault

Data Classification (AIP) Data Loss Prevention (PowerAutomate)

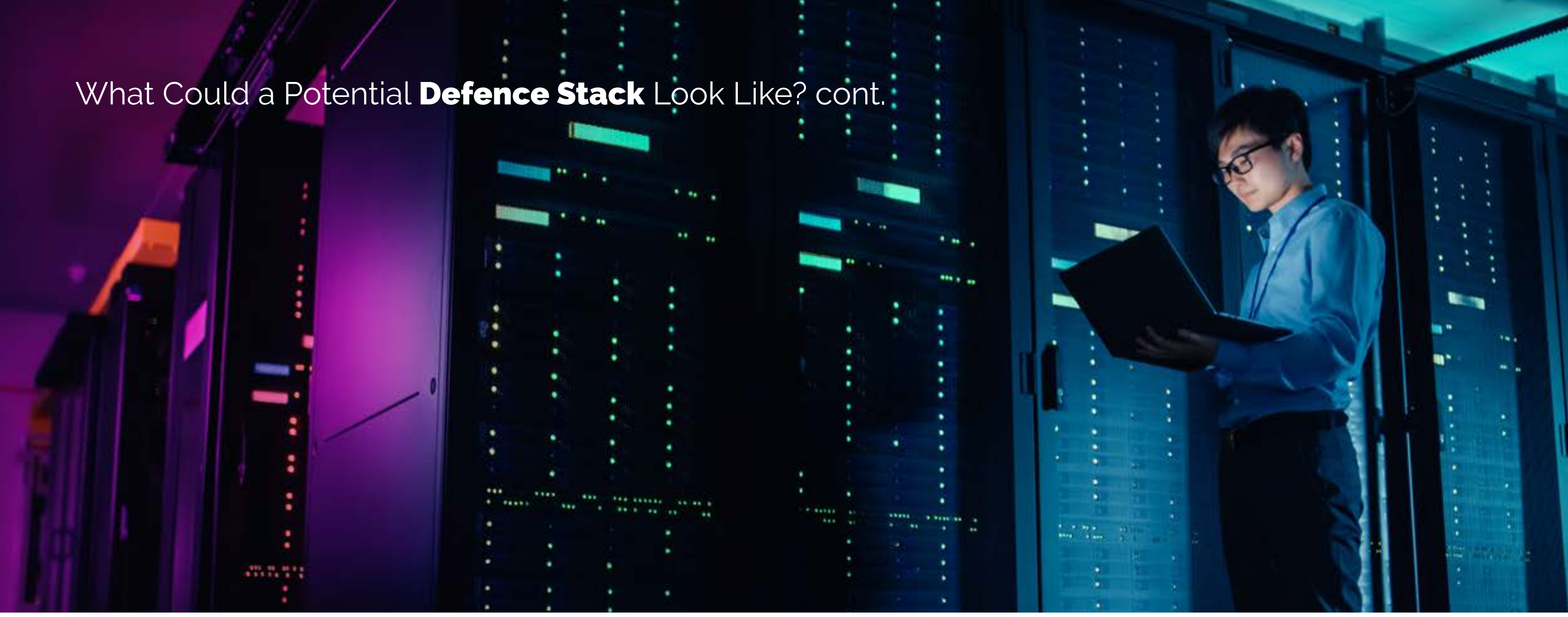


■ Proactive Monitoring

■ Identity & Access

■ Network, Compute & Data

■ Encryption



Proactive Monitoring:

Monitoring technology and bringing some intelligence to bear via AI and ML is critical to get the balance between proactive alerting and filtering out background noise for the SOC team. A SIEM tool is of importance here.

Azure provides a cloud-based SIEM tool called Azure Sentinel. This also qualifies as a SOAR tool. However, other Microsoft elements of the security onion can work with third party SIEM tools like Splunk via Azure Graph APIs.

Identity and Access:

Azure Active Directory P2 includes Azure Identity Protection, password protection, multifactor authentication. AAD P2 can also be purchased as part of EM+S (Enterprise Mobility and Security Suite) which in turn is part of Microsoft 365. This also includes MCAS, the Microsoft CASB solution.

Microsoft 365 combined with a SIEM (Sentinel) tool would cover most of the proactive monitoring stack as well as the Identity and Access stack. Role Based Access Control and Azure Policy are part of the Azure platform and there is no added cost for these.

Network, Compute & Data:

- Layer 3 and 4 Firewalls (Azure Firewall, Sophos XG, Barracuda NGF etc.)
- Layer 7 Application Gateways (Azure WAF, Sophos XG, Barracuda WAF)
- CASB (includes the above, but is also offered through third parties such as ZScalar)
- Firewalls for individual components – Azure Storage, Azure SQL, Containers
- NSGs (Network Security Groups) for all subnets

Encryption:

- Encryption at rest – All Azure storage accounts are encrypted at rest
- TLS – to ensure data in transit is secure
- Use of Azure Key Vault to store encryption keys
- Azure SQL Always Encrypted – Column Encryption Keys and Master Encryption keys both stored outside of SQL
- Data Lake Encryption, if applicable

Conclusion

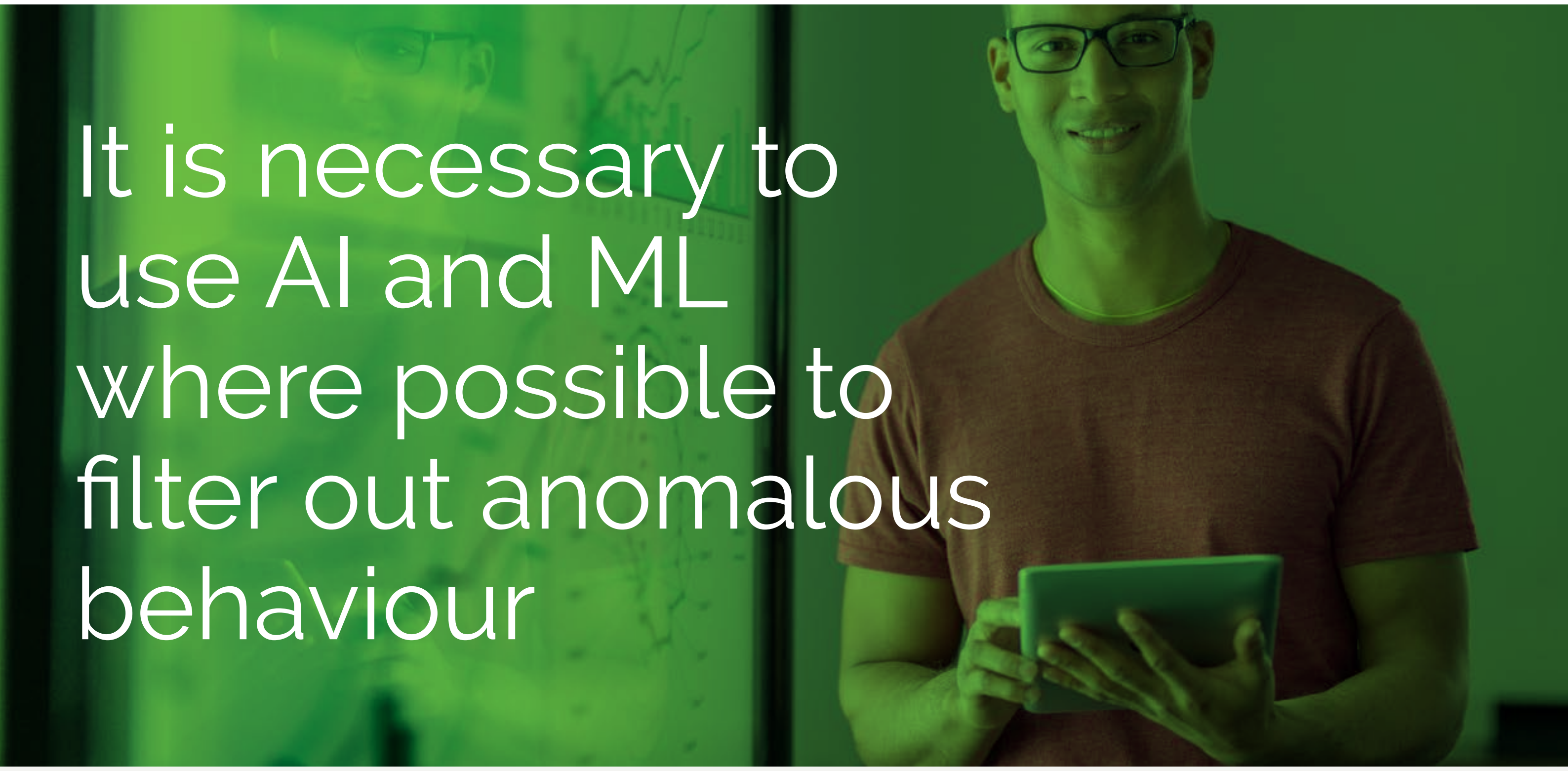
As hackers, malware and cyber attacks get more sophisticated, the only way to protect the goldmine that is a company's data is via a multi-layered defence.

In order not to overwhelm a SOC with false positives and an avalanche of information, it is necessary to use AI and ML where possible to filter out anomalous behaviour. Many SIEM and CASB solutions come packed with these.

A centralised view of the landscape in a business is essential, which is where a SIEM tool, or overarching security monitoring tool becomes essential. Like Azure Security Centre with Azure Monitor.

On top of this, identity protection is critical, alongside hybrid cloud perimeter security and encryption of data at rest, in transit and while in use.

We will be attacked and possibly compromised, but with a multi-layered security strategy we can block and slow the advance of hackers and malicious code enough to take remedial action before data is affected.



It is necessary to use AI and ML where possible to filter out anomalous behaviour

References:

Research Cosmos
https://www.researchcosmos.com/reports/cloud-computing-market/92916729

ESG
https://www.esg-global.com/hubfs/images/Infographics/ESG-Infographic-2020-Technology-Spending-Intentions-February-2020.pdf

Gartner
https://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf

Netwrix
https://www.netwrix.com/2020datariskandsecurityreport.html

Microsoft Docs
https://www.microsoft.com/en-gb/microsoft-365/enterprise-mobility-security/cloud-app-security

Microsoft Docs
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

Microsoft Docs
https://techcommunity.microsoft.com/t5/azure-security-center/bg-p/AzureSecurityCenterBlog

Barracuda Networks
https://www.barracuda.com/products/webapplicationfirewall

Sophos XG
https://www.sophos.com/en-us/products/next-gen-firewall.aspx

ZScalar
https://www.zscaler.com/custom-product-demo

Splunk - Cybersecurity
https://www.splunk.com/en_us/cyber-security.html

Strengthen your security with Trustmarque

Why choose Trustmarque? When it comes to cyber security in the cloud we are vendor agnostic. Our goal is to help customers move to the cloud by removing the security pain points that impede many cloud strategies. We use our experience and relationships with multiple security and cloud vendors such as Microsoft, Sophos and Barracuda to bring the best security solutions to market for both cloud and on premises customers.

We are Trustmarque

Trustmarque are an award-winning IT partner who delivers customer-centric IT solutions that deliver better outcomes. For over 30 years, we've empowered our customers to work smarter and run their businesses more effectively, with long-standing relationships in the public and private sectors.

info@trustmarque.com | www.trustmarque.com | 0845 2101 500

TRUSTMARQUE
Part of Capita plc