Cyber security for banking and finance: navigating risk and maximising reward

Strategies for effectively managing digitalisation, cloud acceleration and tightening regulations.

Introduction

Effective cyber security should flex to your organisation's needs and, critically, take its lead from your individual requirements – rather than providing set protections and expecting your organisation to operate within those confines.

Security must enable, not define. So, understanding your organisation's operational environment and what optimum performance looks like must come first.

Of course, in sectors like banking and financial services, where trust and data security are fundamental, cyber security requirements do become more complex. Potentially, the stakes are higher.

But this just reinforces the importance of getting it right, by building security out from a place of comprehensive insight into your organisation and its challenges. Right now, we believe ongoing digital transformation, cloud acceleration and growing governance pressures are exacerbating security vulnerabilities within finance and banking – but we also know each individual organisation will face unique additional issues on top of that.

This is why we approach every engagement within the banking and financial services environment by creating a clear picture of requirements first, and only then tailor a cyber security solution.

You'll see this thinking reflected in the structure of this paper. We'll take you through our understanding of your landscape and challenges, and progress to exploring how our solutions map onto your organisation's security requirements. At that point, our specialists are ready to answer your questions and help you move closer to the solution that'll enable your organisation to thrive securely.

Industry evolution is increasing cyber security pressures

Evolution is essential to business longevity and success but, right now, the financial industry is finding out that positive change in one area can exacerbate security vulnerabilities in another. Significant and valuable progress in three key areas is creating cyber security implications that require immediate attention.

The three dominant waves of evolution today:

1. Ongoing digital transformation

Organisations are going digital and incorporating automation with a main objective of improving the customer experience (54%), achieving operational excellence (44%) or delivering new products and services (35%).

2. Cloud acceleration

Hand-in-hand with digitalisation comes an increased rate of cloud migration. As an established technology, financial institutions are exploring and adopting cloud solutions at pace; in 2022, 53% of CIOs stated their commitment to increasing investment in cloud platforms.

3. Growing governance pressures

Banking and financial services organisations are embracing Environmental, Social and Governance (ESG) goals as an essential part of their brand, product, sales, customer and talent strategies, as well as investment decision-making. The governance aspect is increasingly reflected in a tighter regulatory focus on operational resilience, business continuity and the management of third-party risk.

The impacts of these evolutions on cyber security:

1. The organisation's attack surface increases significantly

The combination of greater digitalisation and accelerated cloud adoption creates more potential access points for cyber criminals to attack, more areas for the organisation to protect and more demand for cyber security expertise and resource.

Global Chief Risk Officers are aware of this, with 72% seeing cyber security as the top year-ahead risk – but are they investing in the right areas?

2. Business interruption threats are more likely

Digital transformation and shifting infrastructure to the cloud brings more connections and deeper dependences with third parties. And, although these third parties bring extra, specialist capabilities in areas such as cloud-based applications and services, they also expand the lead organisation's attack surface. There's a risk that the third party's security will be an easier entry point into the organisation's network than a direct attack on the organisation itself.

Banks, insurers and other players in the financial services industry are aware of this, flagging business interruption and supply chain disruption as their second top risk – but are they tackling it in the most effective way?

3. Regulators are taking a tougher stance

The finance and insurance sector is a prime target for cyber criminals, second only to manufacturing, accounting for 19% of all global cyber attacks in 2022. After cyber incidents caused a number of major outages at banks and payment processing companies, regulators are taking steps to require greater operational resilience to defend against business interruption and supply chain disruption.

This may require a shift of focus within some banking and financial services organisations since, in 2022, only 34% of Chief Risk Officers saw operational resilience as a key priority. Will upcoming legislation change this?

Get ready for DORA

The Digital Operational Resilience Act (DORA) will apply to financial sector organisations operating in Europe from 17 January 2025.

This means that the regulation impacts not only banks and other financial institutions, but also the technology firms that support them. For example, DORA will apply to a financial services firm regardless of whether they use a hyperscale cloud provider or a small fintech.

Purpose: to strengthen resilience to IT-related incidents by requiring organisations to focus on a Digital Resilience Strategy and accompanying Digital Resilience Framework.

Impact: DORA will mean that all financial services firms must prove they can withstand, respond to, and recover from all types of IT-related disruptions and threats. The responsibility and accountability for institution-wide digital resilience will sit with CEOs and the executive committee, covering governance and organisation, IT risk management framework, ICT incident management, classification and reporting, digital operational resilience testing, third-party provider risk management, and information sharing.

Potentially the most challenging area will be achieving oversight of 'Critical IT Third Party Providers' (CTTPs), such as network providers, cloud platforms, and data analytics services as well as financial services firms.

Actions: banking and financial services organisations need to review their cyber security to ensure compliance with DORA, and to protect their ability to operate digitally.

Significant cyber threats today… and more on the horizon

The scale of the cyber security problem facing banking and financial services is becoming increasingly evident.

In 2022, the financial sector was the second most targeted industry by cyber attackers globally. Europe received the greatest volume of attacks, accounting for 33% of the total. This means that 74% of all financial institutions experienced one or more ransomware attacks, and 63% of affected organisations paid a ransom.

This needs to change. However,

81%

of bankers fear that, instead, there'll be an escalation, driven by unsettled geo-political situations.

Most organisations recognise the urgent need to tackle this, but are hampered by the market-wide shortage of cyber security experts. It's estimated that 3.4 million more cyber security workers are needed globally to secure assets effectively. This is exacerbated by the level of skill required to build defences within and across such complex, shifting attack surfaces. And then further expertise is needed to scale up these advanced defences to an organisation-wide level, particularly when the organisation operates globally.

This leaves banking and financial services organisations uncertain how to make the best use of their limited resources.

In 2022,

43%

of executives expressed concern that their bank may be ill-equipped to protect customer data, privacy and assets in the event of a cyber attack.

This constantly evolving landscape needs a different cyber security approach – but what does that look like?

Know your infection vectors to better know your enemy

In 2022, spear-phishing was the top infection vector for the banking and financial services industry. It exploits the humanity of employees, using emails designed to convince the user to open a link or attachment to allow malicious software into the organisation. People want to be helpful, to respond to someone in authority, or to explore something that looks interesting – and the damage is done.

Our point of view

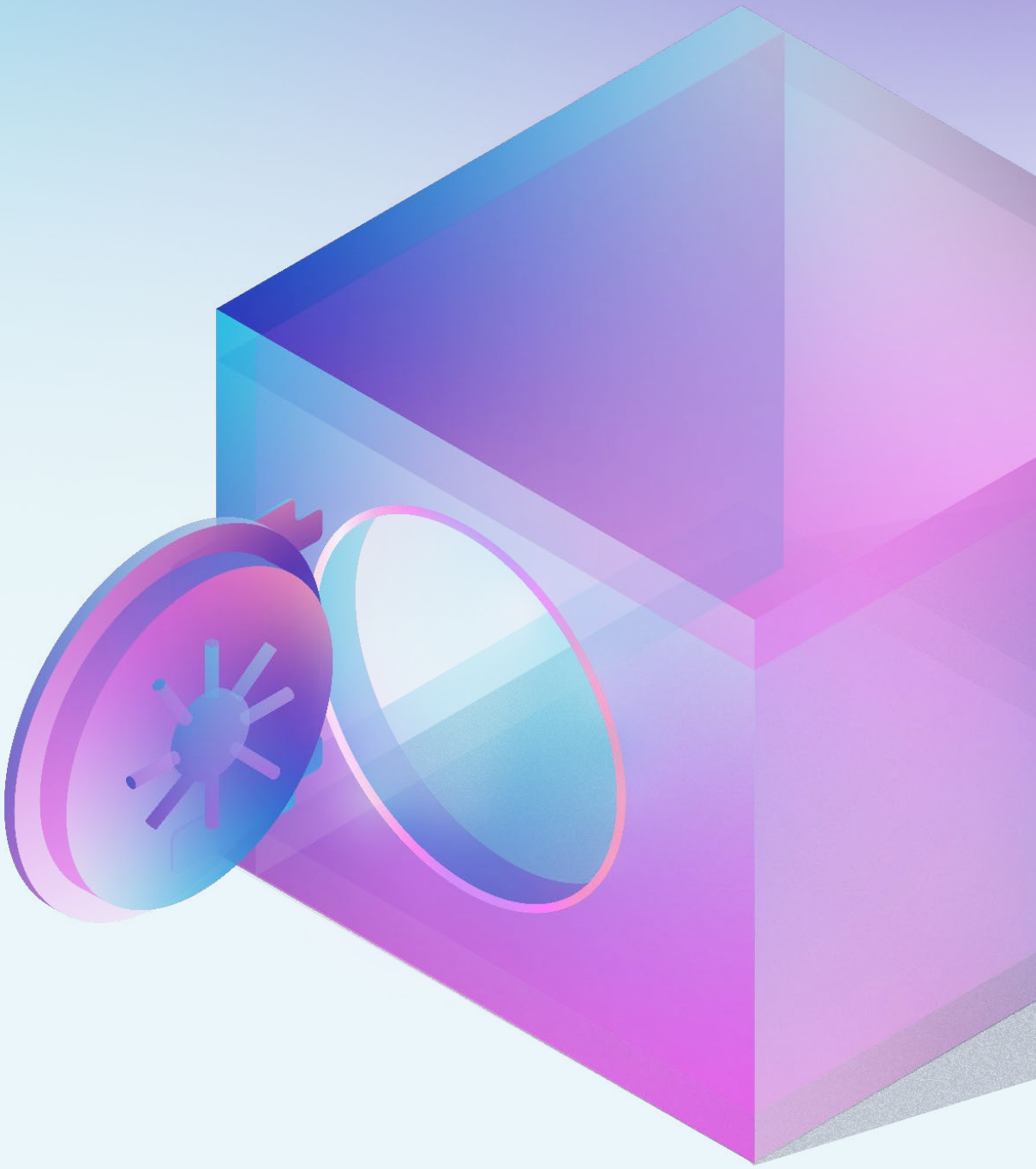
Although these market evolutions change the risk landscape for the banking and financial sector, this change is ripe with potential – providing it's paired with Zero Trust thinking and development that keeps pace.

This new cloud-centric, more regulated environment calls for a robust cyber security posture, particularly for organisations that are high-value cyber targets. Key to building this posture is prioritising operational resilience and protecting data and end users.

Based on our global experience, we've created an approach for banking and financial services organisations that recognises the singularity of the sector's challenges. It prioritises supporting change in three areas.

1. **Securing your multi-cloud**
   Helping you achieve better control, visibility and security across your cloud infrastructure.
2. **Securing your end users and data**
   Establishing defences for your customer information and company data when your employees are working from anywhere.
3. **Improving your operational resilience**
   Identifying security risks across your third-party interactions and internal infrastructure and defences to protect business continuity and regulatory compliance.

The following sections take you through why it's important to action these priorities, and what that could look like for your organisation.



1. Securing your multi-cloud

Financial institutions are prioritising the shift to dynamic, multi-cloud environments to capitalise on the cloud's cost, performance and ESG advantages.

In a competitive financial marketplace, innovative digital disruptors are constantly encroaching on market share. To stay one step ahead of fintech challengers, financial organisations need to invest in agile business models that support innovation and deliver speed to market.

The cloud's scalability and flexibility meet these needs, while also offering a more energy efficient way to store and process vast amounts of data and applications. By reducing the burden of powering onsite infrastructure, cloud migration could cut global carbon emissions by 59m tons of CO_2 per year.

Replacing on-premises data centres with cloud solutions has significant cost implications, too, as legacy infrastructure is typically expensive, labour-intensive and inefficient. Moving from physical hardware to hybrid cloud eliminates ongoing procurement, installation and maintenance expenses, while fixed and pay-as-you-use cloud pricing unlocks scalability and computing power without ongoing additional costs.

Understanding the risks of cloud transformation

While innovation and efficiency gains are driving cloud migration, businesses must be prepared for the impact hybrid cloud has on their security posture.

Migrating to a hybrid cloud environment can make it harder to see where data sits, who has access to it and how it's being protected. Blind spots are a significant risk. CISOs who are in the dark about their attack surface can find it increasingly difficult to ensure the right cyber security controls are in place. This lack of visibility heightens risk and intensifies three key vulnerabilities:

1. Data breaches

Financial organisations' hybrid cloud environments are a popular target for cyber criminals thanks to a sprawling attack surface and incredibly lucrative data. The second most targeted industry globally, in 2022 alone, data breaches on average cost financial organisations $5.97m.

2. Compliance failures

Cloud migration doesn't secure organisational compliance with industry regulations like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Significant fines are just the tip of the iceberg, as non-compliance can bring additional consequences including reputational damage and divestment.

3. Unauthorised access

Complex layers of infrastructure and services make cloud environments challenging to monitor and control. Investing in the right security monitoring tools to prevent unauthorised users from accessing and moving around within cloud infrastructure unnoticed should be a top priority for financial institutions.

How our solutions secure cloud transformation

Our core cloud security services give you clear visibility over your devices and applications and combine to ensure maximum protection across your cloud environment.

Cloud security consultancy and advisory services

For first-time cloud migration, our cloud security consulting advisory service works with you to devise a transformation strategy based on your unique risks, goals and infrastructure. This tailored approach ensures smooth, secure migration, in compliance with all relevant regulations. Those further along in their cloud journey can benefit from our risk visibility tool which assesses your cloud security and infrastructure to give you visibility of potential risks and an action plan of how to mitigate them. Our co-management approach can help you to set up, monitor, manage and respond to any security incidents 24/7/365.

Identity and access management

To secure the multi-cloud, our approach highlights the importance of the identity of human and non-human users, admin accounts and endpoints. Our managed identity and access management solution secures access to cloud-hosted applications based on identities, permissions and roles and rapidly detects and responds to threats. By helping you to adopt a Zero Trust approach, our solutions mean your employees, partners, and customers can quickly and securely access all the applications they need.

Secure Access Service Edge (SASE)

SASE combines SD-WAN and Secure Services Edge (SSE) into a secure, holistic solution that safeguards an organisation's future in the cloud. We know that every organisation starts from a different point, with a unique set of existing security products and use cases, so we offer choice and flexibility of either a single vendor SASE ecosystem or a hybrid SD-WAN and SSE approach. The result is always a seamlessly integrated solution that builds on the Zero Trust framework of security and seeks to eradicate threat and improve business performance – all while meeting the diverse and increased demands of users.

The benefits of our cloud security solution

- **Access expertise for your multi-cloud strategy**
  We have specialists who can help define a security strategy and cloud architecture that's tailored to your individual business, supports your digital transformation and aligns resources to your goals, regardless of what cloud vendors you use.
- **Achieve better control and auditability over your cloud infrastructure**
  We can give you the power to control user access to all your classified information before and after migration across both your legacy and hybrid cloud ecosystem.
- **Better secure your cloud and reduce data breaches**
  We assess and test your cloud implementation against industry standards, so you can be confident your migration won't leave your data exposed or open to abuse.

2. Securing your end users and protecting your data

As remote working increases the number of smart devices connecting to your network, securing your end users is vital to prevent cyber criminals from infiltrating your data and systems.

As with many industries, working from home is now commonplace in banking and finance, with employees connecting and interacting remotely. But while hybrid working is helping businesses unlock greater productivity and employee satisfaction, the ability to connect any device from anywhere has expanded the perimeter of the corporate network, creating a broader attack surface.

Organisations need to urgently reassess their security infrastructure to give remote users the same level of protection as their office colleagues, particularly any legacy anti-virus products that are only able to detect known threats. Because these solutions are unable to detect file-less malware or suspicious behaviour at the endpoint, they're prone to miss today's sophisticated attacks, leaving an organisation at risk of inadequate detection, response and remediation. To stay effective, regular manual updates are in order but this is less than ideal for organisations with limited cyber resource.

The risks of failing to secure your endpoints

Robust endpoint security acknowledges that employees are a security vulnerability and gives them the right support to keep your network safe against a myriad of threats.

Malicious or inadvertent threats involving staff and suppliers are on the rise, and it only takes one employee slip-up to give an attacker access to your entire network. Today, 70% of all successful breaches originate at the endpoint. To help employees avoid security traps and understand the extreme lengths cyber criminals will go to access confidential financial information, the right training programmes and processes are crucial. Fraud prevention and cyber security best practice awareness should be foundational, with regular updates and reminders to help teams spot suspicious activity and reduce human error. Organisations who fail to secure their endpoints risk:

1. Phishing breaches

Spear-phishing attacks were the top infection vector for the industry in 2022, representing 53% of attacks. They're are an easy option for cyber criminals looking to circumvent sophisticated network and data security to access sensitive personal and financial information.

2. Exposed gateways

Without the right endpoint monitoring solutions, security teams can't maintain visibility, detect and control all the connected devices across your estate, or safeguard them against malicious activity. This means you could be leaving several gateways into your network vulnerable.

3. Regulatory breaches

Office-based and remote workers are equally culpable under GDPR and the PCI DSS. Endpoint protection outside of the traditional security perimeter is critical to ensure remote workers are compliant with these regulations and don't run the risk of organisational data breaches, fines and reputational damage.

How our solutions protect end users and data

Our fully comprehensive solutions for endpoint protection provide best-in-class prevention, detection, and response capabilities.

Thorough endpoint security advice
We'll assess your current endpoint security, infrastructure and data loss prevention processes to provide you with a clear overview of your security posture, including gaps that could introduce potential risks. We can also take appropriate action to identify and auto-remediate incidents before they can become headline news.

Endpoint detection and response
As attacks become more sophisticated, so must your defences. That's where our elite partnerships with Microsoft and CrowdStrike come in – combining machine learning and artificial intelligence (AI) with next-generation antivirus technology to provide unparalleled endpoint visibility and protection. By speeding up threat detection, investigation and response, we can maximise the protection of your IT environment and maintain the integrity and availability of your endpoint devices.

Co-managed Endpoint Detection and Response (EDR)
Our co-managed approach delivers round-the-clock monitoring, management and response assistance - easing the pressure on your security team without compromising your defences.

The benefits of EDR

- **Get better visibility and protection across your endpoints**
  With EDR you can stay in control of your network with full visibility and threat prevention as our solutions constantly look for file and non-file-based attacks at the endpoint.
- **Reduce your threat response time**
  EDR doesn't need a continuously updated list of virus signatures as it constantly scans files and monitors for suspicious behaviours at the endpoint to quickly detect and isolate threats.
- **Gain round the clock endpoint security**
  Our experts take the pressure off of your in-house security teams. They will set up, monitor and / or manage your security controls, so your team can focus on critical tasks.

3. Improving operational resilience in your organisation

Digital services are evolving the way the finance industry does business, but it's important to take a second look at the third parties they're depending on to help deliver these digital solutions.

As digitalisation deepens, so does the dependence on third-party suppliers helping to provide innovative new banking and payment solutions. But, from a security perspective, every digital third-party supplier needs to be considered as a potential gateway for cyber attackers to gain access to critical business operations.

As cyber criminals increasingly leverage gaps within software supply chains, organisations need to adopt a holistic approach to risk management across both internal and external partners. This is especially important as legislation like DORA tightens the rules around operational resilience and management of third-party risks.

Systematic partner audits, rigorous internal testing and comprehensive threat intelligence reporting are just some of the areas where financial organisations will need to step-up their efforts. But these demands will put already stretched security teams under even greater pressure.

A lack of operational resilience increases your risk

Security and data protection practices are only as strong as the weakest link in your supply chain, making holistic third-party risk management and intelligence sharing vital.

Due to the modern business landscape that's intertwined with intricate supply chains and interdependencies, a comprehensive approach to operational resilience is needed to consider both internal processes and external collaborations. Without adequate safeguards in place, organisations become more susceptible to:

1. Security breaches

Extensive, complex supply chains are increasingly leaving security gaps for criminals to exploit. Data breaches stemming from these vulnerabilities are on the rise, exposing sensitive customer data and critical business systems.

2. Outages and business interruption

Cyber attacks often disrupt business operations, knocking out core functionalities that lead to poor customer service and impeded business processes. The resulting financial consequences – from customer compensation to income loss - can be devastating, while the impact these outages can have on brand reputation and share price are also significant.

3. Non-compliance and regulatory fines

For organisations grappling with the fallout of business interruption, there's also the risk of regulatory fines. Financial institutions that fail to meet DORA requirements from 2025 may face fines of up to €10m or 5% of their total annual turnover.

How our solutions boost operational resilience

Our protection solutions make sure your organisation can adapt to change and stay resilient at all times.

Operational resilience advice
We'll risk assess your estate and those of any third parties you're working with, using the results as a springboard to define your digital operational resilience strategy and ICT risk framework. Our cyber risk quantification tool, SAFE, can also deliver full visibility and quantify risk across your people, processes, technology, cyber security products and supply chain.

Digital operational resilience testing
We can carry out vulnerability scanning, open-source analysis, physical security reviews, software scanning, NIST (National Institute of Standards and Technology) health checks and Threat-Led Penetration Testing across your internal infrastructure and the third parties in your software supply chain. Our experts will alert you of any vulnerabilities and provide thorough recommendations on how to fix them.

Cyber resilience boosting security tools
The right security tools depend on where you are on your cyber security journey and your unique organisational needs. To make sure we cover all bases, we've partnered with industry leaders to offer a range of solutions from EDR to SD-WAN, threat detection and response and managed cloud security. Working alongside your team, our experts can select the options that are right for you and help to implement them.

The benefits of our operational resilience strategy

- **Managed compliance and regulatory obligations**
  Our experts can help take the pressure off your team by risk assessing your IT infrastructure and building up your resilience strategy and processes to fulfil the latest regulations and requirements, including DORA. We can also manage your threat posture, proactively respond to security incidents on your behalf and run all of your digital operational resilience testing.
- **Reduce the risk of costs from service disruption**
  With improved operational resilience, you can safeguard your business' operations and reduce the impact of service disruption costs, like customer compensation or loss of income.
- **Less risk of data breaches**
  Our advisory services thoroughly assess internal and third-party security gaps and, with our recommendations and security controls in place, you'll be able to considerably reduce the risk of data breaches across your organisation and beyond.

Why BT for security in banking and financial services?

We're at the heart of the banking and financial services community

For over 50 years, we've been an active member of the industry, working closely with the Financial Conduct Authority and financial regulators to shape policy and make sure our solutions always deliver risk and compliance outcomes that are fair, explainable and auditable. That's why we serve 78 of the world's top 100 banks, because we're always listening closely to financial organisations and working alongside them as their operational landscape evolves to create the bespoke solutions they need.

We're global security specialists

Our experience and expertise in protecting governments, nation states, critical national infrastructure and large global corporations from cyber attacks every day gives us a ringside seat on the complex security threat landscape. We use this unique position to support organisations to detect and respond to threats in a Zero Trust world with real-time visibility and monitoring, drawing on the expertise of our 3,000 security professionals, 350 highly skilled consultants and our security operations centres operating around the globe. We're also named as a leader in the IDC MarketScape European and AMEA Managed Security Services 2022 vendor assessments.

We have a renowned global network

We're a reliable partner with global experience and credentials, and the research and development capabilities to turn the latest innovations into resilient and trusted services on a global scale. We've delivered thousands of solutions globally with our ever-increasing choice of secure services and solutions. Our approach means that multiple technologies and legacy systems can be easily managed to create a single, secure global network infrastructure for your business. Our network services have been recognised as a leader in Gartner's Magic Quadrant for 17 years.

We're vendor agnostic

With longstanding partnerships and decades of experience working with many leading suppliers, we're in an exclusive position to advise you on the right partners for your unique journey. Our Cyber Assessment Lab cuts through the vendor noise and identifies the appropriate technologies needed for your specific operation. Plus, we're fully vendor agnostic so know how to secure your cloud infrastructure regardless of what vendor you use. This means as the market evolves and you want to build-on your investments, you can easily swap solutions and stay secure.

We have a longstanding commitment to sustainability

We've been on a climate action journey for over 25 years, pledging to become a net zero and circular business by 2030, and 2040 for our supply chain and customers. Our platinum EcoVadis rating puts us in the top 1% of sustainable organisations worldwide, so we're confident we perform well on ESG metrics.

Financial security in action - case study

Helping a major UK building society evolve their security

The challenge

Our customer, a major UK building society, wanted to take a fresh look at their threat management and operational resilience. Particularly because many of their members were embracing new digital services, like mobile and online apps, to manage their money. As these services evolved, they wanted to ensure that data protection remained central to their strategy and maintain an intense focus on security. But they also recognised that coping with the shifting threat landscape would require a revised security approach that wasn't just rigorous, but more agile too.

The solution

We offered them a six-year contract to cover substantial aspects of their entire security – from design and implementation to 24-hour proactive and reactive monitoring. We brought together reliable products and services from leading providers to ensure security was covered effectively at every level. Every improvement we made then had to satisfy both our own quality criteria as well as the relevant financial industry standards, like ISO 20000 service management accreditation and PCI DSS compliance.

The result

We're now permanently based inside the organisation's Enterprise Command Centre. We've implemented an effective security strategy and operational model that's designed to grow and evolve rapidly with the changing nature of threats that face both the retail banking industry and also IT organisations in general. This also allows them to be flexible and responsive in delivering more secure and improved services to customers. Moving forwards, they're confident they have an environment that will keep them one step ahead of would-be attackers and that prepares them for whatever might happen in the future.

Secure your digital transformation journey

No matter where your financial organisation is on its journey to harness the benefits of digital transformation in the cloud, our dedicated experts and market-leading security solutions can help ensure your next steps are secure.

Discover more by getting in touch with your account manager.

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to the respective British Telecommunications plc standard conditions of contract. Nothing in this publication forms any part of any contract.

October 2023