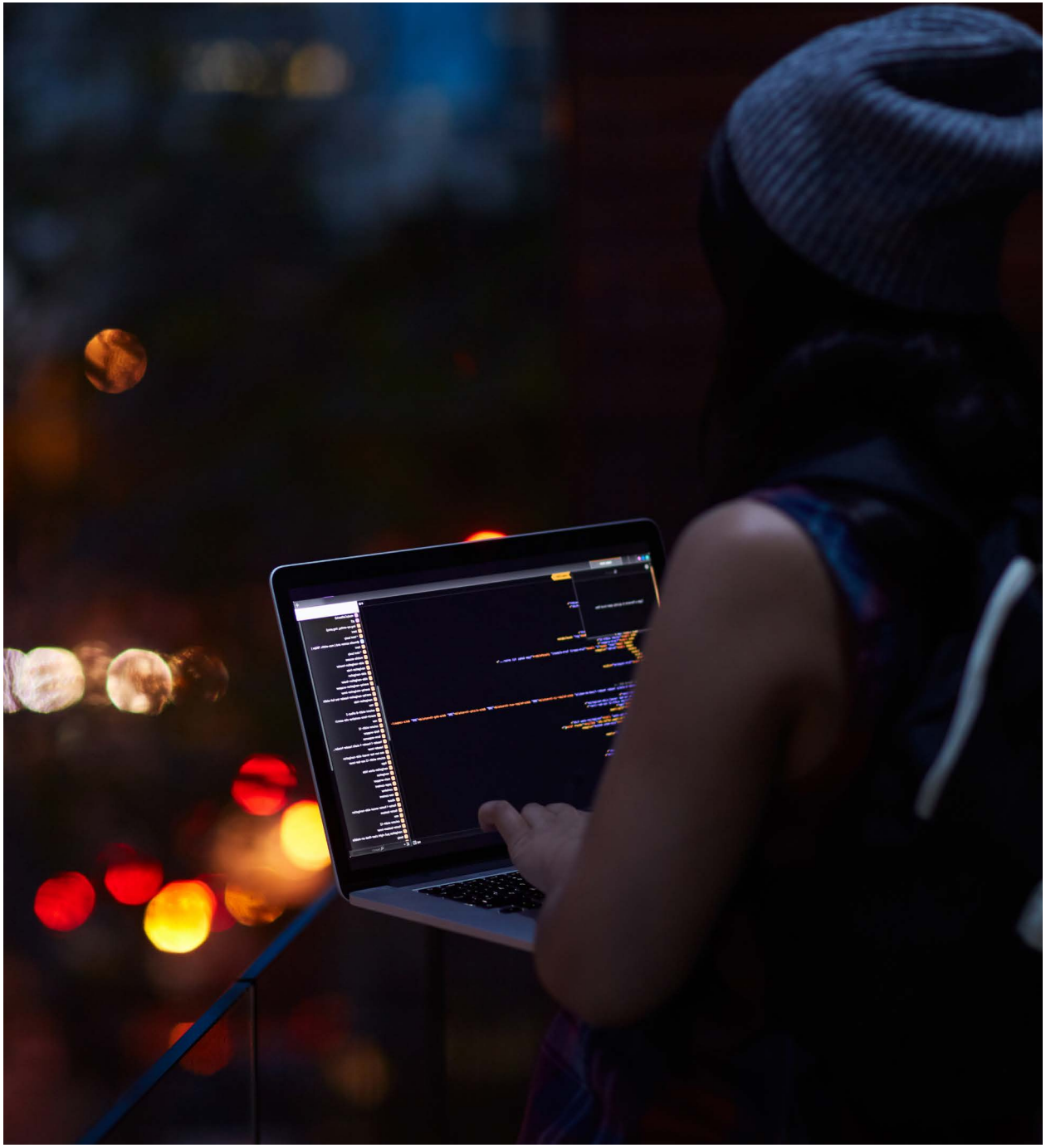
Why you need to turbo-charge your Zero Trust journey

How the banking and financial services sector can use micro-segmentation to defend their cloud environments

Contents



Introduction

When it comes to adopting a Zero Trust approach, many organisations in the financial services sector already have most of the constituent parts required. But moving from existing approaches to a new security model is a challenge. They need to adapt and bring robust security defences into their existing network infrastructure to form a coherent protective whole.

A Zero Trust approach is not new, but it's now an imperative to keep your organisation safe when you're operating in an environment that's constantly shifting in ways that open up new vulnerabilities.

Banking and financial services organisations are in an excellent position to make a swift move to Zero Trust. We estimate organisations already have between 60-80% of the security building blocks that they need to adopt a Zero Trust approach. What needs to come next is a change of stance, and a unification process to protect their business as they evolve.

In this whitepaper, we take you through those vital next steps to achieving a Zero Trust network. As ever, your account manager is ready to put you in touch with the right experts to take things further – just ask.

Start your Zero Trust journey today.

Michala Hart
Director, BT Security

It’s all change in your threat landscape

It’s imperative that the banking and financial services sector recognises and tackles what’s going on in its security threat landscape. It’s a fast-moving, complex environment that’s going through a time of rapid change and there’s no guarantee that what you understood last month will hold true today. The security of your whole operation depends on recognising these factors and planning for their impact on your business:

A huge jump in cyberattacks

The general disarray caused by the pandemic has become a fertile breeding ground for financially motivated attacks, and your sector is a prime target. Adversaries are innovating and leveraging broken, abandoned or antiquated business processes via multi-level / domain attack packages.

Attacks on financial organisations increased by

238%

between February and April 2020.

A reshaping of working practices

The mass move to homeworking followed by a recalibrated balance of office and home work means you have to rethink your security approach. New endpoints aren’t protected by the disappearing security perimeter, so it’s essential to assume you’re now operating in a hostile environment.

The cloud is redefining security priorities

A move to the cloud to boost agility and support hybrid working brings a renewed focus on key security factors. Now it’s imperative to prioritise threats, achieve visibility and control, adopt targeted automation and always operate as though the network has been breached.

A lag in securing new business models

Changing ways of working are accelerating digital transformation and driving the rapid adoption of new business models – and security is struggling to keep up.

79%

of business leaders say new business models introduce technology vulnerabilities faster than they can be secured.

Ongoing human vulnerabilities

Your business is heavily dependent on giving your workforce access to large amounts of data, and the more people in your organisation, the greater the risk of human error or fraudulent activity causing a breach of your defences.

New dynamic security approaches

Applications are increasingly set up as distributed services which is changing the ground rules of security, introducing the idea of security as software. This uses containerisation to provide pre-certified and pre-configured security for applications, making security more transparent, predictable and robust.

Zero Trust is the only viable answer

When you're operating in an environment that's constantly shifting in ways that open up new vulnerabilities, adopting a Zero Trust approach is essential.

Trust no one
In a Zero Trust environment you assume that all application access is potentially malicious or undesirable. Instead of trying to police all the borders and paths across your network, you push controls much closer to the asset, assuming you'll always be operating in a compromised arena. With Zero Trust, you check the identity and integrity of devices regardless of their location, combining the results with strong user authentication.

The perimeter's dead: long live the new perimeter – identity

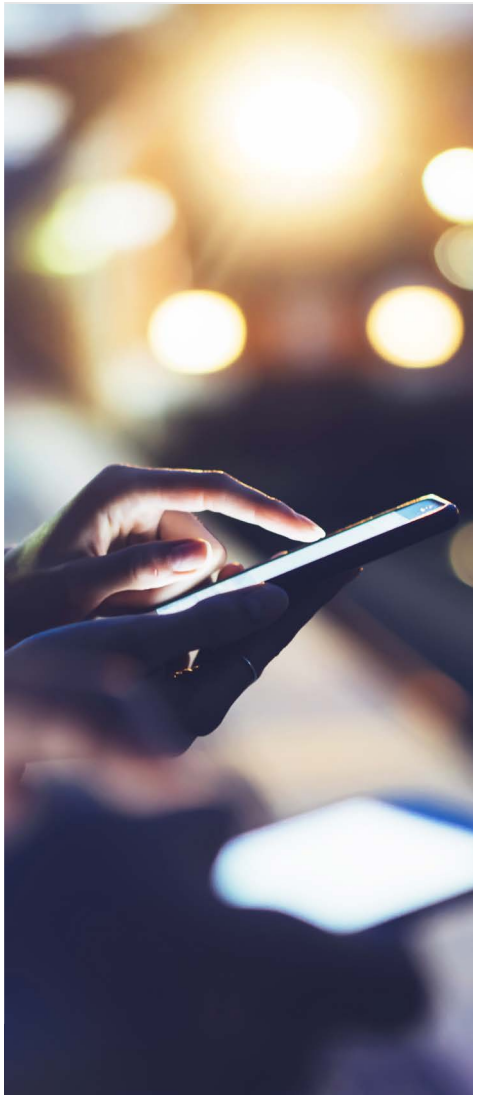
The days of protecting a closed environment with a fixed perimeter have gone, as has the idea of trusting devices connected to a managed corporate network, even if they have been verified before. Today's more open infrastructure incorporates a greater use of the cloud and the internet and makes it impossible to draw a strong line around what you need to defend. Now, your assets are scattered into interconnected segments spanning cloud-based services and infrastructure, remote and mobile environments and the Internet of Things.

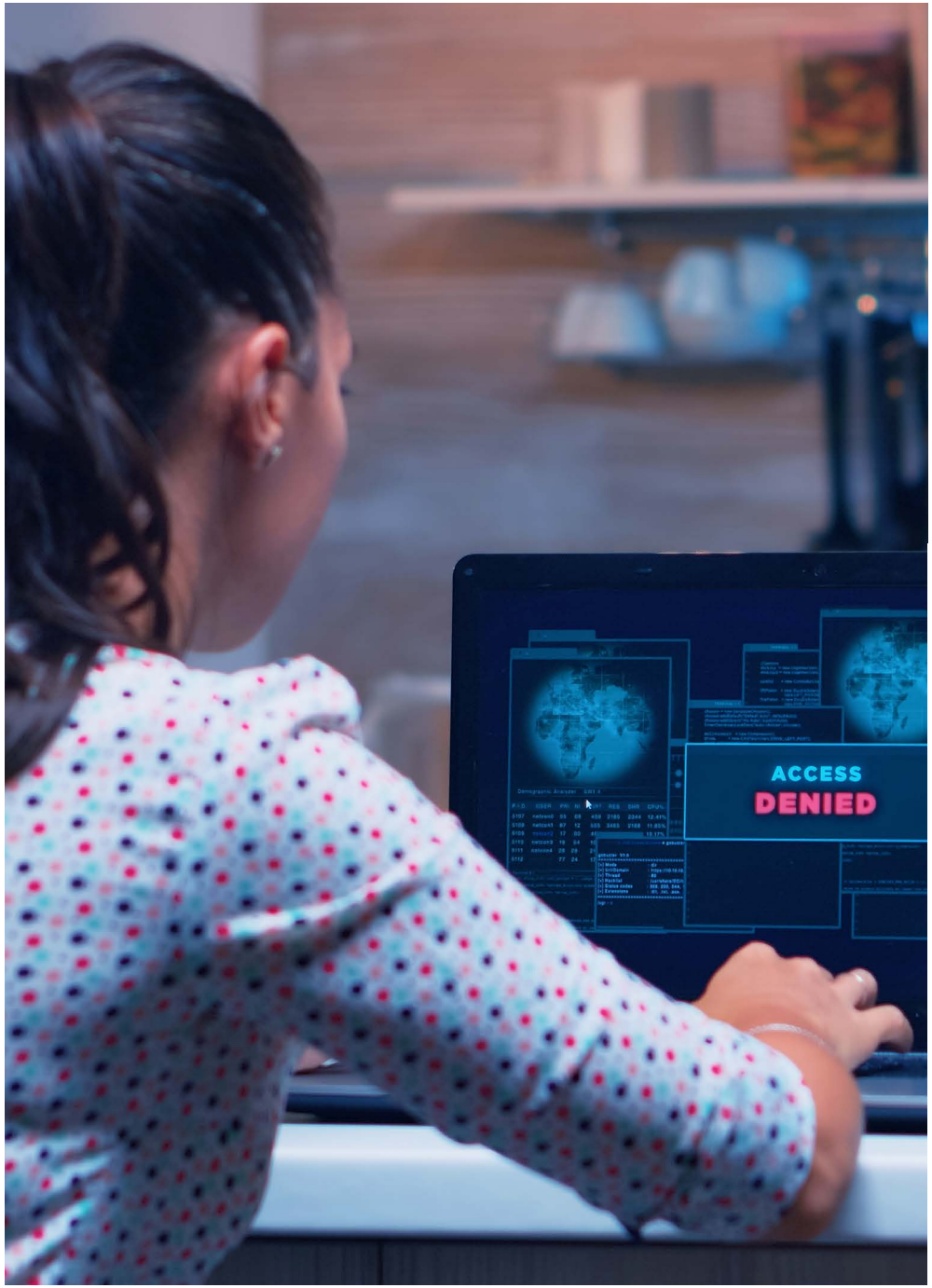
Even if you could create a single perimeter, relying on it for cybersecurity would be too risky when an attacker breaking through it will have easy, open access to your data, systems and applications. This flat network structure is the reason ransomware attacks spread so easily and have the power to stop your organisation's day-to-day operations almost instantly.

Limit an attacker's reach

A Zero Trust approach is widely accepted as the most effective way to protect your network from attack. In fact, the US National Security Agency (NSA) strongly recommends that all critical networks, government or otherwise, adopt a Zero Trust security model, seeing it as the only solution for defending against ransomware.

If you take a Zero Trust stance, you build systems that assume you're operating in a hostile environment. This puts you in the best position to shut an attacker down as soon as they get into your network. Most attacks use known vulnerabilities and known ports to move around, but Zero Trust segmentation eliminates these paths, without affecting existing application traffic. The attacker moves fast, but so does your Zero Trust policy. Denying an adversary the ability to pivot and explore allows you to dramatically reduce your known attack surface, which can effectively neutralise the impact of entire classes of attack.





It’s time to rethink what we mean by ‘Zero Trust’

Your security challenges are evolving. New ways of working, new cloud environments and an ever-increasing number of incidents to manage mean nothing can stand still. There’s no place for assumptions, so what do you need to know about Zero Trust today?

See through the Zero Trust hype

There’s a trend right now to label products and services as ‘Zero Trust’, but the reality is a lot of multinationals have been moving towards a Zero Trust stance using ‘ordinary’ security controls. The danger is that organisations buy Zero Trust products but leave them operating in isolation so they’re not maximising their use of the controls available by integrating the controls together into one solution.

For example, they might introduce a new device but, by not using it to its full potential, it doesn’t work effectively with all their other devices. This doesn’t create a true Zero Trust approach.

Many organisations are not optimising the value of their current control spend, which is creating ‘latent capabilities’ that can be leveraged in a cohesive Zero Trust journey. Currently, we’re finding that organisations have overspent on some controls and have a high level of maturity in those areas but have underspent in other crucial control areas. They’ve started the journey but have a way to go to optimise the value of their security.

The good news is that, in our estimation, most organisations already have between 60-80% of the security they need to adopt a Zero Trust approach, they just haven’t brought those capabilities together into a single Zero Trust strategy.

Constructing a Zero Trust approach for today's requirements

Just as you can't move to the cloud by lifting and shifting your data centre services, you can't just extend your existing Zero Trust approach to the cloud. To stay protected, you need to rebuild your Zero Trust strategy for the cloud.

Increased visibility and control will be the foundations of your security as you move to a more dispersed infrastructure, and micro-segmentation will be critical to achieving that.

What is micro-segmentation?

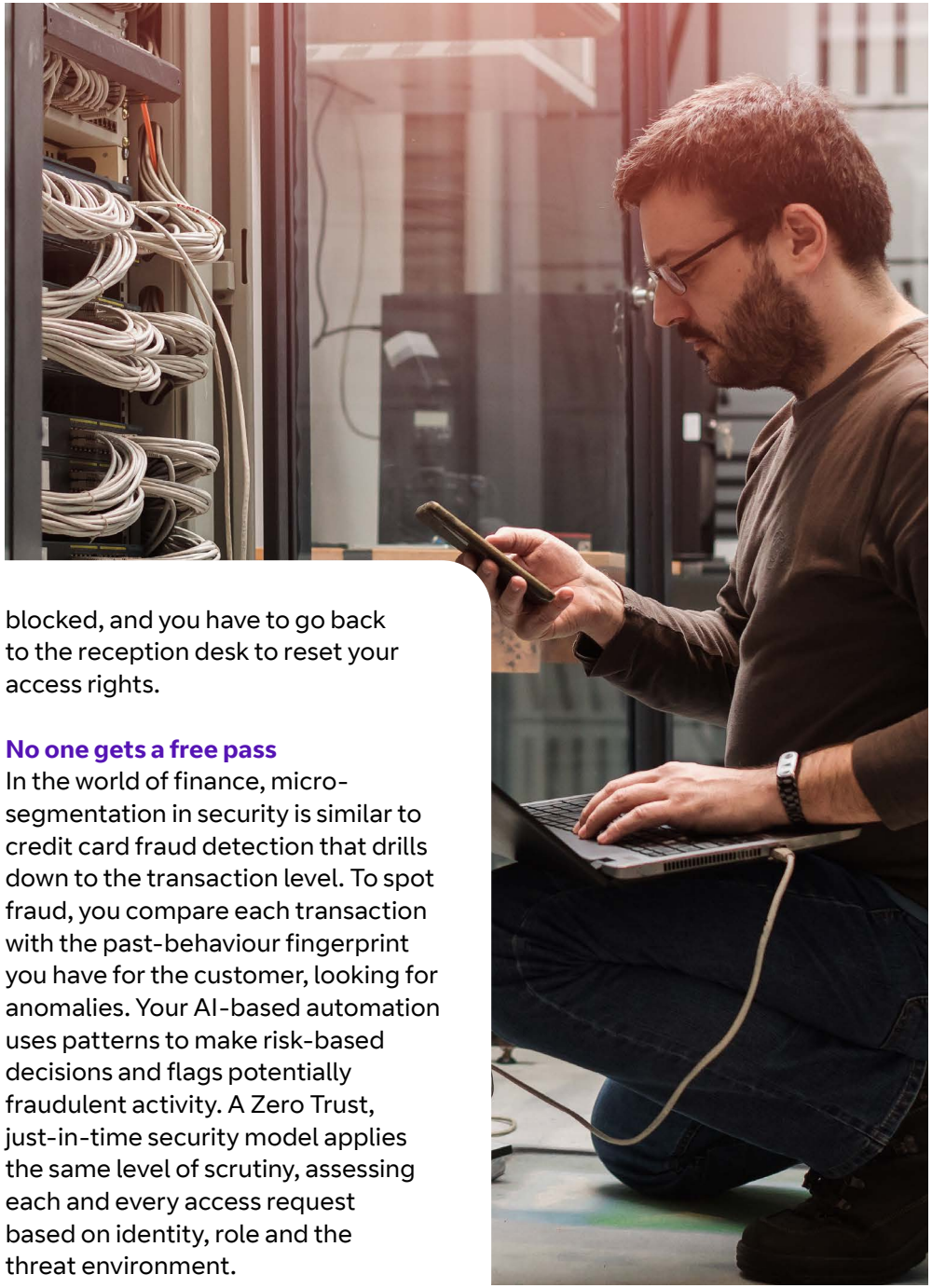
Micro-segmentation greatly reduces the 'zone of trust'. It's an evolution of network segmentation that goes beyond providing granular control of traffic at the application layer. It grants users access to only the applications and data they need based on their identity, role and known vulnerabilities and threats. Security becomes about the individual user, limiting dangerous lateral movement within a network, and introducing policy enforcement points closer to the workload.

How to visualise micro-segmentation in action

Imagine your environment is a hotel with a key card system in a country that's not your own. If you want to stay in the hotel and get further than the lobby, you need two things: your passport that authenticates who you are, and your key card that authorises where you want to go.

But, once registered as a guest at the hotel, the trust is limited, and you're not allowed to go wherever you want. Imagine different parts of your estate are on different floors of the hotel and the lift will only take you to the one you have authorisation for when you insert your key card. Now imagine that your cloud applications are different hotel rooms, and you have to pass more security scrutiny to get access to your suite and the hall for the function you're attending. You have to swipe your key card again and show ID to the staff on the door and, to accurately represent micro-segmentation, there'd be more checks – on the purpose of your visit and further security policies would be applied, such as a search of your bag. The bottom line is that each room is independently protected, and every visitor is judged against a series of criteria before being allowed entry, keeping the zone of trust tight.

And, if you try to use your key card to access a room you don't have authorisation to enter, your key card is blocked, and you have to go back to the reception desk to reset your access rights.



No one gets a free pass

In the world of finance, micro-segmentation in security is similar to credit card fraud detection that drills down to the transaction level. To spot fraud, you compare each transaction with the past-behaviour fingerprint you have for the customer, looking for anomalies. Your AI-based automation uses patterns to make risk-based decisions and flags potentially fraudulent activity. A Zero Trust, just-in-time security model applies the same level of scrutiny, assessing each and every access request based on identity, role and the threat environment.

Eight guiding principles for Zero Trust in banking and financial services today

1

Identify your goal and pull it through your planning

Form your security strategy around the fundamental assumption that you will always be operating a dynamic network in a hostile environment. Centre your thinking around how you can best use automated processes to create security rules that change dynamically in response to context. But remember that automating a broken process is a swift route to failure; make sure you're training your AI to make correct decisions about risk so it can automate the appropriate response.

2

Assess existing capability before investing in more

Don't rush to spend money on 'Zero Trust' point products because you may be duplicating capability or investing in areas that aren't a priority for your organisation. Instead, optimise the value you already have in your security estate by establishing what latent capabilities you possess. For example, layer 1, 2 and 3 segmentations along with very narrow access lists could be a fruitful first step on your Zero Trust journey.

3

Focus on removing peer-to-peer protocols

Segmentation is your key defence in a Zero Trust environment, but you won't be able to segment your network if you're running peer-to-peer protocols. A vital part of any attacker's kill chain is the ability to pivot from one host to another, but if you limit their ability to move easily, then you neutralise entire classes of attack. Think about how 5G architectures cut out peer-to-peer connections, forcing every call to go through a central gateway – this model should be your aim.

4

Control access to core assets

Leverage your security investments to secure your cloud and data centre servers, using Zero Trust segmentation to coordinate traffic authorisations across your estate. This needs to be universal so it's as watertight as possible and servers only accept traffic sent by authorised users. Consider investing in red teaming ethical hacking exercises to check the security of your key assets.

Eight guiding principles for Zero Trust in banking and financial services today

5

Incorporate user identification

Limit your exposure to risks by only opening ports in your environment when they're needed. Make user identity the first key to access your systems and make sure permissions are revoked as soon as the user logs out.

6

Build in security by design to your projects

Investigate how containerisation can be a springboard for your security DevOps, providing a pre-certified and pre-configured software 'container' that you can build on to create automation and machine-to-machine application service models. Containerisation is an ideal opportunity to leave waterfall cycles of patching behind, offering instead security that flexes with context.

7

Segment, segment, segment

Introduce micro-segmentation to segregate – and protect – your network at a granular workload level. This will give you the real-time visibility you need, as you monitor application behaviour and connections to understand what is talking to what and to identify risks. It will also give you the level of control you need to improve your breach containment, preventing lateral movement and reducing the blast radius of any attack.

8

Activate your human firewall

Remember the user in all this and make it easy to do the right thing and hard to do the wrong thing. Educating and motivating your workforce to follow protocols and stay vigilant against potential attacks is just as important as any other aspect of your Zero Trust security journey.

Why BT?

We speak your language

At BT, we understand the unique challenges of the banking and financial services industry because we've been an integral part of your ecosystem for 50 years.

In the financial markets we're trusted by over 1,500 firms consuming more than 10,000 services across over 60 countries. And in the banking and insurance markets we facilitate over 20 million card payments and the settlement of £250 billion of transactions every day.

We use this experience of working with global multinational organisations in the banking and financial services market to filter our expertise in other areas so that our recommendations are always set in the context of your business.

We bring together expertise

We have a long heritage of innovation in network and cloud solutions, providing the hands-on expertise to help the financial services sector through digital transformation, and beyond. In our own right, we offer choice, expertise and experience in deploying cloud-focused infrastructure solutions.

And, through leading industry partnerships, we blend the latest specialist technologies into what we offer. For example, in the Zero Trust environment we partner with Illumio, a pioneer in security segmentation, named as a leader in the Forrester Zero Trust Wave.

Our solutions are an exact match for your requirements

Illumio technology powers our micro-segmentation solution that provides visibility and control of server resources for physical and virtual devices and applications hosted on those devices. It allows users to build a real-time network map and then segment the network, reducing the attack surface.

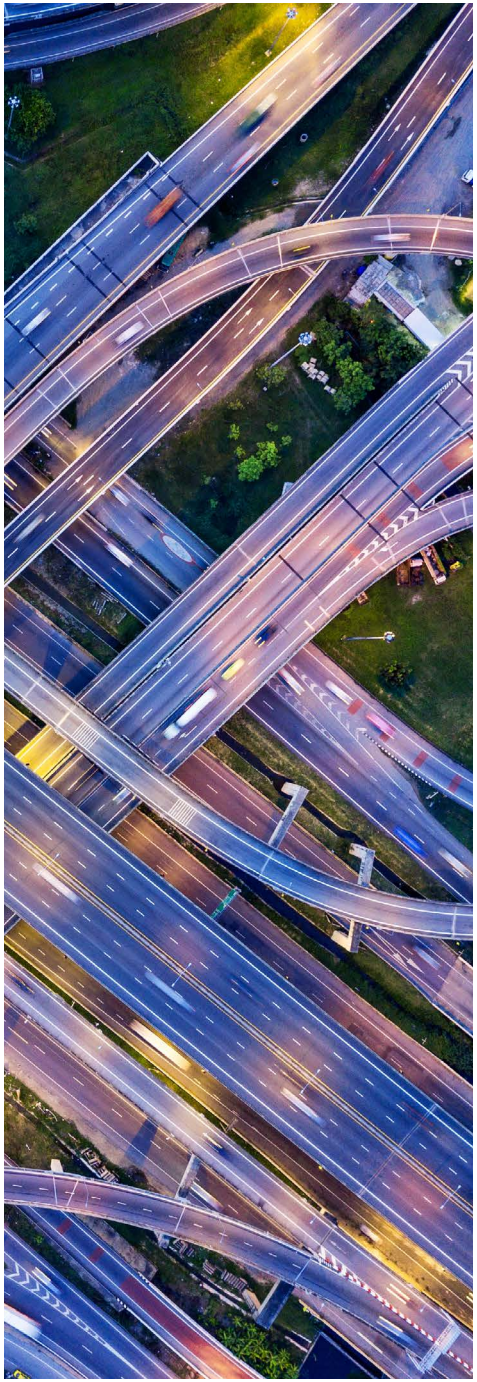
Our new Eagle-i platform provides early visibility and context of potential cyberattacks against your organisation, helping you to prepare in advance and react faster in the face of an attack. The platform uses our insight into what is travelling across the global network to understand the threats before they hit you. Our platform comes with the people who have the skills to continually test your entire solution, removing the headache of recruiting enough security professionals to keep your estate protected.

We're committed to optimising your existing investment

Our approach to Zero Trust is about extracting and extending value from your existing investments rather than jumping straight to recommending new investments. We focus on identifying latent capabilities that you can leverage immediately. Our advisory services will then help you assess how far this takes you on your Zero Trust journey before supporting you to identify a winning business case to address your specific security, safety and privacy challenges.

We specialise in security

Our experience and expertise in protecting governments and countries from over 6,500 cyberattacks each 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 experts and 350 consultants based in our 16 security operations centres around the globe.



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 British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc 2020. Registered office: One Braham, Braham Street, London, England E1 8EE. Registered in England No. 1800000.

November 2021