Transforming Financial Services

Modernize to Secure, Simplify & Comply with Confidence

EBOOK

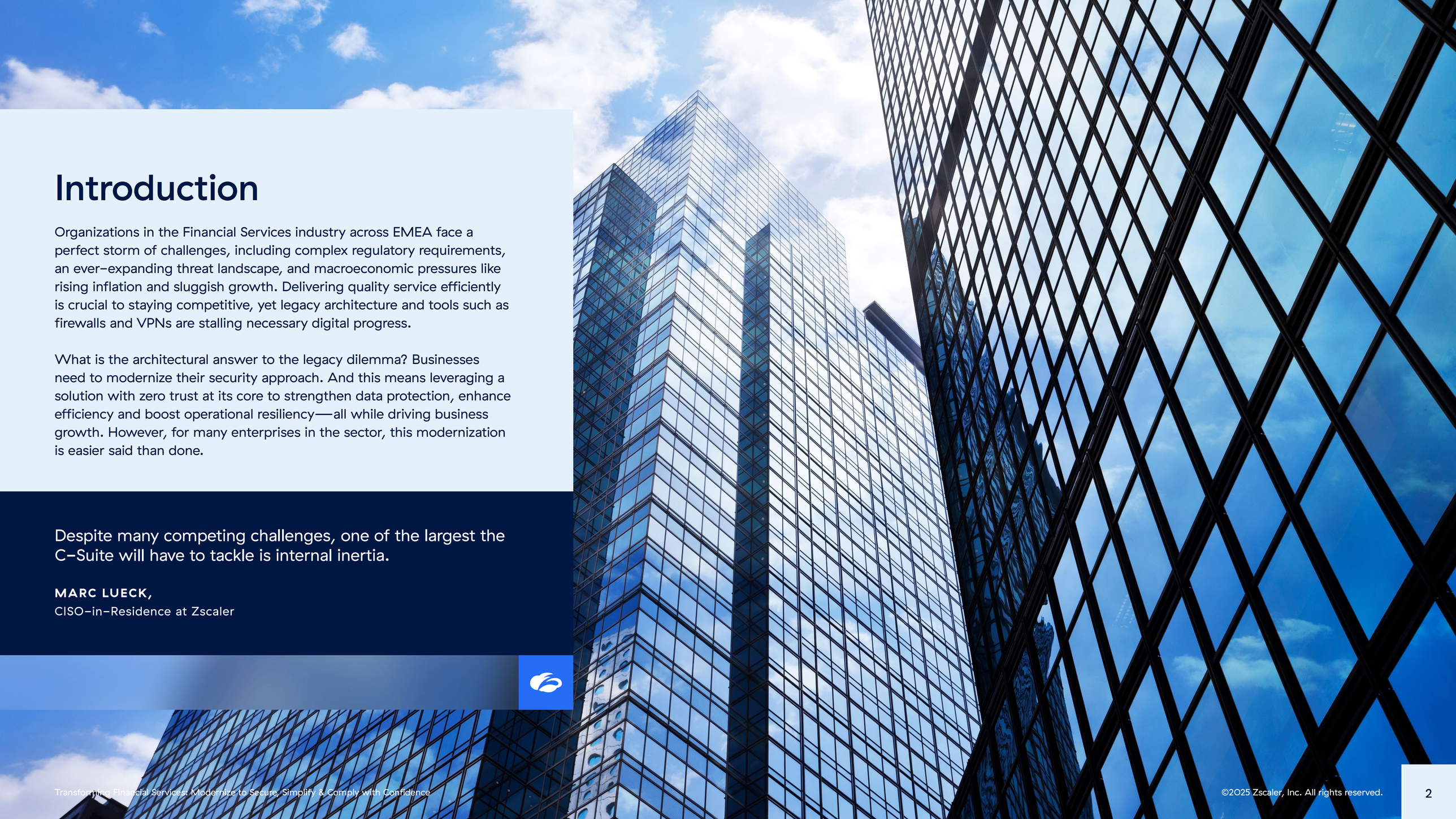
Introduction

Organizations in the Financial Services industry across EMEA face a perfect storm of challenges, including complex regulatory requirements, an ever-expanding threat landscape, and macroeconomic pressures like rising inflation and sluggish growth. Delivering quality service efficiently is crucial to staying competitive, yet legacy architecture and tools such as firewalls and VPNs are stalling necessary digital progress.

What is the architectural answer to the legacy dilemma? Businesses need to modernize their security approach. And this means leveraging a solution with zero trust at its core to strengthen data protection, enhance efficiency and boost operational resiliency—all while driving business growth. However, for many enterprises in the sector, this modernization is easier said than done.

Despite many competing challenges, one of the largest the C-Suite will have to tackle is internal inertia.

MARC LUECK,
CISO-in-Residence at Zscaler



Rethink the status quo

Zero trust is a change, and in this economic climate, change is deemed risky. What's more, the Financial Services sector has already invested millions bolstering their security over the years, doing far more to secure data than businesses in other industries have. But this progress means they've built a significant amount of technical debt—let's call it 'momentum'—on this traditional-security path. Changing direction now is considered 'difficult' and costly, so the security status quo wins.

The problem is that this legacy approach doesn't equip organizations to meet the evolving demands for better data protection, compliance, competitive edge, and user experiences. Understanding this failure should be the incentive business decision-makers need to break free from their internal inertia; of not wanting to do something different. They need to gain momentum in another direction: on a new, modern path toward zero trust.

Why zero trust?

To help you **address the issue of internal inertia**, this eBook will unpack four key industry challenges to highlight why changing to a zero trust approach now is so critical. You will:

- **Discover how modern zero trust platforms meet the needs of the Financial Services sector**, de-risking change while addressing concerns from your network architects and security architects alike.
- **Gain insight into the features such a platform offers to keep you covered on multiple fronts**—from navigating external pressures to safeguarding data, ensuring regulatory compliance and building a resilient tech stack to power every action.

CHALLENGE 01

Navigating External Pressures

What enterprises are experiencing right now

The volatility and uncertainty of the economic market has created a precarious tightrope for the Financial Services sector to walk. Increasingly, organizations are having to balance the tension between two activities at odds with each other: cost-reduction and operational resiliency.

While the rise in enterprise IT spend in 2025 seemed positive, Gartner noted that "price hikes [would be] absorbing some or all of budget growth".[1] The implication is that there's less to spend on 'nice-to-haves' such as keeping pace with tech changes or driving innovation. At the same time, competition from fintech companies and other digital-first challengers will continue to intensify.

DECREASED TECH SPEND WILL SHIFT THE TRANSFORMATION FOCUS...	
FROM	**TO**
investing in growth	reducing the overall cost of conducting business
moving all key infrastructure to the cloud	moving only those dynamic workloads that will enable agility
exploring new systems and solutions	operationalizing foundational deployments

Recognition of the competitive risk is clear in the recent rise in Merger and Acquisition (M&A) activity in EMEA. Per PWC, Financial Services organizations are increasingly pursuing M&As to bring the new-age challengers in-house.[2] This reduces external competition while simultaneously accelerating their own growth or enabling them to fulfil market promises with fresh expertise.

On the other end of the spectrum, there's been an equally strong focus on divestitures, as certain companies double down on their core business to ride out the tough economic conditions.

The one area enterprises can't afford to cut back spending is business continuity, which is under constant attack from multiple external threats. A focus on threat prevention or risk mitigation alone doesn't protect a business during a failure scenario or cyber disruption. Quick recovery is prized. As such operational resilience is increasingly viewed as a valuable return on investment.

How is your network architect coping?

They are feeling the strain of having less budget to maintain the same or an even greater level of performance and reliability to support business continuity. Pressure points include:

1. **Trying to keep up with new network technologies**, protocols and best practices.
2. **Growing demands of users**, applications, and data—especially in the AI era and with workforces more distributed than ever.
3. **Increasing network complexity** to unpick in the wake of M&A deals.

[1] Gartner Forecasts Worldwide IT Spending to Grow 9.8% in 2025, January 2025. Available at: https://www.gartner.com/en/newsroom/press-releases/2025-01-21-gartner-forecasts-worldwide-it-spending-to-grow-9-point-8-percent-in-2025

[2] Global M&A Trends in Financial Services, January 2025. Available at: https://www.pwc.at/en/deals/trends/financial-services.html

Is your security architect keeping up?

Constrained by spending cuts, they feel increasingly stretched trying to protect the company's data. Pressure points include:

1. **Securing operations despite resource gaps** (from both team–skills and tech–tools perspectives)—because there's no budget to bridge them.
2. **Enabling business growth** by securely accelerating a merger/acquisition, while reducing risk through proper due diligence.
3. **Ensuring security doesn't hinder** continued transformation and business agility.
4. **Evolving resilience strategies** to bring in proactive mitigation capabilities.

Architecture solution: zero trust

A modern zero trust platform solution can help your enterprise de–risk ongoing transformation on multiple fronts: by boosting operational efficiency, agility, and scalability. It will also be able to achieve this in a way that is cost–effective to help your business navigate external pressures. Refer to the checklist to ensure you select a zero trust platform that can meet your business needs.

PLATFORM CHECKLIST

The right zero trust solution should:

- Reduce your operational overheads by consolidating multiple security point products into a single platform.
- Boost your productivity and therefore your competitiveness by delivering secure and agile IT optimization.
- Unlock rich business intelligence into your SaaS apps and workspaces to help drive efficiency, productivity and savings.
- Support secure innovation to generate positive cash flow and incremental revenue.
- Accelerate integration following M&A activity to drive value creation and value capture.
- Unlock deal value by assisting in the secure separation of divestitures and carve–outs, enabling an enterprise to focus on core business priorities

CAPITEC

CASE STUDY

Banking app cloud switchover took around 3 seconds, with no downtime to improve security posture

CAPITEC TO LEAN INTO THIS POTENTIAL FOR ACCELERATING FUTURE M&AS

Capitec, the largest retail bank in South Africa, is ranked #1 for client satisfaction. A large part of this is down to the enterprise's cloud–first digital transformation journey. Andrew Baker, Capitec's CTO, advocated for the company's implementation of the Zscaler Zero Trust Exchange platform, having experienced successes with it at previous companies.

The platform was critical for ensuring there was zero downtime during Capitec's migration of its banking app and call center to Amazon Web Services. Zscaler vastly simplified the infrastructure and now supports 17,000 users at the bank.

A key area Andrew expects Zscaler will help accelerate is Capitec's future M&As. One of the bank's recent acquisitions, completed before Zscaler was deployed, was a domain migration project that required significant time and effort from the security team. **"Zscaler will make M&As a lot easier than doing a domain migration. When joining two entities together, you can't beat Zscaler on speed and velocity."** Andrew Baker, CTO – Capitec

Read the full case study here →

CHALLENGE 02

Safeguarding Data

What enterprises are experiencing right now

Let's talk about who and what can connect to the network—and the issues this is causing.

NETWORK ACCESS

Legacy security solutions like VPN aren't sophisticated enough to correctly tailor permissions. One possible result of this is that if permissions aren't properly maintained by IT, relevant users might find themselves locked out of the data they need. If the access policy is set to keep everyone in their departmental lane, for example, an employee won't be able to cross-sell additional financial products from another area of the business.

Of course, the far greater issue with legacy solutions is that they are more likely to grant broad access and then not monitor after access is granted. This approach leaves data exposed to successful bad actors who are free to move laterally within an organization's system once they've accessed the network.

DATA MANAGEMENT

Most Financial Services enterprises run decentralized operations that make it exceedingly difficult to keep siloed teams on the same page when it comes to consistent data management and security. To make matters worse, data is now increasingly distributed across fragmented locations (from on-prem, to cloud, SaaS and third-party apps), so it's also a challenge to identify and gather it.

DATA SECURITY

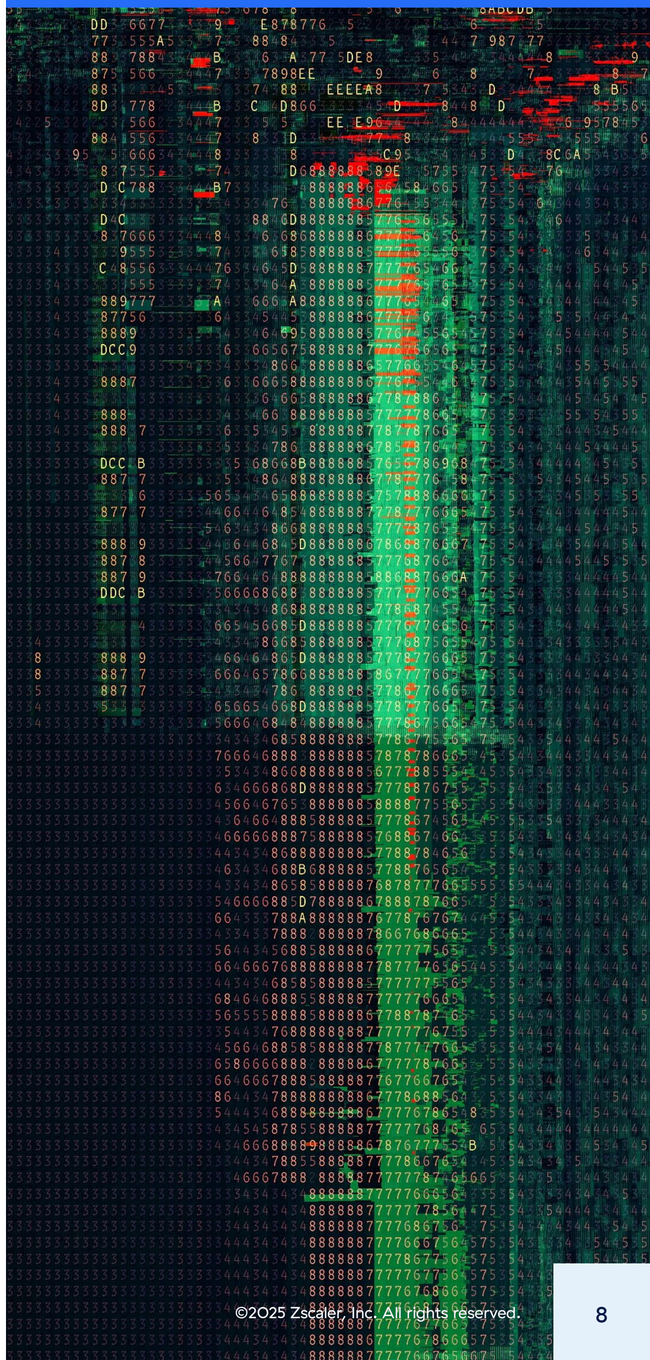
The AI era has introduced a host of new threats that leave data vulnerable. For one, hackers are tapping into the power of AI, and attacks are becoming more and more sophisticated (think about the dangers of the latest banking trojans that can now automate fraudulent activity). Internal usage of AI also presents a data-safeguarding challenge, especially in architectures where visibility of activity is low. Here, employees may unwittingly (or even maliciously) add sensitive data into public-facing tools.

How is your network architect coping?

They are feeling the weight of the increasingly important role the network plays in security. Pressure points include:

1. **Trying to balance fast and instant connectivity with security** by incorporating best practice into their design (from secure network segmentation to firewall placement)—but with more security added on, the architectural complexity is increasingly hard to manage.

2. **Ensuring the expanding number of users and devices can all connect**—even unmanaged IoT devices—but fearing that unauthorized access could turn the network into a direct channel to sensitive data.



Is your security architect keeping up?

They often feel like they're fighting a losing battle against the sheer scope and sophistication of today's attacks. Pressure points include:

1. **Struggling to implement proactive measures** when needing to react to the always-on, threat of cyberattacks from skilled adversaries, including nation-states or organized criminal groups.

2. **Trying to keep data safe** from new attack techniques and emerging technologies like AI.

Architecture solution: zero trust

For Financial Services operators, AI-powered data discovery and classification is a powerful way to secure all data in all locations. These are two capabilities that the right zero trust platform should deliver. By leveraging AI, a future-forward zero trust platform can empower security and networking teams to quickly identify misconfigurations and vulnerabilities, prevent data from being submitted to GenAI apps, and inspect all traffic inline.

PLATFORM CHECKLIST

The right zero trust solution should:

- Safeguard sensitive data and workloads against evolving threats—and protect the brand from the ensuing reputational damage of a breach or data-loss incident. This is something that built-in AI can bring.
- Dynamically mitigate against evolving threats with tools that deliver swift containment, effective response, and minimal to no disruption in the wake of any cyber incidents.
- Protect identities and enable segmented access through robust, consistent access controls.
- Enable instant, real-time visibility of data across endpoints, inline, and in the cloud—even better, if this can all be actioned on a single, central platform for all channels.
- Control GenAI risk with deep visibility into both sanctioned and shadow AI apps, and enforce real-DLP blocking or app isolation.
- Facilitate secure use of AI for internal tooling and automation initiatives to streamline efficiency.

Hastings DIRECT

CASE STUDY

Microsegmentation for sensitive data

LEGACY VPN NOT DELIVERING ON THIS NEED FOR HASTINGS DIRECT

After its migration to the cloud, Hastings Direct, a general insurance provider in the UK, wanted to modernize its security architecture. A key priority for the company was protecting essential private applications (and the customer data within them).

But Simon Legg, CISO at Hastings Direct, couldn't easily segment role-based application access because of the limitations of a legacy VPN solution. Its blanket access policies put the whole network at risk of data leakage or loss.

On the Zscaler Zero Trust Exchange, Hastings Direct could could move away from these VPNs. Simon highlighted several benefits, including the ability to microsegment application access, so users are directly connected only to the resources they need and are authorized to access. **"Zscaler allows us to operate with freedom and flexibility [because] everyone is protected by the same zero trust processes when connecting to the internet,"** Simon Legg, CIS – Hastings Direct

Read the full case study here →

CHALLENGE 03

Navigating Regulatory Compliance Complexity

What enterprises are experiencing right now

Financial Services is an always-on industry, making operational (and therefore cyber) resilience all the more important—network downtime means failed trade, failed payments, reputational damage and customer loss.

The introduction of the Digital Operational Resilience Act (DORA) brought this topic into sharp focus. But it isn't the only regulation that's caught the attention of the boardroom. Other regional and market-specific examples include:

- **The General Data Protection Regulation (GDPR)**
- **The Network and Information Security Directive 2 (NIS2)**
- **The Sustainable Finance Disclosure Regulation (SFDR)**
- **Capital Requirements Regulation 3 (CRR3)**
- **The Saudi Central Bank (SAMA) Regulations**
- **South Africa's Financial Intelligence Centre Act (FICA)**

Given this volume, compliance is becoming an increasingly complex and lengthy task—think about the weeks to months a single audit can take to complete. At a time where resources are stretched in the economic climate, it's also an expensive endeavor, forcing organizations to invest in the people and technology to drive their compliance and risk-management efforts, and ensure these are implemented in day-to-day operations.

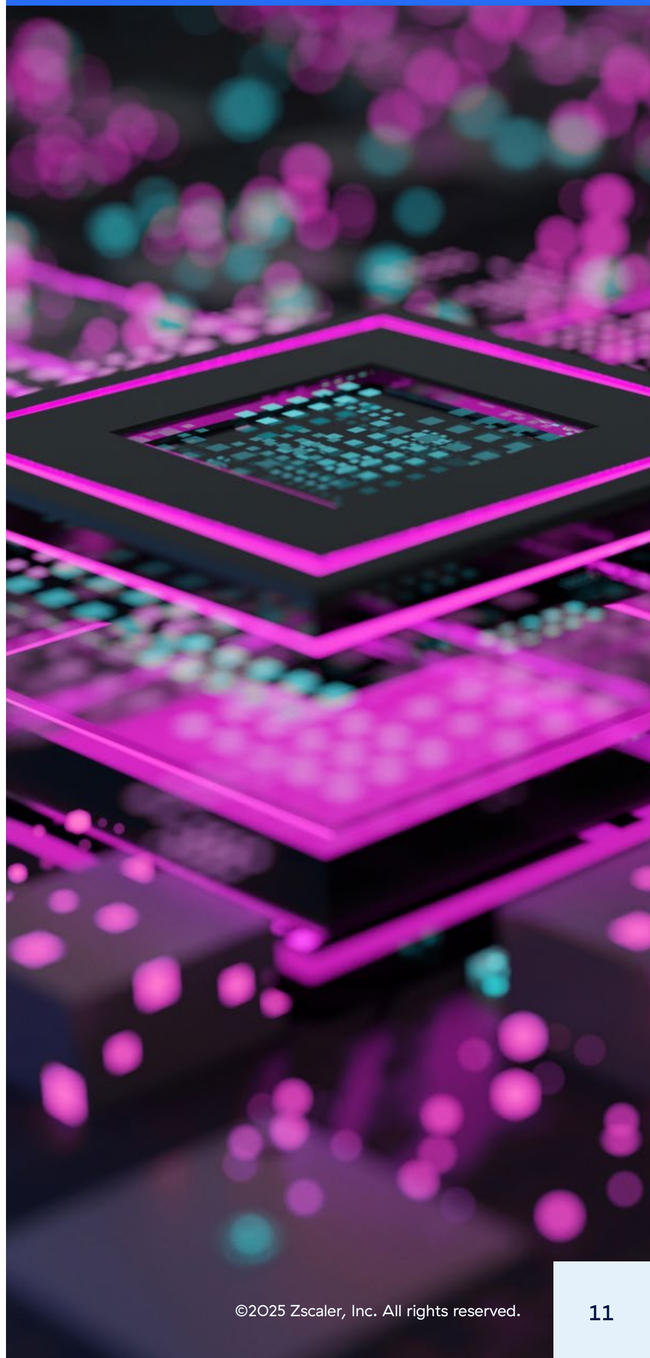
Failure to comply has significant consequences—not all financial. While non-compliance can result in hefty fines for the business or for individuals within it, mandated breach reporting can also cause reputational damage that erodes customer trust. Despite understanding these repercussions, many Financial Services organizations still struggle to meet compliance requirements from an operational standpoint.

How is your team faring?

Usually, both network and security architects are responsible for implementing different aspects of the regulatory compliance strategies set by the CISO. Complexity is a major pressure point across the combined team, as is the time required to roll out compliance operationally. For example, consider the hours needed to surface relevant data, especially if this is being done on legacy architecture.

Architecture solution: zero trust

To mitigate data-compliance risks, Financial Services operators can use a zero trust platform to run regular risk assessments to quickly identify and rectify compliance gaps. They can also support compliance by deploying zero trust access controls and making use of the platform's ability to enforce consistent security policies everywhere.



PLATFORM CHECKLIST

The right zero trust solution should:

- Automate your compliance workflows and risk assessments in a single, integrated console.
- Leverage continuous monitoring capabilities to identify emerging gaps in compliance posture.
- Support standardized application of zero trust policies across fragmented IT environments to protect sensitive data proactively.
- Feature detailed dashboards to support faster and more efficient audits, addressing the heavy time and resource requirements of audit processes.
- Offer access to a full audit trail with remediations to help you remain compliant to DORA, NIS2, GDPR and others.

//ABANCA

CASE STUDY

Tackling poor visibility

ABANCA BANK SEEKS BETTER DATA CONTROL

If you don't have visibility into your data, how can you govern it to meet compliance requirements?

This lack of visibility was a big pain point for Spanish bank ABANCA—but one that they were able to successfully address, thanks to Zscaler. After migrating to the Zscaler Zero Trust Exchange platform, the bank gained the necessary 360-degree visibility into their digital environment, and the ability to pull granular stats from the platform on a per-user per-transaction basis.

Visibility gives insight into compliance gaps, but it must be supported by effective security controls to bridge what you've identified. Zscaler's platform supports this by creating a single enforcement point with a single set of policies.

Read the full case study here →

CHALLENGE 04

Banishing Legacy Liabilities

What enterprises are experiencing right now

Both traditional and neo banks must navigate compliance complexity and data safeguarding in a tough macroeconomic environment. However, these challenges are made more complex for those organizations trying to address them on legacy infrastructure. Often, this is what makes the task of business continuity harder for established enterprises than their start-up counterparts, widening the gap of competitive advantage.

LATERAL THREAT MOVEMENT

Networks secured with legacy tools such as VPNs and traditional firewalls aren't effectively protected against evolving threats. As pointed out earlier when considering data safeguarding, one of the biggest issues is that these solutions don't prevent lateral threat movement. VPNs, for instance, run network-centric instead of application- or resource-specific access policies. In the event of a breach using verified credentials, a bad actor is then free to access every corner of the network (and any data within it) fairly easily.

NETWORK VISIBILITY

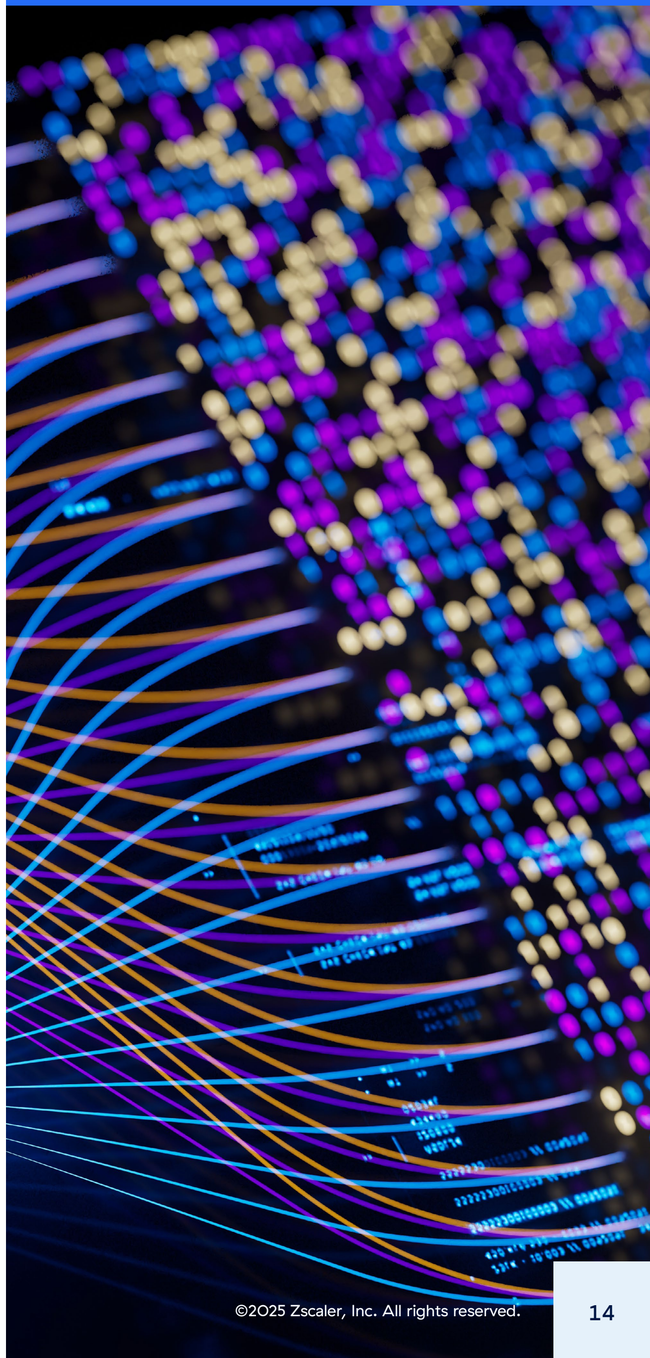
Legacy infrastructure doesn't provide visibility across the network either, which, as we discovered when considering compliance, is a significant obstacle. It's often a complex environment with multiple security solutions bolted on over the years (adding to ongoing management costs). As a result, security teams will find risk monitoring and threat management difficult. The lack of visibility is an issue for maintenance too, meaning proactive management isn't supported. Additionally, the complexity of the network, with resource-heavy legacy tools featuring multiple disparate user interfaces, means networking teams are contending with slow performance and poor user experiences.

SYSTEM UPGRADES

Another point to consider is vendor-mandated upgrades to new systems—something that many businesses will have to contend with as service providers move to the latest software updates. In the Financial Services sector, a common example of this scenario involves SAP. There is broad adoption of the SAP Enterprise Central Component (ECC) for core business processes such as finance, risk management, and regulatory compliance, but SAP will soon end support for this system, requiring users to migrate to newer more secure platforms such as SAP S/4HANA. The mandated migration of this legacy app, which contains highly regulated business data, is a challenge for some, creating further access issues and data security risk.

M&A

Finally, we turn to a unique characteristic of how the Financial Services sector works: deal cycles for processes like M&A are long. Compounding this slow pace is the fact that implementation times can be even longer because of the complexity of changing anything on legacy systems. Additionally, when businesses operate on legacy architecture, there's traditionally a siloed way of working with ownership over security and networking tasks split between internal teams. This adds to the visibility issue, with departments not in the loop on actions carried out by other teams. Implementing change in this context can be extremely difficult.



How is your network architect coping?

The complexity of managing and integrating different network technologies, protocols, and systems—especially in multi-vendor environments—can be overwhelming, leading to bottlenecks that impact performance. Pressure points include:

1. **Ensuring new technologies can be effectively and securely integrated** into this sprawling environment.
2. **Struggling to get ahead of network performance issues** due to limited visibility.

Is your security architect keeping up?

Similar to their networking counterparts, these professionals are fighting an uphill battle against legacy infrastructure. Pressure points include:

1. **Trying to standardize security protocols** across the business but with multiple disjointed security tools.
2. **Navigating system complexity** to identify and remediate vulnerabilities in a timely manner before they can be exploited by attackers—visibility is a critical missing piece of the puzzle.

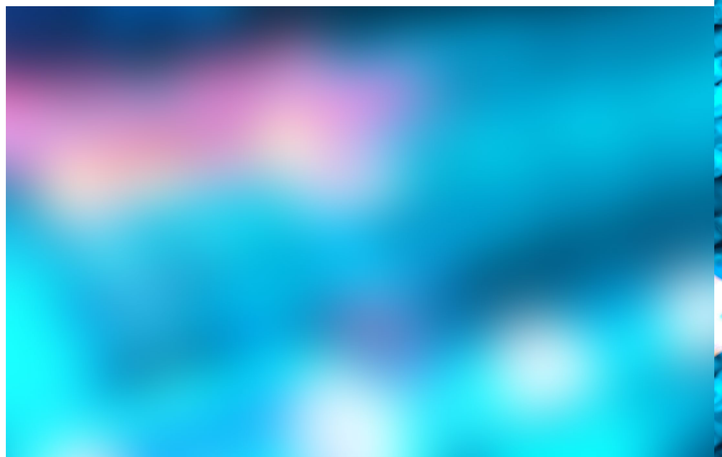
Architecture Solution: Zero Trust

To close gaps in legacy architecture, a modern zero trust platform enables network and security teams to consolidate disparate security products in one place: this reduces the risk of breach and enables secure, scalable access for users, apps and workloads. This move will also decrease the attack surface, stopping lateral threat movement and strengthening resilience posture. Banishing legacy architecture through a platform approach should contribute to your ability to navigate external pressures, safeguard data, and support compliance as well.

PLATFORM CHECKLIST

The right zero trust solution should:

- Replace multiple outdated tools with a single, scalable, cloud-native zero trust solution. This helps you simplify IT infrastructure, while still delivering seamless connectivity.
- Dynamically reduce the attack surface while enabling secure connections for users, apps, and devices across hybrid environments.
- Support secure, scalable access when you're navigating migration sprawl—compatibility with 'RISE with SAP', for example, enables this so you can simplify and de-risk your transition from on-prem to cloud environments.



Simplify, Secure and Transform: For Today and Tomorrow

Transformation is a big word and often thrown around by digital service providers without credibility, leaving Financial Services businesses no better off.

There's a reason why Zscaler's customer list comprises 13 of the top 15 banks in the Forbes Global 2000 ranking, and why we've appeared as a Leader in Gartner's SSE Magic Quadrant for four consecutive years—it's because we do things differently.

As a market leader in zero trust and AI-powered security, Zscaler has pioneered a new approach that secures access for all users, apps, and locations in a way that is simple, streamlined and effective. Our continuous investment in innovation means our solution always keeps pace with market needs. We are committed to making the zero trust journey smooth and worthwhile for Financial Services operators across EMEA—this is because we're deeply connected with the specific needs of multiple stakeholders (from your cybersecurity and network architects all the way up to the rest of your C-Suite peers) and the region's unique demands.

Four facts about the Zscaler Zero Trust Exchange

The Zscaler Zero Trust Exchange™ is a comprehensive integrated platform that delivers against every requirement we have listed in the platform checklists. It enables Financial Services enterprises to unlock zero trust transformation for all users and workloads, meeting both networking and security needs in a consolidated way that streamlines visible operations.

Our platform works because it:

Eliminates lateral movement: It makes access control granular so more secure by connecting authorized users and devices directly to apps, not to the network.

Stops data loss: The system automatically identifies and protects sensitive data in motion, at rest, and in use.

Prevents compromise: It makes it possible for teams to inspect all traffic (including encrypted traffic) to block threats in real time.

Minimizes the attack surface: Applications are hidden behind the Zero Trust Exchange, making them invisible to the internet.

This is the modern security approach that enterprises not only want but need, to handle the ‘now’ and prepare for ‘what’s next’—are you ready to reach your next level of transformation?

Discover how to transform your organisaton →

zscaler™ | **Zero Trust Everywhere**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**