ZSCALER

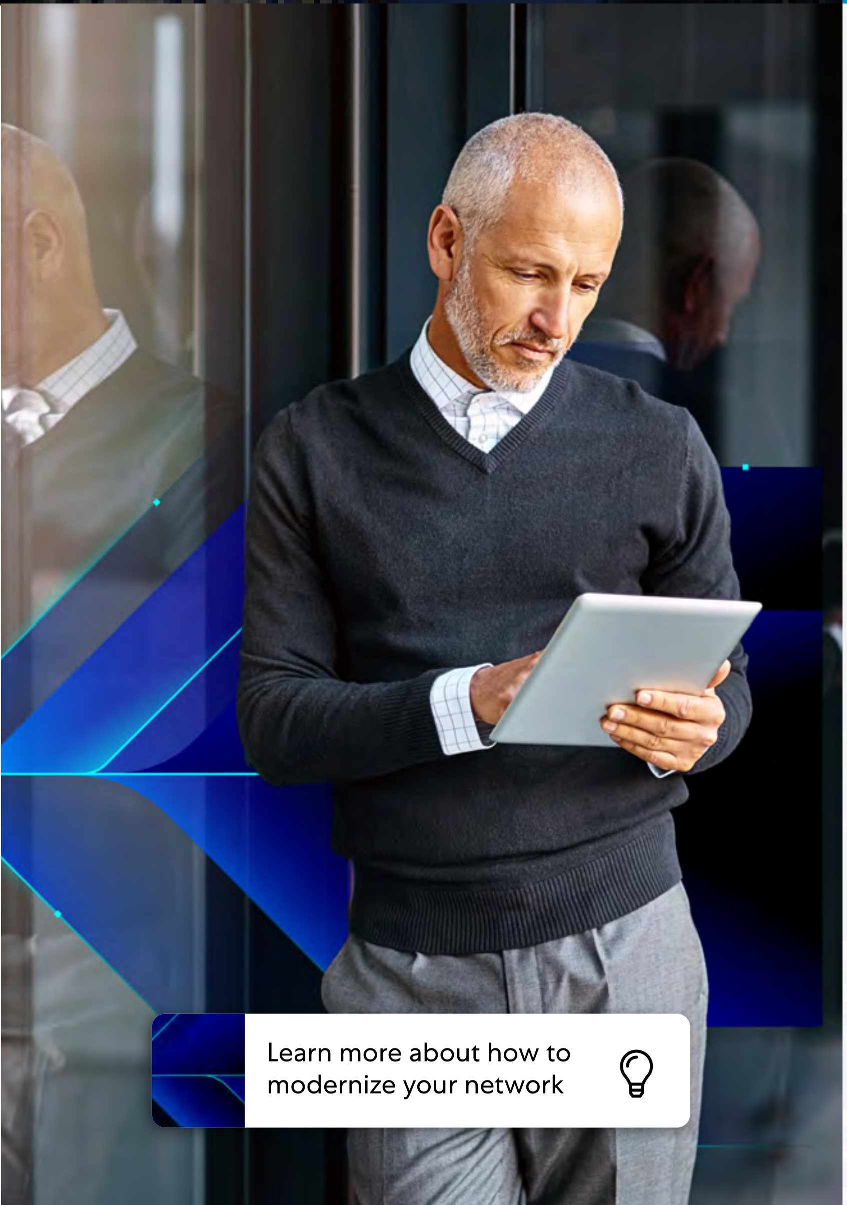
FOR BANKING & FINANCIAL SERVICES

CONTENT

1

THE FAST-CHANGING TECHNOLOGY LANDSCAPE

Whatever disruptive effects are happening around the globe, the most pertinent, quantitative, and sensitive barometer of world status is the health of the financial services sector.



Learn more about how to modernize your network

In order to survive and thrive in the fast-changing international economic landscape, the sector has taken a holistic and strategic approach, reinventing itself and embracing new FinTech platforms based on cloud computing, mobile ubiquity, and the latest advances in artificial intelligence (AI) automation.

Until 2020, the millennial youth were the key adopters of new banking technology, such as contactless "tap & pay" systems, but the learning curve has flattened and widened considerably, with all age groups now finding convenience in contactless payment methods. The COVID- 19 era has further expedited the shift to online banking and a cashless society.

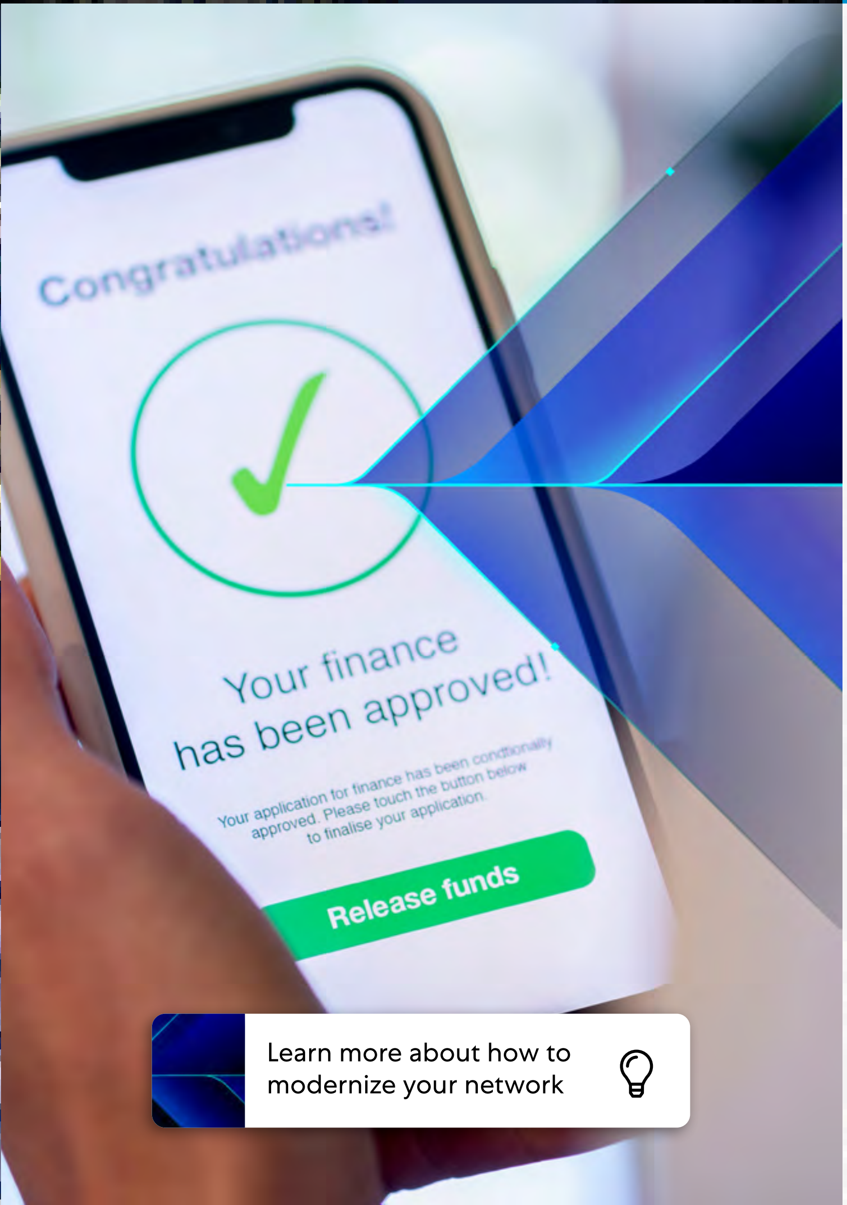
At the same time, advances in technology have opened up the market to disruptive digital competitors. The rise of so-called challenger banks has developed in line with consumers' readiness to embrace ecommerce through the use of a smartphone and the wider use of e-payments.

Whether someone is looking for a mortgage, an insurance policy, an investment plan, or simply moving money and carrying out their normal current/checking account activity, performing those tasks digitally is quickly becoming the norm. Market dynamism and unprecedented choice have cultivated customers who are extremely demanding and expect real-time, customised, value-added, seamless experiences.

2

THE STATE OF DIGITAL TRANSFORMATION

Digital innovation and business agility are key to attracting new customers, growing market share in home territories, and addressing growth opportunities in new business segments.


Congratulations!
Your finance has been approved!
Your application for finance has been conditionally approved. Please touch the button below to finalise your application.
Release funds

Learn more about how to modernize your network

But at the heart of most mature financial organisations are core systems, often based on proprietary on-premises technologies that have been extensively customised over the years, creating multiple dependencies and many tiers of interconnected IT functions. Citing financial regulations, governance controls, and data privacy laws as another key inhibitor to cloud adoption, it's understandable that most financial services organisations were slow or late to take advantage of the efficiency and agility provided by the public cloud.

Since those early days, financial regulators established standards and guidance around the use of cloud computing for security and privacy. This has allowed cloud to become an enabler of regulatory compliance, allowing financial institutions to develop effective approaches to risk management, data integrity, and confidentiality, without stifling innovation. Although most financial institutions now live in a hybrid environment with some legacy infrastructure, cloud steadily pervades the IT landscape with platforms and applications for everything from ERP, market data, CRM research, sales collateral, and onward, to market commentary analyses and much more. Even simple training for FINRA qualifications have moved online and FINRA itself has moved 100% of its own applications to the cloud.

According to a Zscaler survey of 600 EMEA CIOs in 2020, digital transformation is well underway in the financial services sector. Many organisations have now adopted a cloud-first strategy, leveraging multiple public clouds and software-as-a-service (SaaS) applications for customer-facing solutions, back-office operations, and integration with partners in the financial ecosystem—shadow banks, FinTech providers, and so on.

The survey reports that two-thirds of enterprises have shifted 50% of their applications to the cloud and a quarter of enterprises have shifted 75% of their applications to the cloud.

3 DIGITAL DONE RIGHT, DIGITAL DONE WRONG

As financial services evolve from the high street to online, providers are faced with the challenge of attempting to replicate online the level of in-person customer service that they delivered in their branches.

Learn more about how to modernize your network

To mitigate the risk of losing clients, customer experience has made its way to the top of the list of business priorities for most financial organisations. When services are delivered correctly and seamlessly, the customer asks for more, engages more, and potentially buys new services. Delivered wrong, slow, or with a lack of trust…and the customer leaves in a heartbeat.

With a firm eye on the future and emerging competition, progressive financial services organisations are now looking ahead to technologies based on 5G, AI, blockchain, Robotic Process Automation (RPA), and the wider use of internet of things (IoT). Progress to adopt, implement, and deploy these technologies was abruptly stopped in its tracks due to the effects of the COVID-19 pandemic, which had a massively disruptive impact on commercial and organisational development strategies at all levels.

Organisations everywhere were rapidly forced to switch gears and focus on business continuity. Within days, most IT departments had risen to the challenge and showcased their mastery of project management by re-prioritising and accelerating projects that enabled local and international economies to keep moving. Thousands of office or branch-based staff were enabled to work remotely, while cashless payments and other forms of frictionless and remote processes were rolled out early, some ahead of anticipated go-live timelines.

4 LEGACY INFRASTRUCTURE. AN ENABLER OR INHIBITOR?

While financial services organisations have made significant progress embracing cloud and mobile as part of their digital transformation journey, the evolution has presented several new challenges.

Existing investments that still serve business operations on a daily basis are frequently stretched to their maximum lifetime for the highest return on investment. The trouble is that legacy infrastructure was never designed for the transactional, analytical, and procedural demands of today's cloud and mobile world. These inadequacies came to the forefront during the pandemic.

Prior to the crisis, most financial services sector staff were based in a branch or office environment. A small percentage travelled on business for in-field meetings or worked from home, connecting to the organisation's core banking and insurance systems via virtual private network (VPN) or virtualized desktop interface (VDI).

In the wake of the crisis however, IT was faced with the challenge of enabling secure remote access for a record number of remote workers locked down at home. Even though mobile staff could still access business systems and cloud applications, VPNs were not designed for use by the majority of staff, requiring traffic to cross a stack of appliances such as load balancers, DDoS protection, firewalls, and VPN concentrators. Backhauling traffic through the existing network and legacy infrastructure and through multiple appliances caused latency, user frustration, and lower productivity. In worst-case scenarios, employees bypassed security policies and VPN controls, causing security vulnerabilities.

VDI technology allowed remote users to connect to core systems, email, and other applications using unmanaged devices (BYOD), mitigating classic issues such as data exposure and theft. But VDI solutions are not only notoriously difficult to set up and costly to maintain, but they also became over-used and an additional security risk during the pandemic.

Learn more about how to modernize your network

Typically, IT organisations resolve an underperforming network with additional infrastructure. This not only adds further complexity and cost but also increases security risks. As organisations travel further down the path of "feeding the dinosaur," they become less agile, innovative, and competitive.

Over recent months, this trend has been accelerated due to COVID-19, causing a majority of staff to work remotely and the financial services industry expediting its deployment of Microsoft 365.

SPECIFIC PAIN POINTS AROSE AS A RESULT:

- Remote access solutions based on VPN technology have been unable to deliver service levels required by the business, leading to latency and poor user experience.
- VPN-based remote access, which puts remote computers on the corporate network, has long been known to be the primary vector for endpoint infection. This has been exacerbated by the increase in home working.
- Microsoft 365 requires higher bandwidth and lower latency to deliver acceptable service levels.
- Expanding the hub-and-spoke architecture is very costly and ultimately doesn't deliver the service levels needed.
- Expanding the surface area of existing security architectures makes companies more vulnerable particularly to Trojan horse attacks, whilst not fully protecting against insider threats.

Many IT heads recognise that the hub-and-spoke architecture no longer maps to today's distributed cloud and mobile environment and struggles to support remote users or lacks the ability to scale with rising traffic volume. But it's not just the pain and cost of securing legacy infrastructure that is driving the need for architecture transformation; IT must design and implement an architecture that underpins a wealth of new innovations in diverse, dynamic, and complex environments.

The goal is to create a digital world that can understand and process natural language, gather big data, identify patterns, and interpret, perceive, reason, and advise in real-time to support next-generation guided learning, operational technology, robotics, wearables, and more.

5 THE ART OF BALANCING SECURITY WITH USER EXPERIENCE

Banks, insurance companies, and other financial services organisations are naturally responsible for holding and managing vast amounts of customer money and financial information.

Discover more about the Zscaler Zero Trust Exchange

With the ever-evolving challenge of staying ahead of criminals and keeping up with stringent financial regulations, it's no surprise that financial organisations are among the heaviest spenders on cybersecurity.

New digital developments create opportunities for criminals, who are poised to exploit vulnerabilities. In a matter of seconds, staff responding to a phishing email can have their credentials compromised and become the victim of a data breach, a ransomware attack, or both. But there's a balance to strike. How do you cost-effectively and securely push core business processes and applications to a mobile and remote workforce without compromising user experience?

Multiple security steps can add a lot of friction to the user experience. Customers and employees can become frustrated, affecting productivity. Heads of IT acknowledge that they are competent at delivering both security and user experience, but that it's a challenge to achieve both together.

6 CREATING A BALANCE OF SECURITY AND USER EXPERIENCE WITH SASE AND ZERO TRUST

Secure access service edge (SASE) is a security model defined by Gartner specifically to address the security challenges posed by apps, devices, and users moving outside the traditional network perimeter.

Discover more about the Zscaler Zero Trust Exchange

SASE architecture combines comprehensive WAN capabilities and network security functions such as secure web gateway, CASB, firewall as a service, and zero trust network access (ZTNA) to support the dynamic, secure access needs of digital enterprises.

Unlike traditional network access, zero trust adaptive business processes broker connections and grant access based on the user, device, location, and app, providing fast, secure access for authorized users, no matter where they are and without placing users on the network. With ZTNA, the web becomes an untrusted transport, and access to applications occurs through an intermediary cloud service controlled by a third-party provider or a self-hosted service.

As this model negates the need for cumbersome, traditional VPN hardware and processes, it creates a seamless process for the user and better overall experience.

ZTNA provides controlled access to resources, improves connectivity, and removes the need to directly expose applications to the internet, which reduces the surface area for attack. It became widely adopted in the face of the pandemic, allowing remote and home workers to access core applications with the same level of security controls as headquarters-based workers. So today, ZTNA is quickly becoming a best practice that companies are adopting across the business. Whether users are accessing the data center, private apps, or the public cloud, and regardless of whether they are in the office or working remotely, the experience will be identical.

ZERO TRUST EXCHANGE™

Zscaler's Zero Trust Exchange is a purpose-designed, cloud-based SASE platform that securely connects users, devices, and apps using business policies over any network. Fast, secure, and scalable, it balances the security priorities of the organisation with user experience to make the cloud a safe place to do business.

7

WHY ZSCALER?
AN INTRODUCTION

Regardless of the priorities of new banking solutions, like working with cryptocurrency, supporting new cross-border services, limiting fraud, or managing new regulatory compliance processes, financial services organisations need to underpin their strategy with a modern, robust, agile, and scalable platform that enables the business to innovate at pace and mitigate competition.

Discover more about the Zscaler Zero Trust Exchange

Operating for more than ten years and distributed across 150 data centers globally, Zscaler's SASE-based **Zero Trust Exchange is the world's largest in-line cloud security platform**, stopping over 100 million threats a day. The platform processes over 160 billion transactions per day—more than 10 times the number of daily Google searches—and receives 175 million unique security updates per day.

Zscaler is proven in the financial services sector with more than 500 financial services customers, six of the top ten U.S. banks, seven of the top ten European banks, and two of the top five Australian banks—underpinning their banking infrastructure with Zscaler's Zero Trust Exchange. Overall, Zscaler is a trusted partner to 4,500 customers across 185 countries, including 450 of the Forbes Global 2000 companies. The Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications, in any location, using business policies.

Core benefits of the platform are its ability to overlay existing architecture to instantly accelerate digital transformation and deliver efficient, secure, customer-centric, and scalable services:

- Efficient: Simplifies IT, reduces complexity and cost.
- Secure: Improves resilience and security posture and mitigates data loss and security risks with a single view of security posture across multiple divisions.
- Customer-centric: Supports the work-from-anywhere environment, increases capacity, reduces latency, and creates a consistent user experience to improve productivity.
- Scalable: A modern and agile platform that underpins digital innovation, accelerates digital transformation, and creates capacity for growth.

National Australia Bank (NAB) provides a comprehensive and integrated range of banking and financial products and services, including wealth management, with operations in Australia, New Zealand, parts of Asia, the United Kingdom, and the United States.

Faced with the COVID-19 lockdown, the bank needed to rapidly enable staff to work from home while continuing to provide services for more than nine million customers.

"Prior to the COVID-19 pandemic, we had never had more than 5,000 of our staff working remotely," said Steve Day, EGM Infrastructure, Cloud and Workplace at NAB. "We had to quickly find a way to equip contact centre staff so they could deal with calls from home, so that they could remotely access our apps and data stores," he said. "All of this, while managing four times the usual call volumes."

Working with Zscaler, NAB provided secure remote access for more than 32,000 staff, including the call centre teams, in just three weeks. NAB embraced zero trust to reduce cost and attack surface while creating an infrastructure that supports future operations.

"Zero trust has two big benefits. Firstly, we no longer need to run a separate corporate network, which delivers significant cost savings. In the new model, we only offer public internet access within our corporate offices. Secondly, we have increased our security posture, not by installing more expensive security infrastructure, but by removing all data and applications from the corporate environment to reduce our attack surface. We now have a secure networking infrastructure that can support NAB during the current crisis as well as when operations return to normal.

"People go home, turn on their PC, and it operates in exactly the same way as it does in the office. They don't have to worry about extra login steps or deal with security tokens—it just works," said Steve Day.

nab

Steve Day

National Australia Bank, Australia

nab.com.au

8 MERGERS AND ACQUISITIONS

Mergers, acquisitions, and divestitures are prevalent in the financial services sector but challenging for network and security teams that are responsible for ensuring user connectivity to internal apps and the security of sensitive data.

Discover more about the Zscaler Zero Trust Exchange

Converging disparate networks, managing overlapping IP addresses, and creating consistent security standards are just a few examples of the challenges that IT faces. Projects are time-consuming and resource-intensive, often taking months or years to complete.

Speed, security, and user experience are paramount during these complex transitions. By working with Zscaler, organisations can greatly simplify M&A and divestiture projects:

- Simply deploy software and route users to apps within minutes without converging networks at all.
- Standardize security for all assets—apps are only viewable to authorized users and users are never on the network.
- Provide users with a consistent access experience regardless of device, app, or location.

9 WHAT'S NEXT WITH DIGITAL TRANSFORMATION?

While financial organisations were able to react fast to the pandemic, IT and security teams are looking back to ensure they have successfully adapted to the new normal.

Explore more work-from-anywhere resources

Once temporary solutions have been addressed, attention will turn to the next stage of the digital transformation journey. Building a modern infrastructure to underpin future innovation is paramount.

As 5G unfolds and the financial services sector embraces more operational technology, advanced robotics, wearables, and other customer-centric innovations, new challenges and security vulnerabilities will emerge. Cybersecurity needs to remain one of the top priorities for financial institutions.

Over time, it becomes more important to partner with trusted infrastructure vendors that are not only well equipped to handle today's demands, but also have the vision and ability to drive and lead the way forward for financial organisations on a global scale.

10 WHY ACT NOW?

The cost of doing nothing is high, whether it's a simple increase in infrastructure and MPLS costs, loss in productivity, or the cost of recovering from a cyberattack.

Explore more work-from-anywhere resources

By acting now, your organisation can immediately gain an increase in security posture and have a single view of security across the business, while effectively supporting the new norm of remote working.

At the same time, IT investments become forward-looking and are channeled into scalable, new architectures that can accelerate business priorities and new innovations.

REGULATORY COMPLIANCE

Independent banking authorities work to ensure effective and consistent regulation and supervision of the banking and financial services industry. These bodies, with input from industry-leading organisations, have developed guidance and recommendations on the adoption of cloud technologies, the process and practice of outsourcing to cloud services providers (CSPs), and the adoption of a principles-based approach toward managing and measuring risk in cloud technology environments.

Zscaler is committed to helping customers with their compliance journeys by providing robust security and privacy protection, and support in meeting current and emerging regulatory risk and compliance obligations.

Zscaler provides transparent information and best practice support to ensure deployment and management of Zscaler solutions meet the governance framework.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com