netskope

for Financial Services

White Paper

Risk. Velocity. Vision.

The metrics of modern financial services

Table of Contents

THE HIGH-STAKES TRANSFORMATION OF FINANCIAL SERVICES

The banking, financial services, and insurance (BFSI) industry is going through a profound transformation. Over the past three decades, the sector has shifted from the branch-based, service-led model that dominated since the late 1800s toward digital-first, product-led operations.

In the past, a typical retail bank might have launched a new product every few years through in-branch promotions. Today, that same bank might roll out an AI-powered mortgage approval feature on its mobile app in a matter of weeks, while piloting a personalized savings tool in another market to scale globally the very next quarter. All without ever touching the traditional branch network.

Old world

Slow product cycles, physical access, and local services

New world

Mobile apps and AI, hybrid teams, and cloud operations

In this new era, financial institutions compete on the speed and seamlessness of digital product delivery. To keep up, they've moved more operations to the cloud, and rapidly adopted new AI tools—essentially behaving more like technology companies. While this shift has brought major benefits for both firms and customers, it has also expanded the scale and nature of the risks they face.

Personal app misuse, unchecked AI adoption, and increasingly sophisticated social-engineering tactics have converged to create a fast-moving, high-stakes threat landscape. Sensitive data now routinely flows through channels outside the traditional corporate network, AI tools are widely embedded into everyday workflows—often without consistent governance—and attackers are finding ever more creative ways to exploit trusted platforms.

As the risk landscape continues to intensify, threats are multiplying.

In response, security has become a clear boardroom priority, with decisions on architecture and controls now directly shaping how quickly an organization can innovate, how resilient it is to disruption, and how confidently it can respond to regulatory or market changes.

Legacy decisions and systems make these new challenges harder to navigate. An example can be seen in numerous pandemic-era VPN rollouts and fragmented point solutions. Organizations deployed these in haste to support remote work and they now represent significant technical debt and create operational friction, both of which lead to inconsistent protection.

Across banking, financial services, and insurance, the average user interacts with an average of 23 cloud apps per month, higher than all other industries[1]. The sector's cloud footprint is expected to keep expanding, further broadening its attack surface and creating fresh opportunities for attackers.

This leaves financial services leaders facing a strategic dilemma: How to move fast enough to seize market opportunities while keeping risk within acceptable bounds?

This whitepaper offers a framework to address that question, built around three strategic imperatives: **Risk**, **Velocity**, and **Vision**. Taken together, they form a blueprint for modern financial services security that positions zero trust principles and secure access service edge (SASE) not as constraints, but as the foundation for secure, sustainable innovation.

Financial services firms are under pressure to:

- **Manage risks:** From regulatory fines and reputational damage to sophisticated cyberattacks
- **Move faster:** Continuously deliver new features, products, and experiences at the speed of market demand
- **Plan for the long term:** Build the technology foundations that'll evolve with the business for the next decade

RISK

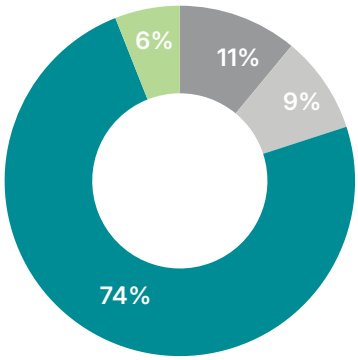
Strategic imperative: Control converging data, AI, and social engineering threats

Financial services firms have long been prime targets for attackers seeking to steal money, access sensitive data, or disrupt operations. Successful breaches result in regulatory penalties, financial losses, and lasting reputational harm. The sheer value of the data they hold, coupled with the high stakes of regulatory compliance, means even small lapses can have outsized consequences for financial services organizations. And today, those risks converge from multiple fronts.

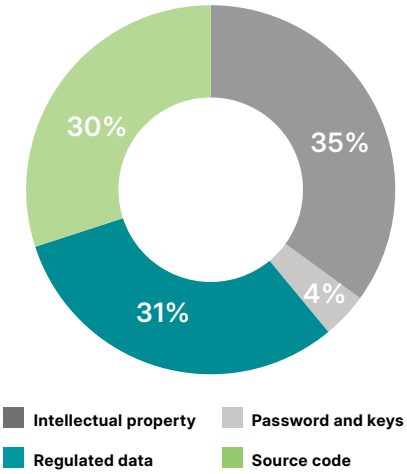
Personal app misuse is a major blind spot, with 92% of FS employees using personal apps in the workplace[1], often bypassing corporate controls entirely. Some 13% attempt to upload sensitive corporate data to these personal apps, with nearly three-quarters (74%) of those uploads involving regulated information. Left unchecked, these behaviors can create costly regulatory exposure, yet they're just one example of the way in which human behaviors increase organizational risk exposure.

Financial services leaders face a three-sided challenge: risky user behavior, persistent social engineering, and increasingly convincing attack campaigns. This spectrum runs from everyday tool use to deliberate manipulation by attackers, and all paths lead to measurable compromises.

Data policy violations for personal apps in financial services.



Type of data policy violations for genAI apps in financial services.



1. Netskope Threat Labs Report: Financial Services 2025: https://www.netskope.com/resources/threat-labs-reports/threat-labs-report-financial-services-2025

More recently, with generative AI now embedded in daily workflows, financial institutions face an even broader and faster-moving set of exposures. Employees within 95% of financial services organizations now regularly use genAI tools at work, and AI-related data policy violations regularly occur in the handling of intellectual property, source code, and regulated data. So, with adoption spread across multiple teams and tools, leaders are left attempting to govern AI use without slowing its legitimate benefits.

These new AI behavior-related data security risks are compounded by social engineering, perhaps the most adaptable and persistent threat methodology that financial services organizations face. Attackers exploit trust, familiarity, and urgency to trick users into granting access or carrying out malicious actions, often through legitimate channels like cloud apps. Social engineering is a component in 70–90% of cyberattacks, and notably around 68% of data breaches involve human error such as phishing[2].

Using humans as the weak link in the defense is consistently successful for attackers, and in recent years we have seen a steady stream of successful compromises, with 8.4 out of every 1,000 users in the average organization clicking on a phishing link each month[3]. Campaigns impersonating trusted brands such as Microsoft, DocuSign, Adobe, and other major banks show how convincing these lures have become—proof that even well-trained employees are often just a click away from compromise.

The modern approach

A future-ready risk strategy in financial services requires more than siloed tools or reactive controls. Chief Risk Officers (CROs) need unified visibility across data, AI, and user behavior that's anchored in a zero trust, cloud-native architecture. The goal is not just to contain threats, but to instill confidence in every transaction, service, and innovation.

By consolidating and adapting controls, financial organizations can reframe security as a catalyst for enterprise growth and innovation.

Leaders who take this approach can show regulators provable control, empower employees with safe access to modern tools, and assure customers that their data is secure in a digital-first economy.

At the board level, this approach also assures that security investment translates into measurable business value. Leaders gain the foresight to make bolder strategic bets—from digital product launches to M&A integrations—while giving investors confidence that risk is being managed proactively. A modern, secure architecture reinforces a culture of innovation, helps attract and retain top talent, and positions the institution to grow as a trusted, technology-driven leader.

Key elements:

- **Real-time data protection:** Combine data loss prevention (DLP), and data security posture management (DSPM) with user coaching for end-to-end protection, providing visibility and control of the complete journey of any data to reduce the risk of a severe breach by up to 80%[4].
- **Responsible AI adoption:** Continually assess the risks of genAI tools and AI-augmented apps, then allow, enforce granular controls, or educate in real time (or a combination of all three) depending on context. This gives institutions true oversight of AI adoption and ensures their data governance investments remain effective.
- **Inspect all traffic:** Deliver high-performance inspection across all cloud and web traffic, detecting phishing, malware, and advanced attacks in real time, while preserving a seamless user experience.

2. Secureframe: 60+ Social Engineering Statistics 2024: https://secureframe.com/blog/social-engineering-statistics, 3. Netskope Cloud and Threat Report: 2025: https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-2025, 4. Forrester Total Economic Impact TM (TEI) Study for Netskope SSE: https://www.netskope.com/resources/analyst-reports/forrester-the-total-economic-impact-of-netskope-sse

Compliance benefits

By aligning security controls with operational priorities and regulations such as GDPR, GLBA, PCI DSS, and DORA, CROs of financial institutions can reduce regulatory risk, accelerate audit readiness, and deliver secure digital products to market faster. In doing so, security shifts from a compliance obligation to a predictable enabler of agility, resilience, and sustained growth. It becomes the foundation for long-term success in a digital-first, product-led market.

"Netskope showed us all these issues that we didn't really know we had. We found systems on the internet that weren't going through our security controls... we were shocked [and] we fixed... It was avoiding all our antivirus, malware, and data loss protection controls."

VP of Digital Experience, Financial Services

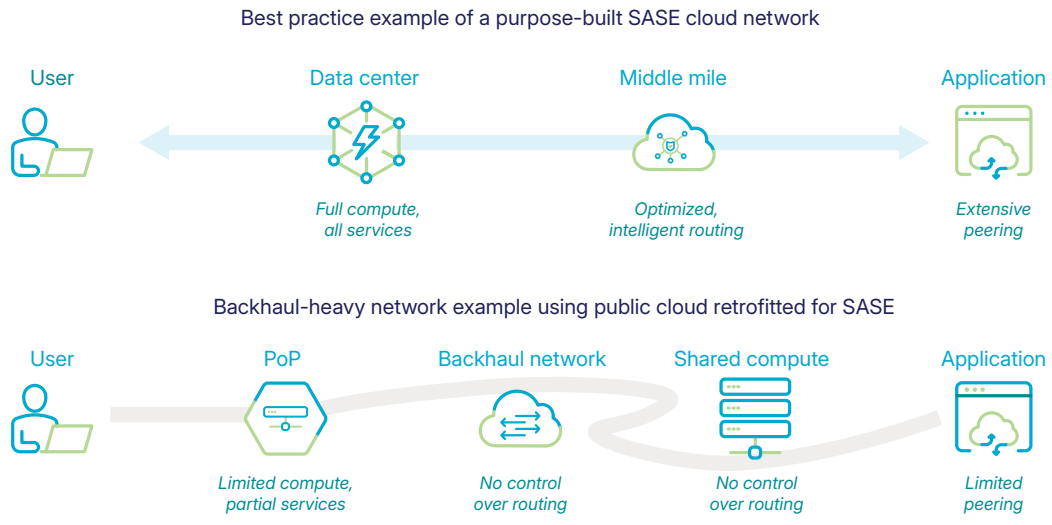
VELOCITY

Strategic imperative: Enable product-led growth without security or performance trade-offs

Financial services innovation cycles have accelerated sharply. Customers now expect a wide range of digital tools delivered seamlessly, with little tolerance for delays or downtime. And in a competitive, product-led environment, speed to market can mean the difference between winning a customer or losing them to a more agile competitor.

Legacy technology stacks weigh organizations down with redundant systems and overlapping controls, creating complexity, inconsistent policies, and integration headaches. At the same time, backhaul-heavy network designs using public cloud retrofitted for SASE introduce latency that frustrates users and undermines the performance of critical applications.

Two different approaches to architecture and implementation



Combined, these factors make change management cumbersome, with every update risking the breakage of a vital connection. The result is a fragile infrastructure at the very moment financial institutions most need secure, fast traffic to guarantee seamless user experiences.

The impact goes beyond internal inefficiency. Asia's financial markets are booming, with APAC now accounting for more than 40% of global IT spending, with hubs such as Singapore and China leading the charge[5]. For firms eager to seize these opportunities, ensuring high-performance connectivity, strong data security, and compliance with local residency rules is essential to sustaining growth. For critical applications organizations rely on, even milliseconds of delay can influence revenue or trigger regulatory scrutiny, making resilient, compliant infrastructure a direct enabler of expansion.

It's also important to remember just how damaging poor user experience can be on a firm's reputation. Poor performance can erode customer trust in new services, meaning that even a well-designed feature may struggle to gain adoption if it follows earlier failures. That's a particularly precarious position to be in when AI-powered competitors are continuing to set new benchmarks for personalized experiences, raising expectations, and widening the gap between nimble challengers and incumbents unable to keep pace.

The modern approach

Velocity in financial services isn't just about moving faster, it's about moving faster with purpose. For financial institutions, this represents more than a security or networking upgrade; it's about making the fundamental shift necessary to keep innovating at the pace required to remain competitive in the modern BFSI market. Zero trust and SASE are the enablers that give firms the coverage, speed, and resilience to accelerate growth rather than slow it down.

That's because a modern SASE architecture eliminates the foundational frictions of legacy patchwork systems, where overlapping controls and backhauled traffic create complexity and delay. By replacing that sprawl with a unified security and networking environment, SASE ensures traffic flows directly and securely, giving financial institutions the agility to expand into new markets or launch new services without adding latency or risk.

The languages of the modern internet

Application programming interface (API)

A set of rules and protocols that let software applications talk to each other and share data. They're the building blocks for countless digital services we use every day.

JavaScript Object Notation (JSON)

A human-readable format used for sending data between different systems. It's the standard for structuring data in web applications.

Model Context Protocol (MCP)

A framework for how AI agents connect with each other, as well as with tools and data sources, to access the information they need.

Key elements:

- **Direct-to-internet performance:** Use a carrier-grade private security cloud to eliminate backhaul bottlenecks and deliver low-latency access for users everywhere
- **Platform consolidation:** Replace multiple point products with an integrated SWG, CASB, ZTNA, and DLP stack to simplify operations and accelerate service delivery
- **Proactive safeguards:** Apply pre-emptive file inspection, real-time user coaching, and AI/API monitoring to remove delays and avoid late-stage setbacks
- **Secure AI and API enablement:** Embed security into AI workloads, MCP, and API traffic from the start to ensure compliance and resilience without slowing development

5. HG Insights: Financial Services Industry: IT Market Size & Trends Report 2024: https://hginsights.com/market-reports/financial-services-industry

With the assistance of real-time DLP and user coaching, teams are better able to remain within compliance boundaries without slowing their workflows, reducing delays caused by avoidable mistakes further down the line.

Finally, through continuous monitoring of AI apps and API activity, emerging risks can be caught early, avoiding costly rework or market pullbacks. Unlike legacy tools that are often blind to hidden threats, risky behaviors, or malicious activity, SASE platforms natively understand API, JSON, and MCP traffic—the languages of the modern internet, cloud, and AI. This means it can pre-emptively inspect all traffic, remove blind spots, and prevent incidents before they happen.

So, whether it's integrating real-time fraud detection into mobile apps or supporting on-demand insurance claim processing, security is built into the architecture from day one, not added after the fact.

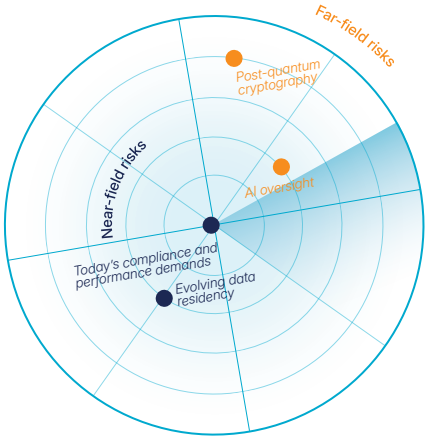
Velocity benefits

By aligning high-performance networking with integrated security, financial services organizations can launch new features faster while maintaining compliance, customer trust, and service performance. With technology investment reaching 4-5% of revenue in some mature markets[6], the ability to deliver secure, compliant services at speed has a direct impact on ROI. From real-time fraud detection to on-demand insurance claims, security becomes a growth accelerator that enables product-led innovation at the pace the market demands.

VISION

Strategic imperative: Build an architecture that lasts

The speed and uncertainty defining the global economy show no sign of slowing, with new challenges and innovations emerging almost daily. So, financial services leaders, including CIOs, CISOs, and CTOs, must make platform decisions on two horizons at once: sustaining near-term momentum while safeguarding long-term resilience and innovation.



These are not mere technology choices; they're strategic bets with multi-year implications for competitiveness, compliance, and the ability to seize new market opportunities. The challenge is placing those bets on a future that's far from certain, requiring leaders to anticipate how shifts like post-quantum cryptography, AI oversight requirements, and evolving data residency laws will affect the business.

Choosing the wrong architecture today can have consequences that echo for years. With technology spending at around 4-5% of revenue in mature markets[6], a misstep locks a significant portion of that investment into systems that hold the business back.

Once embedded in compliance processes, fraud systems, and trading platforms, the wrong solution is costly and difficult to replace. Many firms end up running overlapping systems in parallel just to maintain operations, adding technical debt, extending migrations, and delaying innovation. Global expansion only raises the stakes, with each new geography bringing additional layers of compliance, performance, and data residency complexity.

6. Deloitte: The Paradox of Money, May 2024: https://www.deloitte.com/uk/en/Industries/financial-services/research/show-me-the-money.htm

The challenge is clear: How can FS leaders design an architecture that meets today's needs for security, AI enablement, and performance while remaining ready for the unknowns of tomorrow?

The modern approach

For financial services leaders to achieve their vision for tomorrow, the architecture they choose must be designed to withstand at least a decade of change. That means the platform needs to be "open by design," so it can continuously adapt as regulations, technologies, and market models evolve.

What does "open by design" mean? It means being able to integrate seamlessly with other security, compliance, and analytics tools, and be built on an API-first approach so it will be able to connect with services and capabilities that don't yet exist. Zero trust policies depend upon signals and context collected from across the ecosystem, creating a unified and continuously adapting control environment.

A single-pass inspection model and unified policy engine keep controls consistent across every user, device, and data flow, no matter the origin. This consistency reduces operational friction today while avoiding the technical debt of duplicating inspection and policy layers tomorrow. Scalable, cloud-native infrastructure ensures capacity keeps pace with growth, whether driven by new digital products, M&A activity, or the rollout of AI-enabled services.

Equally important is how regions connect. Replacing brittle point-to-point cloud interconnects (which depend on fragile links between each location) with network peering allows traffic to flow through a globally interconnected security cloud with direct links to major networks, cloud, and SaaS providers. The result is low-latency, compliant data flows between regions, avoiding the fragility that slows expansion or forces compromises on user experience.

Platform resilience needs to be foundational, and proactive performance and security monitoring help assure this. Using full compute data centers for all SASE services close to users, architecture will remain steady even during internet "weather," third-party outages, or regional surges in demand.

So, as AI continues to advance, deep visibility into AI and API activity paired with flexible policy controls lets financial services firms adopt and govern new capabilities without disruptive re-architecture, keeping innovation continuous.

A VP of digital experience in the financial services industry reported that their organization was able to ameliorate the chronic downtime issues that plagued its poorly configured prior networking environment. This resulted in up to a 10% increase in uptime for the organization's core network services[7].

Key elements:

- **Single-pass inspection and unified policy control:** Reduce latency, improve consistency, and eliminate the drag of duplicated inspection engines
- **Scalable, cloud-native infrastructure:** Expand capacity and coverage seamlessly as business needs grow and change
- **Extensive peering and optimized connections:** Replace brittle interconnections with resilient, high-performance connectivity to critical applications and across regions
- **Proactive monitoring and distributed data centers:** Sustain performance and availability even during outages or high-demand events
- **AI-ready policy framework:** Adapt quickly to new AI and API usage models without re-architecting core systems

Long-term benefits

For financial services organizations, this approach provides the confidence to enter new geographical markets without the risk of building on an inflexible or compliance-vulnerable foundation. By consolidating controls, embedding resilience, and anticipating regulatory and technological shifts, CIOs can ensure their platform choice remains an asset, not a liability, for the next decade of growth. The result is consistent security, performance, and compliance worldwide, delivered without the overhead of managing complex vendor ecosystems or costly re-platforming projects.

7. Forrester Total Economic Impact TM (TEI) Study for Netskope SSE: https://www.netskope.com/resources/analyst-reports/forrester-the-total-economic-impact-of-netskope-sse

RISK, VELOCITY, VISION: WHEN SECURITY BECOMES A COMPETITIVE ADVANTAGE

Financial services institutions have always been early adopters of technology, making long-term bets that shape their organizations for years. A decade ago, VPNs felt like the right answer, and few could have predicted the speed at which cloud and AI would reshape the industry.

Today, technology leaders find themselves in another moment of evolution, consolidating onto a smaller number of integrated platforms that will carry them through whatever comes next. A modern strategy provides the unified foundation to align risk, velocity, and vision, enabling product teams to move at pace without losing compliance or trust, and lead the way to the future, rather than merely react to it.

With every attempt at innovation carrying a degree of exposure to breaches, regulatory penalties, and reputational loss, every financial services strategy has to begin with proactive risk control. Addressing **risk** first creates the foundation for consistent threat and data protection, policy enforcement across environments, and governance that satisfies regulators, the board, and customers.

From that stable foundation, firms can ramp up **velocity** by shedding the drag of point products, brittle networks, and manual compliance reporting. With high-performance private clouds that deliver direct-to-internet access, and by consolidating network capabilities into a single platform, financial services organizations can remove friction points, streamline deployment, and accelerate change management.

And when all of this is built on an open, cloud-native design that anticipates what's next and embraces new technologies without constant re-architecture, leaders achieve vision: The ability to deliver a clear, confident view of the future.

Taken together, **risk, velocity,** and **vision** form a comprehensive financial services security strategy that not only protects the business but also positions it to compete and grow in a digital-first economy. The objective is not simply to contain threats but to build confidence in every transaction, service, and release, reducing overhead, shortening time to market, and turning regulatory pressure into operational clarity.

> "Netskope provides us with the tools and capabilities to securely embrace cloud technologies while maintaining control and compliance."
>
> — Security Executive, Apex Group

Mapping the blueprint

- **Risk (unified control):** One control plane for data, cloud, and AI, shifting from reactive tickets to predictive controls and continuous audit readiness
- **Velocity (no trade-offs):** Single-pass inspection and fewer moving parts mean faster rollouts with less operational drag, eliminating brittle choke points and reducing latency
- **Vision (future-proof):** A cloud-native, zero trust architecture that scales with new markets, new apps, and new AI models

Key shifts that make this real, from:

- Point products and manual evidence – Unified platform policies plus real-time signals and context
- Siloed security and risk management – Converged threat and behavioral intelligence
- Perimeter-centric access – Data-centric zero trust everywhere people work
- Backhaul heavy network – Optimized routing and extensive peering for best experience
- Shadow AI and ad hoc guardrails – Approved AI with usage and data governance

Architecture principles to hold:

- Single-pass inspection and unified policy, for lower latency, fewer inconsistencies
- Cloud-native scale and distributed data centers, providing resilient performance through outages or spikes

- Extensive peering and optimized connections, for high-performance connectivity across regions
- AI-ready policy framework to govern prompts, models, and APIs without re-architecting
- Deep observability and digital experience management (DEM) to manage user experience and fix issues before users feel them

What leaders get: Business impact you can prove in Q1:

- **Boards and investors:** Assurance that security spend maps to measurable value, with early deltas including the removal of overlapping or redundant controls, shortening of audit response cycles, and a defined percentage of VPN traffic decommissioned.
- **Regulators and customers:** Provable control through automated evidence and inline guardrails. High-risk exfiltration attempts intercepted and coached at the point of action, with shadow AI managed and documented.
- **Product and operations teams:** Faster time-to-market for a target release, fewer handoffs, and shorter change windows. Experience scores improve for priority apps in target regions, with issues detected and resolved earlier.
- **Talent and culture:** A modern platform that attracts builders, reduces toil, and reinforces an innovation mindset.

Building from the blueprint

Risk, velocity, and vision may form the blueprint of a future-ready financial services security strategy, but no one can live in a drawing. Turning that blueprint for a house into solid rooms requires practical use cases and integrations that bring the strategy to life.

In practice, this means protecting data everywhere, governing AI use, defending against cloud-based threats, and ensuring performance through a private SASE cloud with distributed data centers with full compute for all SASE services. It also means using localization zones, automated guardrails, and user coaching to address user experience and insider risk while reinforcing a culture of security that doesn't slow productivity.

With Netskope, the SASE journey moves from blueprint to build. Recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for SASE Platforms and Security Service Edge (SSE), Netskope delivers a unified solution designed for the realities of financial services. Backed by vision and proven capabilities, Netskope provides financial institutions with a clear, future-ready path to comprehensive security, optimized performance, and long-term success.

With a modernized approach to risk, velocity, and vision, financial services leaders can secure today and prepare for tomorrow with one platform, unified control, and no trade-offs.

Visit Netskope.com/financial-services **for real-world financial services use cases and customer success stories.**

Ready to learn more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.