Point of View

Securing the Future of Financial Services

Despite Rapid Digitalization, Cloud Adoption and Rising Threats—Security Still Lags

Today's Challenges with Securing Financial Services

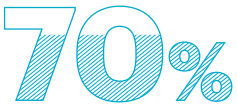
Nearly three-quarters (72%) of financial services companies report that cyber threats against their organization have increased over the last two years.[4] But the rising volume of attacks (such as ransomware) is only the first of many security challenges in the finance sector. The risks are getting higher, and the rewards are now being pursued by a host of newcomers to the industry.

The numerous connections required of financial organizations to collaborate with one another increases the surface area for compromise.[5] Technology leaders are under pressure to secure financial transactions and data in a world that is increasingly distributed. Banking, insurance and other financial services companies are rapidly adopting cloud solutions for greater productivity and cost savings. The cloud helps them onboard customers more quickly, cross-sell products, gain insights from data, and deliver more personalized products and pricing. Customers are on the go, using a range of devices to conduct transactions on all kinds of networks, while employees are working in hybrid and remote environments. Everyone expects mobile-enabled, anytime-anywhere access to accounts and services. As access points grow and hybrid work becomes the new normal—amid the use of web, cloud services, and applications—traditional perimeter defenses are no longer enough.

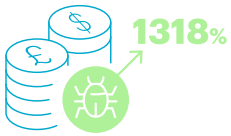
The competitive nature of the financial industry in the current moment may translate to even more complexity via mergers and acquisitions (M&A). Pressure from Fintech and Big Tech seeking to disrupt the market with new low-code/no-code offerings has prompted a drive to add new digital tools and capabilities to keep pace. This further increases both risk and infrastructure complexity—while adding strain to limited Technology and security staff resources. And slower responses to an incident can significantly increase attack damages.

Facts

Nearly three-quarters (70%) of financial services groups have reported a recent cyberattack.[1]



Ransomware attacks against the banking industry took a staggering 1318% jump last year.[2]



The average cost of a data breach in the financial sector is currently $5.85 million.[3]

[1] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.
[2] "Banking industry sees 1318% increase in ransomware attacks in 2021," Security Magazine, September 20, 2021.
[3] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.
[4] "Financial Cyber Survey," Deloitte, June 2021.
[5] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.

Growing Systems at the Speed of Business

Future-proofing digitalization. Competition from start-ups, internet giants, and industries outside of banking, along with increased regulations, are forcing banks to accelerate their digitalization plans.[6] A recent executive survey found most organizations have developed digital-transformation strategies and nearly half were accelerating existing plans—whether commencing an initiative earlier than planned or bolstering those projects already underway.[7]

The urgent need for traction in a changing landscape can also be seen in dynamic industry growth patterns. Banking M&As showed an 89% year-over-year increase.[8] The established pattern of deals surging after an economic downturn should continue in 2022, with companies actively exploring M&A, divestitures and other transactions.[9]

New digital tools and capabilities are critical to remaining competitive by serving modern customer expectations–greater banking convenience, exposure to new products, customized features and pricing. At the same time, risk management has not kept pace with digital transformation—a gap is opening that can only be closed by risk innovation at scale.[10] A recent survey showed nearly half (48%) of respondents in the financial sector said that their data security measures were falling behind their digital transformation deployments (below the overall average of 39%).[11] Financial organizations need security that anticipates rapid expansion of digital infrastructure and associated challenges, such as:

- **Fraud.** Digital lenders are seeing a 143% year-on-year increase in monthly fraud cases–and most consumers (67%) expect their bank to foot the bill for successful scams, regardless of the total amount lost.[12]
- **Insider threats.** One out of every four breaches in 2022 was the result of social engineering attacks. When you add human errors (such as misconfigurations) and misuse of privilege, the human element accounts for 82% of analyzed breaches over the past year.[13] The vast majority of breaches in the financial industry target servers via web applications—and a key component of these attacks is that they usually involve the use of stolen credentials.[14] Outdated access controls based on implicit trust need to be replaced with those that use contextual information within a zero trust model.
- **Vendor lock-in.** Many companies get locked in to outdated security infrastructure—limiting their ability to adopt the latest tools and capabilities needed to protect a rapidly expanding digital attack surface. Financial organizations need a dynamic security strategy that's designed to keep pace with emerging risks and an evolving threat landscape.
- **Software supply chain risks.** As geopolitical tensions rise, analysts warn that the financial services sector is becoming an increasingly sensitive target for nation state hacking campaigns that exploit weaknesses in the software supply chain (open source code, APIs, etc.)—such as the highly publicized SolarWinds attack of 2020.[15]

Critical Questions to Ask

- ☐ Is digital transformation outpacing our ability to protect the organization?
- ☐ Can I identify the sources of risk to our organization—both inside and out?
- ☐ Will our current security infrastructure adapt to new risk exposures and emerging threats in the coming months?
- ☐ Do I have the visibility and the data I need to make informed, risk based decisions?
- ☐ Does my security program support the broader Technology team to deliver services faster, cheaper and safer?

[6] "The State of Digital Transformation in Banking," International Banker, March 18, 2022.
[7] "The State of Digital Transformation in Banking," International Banker, March 18, 2022.
[8] "2022 banking and capital markets M&A outlook," Deloitte, May 22, 2022.
[9] "Deals 2022 outlook," PwC, May 2022.
[10] "Derisking digital and analytics transformations," McKinsey & Company, January 5, 2021.
[11] "Report finds 'glaring gaps' in financial sector's cybersecurity measures," Insurance Business Magazine, December 1, 2021.
[12] "Financial Firms Poised for Worse Cyber Threats After Trying Year," Bloomberg Law, March 10, 2022.
[13] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.
[14] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.
[15] "Fintech cybersecurity: How to keep banking and finance safe in 2022," International Accounting Bulletin, updated April 29, 2022.

Digital Transformation Fundamentally Includes Security Transformation

If security inhibits core operations of the business or contributes to a poor user experience, controls and protections will be bypassed. Many organizations report that outdated security is causing an unreliable, high-latency user experience that degrades productivity.[16] But gaining the efficiency of new digital tools without protection against attack is also an impossible situation. Successful system intrusions have doubled from 14% to 30% since 2016 (primarily as a result of ransomware)—and DoS attacks remain a major problem in the financial industry—accounting for 58% of security incidents (nearly doubling other industries).[17] Security and networking need to work together for fast, efficient, and safe operations at scale. This includes confronting the following:

- **Legacy technology.** Simply put? Out with the old. Traditional security infrastructure wasn't designed for today's distributed networks, multiple edges, and a large percentage of "work-from-anywhere" employees now part of a decidedly hybrid workforce. To achieve the agility that digital transformation promises, financial services companies need a fully-converged, cloud-native network security platform—one that eliminates the architectural inefficiencies of outdated security solutions while improving visibility across the organization—including cloud infrastructure.
- **Cost and complexity.** Traditional approaches to security rely on siloed tools that carry ongoing capital investment and increasing operating costs over time. The average organization manages 76 disparate security tools—and every time a new threat emerges, organizations must consider adding a new one-off solution to close the gap.[18] Security consolidation can reduce TCO by 30%+ through elimination of appliances, reduction of software license spend, reduction in administration overhead, and fewer tasks that need to be performed by human security staff (thanks to AI/ML automation).
- **The cloud and compliance.** Many financial services companies have been slow to adopt cloud technologies over concerns that computing over the internet will open the door to cyberattacks.[19] But as institutions in the sector embrace cloud to gain competitive leverage, financial regulators around the globe have become increasingly focused on ensuring firms use sound risk management practices during cloud implementation.[20] Overall, regulatory expectations have increased for financial services institutions in recent years—with operating costs spent on compliance increasing by over 60% for retail and corporate banks.[21]

Critical Questions to Ask

- ☐ Can I protect all my workers (remote and on-site) without impacting user experience or productivity?
- ☐ Are my network teams bypassing security to improve performance?
- ☐ How can I enforce controls and maintain compliance requirements without restricting users or slowing down the network?
- ☐ As I adopt new cloud environments, can I still ensure compliance with all applicable regulations (e.g., GDPR, SOX, PCI DSS)?
- ☐ Does my security program take operational costs out of the organization?
- ☐ Can I uplift the security posture from what we have today by taking advantage of new innovation?

[16] "The Economics of Network and Security Transformation," SDxCentral December 21, 2021.
[17] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.
[18] "Organizations Now Have 76 Security Tools to Manage," Infosecurity Magazine, December 1, 2021.
[19] "Banks Tiptoe Toward Their Cloud-Based Future," New York Times, January 3, 2022.
[20] "Financial Sector and Cloud Security Providers Complete Initiative To Enhance Cybersecurity," Cloud Security Alliance, March 23, 2022.
[21] "Regulatory productivity: Is there an answer to the rising cost of compliance?," Deloitte, May 23, 2022.

Closing the Cyber Skills Gap with Digital Dexterity

The persisting shortage of skilled cybersecurity professionals worldwide causes significant problems for virtually every organization in every vertical–including increasing the cybersecurity team's workload (62%), unfilled open job requisitions (38%), and high burnout among staff (38%).[22] The dual COVID-related impacts of an increase in cybercrime and a tight labor market have further compounded cybersecurity problems in the banking industry, leading technology teams to be stretched beyond capacity. These can all present openings for criminals to exploit.[23] At least 22% of financial services companies say they find it difficult or very difficult to attract new cyber and information security employees.[24]

The problem of hiring and retaining security talent extends all the way to the top of the order. Recent research also shows that 24% of Fortune 500 chief information security officers (CISOs) last only one year in the role—with the average tenure being just 26 months.[25] Financial services companies need security that alleviates the burden on the resources in-hand.

Faster responses. It currently takes an average of 233 days to find and contain a breach in the financial sector.[26] To augment under-resourced security staff, financial organizations need better visibility and control to accelerate responses to incidents. Organizations need to mitigate risk exposures even as their applications, data, and users move beyond the network perimeter. As such, a modern security infrastructure must provide:

- **Simplified integration:** A platform with powerful security capabilities across the policy administration life cycle.
- **Modern cloud security:** Sophisticated cloud security that uses granular context and provides deep visibility.
- **Continuous adaptive controls:** A solution that adheres to a zero trust model with adaptive controls for access, data movement, and threat protection.
- **AI/ML-driven data protection:** Single-pass inspection across all channels with advanced behavioral analytics using AI and ML for scale and efficacy.
- **Productivity and agility:** A faster user experience that boosts business and security capabilities.

Critical Questions to Ask

- ☐ Are the demands of our current security infrastructure too much for our existing staff to handle?
- ☐ Do I have full visibility across the entire infrastructure—including all data and applications in different clouds?
- ☐ Short of hiring more people, what can I do to inform and accelerate our security team's response efforts?

[22] "Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment," ISSA, July 28, 2021.
[23] "Cybersecurity in Financial Services and Insurance: A Growing Skills Gap," Emeritus, January 12, 2022.
[24] "Financial Cyber Survey," Deloitte, June 2021.
[25] "CISO churn – why it's happening and how to stop it," Raconteur, August 31, 2021.
[26] "How can a zero trust policy improve your industry?," Security Intelligence, January 14, 2022.

Choose a Security Platform That's Ready for Anything

Cyber incidents outpace other risks to financial firms—including COVID-19, business interruptions, regulatory changes, and even global macroeconomic shifts.[27] To regain insight and control, security professionals are rapidly adopting a security service edge (SSE) approach to deliver smooth, low-latency connectivity that consolidates and simplifies network security. SSE is the essential set of services—including cloud-native secure web gateway (SWG), multimode cloud access security broker (CASB), and zero trust network access (ZTNA)—that make up the security component of SASE (Secure Access Service Edge), an architectural framework for converging security and networking rapidly being adopted across the enterprise.[28] SSE transforms security for modern environments because it moves controls closer to both users and the data–providing consistent policy enforcement (regardless of location), a consolidated policy control plane, as well as comprehensive visibility of sensitive files and data.

As financial services organizations seek to manage and secure financial services and transactions everywhere people go, SSE is a critical step in securing the growing number of access points across web, cloud services, and private applications. By 2025, for example, 70% of organizations that implement agent-based ZTNA will choose an SSE provider for ZTNA, rather than a stand-alone offering, up from 20% in 2021.[29]

SSE and SASE can seem daunting, especially for slow-moving financial services organizations with lots of legacy infrastructure. At a tactical level, some ways to start or continue a SASE journey that break a lot of the steps in that journey down into digestible chunks include:

- Adding ZTNA for private applications to increase security for specific private apps to augment existing VPN solutions
- Replacing legacy on-premises SWG appliances with a cloud-based SWG offering
- Securing just your remote workers who expect to remain fully remote or hybrid in the next 12 months
- Moving from inefficient, "hair-pinned" branch office networks to network infrastructure that favors direct-to-net connectivity
- Securing managed SaaS applications, such as Microsoft 365 and Google Workspace

Each of these projects can be tackled separately or grouped together as needed and makes sense for the organization, and will provide a manageable step towards SASE for the organization. **Above all, remember the key role of data protection.** Data protection remains the grand strategy of security. The way in which we protect data has fundamentally changed—it's now everywhere, vs. within the confines of a traditional corporate perimeter—but we still want to protect data alongside every organization's most other important asset, its people. That's true in financial services, and it's true everywhere in business.

---

[27] "Cybersecurity in Financial Services and Insurance: A Growing Skills Gap," Emeritus, January 12, 2022.
[28] [Cite Gartner https://blogs.gartner.com/andrew-lerner/2021/03/26/checking-in-on-sase/]
[29] "Critical Capabilities for Security Service Edge," Gartner, February 16, 2022.