An IDC Vendor Spotlight sponsored by Zscaler
August 2025

Zero Trust: The Foundation of Resilience, Compliance, and Secure Innovation

Romain Fouchereau
Senior Research Manager
European Security, IDC

George Briford
Research Director
IDC Financial Insights, IDC

Zero Trust: The Foundation of Resilience, Compliance, and Secure Innovation

Introduction

Cyber-resilience transcends reactive measures and necessitates embracing a proactive mindset throughout the organization. It is about bouncing back from incidents and adapting and progressing in advance of cyberthreats to create an overall approach to resilience. As cyberthreats evolve and become more persuasive and sophisticated, finance organizations must continuously adapt their strategies and approaches to stay ahead. By embracing resilience and integrated risk management, finance organizations can mitigate risks, respond effectively to incidents, and maintain their operations and trust amid ever-present challenges.

AT A GLANCE

According to IDC's *EMEA Security & Strategies Survey, 2025*:

KEY STATS

- 78% of finance organizations say that adopting zero trust is part of the organization's cybersecurity strategy.
- 26% of financial services institutions (FSIs) cite the increasing resilience of business processes as a top operational cybersecurity priority.
- 62% of FSIs state that balancing security priorities with business priorities significantly limits their ability to improve cybersecurity posture.

However, this is often far from the truth, as the shift from regulatory frameworks to enforcement is exposing deep gaps in how finance organizations manage risk, automate controls, and ensure audit readiness across complex environments.

With the growing demand for business continuity, finance organizations must treat cyber-resilience as an outcome of strategic design, not just incident response.

Operational resilience and cyber-resilience must be embedded into operations by default to avoid applying remedies and fixing gaps after an incident. Getting things right the first time is a prerequisite for frictionless innovation.

Operationalize Compliance Across the Organization

Finance organizations are under increasing regulatory pressure to improve the efficiency and effectiveness of their compliance systems. In Europe alone, the Digital Operational Resilience Act (DORA) came into effect in January 2025. Other relevant regulatory requirements include NIS 2, CUABE, and the EU Cyber Resilience Act, which aims to address cybersecurity standards for connected digital products. All these regulations are highly relevant for finance organizations and how they should deal with resilience and cybersecurity.

Although DORA has been in force since January 2025, most European finance entities (84%) claim they are still working toward compliance, moving from regulatory awareness to enforcement. These new frameworks have raised the bar for operational resilience and cyber-readiness.

The rising burden of new and constantly increasing legislation manifests in rising compliance costs. Another factor driving the gap between regulatory awareness and efficient

implementation, particularly enforcement and operations, is keeping up with technology trends and changing security architectures. This often leads to siloed processes, making it difficult to maintain a holistic overview and respond to threats quickly and automatically.

Given all this manual and siloed compliance, workflows are too slow and costly to support continuous readiness or real-time reporting. A higher level of automation and more efficient cybersecurity frameworks are needed to promote overall resilience.

Breaking up siloed processes will enable embedding compliance into everyday operations through policy automation, continuous monitoring, and unified controls. This will deliver faster response times and significantly reduce audit complexity.

To meet these multiple requirements, finance entities need to think of ways to improve resilience standards and transform their compliance functions from pure cost centers into strategic centers and enablers of business resilience and innovation. The compliance center will thus support innovation by reducing complex and unconnected processes and avoiding unnecessary security reiterations — for example, during product deployment.

Cybersecurity is central to operational resilience, particularly as threats continue to expand in scale, sophistication, and impact. As a result, the roles of compliance and security functions are to provide advisory and remediation services and to steer the finance organization toward proactive compliance and risk management.

Building a Cyber-Resilient Organization — an Integrating Process

Both technology and business leaders understand the importance of protecting information and systems from cyberthreats and have invested significantly in cybersecurity programs focused on achieving the goals of confidentiality, integrity, and availability. However, while these goals are well-rounded, most cybersecurity programs tend to focus on the confidentiality and integrity of information and systems and leave availability to other technical disciplines to address.

To security leaders, the drivers of cyber-resilience may be obvious — shorter and fewer downtime incidents, fewer successful attacks, and faster overall resolutions, to name a few. But cyber-resilience also has several meaningful impacts at business levels and needs to be understood at the board level and by other major stakeholders. Cyber-resilience has become a top business priority and a board-level mandate, not just an IT concern, driven by rising expectations for continuity, regulatory accountability, and trust.

Yet progress stalls when business and security objectives diverge, underscoring the need for a shared security culture, especially when executive sponsorship is limited. With business continuity demand growing, FSIs must treat cyber-resilience as an outcome of strategic design, not just incident response. A large majority of finance entities point out that balancing security priorities with business priorities significantly limits their ability to improve cybersecurity posture. A further constraint is limited engagement from senior management. Only 27 % of finance institutions rank security culture and awareness among their top operational priorities. Without leadership's focus on these human factors, transformation initiatives risk losing momentum, leading to inertia.

The solution to this dilemma is to adopt a holistic methodology and policy-driven control framework. Embedding security means building policy-driven safeguards and automated fail-safes into every critical workflow. For example, a payments service should keep operating while a compromised component is isolated. This moves resilience from an after-the-fact response to an everyday operating standard. Once security is part of the operational rhythm, security becomes an accelerator of innovation.

Embedding a zero trust framework ensures a broad and integral approach to cybersecurity and thus to cyber-resilience, as it requires the continuous verification of every access request. Zero trust strengthens digital banking platforms by providing continuous verification, minimizing cyberthreat risks, and ensuring secure access across all channels for any device, user, or workload.

A key step in building a resilient organization through zero trust is ensuring finance entities have a clear picture of what assets and critical services need protection and how. The initiative requires knowing who has access to what, including third parties, as stipulated by DORA.

But a true transformational approach to cyber-resilience must be aligned with a "secure by design and default" mindset, whereby security is an integral part of every process and asset usage in the technology landscape.

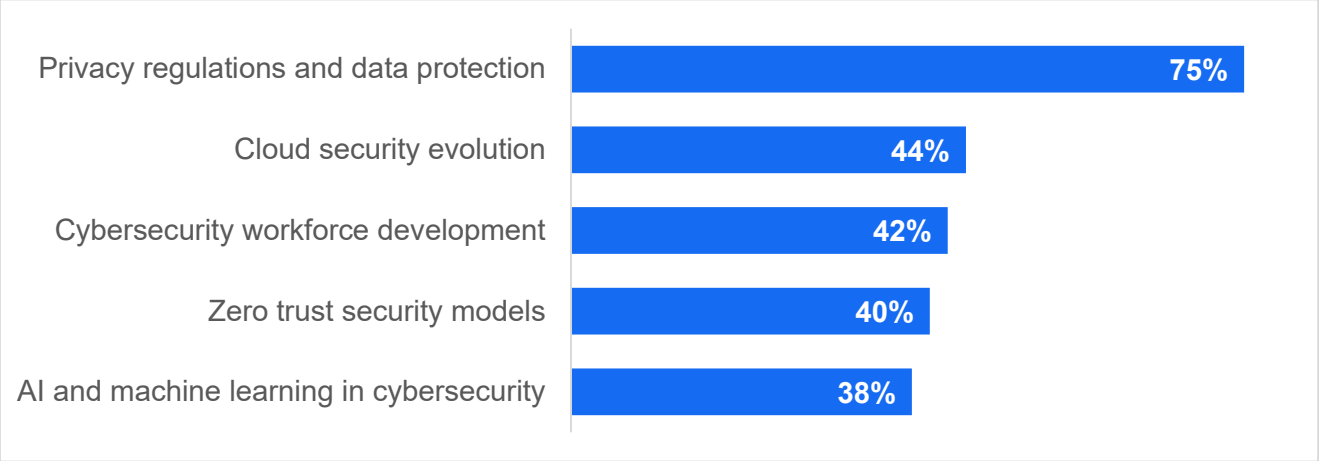
Secure Innovation in Practice — Embedding Security Practices

A major factor significantly limiting a finance entity's ability to improve its cybersecurity posture is that business innovation outpaces security capabilities. Reliance on third parties for critical technologies and services adds further complexity.

Finance organizations must innovate endlessly, or they start losing clients and the trust of stakeholders, including their regulators, because they cannot track, reliably implement, and enforce regulatory requirements. The thrust needed for innovation is expanding in many directions, such as AI, data-driven services, and platform modernization. Embedding security early is essential to scaling the adoption of all new digital initiatives responsibly. Finance institutions that embed safeguards into AI, analytics, and open-source initiatives are better positioned to scale these efforts securely and efficiently. Once resilience is woven into operations, security becomes an innovation accelerator, not a speed limit. Organizations that add security later risk introducing avoidable vulnerabilities and costly rework.

Finance entities must pay attention to cyberthreats such as ransomware attacks and AI-driven cyberattacks (e.g., deep fake phishing). The following figure presents examples of finance organizations' zero trust-related security initiatives to mitigate these risks.

Figure 1: Most Critical Cybersecurity Projects, 2025–2026



Source: IDC, 2023

Much of the innovation in the finance sector is driven by cooperation with other technology providers and third-party actors. Such inter-party innovation and subsequent service offerings depend highly on managing data privacy. Finance entities must therefore respect strict privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and the revised Payments Services Directive (PSD2). By adopting zero trust, they improve the efficiency of the compliance function by allowing access to data across decentralized environments, such as mobile apps, cloud platforms, and third-party application programming interfaces (APIs).

Over the past few years, a hybrid workforce has become the norm for many finance organizations. This shift brings a growing need to empower users and business partners with secure access to software-as-a-service (SaaS) applications, cloud storage, and a remote computing environment. This approach provides secure and optimized access to applications and resources for users and devices, regardless of location. By implementing zero trust, finance entities can strengthen customer confidence in the safety of their digital transactions while securing sensitive data.

Whether an initiative involves open-banking APIs or cloud-native applications, trust must be engineered in from the start. Aligning security with transformation and product teams, particularly through zero trust, is key to enabling secure and scalable innovation.

Vendor Profile

Zscaler is a cybersecurity vendor based in San Jose, California. Its products are designed to protect data, connections, and devices wherever they are. Zscaler's Zero Trust Exchange is a cloud-native platform that securely connects users, apps, and devices — using business policies — over any network in any location. With 160 datacenters worldwide and users in 185 countries, Zero Trust Exchange operates globally, enabling increased user productivity, reduced business risk, lower costs, and far less complexity.

Zscaler focuses on delivering security from the cloud and has built out functionality and integrations to deliver on the value and agility promised by cloud security. With a track record in cloud scale and reliability and a breadth and depth of security capabilities, Zscaler has proven its ability to support demanding finance organizations.

Zscaler has a four-step approach:

- **Verify Identity:** Verify whoever or whatever is attempting to gain access. The platform confirms user, device, or workload identity through integrations with third-party identity providers.
- **Determine destination:** Identify where the connection is going — to a webpage, SaaS app, private app, or anywhere else — and ensure the destination is known and understood.
- **Assess risk:** Use AI to determine risk based on context, considering factors like user behavior, device posture, destination, content, third-party intel, and intelligence gained from inspecting traffic globally, from which more than 500 trillion signals are derived daily.
- **Enforce policy:** Determine whether to grant access, block, isolate, deceive, or do something else. The platform enforces policy in real time, on a per-session basis for each request.

Zscaler supports the development of cyber-resilience by:

- Providing a policy-driven control framework, which regulations like DORA ask for when they demand integrated ICT-risk management across the whole organization
- Delivering continuous and measurable assurance, making it easier to prove that resilience controls work in real time, not just on audit day
- Making incident detection, containment, and reporting faster, helping firms hit regulatory notification and testing deadlines
- Reducing exposure from suppliers and partners, addressing DORA's third-party and outsourcing risk scrutiny

Challenges

Finance organizations have several challenges:

- Many organizations still operate a vast silo of legacy firewalls and VPN concentrators with associated technical debt, all of which were not designed for zero trust principles, such as micro-segmentation and identity-centric security.
- The architecture is highly complex and offers only a limited view of all assets, including business-critical assets and supporting services. Also, organizations are still struggling to implement regulatory requirements, and an architecture change must be aligned with audit requirements and may require prior regulatory approval or risk assessment.
- Given the ongoing work to achieve regulatory compliance, organizations rely heavily on third parties to conduct risk assessments.

- Senior management is not fully on board. Although board members understand the importance and urgency of the situation, they are still unfamiliar with the zero trust concept.

Conclusion

IDC believes zero trust is an important, if not a vital, part of finance organizations' overall strategies to build up and maintain operational resilience and cyber-resilience.

Embedding resilience into every security aspect of operations equips banks, insurance providers, and other finance organizations with the right tools for swift threat detection and containment, effective response, and minimal to no disruption from cyberincidents.

Zero trust supports cloud security platform architecture, enabling it to deliver an always-on level of resilience that underpins network availability and data confidentiality, no matter what.

MESSAGE FROM THE SPONSOR

The financial services industry faces growing challenges as it adapts to an increasingly digital and interconnected environment. These include the rising complexity of cyberthreats, regulatory oversight, and the need for operational resilience to safeguard critical systems and data. Building trust while ensuring secure and scalable innovation remains paramount as organizations manage these pressures.

Finance institutions can address these challenges by adopting a zero trust architecture to protect sensitive data, support compliance efforts, and reduce risk in cloud-first environments, all while reducing technical debt by removing their reliance on legacy security appliances like firewalls. Zscaler's expertise in secure digital transformation provides financial services organizations with the resilience needed to innovate while staying secure in an ever-evolving threat landscape.

Learn how adopting zero trust can help secure your organization's transformation journey while reducing security costs.

About the Analyst

Romain Fouchereau, Senior Research Manager, European Security

As senior research manager for IDC's European Security group, Romain Fouchereau focuses on network security and security technologies linked to the extended enterprise, such as IoT, edge, and IT-OT convergence. Romain closely monitors the development, evolution, and market penetration of these technologies and the approaches vendors are taking to stimulate adoption at channel and end-user levels.

Romain joined IDC from a manufacturing company, where he specialized in market research consultancy. In this role, Romain handled go-to-market projects for various products and vendors, focusing on the French and Italian markets.

George Briford, Research Director, IDC Financial Insights

George Briford's vast experience includes designing pragmatic operating models and leading transformation and change management initiatives as a project and program manager for universal banks in Europe, Eurasia, and East Asia.

George has experience working for major management consulting firms and in various bank roles. His main domains are retail and small-business banking, focusing on strategy development in sales and distribution operating models, customer relationship management, and business architecture, including the digital enablement of key components.

Several of these engagements related to optimizing customer experience through improved journeys, developing omni-channel capabilities, and adopting a human-touch-first, technology-enablement-later approach.

George also has experience with controlling and budgeting, including developing performance measurement operating models, such as balanced scorecards with aligned objectives and KPIs.

George is a keen advocate of design thinking, blending agile methods with a waterfall approach to implementation. He is an experienced business architect who is familiar with the major frameworks.

George has an MBA from the IESE Business School and a BSc in economics and business studies from Lund University.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions to achieve their key business objectives.

Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data, and marketing services company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road,
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B,
Needham
MA 02494
+1.508.872.8200
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.