EBOOK

The Rising Cost of Trust: Cyber Resilience for Financial Security Operations Leaders

VECTRA®

Introduction

Trust has always been the currency of financial services. Today, that trust is under siege. Cyberattacks are escalating in scale and sophistication. From AI-driven fraud to ransomware-as-a-service, adversaries now innovate as fast as the industry itself. For Security Operations leaders, the question is no longer if defenses will be tested, but how resilient operations will be when they are breached.

This eBook explores the new threat landscape and why legacy security approaches fall short in a cloud-first world built on AWS. It unpacks the true costs of breaches, including financial, regulatory, and reputational losses, as well as the trust deficit that follows when customer data is compromised. It also examines emerging risks: AI-enabled cybercrime, looming quantum disruption, and intensifying compliance pressure.

Most importantly, this eBook outlines a framework for resilience. You will see how Security Operations teams are driving resilience through continuous detection, rapid response, automation, and visibility across hybrid and multi-cloud environments. And you will see how AWS and Vectra AI help financial institutions strengthen resilience with security that withstands today's attacks and prepares for tomorrow's unknowns.

The rising cost of trust makes resilience the defining imperative for Security Operations leaders in financial services.

The Modern Threat Landscape in Finance

Financial services are the most consistently targeted organizations in cyberspace, with attackers innovating faster than most institutions can adapt.

Context & Expansion

The sector has always been a prime target for money, sensitive data, and critical infrastructure. But today's threat landscape is different. Fraud schemes are AI-driven, ransomware-as-a-service has lowered barriers to entry, and state-sponsored actors relentlessly probe resilience. For Security Operations teams, this means non-stop campaigns against networks, identities, and cloud workloads.

Unlike other industries, financial services face the dual challenge of protecting assets while meeting stringent regulations. Every breach is not just a technical failure; it's a reputational and compliance crisis. For institutions running hybrid and multi-cloud environments, the attack surface is expanding in ways legacy defenses can't cover.

Business & Operational Implications

For Security Operations leaders, this is a resilience challenge. Teams cannot scale manually to match attacker speed. Operational resilience now depends on AI-driven detection, cross-domain visibility, and automated response that prevents incidents from escalating into systemic risk. Leaders who treat resilience as a strategic imperative, not just a compliance checkbox, will safeguard both business continuity and analyst capacity.

Data & Research

200-300%

China-nexus intrusions against financial services surged 200-300% in 2024

– Crowdstrike 2025

54%

click-through rate for LLM-generated phishing lures vs. human-written ones

– Crowdstrike 2025

24%

of ransomware attacks worldwide target financial services

– Trustwave 2024

50%

Over 50% of Security Operations practitioners say they cannot keep pace with rising threats

– Vectra AI 2024

Takeaway

The modern threat landscape is a continuous, adaptive campaign. Security Operations teams must evolve to handle AI-driven attacks, ransomware networks, and state-sponsored campaigns with resilience built into their processes and platforms.

The Cost of Breaches and the Trust Deficit

In financial services, a cyber breach is never just a technical failure; it's a business event with steep financial costs and an even greater impact on trust.

Context & Expansion

Financial institutions operate under some of the strictest regulations, and customer expectations for security are uncompromising. A single breach can trigger fines, lawsuits, and customer churn. Security Operations leaders know that downtime and missed detections don't just affect security metrics; they drive real losses in accounts, market share, and reputation.

Digitization expands exposure. The very cloud adoption and digital channels driving growth also increase the attack surface. For SecOps leaders, cyber risk management is core to revenue and reputation protection.

Operational Implications

For Security Operations leaders, resilience must deliver measurable results: fewer escalations, faster MTTR, and stronger communication with regulators and executives. Teams need automation, noise reduction, and actionable visibility to meet these expectations under constrained budgets.

Data & Research

$6.08M

Average cost of a financial services breach

– IBM 2025

Transparency in incident response is now a core expectation

– FS-ISAC 2025

DORA and SEC disclosure rules demand frequent, detailed resilience reporting

Takeaway

The cost of breaches is rising, but the trust deficit they create is even more damaging. Security Operations leaders who embed resilience into detection and response workflows not only reduce exposure but also preserve customer trust.

Building Cyber Resilience in a Cloud-First World

Resilience is no longer optional; it is the foundation of trust, growth, and compliance. For SecOps, it means continuous operations under attack conditions.

Context & Expansion

Cloud adoption is transforming financial services, but legacy perimeter defenses can't protect hybrid and multi-cloud environments. Security Operations leaders must ensure continuous monitoring, incident containment, and regulatory reporting across dynamic infrastructures.

Operational Demands

✓

Continuous Detection

AI-driven monitoring to cut alert noise and surface attacker behaviors.

✓

Rapid Response & Automation

Playbooks integrated with SIEM, SOAR, EDR, and NDR to cut containment time from hours to minutes.

✓

Cost Efficiency

Visibility that reduces SIEM log ingestion, freeing budgets for higher-value activities.

Data & Research

99%

of alert noise triaged with AI-driven detection

– Vectra AI 2024

Shared responsibility model: AWS ensures infrastructure resilience; institutions secure workloads and data

– AWS 2025

Takeaway

In a cloud-first world, resilience is measured by faster detection, faster response, and lower operational drag on Security Operations. AWS provides resilient infrastructure, while Vectra AI provides cross-domain visibility and automation.

AI and Quantum – The Next Frontier of Financial Threats

The same technologies transforming financial services, AI, and quantum, are also fueling the next wave of cyber threats.

Context & Expansion

AI enables fraud detection and risk modeling, but adversaries are weaponizing it with deepfakes, adaptive phishing, and fraud-as-a-service. Meanwhile, quantum disruption threatens to undermine today's encryption. For SecOps leaders, the challenge is preparing teams and processes for these next-generation threats before they hit production environments.

Operational Implications

SecOps teams cannot focus only on today's indicators. They must invest in AI-driven detection that adapts, adopt quantum-ready cryptography, and build resilience strategies that anticipate, not just react to, emerging risks.

Data & Research

Growth of phishing-as-a-service kits designed to bypass MFA

– Sekoia 2024

Brute force and phishing still dominant breach vectors, amplified by AI

– Trustwave 2024

FS-ISAC 2025 recommends adopting cryptographic agility now to prepare for quantum disruption.

Takeaway

Financial leaders who prepare their Security Operations teams for AI and quantum threats today will be positioned to maintain trust tomorrow.

Strategic Pathways to Resilience

Resilience is not a tool; it is a strategy that unites people, processes, and platforms to ensure continuity.

Context & Expansion

Prevention-only models no longer work. Security Operations leaders must shift to proactive resilience, where continuous detection, automated response, and regulatory alignment are baked into daily workflows.

Three Pillars for SecOps Resilience

✓ **Continuous Threat Detection**

AI-driven visibility across cloud and on-premises.

✓ **Rapid Response & Recovery**

Automated playbooks and faster MTTR.

✓ **Regulatory & Risk Alignment**

Demonstrating resilience to meet DORA, SEC, and global requirements.

Data & Research

> Resilience testing and third-party risk management are now mandatory expectations
>
> **– FS-ISAC 2025**

> Regulators demand proof of resilience planning
>
> **– DORA, SEC rules**

Takeaway

For SecOps leaders, resilience means moving from reactive defense to proactive trust-building. AWS provides infrastructure resilience, while Vectra AI empowers operations teams with signal clarity and automation.

How AWS and Vectra AI Build Resilience Together

Security Operations leaders don't need more tools, they need solutions that close gaps in detection, response, and resilience. That's where AWS and Vectra AI align.

Solution Alignment

1 **Stopping Today's Attacks**

Vectra AI detects privilege abuse, lateral movement, and identity misuse across hybrid and multi-cloud environments.

2 **Meeting Regulatory Demands**

AWS frameworks align with DORA and SEC. Vectra AI provides reporting and visibility for regulators and executives.

3 **Reducing Breach Impact**

AWS delivers resilient infrastructure; Vectra AI triages 99% of alert noise and prioritizes real breach signals for faster analyst action.

4 **Preparing for What's Next**

AWS offers cloud scale; Vectra AI adapts detection to emerging attacker techniques.

Takeaway

AWS provides the foundation. Vectra AI delivers visibility and automation. Together, they enable Security Operations teams to strengthen resilience against today's and tomorrow's threats.

Conclusion

The financial services industry faces relentless innovation from attackers and rising regulatory demands. AI-driven fraud, ransomware, and state-sponsored campaigns dominate today, while looming quantum risks threaten the future. For Security Operations leaders, resilience is no longer optional, it sustains trust and ensures continuity.

Resilience requires continuous detection, rapid response, and regulatory alignment. With AWS delivering the resilient foundation and Vectra AI providing visibility and intelligence, SecOps leaders can build security that withstands today's attacks and prepares for tomorrow's unknowns.

Build Resilience Now

Discover how Vectra AI and AWS strengthen resilience with AI-driven detection and cloud-enabled defenses.

Available directly through AWS Marketplace, Vectra AI accelerates adoption, aligns with AWS budgets, and helps Security Operations leaders strengthen resilience without slowing transformation.

About Vectra AI, Inc.

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. The Vectra AI Platform delivers AI-driven Network Detection and Response (NDR) to surface and stop threats across the data center, campus, remote work, identity, cloud, and OT environments.

In the first-ever Gartner® Magic Quadrant™ for Network Detection and Response, Vectra AI was named a Leader and positioned highest for Ability to Execute and furthest for Completeness of Vision. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't.

For more information, visit www.vectra.ai