CROWDSTRIKE

eBook

# Stopping Breaches at the Speed of Finance

## A New Security Blueprint for Modern Financial Institutions

# Table of Contents

# Introduction

Financial services organizations face an unprecedented convergence of sophisticated cyber threats targeting the very foundation of global commerce. Adversaries are moving faster, striking smarter, and targeting institutions with ruthless precision. And the stakes are uniquely high in financial services.

Banks, credit unions, insurers, and investment firms handle a constant stream of sensitive data, from personally identifiable information (PII) and financial transactions to behavioral signals and customer identity records. These assets move across complex hybrid environments — from on-premises core banking systems to cloud-hosted digital platforms, third-party processors, and mobile banking apps. Each touchpoint, whether in a brick-and-mortar branch or a cloud-native API, becomes a potential point of compromise.

Adversaries are taking notice. In 2025 alone, cyber operations linked to state-sponsored groups in China increased by 38% year over year across several sectors — with financial services among its targets.[1] And these threats are growing, not just in volume but in sophistication — 82% of detections in 2025 used malware-free techniques,[1] exploiting the very identity systems that financial institutions rely on for customer access and employee productivity. Disconnected point solutions, siloed teams, and manual workflows struggle to keep up.

**82%**
*of detections in 2025 used malware-free techniques[1]*

**In today's digital economy, breaches in financial services are inevitable unless security strategies evolve.**

There is a path forward. Leading financial institutions are adopting a unified security approach that consolidates real-time protection across endpoints, identities, and cloud workloads. This modern security strategy, backed by AI-powered defenses and expert-led threat hunting, enables security teams to dramatically improve efficiency and speed up investigations.

This eBook explores the current threat landscape facing financial services, examines real-world attack scenarios, and presents a comprehensive framework for building resilient security operations that can outpace today's most sophisticated adversaries.

Through actual customer experiences and proven methodologies, we'll demonstrate how financial institutions can strengthen their security posture while reducing complexity and operational costs.

[1] CrowdStrike 2026 Global Threat Report

# The Scale and Stakes of Financial Cyber Threats

Financial services continue to stand at the epicenter of adversary activity. Out of all nation-state and eCrime adversaries tracked by CrowdStrike, 53% focus their efforts on this sector.[2] Adversaries view financial institutions as high-value targets, not only for direct monetary gain but also for the wealth of sensitive data they hold and the critical infrastructure they operate.

Modern adversaries bring a level of sophistication that traditional defenses often can't match. Ransomware groups now operate like well-funded businesses, executing targeted campaigns with precision. Business email compromise (BEC) has evolved into a persistent threat vector, especially when attackers pair credential theft with social engineering. Identity fraud schemes exploit weaknesses in verification processes, while AI-enhanced attacks rapidly test and refine intrusion methods to bypass conventional detection. Financial institutions must now counter a coordinated, multi-vector assault that blends automation, deception, and human error.

The economic consequences of these attacks are staggering. The average cost of a data breach in the financial sector is $5.56 million USD per incident.[3] But the financial hit rarely stops there. Regulatory frameworks like GDPR and PCI DSS can impose penalties in the tens of millions. Lawsuits and settlement costs can spiral. And damage to brand trust can ripple through customer bases for years.

The insurance market is responding with higher premiums, more exclusions, and stricter policy requirements. In effect, security lapses now influence insurability, not just operational resilience.

Behind these economic trends lies a shift in adversary intent. Nation-state groups view financial infrastructure as a geopolitical pressure point, targeting payment systems and large institutions to disrupt economic stability. eCrime actors pursue a mix of direct theft and fraud, monetizing stolen credentials, account access, and sensitive financial records. Meanwhile, advanced persistent threat (APT) groups embed themselves deeply into supply chains, spending weeks or months inside networks to gather intelligence or prepare for larger-scale disruption.

Financial institutions face a high-pressure equation: Adversaries are multiplying, their motives are diversifying, and the consequences of failure are escalating.

**53%**
*of named adversaries tracked by CrowdStrike target financial services.*[2]

[2] Adversaries tracked by CrowdStrike Counter Adversary Operations as of 03/06/2025
[3] IBM Cost of a Data Breach 2025 Report

# Core Security Challenges in Financial Services

Adversaries target the finance sector for its high-value data and systems, while also seeing it as a gateway to disrupting global markets. And these threat actors are exploiting weaknesses faster than many defenders can react.

**To stay ahead, financial organizations must confront five key challenges reshaping the threat landscape.**

## 1. Minutes or Even Mere Seconds Is All It Takes

Generative AI is increasing the sophistication and speed of attacks. Adversaries now use it to spin up convincing phishing messages, mimic executive voices, and generate synthetic identities in seconds.

And they're moving at machine speed. Attackers can establish access and begin moving laterally through financial networks in just 29 minutes on average — a 65% increase in speed year over year — and as fast as 27 seconds.[4] These breakout times leave defenders with almost no room to react.

Legacy workflows and disconnected tools can't match the speed of these attacks. Manual investigations delay triage. Siloed systems obscure the full scope of activity. Every gap in coordination gives adversaries a head start. Without automation and AI-driven detection, defenders lose the race before they've even left the starting line.

*"Speed defines the success of both the attacker and the defender."*

***Mike Sentonas***
*CrowdStrike President*

## 2. Trust Is Exploited in Identity Infrastructure

Intruders have traded malware lockpicks for login credentials. In fact, 79% of attacks now rely on malware-free techniques to gain initial access.[4] This tactic allows adversaries to bypass traditional endpoint defenses and blend in with legitimate user behavior.

Attackers are exploiting common identity infrastructure — from Active Directory and single sign-on (SSO) platforms to cloud-based identity brokers. They hijack user sessions, overwhelm authentication systems with credential stuffing, and exploit multifactor authentication (MFA) fatigue to slip through the cracks. Once inside, they operate under the radar while accessing and moving across systems that trust the stolen identity.

## 3. Ransomware Has Been Rewired for Financial Services

Ransomware groups continue to evolve their playbook, and financial services remain a top-tier target. These threat actors now design campaigns specifically for this sector, striking core systems like payment processing infrastructure, SWIFT networks, and automated clearing houses.

Modern ransomware operations combine financial blackmail with data extortion. Adversaries encrypt systems to disrupt operations, then steal sensitive data and demand ransom under threat of publishing or selling that information. This double extortion model pressures organizations on multiple fronts. Some groups escalate to triple extortion, adding denial-of-service attacks or targeted disruptions during critical market periods. These tactics inflict more than financial loss — they undermine customer trust and threaten business continuity.

[4] CrowdStrike 2026 Global Threat Report

## 4. Financial Data Is an Adversary's Jackpot

Financial institutions house some of the world's most valuable data: financial records, PII, transaction histories, and intellectual property. This information commands premium prices on dark web marketplaces.

To complicate matters, the financial services data ecosystem extends far beyond internal systems. Vendors, fintech partners, and open banking APIs expand the attack surface by increasing where sensitive data is stored and accessed. These connections create additional opportunities for attackers to find weak points.

As a result, cloud data stores and SaaS platforms are prime targets. When security controls vary across on-premises, cloud, and third-party environments, attackers exploit the weakest links. Fragmented data governance policies often leave sensitive data exposed or insufficiently protected. Threat actors capitalize on these gaps and spend time mapping these environments to identify high-value data before launching stealthy exfiltration campaigns.

## 5. Tool Sprawl and Team Silos Slow the Fight

Many institutions attempt to defend against advanced threats using a fragmented mix of several different security tools. Each tool produces alerts, demands configuration, and rarely integrates cleanly with the others. This complexity slows down investigations and creates blind spots across the environment — a particular challenge for financial services organizations that must orchestrate security across vast ecosystems serving multiple clients, partners, and transaction types. This complexity slows down investigations and creates blind spots across the environment.

Security teams struggle to connect the dots across endpoints, identities, and workloads. Analysts face overwhelming volumes of alerts. Critical signals get buried in noise. At the same time, organizational silos isolate key security functions. Identity, cloud, endpoint, and network teams often operate with separate tools, metrics, and playbooks — all of which slow collaboration and reduce the speed of response.

# Anatomy of a Modern Financial Services Attack

## How Cross-Domain Attacks Break Financial Defenses

These trends shaping today's financial threat landscape don't stay confined to isolated attack types or single environments. Adversaries have adapted. They now use the gaps between domains — identity, endpoint, cloud, SaaS apps, and data — as pathways to move undetected across environments and escalate their impact.

**This evolution has introduced a more dangerous threat model: cross-domain attacks.**

In these campaigns, adversaries chain together weaknesses across systems and security layers. They breach one domain, pivot into another, and silently build toward their objective — whether it's data theft, financial disruption, or operational sabotage. Because each step mimics legitimate activity within a different siloed environment, most security controls only catch fragments of the full campaign.

What begins as a compromised credential in one system can end with sensitive data exfiltrated from a separate cloud environment. In between, adversaries manipulate misconfigured identities, exploit tool gaps, and move laterally across trust boundaries.

## INSIDE A CROSS-DOMAIN ATTACK ON A FINANCIAL INSTITUTION

BLOCKADE SPIDER is a sophisticated, financially motivated eCrime adversary known for leveraging compromised credentials, exploiting VPN appliances, and deploying stealthy ransomware to infiltrate and extort financial institutions — and this threat actor is one of the most adept at quickly operating across domains. During a 2025 attack described in CrowdStrike's 2025 Threat Hunting Report, BLOCKADE SPIDER gained initial access to the victim's network via an unmanaged VPN appliance. The adversary quickly moved laterally across managed systems, attempting to dump credentials from a Veeam Backup & Replication configuration database, delete backups, and disrupt security controls.

When BLOCKADE SPIDER's efforts to disable the CrowdStrike Falcon® sensor were unsuccessful, the adversary rapidly adapted their strategy by pivoting to identity-based attacks. The CrowdStrike OverWatch threat hunting team traced the initial activity to a VPN service account and observed BLOCKADE SPIDER executing a DCSync attack, dumping credentials, and adding compromised accounts to Active Directory groups.

Leveraging cross-domain data from identity sources and CrowdStrike Falcon® Next-Gen SIEM, CrowdStrike OverWatch hunters tracked BLOCKADE SPIDER's movements as the adversary pivoted between unmanaged on-premises systems and cloud environments. Despite BLOCKADE SPIDER embedding deeply within the victim's infrastructure, this comprehensive visibility enabled defenders to ultimately shut down the adversary's access.

# The Modern Security Approach

The threats are clear. The stakes are existential. The question financial services leaders face is simple: How do you build defenses that can actually win against adversaries that operate faster, think strategically, and exploit every gap in traditional security architectures?

The answer isn't more tools, bigger teams, or higher budgets. It's fundamentally rethinking how security works. Forward-thinking financial institutions are moving away from the siloed paradigm of disconnected point solutions and embracing unified platforms that consolidate detection, response, and hunting across the cross-domain attack vectors — endpoint, identity, and cloud.

This transformation addresses three critical gaps that adversaries consistently exploit: fragmented visibility that creates blind spots, reactive workflows that can't match attack speed, and siloed expertise that wastes critical response time. Financial institutions that close these gaps fundamentally shift the advantage from attackers to defenders.

**The practical framework that makes this shift possible rests on six interconnected capabilities that are built for machine-speed threats, grounded in real risk, and ready to adapt as adversaries evolve.**

## 1. Unified Visibility Across the Attack Surface

Cross-domain attacks succeed because they fragment their activities across systems that don't communicate. An authentication anomaly in identity systems, combined with subtle endpoint process changes and minor cloud configuration modifications, reveals sophisticated adversary operations — but only when these events are correlated in real time.

Resilient security requires integrated data collection across domains — endpoint, identity, and cloud. A unified platform must centralize telemetry, correlate events, and deliver detections that reflect the full scope of activity.

When teams can see how a suspicious login relates to endpoint behavior or cloud access patterns, this threat intelligence fundamentally changes security operations. Analysts spend time hunting emerging threats rather than correlating data between disconnected systems. Investigation time drops significantly while threat detection accuracy increases dramatically.

## 2. Identity-First Security

Financial services environments require a new identity security model: Assume compromise and verify continuously. Every authentication event, privilege escalation, and resource access requires real-time risk assessment based on behavioral patterns, device posture, and business context.

Continuous verification goes beyond traditional MFA to assess the legitimacy of every user action throughout their session. Machine learning algorithms establish baseline behaviors for each identity, then identify deviations that indicate potential compromise. This approach catches credential misuse that static authentication controls miss entirely.

*"Today's interconnected enterprises need a security approach that can keep up with their increasing complexity. A unified security platform addresses these challenges by bridging the visibility gap between domains that adversaries seek to exploit. Providing an integrated view is essential for detecting cross-domain threats early — before they can traverse the wider ecosystem."*

***Elia Zaitsev***
*Chief Technology Officer*
*CrowdStrike*

Identity-centric operations integrate seamlessly with endpoint and cloud security to provide coordinated response. When identity security systems detect suspicious patterns, the unified platform can immediately initiate appropriate response actions, such as endpoint isolation, cloud access revocation, and forensic data collection.

## 3. Real-Time Detection and Response

Once inside, adversaries don't take leisurely coffee breaks. They escalate privileges and move laterally in seconds. Defenders who rely on manual investigations and disconnected alerts fall behind quickly.

Alert fatigue, outdated detection logic, and slow triage workflows in traditional endpoint detection and response (EDR) tools give adversaries too much breathing room to operate. Financial organizations need to reduce noise and shrink response times across the board.

A defense that operates at machine speed starts with behavioral analytics and indicators of attack (IOAs) — core capabilities of modern endpoint security platforms. Detection systems must trigger faster, prioritize high-impact activity, and tie alerts together for rapid triage. Agentic AI accelerates this process by continuously analyzing context, connecting signals, and initiating early-stage response decisions without human lag. Automated containment and incident response must cut off attacker access before they expand their footprint. Security platforms should integrate, streamline, and automate workflows across teams to make every step a high-speed execution in breaking the attack chain.

## 4. Proactive Threat Hunting and Intelligence Integration

Adversaries constantly develop new techniques, tooling, and tradecraft. That's why mature financial services security teams can't rely solely on automated detection alerts. They need proactive threat hunting to uncover stealthy activity, expose emerging attack patterns, and close gaps before attackers exploit them.

Professional hunting services bring expertise that most financial institutions cannot develop internally. These hunters understand both advanced adversary tactics and financial services operational environments. They can identify threats that specifically target banking workflows, payment systems, and regulatory compliance processes.

Real-time threat intelligence integration transforms how financial institutions detect and respond. Embedding intelligence directly into SOC operations gives analysts immediate context on sector-specific threats, which enables faster investigations and sharper responses. Dark web monitoring adds another safeguard by alerting institutions when stolen financial data or credentials appear for sale, providing early warning to contain fraud.

This integrated intelligence creates a defense network across financial services organizations. When a security provider's intelligence team identifies new threats, that knowledge becomes automated protection for every institution using the platform. Attacks that first strike one bank immediately inform safeguards for all, scaling expert knowledge across the industry and strengthening defenses against evolving adversary tactics.

## 5. Data and Cloud Protection at Scale

Financial data remains one of the highest-value targets. With the rise of cloud adoption, data now spans hybrid environments. In this complex landscape, misconfigurations, inconsistent controls, and policy drift are common — often leaving sensitive records exposed. The scale and complexity of modern cloud architectures amplify these risks.

To close these gaps and stay ahead of attackers, institutions need a unified approach to data and cloud protection — one that enforces security and supports compliance wherever data goes while securing the cloud infrastructure that houses it. This means protecting the data, as well as the cloud workloads, containers, APIs, and services, that process and store financial information.

Protecting financial data requires strong governance, consistent policy enforcement, and encryption that travels with the data. Simultaneously, securing cloud environments demands continuous monitoring of cloud configurations, robust access controls, and real-time threat detection across all cloud services.

Security teams must have visibility into where data lives — across cloud workloads, SaaS platforms, and on-premises systems — and know who accesses it, while also monitoring the security posture of the underlying cloud infrastructure. Controls must extend across environments to monitor compliance and prevent accidental exposure or malicious exfiltration. Data and cloud protection can't live in their own silos — they must integrate with detection, response, and identity systems to defend against threats targeting both the data and the cloud platforms that store it.

## 6. Simplification and Scalability

Financial institutions need to eliminate security complexity, not manage around it. Tool sprawl, siloed teams, and manual processes slow down response and drain resources. A modern platform must reduce that burden without compromising control.

Platform consolidation cuts down on vendor bloat, broken integrations, and the constant retraining loop. Fewer tools mean fewer friction points. When teams work from a single architecture, they enforce policies with consistency and eliminate the risk of misaligned configurations.

Unified interfaces give security teams full control across endpoint, identity, and cloud domains. Teams move faster when workflows stay consistent — no toggling between dashboards, no guesswork across environments. That cohesion speeds up decision-making and removes room for error.

Cloud-native platforms handle growth on demand. They scale automatically under pressure, whether it's peak transaction volume or a sudden threat spike. That elasticity keeps operations steady and prevents security from becoming a business bottleneck.

# CrowdStrike's Advantage in Financial Cyber Defense

CrowdStrike redefines financial services security with an AI-powered, cloud-native platform engineered to defeat complex, cross-domain attacks. The Falcon platform unifies endpoint security, identity protection, and cloud defense — bolstered by real-time threat intelligence and 24/7 managed threat hunting — to stop adversaries before they can disrupt critical operations or steal sensitive data.

This unified approach delivers powerful, proactive defense without adding complexity. With industry-leading capabilities built into a single platform, CrowdStrike simplifies security operations, empowering financial institutions to respond quickly, act intelligently, and stay ahead of evolving threats.

The capability framework is not theoretical — it forms the foundation of the Falcon platform through its unified architecture:

- **Unified visibility** from integrated, cross-domain telemetry with real-time correlation reveals complete attack narratives instead of fragmented alerts.
- **Identity-first security** operates through continuous behavioral analysis and risk assessment integrated with endpoint and cloud context for coordinated response to identity-based attacks.
- **AI-native intelligent automation** with CrowdStrike® Charlotte AI™ accelerates detection and response by applying autonomous reasoning to investigate threats, surface key insights, and initiate real-time actions.
- **Integrated threat intelligence** embeds real-time, sector-specific insights and dark web monitoring directly into SOC operations for rapid threat detection and fraud prevention, while creating a defense network where threats targeting one institution automatically strengthen protections across all financial services organizations.
- **Proactive hunting services** from CrowdStrike's expert-led threat hunting team — which understands financial services environments — provide real-time threat intelligence with specific remediation guidance.
- **Cloud security** delivers unified visibility and blocks threats across cloud infrastructure, applications, data, and AI models, delivering unmatched contextual visibility and breach prevention from code to cloud.
- **Data protection** functions through integrated data classification, monitoring, and protection controls that span hybrid environments while maintaining consistency with unified policy enforcement.
- **Simplified management** within a single platform enables consolidation, eliminates vendor complexity, reduces training overhead, and provides consistent user experiences across all security domains through cloud-native architecture that scales automatically.

# Real-World Results from the Front Lines of Financial Security

Real transformation shows up in the numbers. When financial institutions replace fragmented security tools with CrowdStrike Falcon, the operational changes are immediate and measurable.

***"CrowdStrike delivers real outcomes. These customers prove that unified security isn't a tradeoff — it's a leap forward."***

## Commercial Bank of California

**100%**
ransomware protection

**34%**
reduction in cyber insurance premiums

**24/7**
managed detection and response

Before switching to CrowdStrike, the bank managed more than 12 disconnected tools. Each one added noise, complexity, and risk. Falcon replaced the fragmentation with a single platform that spans endpoint, identity, and workload security.

***"The Falcon platform has allowed us to consolidate our security toolbox. It yields big savings for us, but more importantly, it allows us to focus. When an alert hits from the Falcon platform, we're able to address it without being distracted by other tools."***
***–Kevin Tsuei, SVP Information Security Officer***

Read the case study

## Mercury Financial

**89%**
faster threat detection and remediation

**8x**
improvement in incident management

Mercury Financial transformed its response times by consolidating its defenses on the CrowdStrike Falcon platform. Analysts gained a clear view across domains and dramatically improved operational efficiency.

***"By giving us end-to-end protection, CrowdStrike has helped us build a culture of security."***
***–Alex Arango, Head of Cyber Threat Management and Deputy CISO***

Read the case study

### Greenhill

| 75% | $300K |
| --- | --- |
| fewer alerts | in annual savings |

Greenhill cut down noise and cost by relying on Falcon as its global security foundation. The firm replaced its EDR and antivirus tools and eliminated the need for multiple vendors.

***"We probably rely on the Falcon platform more than anything else for our security. We have it deployed globally."***
***–John Shaffer, CIO***

Read the case study

# Conclusion

Financial institutions are prime targets — and adversaries are only getting faster, stealthier, and more coordinated. To defend against the modern threat landscape, the industry needs a different model: a unified security approach that consolidates real-time protection across endpoints, identities, and cloud workloads.

That's the foundation of the CrowdStrike Falcon platform.

From identity misuse to cloud intrusions, lateral movement, and ransomware, the Falcon platform was architected to close the gaps attackers exploit. One sensor. One console. One data model. That unified design powers faster detection, coordinated response, and operational efficiency that multiplies over time.

Cyber threats aren't going away. But the financial sector doesn't have to stay reactive. With the right architecture, the right intelligence, and the right platform, security leaders can stop breaches at the speed and scale of today's adversaries — and regain the advantage.

**See the power of unified security in action.**

# About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

**CrowdStrike: We stop breaches.**

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/