DEFENDING THE FINANCIAL SUPPLY CHAIN

2025 Report: Strengths and Vulnerabilities in Top Fintech Companies

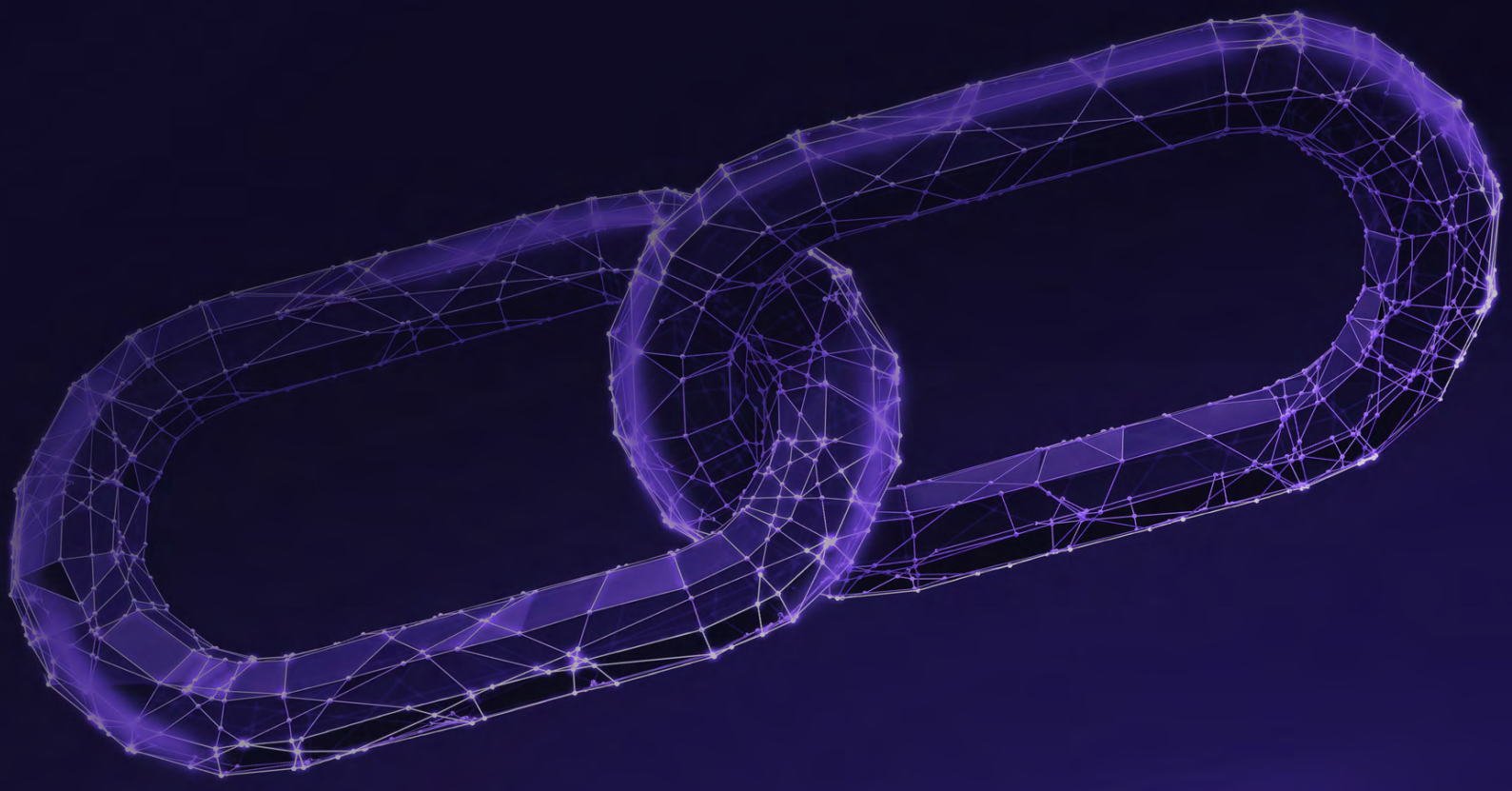


SecurityScorecard

SecurityScorecard

DEFENDING THE FINANCIAL SUPPLY CHAIN

2025 Report: Strengths and Vulnerabilities in Top Fintech Companies



EXECUTIVE SUMMARY

This report presents a comprehensive analysis of the cybersecurity posture of 250 of the world's top fintech companies. As critical enablers of digital finance, these organizations play a central role in the operational infrastructure of financial institutions. Their unique position—at the intersection of finance and technology—places them at heightened risk from both direct cyberattacks and supply chain compromises.

Drawing on SecurityScorecard's security telemetry, breach data, and scoring methodology, the report identifies areas of strength, persistent vulnerabilities, and systemic risk patterns across the fintech sector. It also provides practical insights tailored to security leaders, third-party risk teams, and compliance professionals tasked with managing cybersecurity risk in a complex, interconnected ecosystem.

KEY FINDINGS



Fintech companies demonstrate above-average cybersecurity performance, with a median security score of 90 and over half (55.6%) earning an "A" rating—the highest distribution recorded across any industry sample to date.



Technology products and services enabled 63.9% of third-party breaches, with file transfer software and cloud platforms being the most frequent points of compromise.



Despite strong ratings, 18.4% of companies experienced at least one publicly reported breach. 28.2% of those breached companies had multiple breaches and accounted for 50.7% of all breach incidents.



The weakest security areas were Application Security and DNS Health, with nearly half the companies scoring lowest in the forner category.



41.8% of reported breaches were involved third-parties. An additional 11.9% were fourth-party breaches, a figure more than double the global cross-industry average.



Digital Assets and Business Process Solutions segments showed the lowest overall security scores, raising concerns about potential exposure in areas such as cryptocurrency, fraud management, and back-office automation.

STRATEGIC INSIGHTS BY ROLE

Chief Risk Officer

- Regions with lower GDP do not always equate to higher risk; some firms in India, Eastern Europe, and Brazil outperformed peers in more affluent markets.
- Internal misconfigurations and employee-driven errors still contribute to a significant portion of incidents—underscoring the need for continuous compliance enforcement.
- Breach reporting patterns confirm that repeat incidents are a reliable predictor of risk; this should be integrated into compliance review processes and SLAs.

Security Operations Center (SOC) Teams

- Fintech vendors are frequent targets of typosquatting, malware campaigns, and credential harvesting, especially in the Payments and Digital Assets segments.
- Application security gaps—including unsafe subresource integrity and misconfigured object storage—are common and exploitable.
- DNS misconfigurations (e.g., missing SPF records) and exposed session cookies should be red-flagged in supplier monitoring.

Third-Party Risk Managers (TPRM)

- Third and fourth-party risks are systemic within fintech. Vendor ecosystems must be assessed not only on direct exposure but also on their dependencies.
- Technical enablers like file transfer software (e.g., MOVEit) and cloud services remain high-risk categories that require continuous evaluation.
- Credential stuffing and phishing risk should be evaluated in the context of shared customers across fintech platforms.

Chief Information Security Officers (CISOs)

- Strong in-house controls are not sufficient when third-party breach vectors account for nearly half of all incidents.
- Vendors with a breach history—especially repeat incidents—should be weighted more heavily in security risk assessments.
- High security scores do not guarantee low risk; performance must be contextualized with vendor function, breach record, and segment-level trends.

Fintech companies lead in security fundamentals, but their interconnected nature with financial systems creates concentrated risk points. This report provides evidence-based methods to identify vulnerable vendors, strengthen common infrastructure, and implement specific security controls that reduce exposure in our digital financial ecosystem.

TABLE OF CONTENTS

Introduction . . . 05

FinTech Cybersecurity Posture Overview . . . 06

Third- and Fourth-Party Risk Landscape . . . 08

Breach Trends and Threat Actor Findings . . . 10

Sector-Specific Risk Insights . . . 12

Segment Spotlights . . . 13

Geographic Risk Insights . . . 15

Most Common Risk Factors . . . 17

Interpretation and Risk Implications . . . 18

Specific Technical Issues . . . 20

What these Failures Mean . . . 21

Typosquatting and Credential Leakage . . . 23

Malware and Compromised Systems . . . 25

Attack Enabled Breakdown . . . 27

Credential Stuffing and the Financial Supply Chain . . . 30

Recommended Security Controls . . . 32

Summary of Findings . . . 36

Appendix . . . 38

INTRODUCTION

Fintech companies are now essential components of the global financial infrastructure. Originally positioned as disruptive upstarts, many have evolved into indispensable service providers, powering payments, wealth management, compliance, fraud detection, and more. At the same time, traditional financial institutions increasingly rely on these firms to modernize their systems and stay competitive.

This rapid integration has created a new kind of interdependency—one where vulnerabilities in a single vendor can cascade across the broader financial ecosystem. As this report shows, even fintech companies with strong internal cybersecurity programs can expose their partners to significant third-party and fourth-party risks.

WHY FINTECH IS UNIQUELY EXPOSED

Two forces converge in fintech: the high-value targeting profile of the financial services sector and the vast, dynamic attack surfaces typical of modern technology firms. Unlike industries still tethered to physical infrastructure, fintech operates almost entirely in cyberspace. From neobanks to crypto exchanges, the business model is inherently digital, always connected, and increasingly reliant on code and cloud.

This means:

- Financial institutions are outsourcing critical functions to third parties operating in a fast-moving, high-risk digital environment.
- Attackers can bypass hardened financial networks by exploiting weaker links in fintech vendors or their own supply chains.
- Even companies with strong security ratings can still fall victim to indirect breaches originating from poorly secured partners, software libraries, or service providers.

The risk is not theoretical. Data from SecurityScorecard's broader research shows that financial services and healthcare are uniquely impacted by breaches originating in industry-specific vendor relationships. This report builds on those findings, focusing specifically on fintech's role within the financial supply chain.

METHODOLOGY OVERVIEW

This report evaluates 250 of the world's top fintech companies, spanning multiple regions and industry segments. Each company was assessed based on observable cybersecurity signals across ten core risk factors. The analysis also includes data on malware infections, credential leaks, typosquatting domains, publicly reported breaches, and third- and fourth-party breach attribution.

A detailed breakdown of the scoring methodology and data sources is included in the Appendix.

STRUCTURE OF THIS REPORT

The following sections provide:

- A quantitative assessment of the overall cybersecurity posture across the fintech sector.
- Analysis of third- and fourth-party breach patterns, vectors, and enablers.
- A breakdown of key risk factors and the most common technical issues observed.
- Sector-specific and geographic comparisons.
- Actionable insights for security and risk professionals responsible for protecting financial operations and vendor ecosystems.

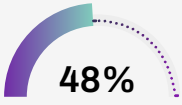
This report is designed to help organizations prioritize controls, evaluate vendors, and strengthen operational resilience across the financial supply chain.

FINTECH CYBERSECURITY POSTURE OVERVIEW

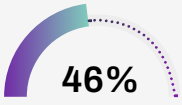
SECTOR-WIDE SECURITY PERFORMANCE

Fintech companies in this sample recorded the highest overall cybersecurity performance observed by SecurityScorecard in the past year. The median score was 90, and the mean score was 89—both significantly above the global cross-industry average of 85. More than half (55.6%) of the companies earned an "A" rating, a higher proportion than any other industry segment assessed to date.

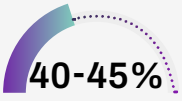
TECH VENDOR COMPARISON



Only **48%** of healthcare, pharmaceutical, and biotech firms achieved an "A".



46% of companies in the S&P 500 reached that mark.



40–45% was typical for top federal contractors and technology vendors.

OTHER INDUSTRY-SPECIFIC BENCHMARK SCORES FURTHER HIGHLIGHT FI NTECH'S LEADERSHIP

Healthcare	S&P 500	Federal Contractors
88/89	86/88	86/88
Energy and Insurance	Aviation	Top 150 Tech Vendors
88/89	85/88	84/87

In total, **87.2%** of fi ntech fi rms scored in the A–B range, with just **12.8%** falling into the C–F categories—making this one of the strongest distributions SecurityScorecard has recorded in any of its industry reports.

INTERPRETING THE RATING CURVE

Despite the high ratings, the dataset was statistically left-skewed. A small number of very low scores brought down the average. In these outlier cases, the lowest performers correlated closely with weak patching cadence, low IP reputation, and persistent application security misconfigurations—indicators of broader systemic issues.

Fintech companies, by and large, appear to prioritize and invest in baseline security. But strong average scores can obscure serious, localized weaknesses. As subsequent sections of this report will show, segments such as Digital Assets and Business Process Solutions exhibit more frequent misconfigurations, breach recurrence, and credential leakage—despite falling within the broader high-score average.

RATING CATEGORIES AND BREACH LIKELIHOOD

SecurityScorecard's internal breach correlation model provides additional context for understanding score categories:

- A "B" rating is associated with a **2.9x higher breach** likelihood than an "A"
- A "C" rating: **5.4x more likely to breach** than "A"
- "D" ratings: **9.2x more likely**
- "F" ratings: **13.8x more likely**

Even within a generally high-performing sector, any downward shift in a vendor's score is a statistically significant risk signal.

STRATEGIC INSIGHTS BY ROLE

CISOs

- High scores across vendors do not equal low risk—outliers within a strong field are still breach-prone.
- Use score trends over time and segment-specific comparisons (Payments vs. Digital Assets) to triage vendors for deeper review.

SOC Teams

- Even companies scoring in the "A" range may be hiding critical technical weaknesses. Outliers in patching cadence and app security (detailed in later sections) should be monitored closely, regardless of overall score.

Third-Party Risk Managers

- Use the breach correlation model to guide onboarding thresholds and contract review flags.
- "B" vendors carry nearly 3x the breach probability of "A" vendors—flag accordingly during vendor tiering.

GRC Professionals

- A company's score is predictive of breach risk and can be used as a continuous monitoring metric in compliance workflows. The concentration of low scores in specific functional segments (e.g., BPS) is relevant for risk segmentation and policy prioritization.

THIRD AND FOURTH-PARTY RISK LANDSCAPE

THE SUPPLY CHAIN EXPOSURE

Third-party and fourth-party breaches remain a significant and escalating source of risk in the fintech sector. Among the 67 publicly reported breaches analyzed in this report, 41.8% were the result of compromises through third-party relationships. A further 11.9% were fourth-party breaches, involving a vendor of a vendor—a figure more than double the cross-industry average of 4.5%.

This elevated exposure reflects the structural interdependence within fintech ecosystems, where service layers often stack atop one another. Risk is no longer isolated to immediate vendors; indirect relationships increasingly serve as attack paths.

BREACH RECURRENCE AND RISK PREDICTION

Breach patterns show a clear correlation between incident frequency and third-party compromise:

- Just 28.2% of breached companies experienced multiple breaches, but those breached companies accounted for 50.7% of all incidents.
- Half of the third-party breaches (14 out of 28) occurred at organizations with repeat breach histories.

This pattern confi rms a critical risk signal: **a history of breaches is one of the most reliable predictors of future incidents**, including those involving supply chain vectors.

BREAKDOWN OF BREACH ENABLERS

SecurityScorecard categorized the 28 third-party breaches based on the nature of the enabling relationship. The findings show:

- **63.9% of enabling relationships were technical in nature**, such as software, platforms, or IT services.
- Among these, cross-industry technologies were slightly more common than fintech-specific tools, but the margin was narrow.
- **36.1% were non-technical relationships**, such as financial partnerships, banking infrastructure, or legal/marketing support services.

Notably, credential stuffing attacks—where compromised customer accounts are reused across platforms—were included in this analysis, due to their scale and impact. These campaigns represent a form of “indirect third-party breach,” especially when they target users across multiple fintech platforms with shared login behavior.

COMMON ENABLING TECHNOLOGIES

Among the third-party breach incidents, the most frequent enabling technologies were:

- File transfer software (e.g., MOVEit, GoAnywhere).
- Cloud data storage services.
- Customer communication platforms.
- Payment processing and accounting software.
- Password managers and collaboration tools.

In multiple cases, these tools were compromised by ransomware groups who used them to gain broader access across customer networks.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Breach history should be a core input in vendor scoring and renewals—especially for vendors who serve critical functions or possess sensitive data.
- Fourth-party risk is no longer optional to monitor. Require vendors to disclose downstream critical dependencies.

SOC Teams

- Monitor for shared infrastructure across fintech vendors. Credential reuse and cross-platform phishing may originate from unrelated vendors. Watch for third-party file transfer or storage tools used internally—these are high-risk vectors in supply chain attacks.

Third-Party Risk Managers

- Triage vendors not just by function, but by historical breach performance and known technical enablers.
- Elevate scrutiny of vendors using common breach-prone tools (e.g., MOVEit, cloud file sharing platforms).

GRC Professionals

- Incorporate fourth-party breach patterns into compliance policy and vendor due diligence. Leverage breach history as an evidence-based risk tiering input—not just a reactive metric.



BREACH TRENDS AND THREAT ACTOR FINDINGS

BREACH FREQUENCY AND RECURRENCE

Among the 250 fintech companies assessed, 46 experienced at least one publicly reported breach—an overall rate of 18.4%. While this is considered moderate by cross-industry standards, the real concern lies in breach concentration: just 13 of these companies (28.2% of breached entities) were responsible for 50.7% of all breach incidents.

This recurrence pattern is consistent with findings in other high-risk sectors, such as U.S. federal contractors. The implication is clear: **a prior breach is not a completed event—it's a future indicator.**

Organizations with repeat breaches were also significantly more likely to experience third-party breaches. Nine of the thirteen firms with two or more breaches had at least one confirmed supply chain-related incident.

INSIDER THREATS AND INTERNAL ACTORS

While the majority of breaches were driven by external attackers, a significant portion—23.5% of attributed incidents—were traced to malicious insiders. These actors have a unique advantage: they can bypass the strong perimeter controls that many fintech firms are known for.

Insider attacks often exploit overlooked internal systems or abuse legitimate credentials. The effectiveness of these breaches reinforces the need for role-based access controls, continuous behavior monitoring, and strict offboarding procedures.

MALWARE AND ENDPOINT EXPOSURE

Malware detections were comparatively low among the 250 companies:

- Only **7.6%** had observable signs of malware infections or compromised machines.
- Adware accounted for **6%.**
- Other threats such as ransomware, information stealers, or TOR-related activity were each observed in less than **1% of cases.**

These low rates likely reflect strong baseline controls. However, they may also indicate underreporting or insufficient visibility. Notably, in a few outlier cases (particularly one Chinese company), malware presence was significantly elevated—correlating with poor overall security hygiene.

Even limited endpoint compromise can act as a foothold for more sophisticated attacks. The presence of malicious repurposing, including TOR exit nodes and scanning infrastructure, suggests potential use in broader botnet or proxy operations.



RANSOMWARE AND THE SUPPLY CHAIN

Ransomware was rare across the dataset—but when it did occur, it strongly aligned with third-party breach vectors. In 70% of ransomware-related breaches, attackers gained access through a partner or external service.

This pattern reflects a broader shift in ransomware operations:

- Less reliance on direct compromise of hardened networks.
- More emphasis on scalable, indirect entry via shared services or supplier compromise.
- Preference for long-term access, data exfiltration, and quiet persistence over noisy encryption campaigns.

Attribution data from the dataset reinforces these trends. Of the 67 total breaches, 17 were linked to specific threat actors. Ransomware groups and data disclosure operations accounted for over half (53%) of attributed incidents, while insider threats accounted for 23.5%.

Notable threat actors included:

- **C10p ransomware:** 3 confirmed breaches.
- **UNC5537:** 2 breaches.
- **LockBit, AlphV/BlackCat, Abyss, RansomHouse, Conti:** 1 breach each.
- **UNC3944, pompompurin, abyss0:** 1 breach each.

While state-sponsored attackers were notably absent from attribution data, this aligns with known patterns. State-sponsored groups tend to avoid financially motivated targets unless pursuing espionage or geopolitical disruption, with the major exception of North Korea, which uses financial attacks as a source of revenue. The dominance of financially driven actors underscores the unique appeal—and risk—of fintech vendors in the supply chain.

STRATEGIC INSIGHTS BY ROLE

CISOs

- A breach is not a one-time event. Recurrence should be monitored across vendors, and internally as a red flag.
- Insider threats remain active. Detection programs should extend beyond perimeter defenses and include behavior analytics.

SOC Teams

- Low malware detection doesn't mean low threat. Even minimal endpoint compromise can signal a breach-in-progress.
- Monitor for TOR, adware, and scanning behavior—these may indicate compromised internal assets repurposed for external operations.

Third-Party Risk Managers

- Vendors with repeat breaches are statistically more likely to be vectors for third-party risk.
- Review vendor breach history as part of annual assessments—not just onboarding.

GRC Professionals

- Breach history and internal compromise indicators should be formalized into compliance triggers.
- Insider threat programs should be considered mandatory in high-sensitivity environments like fintech.

SECTOR-SPECIFIC RISK INSIGHTS

PERFORMANCE ACROSS FINTECH SEGMENTS

The 250 fintech companies in this assessment were classified into eight functional categories. While overall security scores across the sector were strong, performance varied meaningfully between segments. The lowest-scoring groups—**Digital Assets** and **Business Process Solutions (BPS)**—are also among the most consequential from a risk perspective due to their role in enabling access, automation, and financial transactions.

SEGMENT SCORE SUMMARY (MEAN/MEDIAN):

SEGMENT	MEAN	MEDIAN
Alternate Finance	**90**	**92**
Wealth Technology	**90**	**91**
Neobanking	**89**	**92**
Payments	**89**	**91**
Financial Planning	**88**	**93**
Banking-as-a-Service & Open Banking	**88**	**90**
Business Process Solutions (BPS)	**87**	**88**
Digital Assets	**87**	**88**

The median scores suggest high overall performance, but outliers—and their potential impact—are concentrated in specific segments.

SEGMENT SPOTLIGHTS

BUSINESS PROCESS SOLUTIONS (BPS)

This segment includes vendors providing accounting software, invoicing platforms, payroll tools, and compliance automation. These vendors often have system-level access to their clients' internal processes.

- **Lowest average score of all segments.**
- Common vulnerabilities include exposed web assets and misconfigured DNS.
- Their role as intermediaries makes them attractive entry points for attackers targeting financial institutions.

Risk Implication: A compromise at a BPS vendor can enable wide-scale access to multiple customer environments.

DIGITAL ASSETS

This segment includes cryptocurrency exchanges, wallets, and blockchain-based platforms.

- Low scores despite handling high-value, easily exfiltrated assets.
- Frequently targeted by typosquatting domains (high phishing exposure).
- Lower credential leakage than Payments, but still at risk due to user reuse patterns attractive entry points for attackers targeting financial institutions.

Risk Implication: Digital Assets firms face disproportionate targeting due to the liquidity and anonymity of crypto funds.

PAYMENTS

Payments firms—including online processors, gateways, and traditional card providers—were highly represented among:

- Credential leaks (often customer accounts).
- Typosquatting campaigns (e.g., spoofed domains for phishing).

Risk Implication: Their brand visibility and user base make them a favored target for phishing, credential stuffing, and social engineering.

FINANCIAL PLANNING

This segment showed a wide distribution in scores—highest median (93), but with some low-end outliers. The volatility suggests uneven investment in security across providers.

Risk Implication: High variation in controls across similar service providers may complicate vendor selection.

OTHER SEGMENTS
(ALTERNATE FINANCE, WEALTHTECH, NEOBANKING, BAAS/OPEN BANKING)

These groups generally performed above the sector average with few outliers. However, they often operate in newer markets or regulatory regimes, which can introduce additional context-specifc risks not captured by baseline ratings alone.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Prioritize due diligence and technical validation for BPS and Digital Assets vendors, regardless of self-reported ratings.
- For Payments vendors, evaluate typosquatting and customer credential exposure as part of incident response planning.

SOC Teams

- Expect typosquatting, phishing, and credential attacks against customer-facing fintech vendors—especially in the Payments and Digital Assets segments. Monitor web and DNS hygiene for BPS tools integrated with internal systems.

Third-Party Risk Managers

- Elevate risk tiers for vendors in BPS and Digital Assets categories.
- Where high score volatility exists (e.g., Financial Planning), implement compensating controls and contract safeguards.

GRC Professionals

- Use segment-level risk data to prioritize vendor reviews and align internal policy.
- Validate that segment-specific risks (e.g., crypto regulation gaps) are covered in compliance assessments.



GEOGRAPHIC RISK INSIGHTS

REGIONAL SCORE PERFORMANCE

Fintech security performance varies significantly by geography, but not always in predictable ways. While high-income regions generally perform well, several emerging markets have fintech ecosystems that outperform expectations—driven by local innovation, technical expertise, or focused regulatory regimes.

REGIONAL SECURITY SCORE SUMMARY (MEAN/MEDIAN):

REGION	MEAN	MEDIAN
Eastern Europe	**91**	**92**
South & Southeast Asia	**90**	**92**
Oceania	**89**	**91**
North America	**89**	**90**
Western Europe	**89**	**90**
Latin America & Caribbean	**89**	**89**
Northeast Asia	**84**	**87**
Middle East & Africa	**83**	**86**

These scores place Eastern Europe and South/Southeast Asia at the top of the distribution—despite many countries in these regions being classified as developing economies or emerging markets. In contrast, Northeast Asia scored lower than expected, primarily due to weaker performance by firms in China.

WHAT EXPLAINS THESE TRENDS?

EASTERN EUROPE

High technical literacy and a strong base of security engineering talent have enabled fintech firms in countries like Estonia, Romania, Poland, and Hungary to maintain strong cybersecurity hygiene, despite less access to capital and security investments.

SOUTH AND SOUTHEAST ASIA

India and Singapore lead this region's high performance. India's fintech sector has rapidly matured and adopted strong internal controls, while Singapore benefits from one of the most robust regulatory environments in the world.

BRAZIL AND LATIN AMERICA

Brazil, often viewed as a high-fraud environment, emerged as a relative security leader in Latin America. Local fintech firms showed stronger-than-expected DNS and application security maturity.

CHINA AND NORTHEAST ASIA

Chinese fintech firms were a major drag on regional averages, showing poor performance across patching cadence, DNS configurations, and IP reputation.

SUB-SAHARAN AFRICA

Weak security scores were concentrated in a small number of firms in this region. While not representative of the entire region, these outliers had sufficient impact to lower the overall average.

INTERPRETING GEOGRAPHY AS A RISK FACTOR

The data makes clear that geographic assumptions are no substitute for evidence. Some fintechs in low-GDP regions outperform their peers in highly developed markets. Conversely, some of the lowest performers were headquartered in markets with mature economies and regulatory frameworks.

Vendor location should inform risk discussions, but should never override actual security telemetry.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Don't rely on country-of-origin as a proxy for security quality. Use real-time scoring and breach history to validate risk.
- Be prepared to defend vendor selections in high-performing but non-traditional regions (e.g., Eastern Europe).

SOC Teams

- Monitor regional vendors based on observed behavior—not economic profile.
- Pay extra attention to network traffic anomalies or patching delays from vendors in regions with lower scores.

Third-Party Risk Managers

- Implement geographic risk overlays, but always calibrate with actual technical scores.
- Encourage diverse vendor sourcing based on performance, not assumptions.

GRC Professionals

- Ensure that geographic risk assessments include both objective telemetry and regulatory context.
- Be cautious of bias in policy frameworks that assign higher baseline risk based solely on economic classification.

MOST COMMON RISK FACTORS

RISK FACTOR DISTRIBUTION

SecurityScorecard assigns scores across 10 core cybersecurity risk factors. In this assessment, six factors emerged as the most common weak points for fintech companies. These represent the most frequent sources of score degradation, even among high-performing organizations.

MOST FREQUENT LOWEST-SCORING RISK FACTORS

RISK FACTOR	% OF COMPANIES	MEAN SUB-SCORE	MEAN SUB-SCORE
Application Security	**46.4%**	**80**	**81**
DNS Health	**31.6%**	**76**	**78**
Network Security	**15.2%**	**81**	**82**
Patching Cadence	**3.6%**	**74**	**77**
Endpoint Security	**2.4%**	**84**	**88**
IP Reputation	**0.8%**	**46**	**46**

While Application Security and DNS Health were the most frequently observed weaknesses, companies with low Patching Cadence or IP Reputation scored significantly worse overall. These issues, although less common, tend to indicate broader structural deficiencies in cybersecurity posture.

INTERPRETATION AND RISK IMPLICATIONS

APPLICATION SECURITY

Fintech companies often expose complex web applications, APIs, and mobile interfaces to customers and partners. This creates persistent risks related to:

- Unsafe third-party script handling (e.g., Subresource Integrity)
- Misconfigured object storage permissions
- Unsecured redirect chains
- Weak session cookie configurations

These issues increase the likelihood of injection attacks, data leakage, and credential theft.

DNS HEALTH

DNS misconfigurations are a recurring issue, especially missing or malformed Sender Policy Framework (SPF) records. This exposes companies to:

- Email spoofing
- Phishing attacks
- Reduced deliverability of security-critical communications

NETWORK SECURITY

Companies with poor network security scores often have exposed or misconfigured services (e.g., open ports, legacy protocols) that create opportunities for reconnaissance or unauthorized access.

PATCHING CADENCE

Although only 3.6% of companies scored lowest here, those that did had mean overall security scores well below the sector average. Delayed patching increases the risk of known exploit vectors being used before defenses are in place.

IP REPUTATION

Low-scoring companies in this category often host—or have hosted—malicious activity, such as malware distribution, botnet command-and-control, or spam infrastructure. These issues damage trust and may reflect compromised internal systems.

SCORE WEAKNESS AS A RISK SIGNAL

Organizations that performed worst in either Patching Cadence or IP Reputation consistently had some of the lowest overall security scores in the entire dataset. This suggests these two areas may serve as early indicators of broader failures across an organization's security program.

Even among high-scoring fintechs, a single underperforming domain can signal outsized exposure—especially when that weakness relates to application-layer security or core internet infrastructure.



STRATEGIC INSIGHTS BY ROLE

CISOs

- Treat consistently poor risk factors—especially AppSec and DNS—as indicators of latent breach risk.
- For vendors with high overall scores, request visibility into sub-score trends to catch blind spots.

SOC Teams

- Prioritize monitoring and hardening in AppSec and DNS configurations—these are the most common and exploitable gaps.

  Where patching cadence is weak, increase alerting for known exploit activity against public-facing systems.

Third-Party Risk Managers

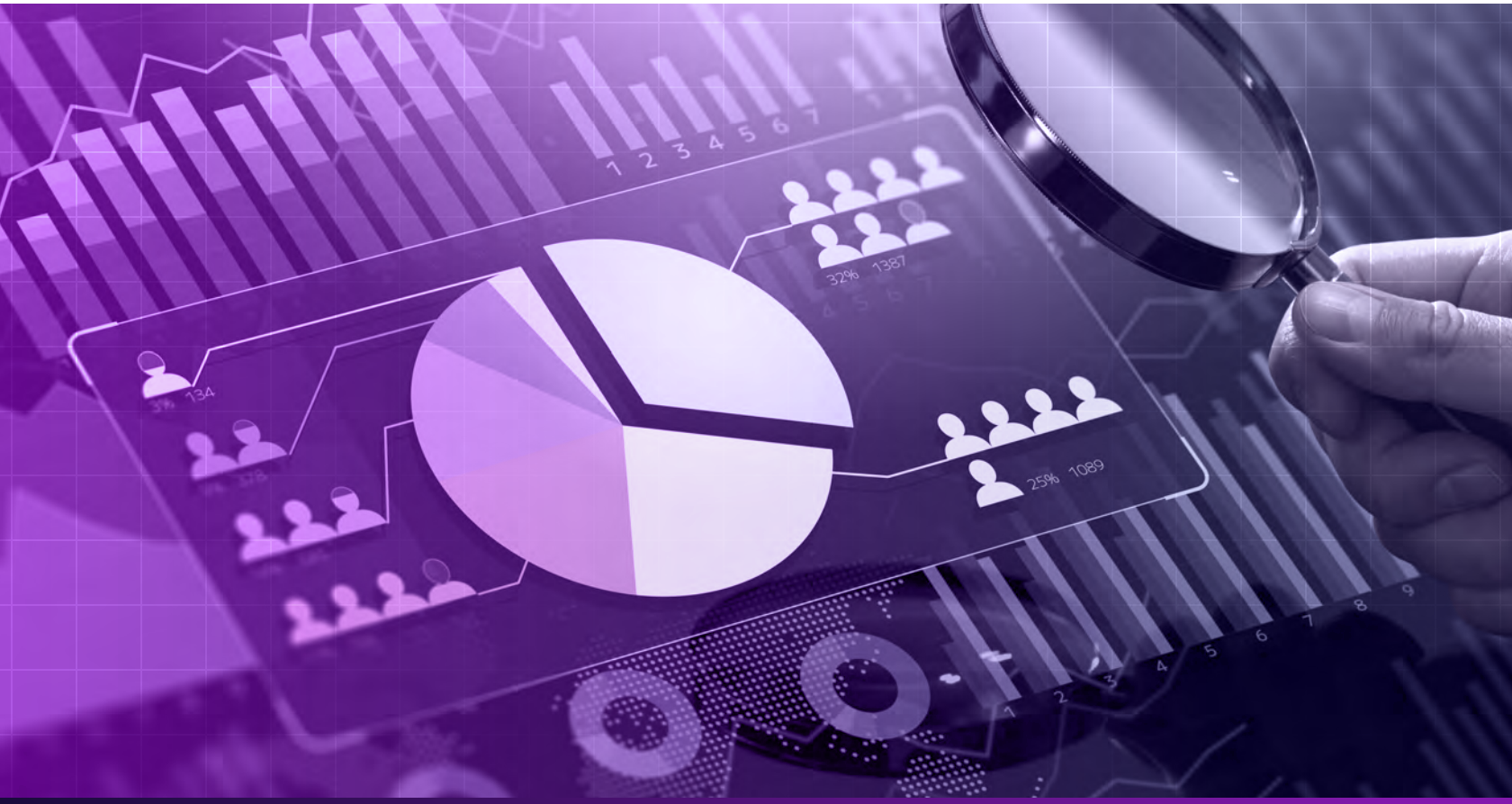
- Require vendors to disclose recent remediation efforts for their lowest-scoring risk factor.

  Use AppSec and DNS scores as critical inputs in tiering and review cadence, particularly for customer-facing vendors.

GRC Professionals

- Incorporate score breakdowns into compliance workflows—overall ratings may mask high-risk configurations.

  Benchmark internal control effectiveness against these common weak points to identify audit priorities.



SPECIFIC TECHNICAL ISSUES

MOST COMMON HIGH-IMPACT ISSUES

Across the fintech sector, score degradation is most often linked to a narrow set of recurring technical failures. These are not exotic vulnerabilities or sophisticated exploits. They are foundational misconfigurations—simple, observable, and highly preventable.

SecurityScorecard identified the individual issues that had the most negative impact on each company's score. These top issues map primarily to three risk areas: Application Security, DNS Health, and Network Security.

TOP TECHNICAL ISSUES BY FREQUENCY

ISSUE	CATEGORY	% OF COMPANIES
SSL/TLS service supports weak protocol	**Network Security**	**32%**
Unsafe Subresource Integrity implementation	**Application Security**	**13.6%**
Website references misconfigured object storage	**Application Security**	**11.2%**
HTTP present in redirect chain	**Application Security**	**10.8%**
Missing SPF record	**DNS Health**	**10%**
SPF softfail without DMARC	**DNS Health**	**3.6%**
Session cookie missing HTTPOnly attribute	**Application Security**	**6%**
Session cookie missing Secure attribute	**Application Security**	**2%**
Outdated web browser observed	**Endpoint Security**	**3.2%**
SPF record found ineffective	**DNS Health**	**1.2%**

WHAT THESE FAILURES MEAN

WEAK SSL/ TLS CONFIGURATIONS

The most common issue, affecting nearly one-third of companies, was support for deprecated cryptographic protocols in their SSL/TLS implementations.

These configurations:

- Allow downgrade attacks.
- Undermine encryption integrity.
- Are widely targeted by automated scanning tools.

UNSAFE SUBRESOURCE INTEGRITY (SRI)

SRI is intended to validate the integrity of third-party scripts. Improper implementation enables attackers to inject malicious JavaScript via trusted sources, leading to cross-site scripting (XSS) and data exfiltration.

OBJECT STORAGE MISCONFIGURATION

Exposed or poorly controlled cloud object storage—such as Amazon S3 buckets—can leak sensitive data or enable file replacement attacks. These are frequent entry points for phishing kits, malware, and unauthorized access.

INSECURE REDIRECT CHAINS

Use of HTTP in redirect sequences downgrades security, enabling attackers to intercept or alter communications. Redirect misconfigurations also facilitate phishing and session hijacking.

DNS SPF/DMARC ISSUES

Poorly configured or missing Sender Policy Framework (SPF) records make email domains vulnerable to spoofing. When not paired with a properly enforced DMARC policy, attackers can send fraudulent messages that appear to come from trusted fintech domains.

SESSION COOKIE MISCONFIGURATIONS

Missing Secure and HTTPOnly attributes on session cookies allows:

- Theft of session tokens over non-encrypted channels (lack of Secure).
- Access to cookies via client-side scripts (lack of HTTPOnly). These gaps enable session hijacking and man-in-browser attacks.

IMPLICATIONS FOR DETECTION AND RESPONSE

These issues are detectable with non-invasive, external scans—yet remain widely unremediated. Their persistence in a sector that scores highly overall indicates a breakdown not in capability, but in prioritization.

Fintech vendors may pass surface-level assessments while still exposing themselves—and their partners—to attack paths that require no advanced tooling to exploit.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Demand technical validation of security claims during procurement—not just certification or score summaries.
- Prioritize remediation of known high-impact issues over low-risk policy gaps.

SOC Teams

- Tune detections to flag weak SSL/TLS handshakes, redirect anomalies, and unexpected cloud object access patterns.
- Regularly validate cookie security headers and SPF/DMARC configurations.

Third-Party Risk Managers

- Require vendors to provide evidence of remediation for these common misconfigurations—especially if they appear in scan results.
- Elevate vendors with persistent SPF, TLS, or redirect issues for manual review.

GRC Professionals

- Align internal audit and compliance controls with known exploit vectors—not just control checklists.
- Advocate for independent testing and scoring validation across business-critical vendors.



TYPOSQUATTING AND CREDENTIAL LEAKAGE

TYPOSQUATTING EXPOSURE

Typosquatting—the practice of registering deceptive lookalike domains—remains a widespread threat across the fintech ecosystem. These domains are typically designed to mislead users, harvest credentials, or host malware.

In this study:

- **184 of 250 companies (73.6%)** had at least one suspected typosquatting domain targeting their brand.
- Among those targeted, the **median number of typosquatted domains was 162.**
- The distribution was sharply right-skewed, with some companies having **as many as 2,300 spoofed domains.**
- The highest concentrations were associated with **U.S.-based companies** in the **Payments** and **Digital Assets** segments.

Well-known firms like Visa, Mastercard, PayPal, and Coinbase had among the highest volumes of spoofed domains. Attackers appear to prioritize brands with:

- High consumer visibility
- Financial transaction functionality
- Known login interfaces or wallet access points

These domains often mimic official URLs by altering a few characters or using similar-looking alphabets (e.g., substituting "l" for "1", or using Cyrillic letters). Their goals include phishing, malware distribution, and credential theft.

CREDENTIAL LEAKAGE

In parallel with domain spoofing, compromised credentials continue to circulate in dark web marketplaces and public breach repositories. These credentials, often obtained via phishing or infostealers, are frequently reused across fintech platforms—creating risk across companies even when their own systems remain uncompromised.

Payments firms, including PayPal, Payoneer, and Alipay, had the highest volumes of exposed credentials. While Digital Assets firms also appeared in the data, they had lower relative volumes—likely due to more common use of MFA or passwordless authentication methods in that segment.

Key findings:

- **198 of 250 companies (79.2%) had at least one compromised credential** in the observed datasets.
- Companies with leaked credentials had a **median of 26** and a **mean of 912.**
- Several firms had over **30,000 compromised credentials** associated with their domain.
- In many cases of companies with large numbers of compromised credentials, these appear to be **customer credentials**, not employee accounts.



COMBINED RISK: DOMAIN SPOOFING + CREDENTIAL THEFT

In many cases, attackers use typosquatted domains as phishing lures to steal credentials. This means the two datasets are not isolated—they represent two stages of a common attack chain:

1. Spoofed domain captures credentials
2. Credentials are reused or resold for credential stuffing, fraud, or account takeover

The combination of high consumer traffic, weak user-side password hygiene, and impersonation opportunities creates significant third-party risk—even when the fintech platform itself remains uncompromised.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Treat brand spoofing as a direct threat to customer trust and user safety—not just a reputational issue.
- Monitor leaked credential volumes tied to company domains and require customer-side MFA where possible.

SOC Teams

- Track registrations of spoofed domains and monitor for SSL cert issuance or hosting activity linked to known phishing infrastructure.
  Flag account access attempts from reused credential datasets, especially if linked to known typosquatted domains.

Third-Party Risk Managers

- Evaluate vendors in the Payments and Digital Assets segments for domain abuse protection programs and credential hygiene awareness.
- Include typosquatting resilience in third-party monitoring platforms.

GRC Professionals

- Incorporate spoofed domain volumes and credential exposure into enterprise risk dashboards.
  Ensure vendors handling customer identity implement layered anti-fraud and phishing controls beyond password protection.



MALWARE AND COMPROMISED SYSTEMS

OBSERVED MALWARE AND ENDPOINT COMPROMISE

Malware presence among the 250 fintech companies was relatively low, but the implications of what was found are significant. SecurityScorecard's IP Reputation factor, which draws from external threat intelligence sources such as sinkholes and honeypots, detected signs of endpoint compromise or malicious use of company infrastructure in 7.6% of firms.

This includes:

- **Adware infections:** 6%
- **Other malware:** 2%
- **Maliciously repurposed machines** (e.g., for scanning, botnets, or TOR relays): 1.6%
- **Ransomware:** 0.4%
- **Information stealers:** 0.4%

These numbers represent machines inside corporate networks that have either been directly infected or are showing behavioral patterns consistent with prior compromise.

WHAT THE DATA MEANS

While 92.4% of companies showed no observable compromise, the presence of even a single infected endpoint can:

- Indicate undetected lateral movement by threat actors
- Serve as an internal launchpad for future attacks
- Be leveraged by attackers to conduct operations on behalf of other campaigns (e.g., scanning, payload delivery, command-and-control)

In most cases, compromise counts were low—often just one or two infected devices per company. The outlier was a single Chinese fintech firm with unusually high infection rates and poor overall security hygiene, which significantly skewed the regional statistics.

ENDPOINT INFECTIONS VS. INFRASTRUCTURE ABUSE

Importantly, not all signs of compromise reflect internal breaches. Some companies may unknowingly host malicious services, such as:

- Botnet C2 nodes
- Proxies for spam or scanning
- TOR exit points

These indicators can suggest:

- Poor egress controls
- Lax internal monitoring
- Missed incident detection

Even if no direct data exfiltration is confirmed, the reputational and operational risk of being an unwitting enabler of malicious activity is significant—particularly in the fintech sector, where trust and reliability are paramount.



THE HIDDEN COST OF LOW-LEVEL COMPROMISE

While ransomware and infostealer infections were rare in this sample, their presence is disproportionately impactful. Both are frequently associated with:

- Initial access brokers selling footholds to ransomware groups
- Credential harvesting for secondary attacks on customers or partners

A low observed rate is not the same as zero risk. These infections may represent the early stages of deeper compromise—or detection gaps in endpoint visibility.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Include external threat intelligence in assessments of vendor and internal security hygiene.
- Treat even low-volume malware detections as signals requiring full investigation—not background noise.

SOC Teams

- Correlate malware detections with lateral movement indicators and beaconing activity.
- Flag TOR-related infrastructure and botnet behavior—even absent full breach confirmation.

Third-Party Risk Managers

- Vendors with signs of malware activity—especially ransomware or repurposed infrastructure—should trigger enhanced due diligence and contractual review.
- Treat adware not as benign, but as a signal of weak endpoint controls and potential hygiene issues.

GRC Professionals

- Integrate external reputation monitoring into vendor assessments and internal reporting.
- Ensure that any signs of compromise lead to documented incident response, root cause analysis, and validation of containment.



ATTACK ENABLERS BREAKDOWN

TYPES OF BREACH ENABLERS

SecurityScorecard analyzed 28 third-party breach incidents among the fintech sample to determine the specific vendor relationships or technologies that enabled the compromise. We also considered the 8 relationships that enabled fourth-party breaches to have cascading impacts on even more organizations. These enablers were categorized by two dimensions:

- **Nature –** Technical vs. Non-technical
- **Scope –** Cross-industry vs. Industry-specific

This classifi cation provides insight into which types of relationships introduce the most risk and which technologies are most frequently abused.

SUMMARY BREAKDOWN OF ENABLERS

CATEGORY	% OF BREACHES
Technical, Cross-Industry	**33.3%**
Technical, Industry-Specific	**30.6%**
Non-Technical, Industry-Specific	**22.3%**
Non-Technical, Cross-Industry	**13.8%**

TOP TECHNICAL ENABLERS

Among the technical vectors enabling breaches, the most frequent were:

- **File Transfer Software** (e.g., MOVEit, GoAnywhere)
  Common target of ransomware campaigns; multiple breaches tied to exploitation of known vulnerabilities.
- **Cloud Storage Services**
  Misconfigurations or abuse of cloud-based object storage enabled data exfiltration or unauthorized access.
- **Email/Customer Communication Platforms**
  Exploited to deliver phishing payloads, launch credential harvesting campaigns, or access message content.
- **Collaboration and Productivity Tools**
  Insecure API integrations or unauthorized access tokens created secondary breach paths.
- **Chatbots and Customer-Facing Tools**
  Used as initial access points through exploitation of exposed interfaces.

INDUSTRY-SPECIFIC ENABLERS

These included both direct fintech infrastructure and behavioral attack patterns:

- **Credential Stuffing Campaigns**
  Reuse of compromised credentials across multiple fintech platforms resulted in account takeover at scale—treated as equivalent to third-party breaches in impact.
- **Payment Processors and APIs**
  Interfaces between core systems and external processors were leveraged for injection, misrouting, or redirection of transactions.
- **Banking & Accounting Software**
  Software with privileged access to financial data and systems was exploited to reach downstream clients.

NON-TECHNICAL ENABLERS

Not all breach enablers were technical in nature. Several involved:

- **Bank Accounts and Payment Cards**
  Attackers abused integrations with financial infrastructure to gain indirect access to customer data.
- **Corporate Structure & Acquisitions**
  Breaches exploited weak controls during M&A integration or in subsidiaries with unaligned policies.
- **Legal and Marketing Vendors**
  External parties with access to PII or sensitive campaign infrastructure became entry points.

WHAT THIS MEANS FOR FINTECH RISK

Technical enablers accounted for **nearly two-thirds of all** third-party breaches, and the margin between cross-industry and fintech-specifi c products was narrow. This reflects the dual nature of fintech risk: firms rely heavily on both general-purpose software and sector-specific platforms that carry embedded exposure.

Credential stuffing, in particular, emerged as a unique hybrid threat. While not a breach in the traditional sense, large-scale campaigns targeting shared user credentials across fintech platforms:

- Caused account compromise at volume.
- Traveled across organizational boundaries.
- Bypassed internal protections via user behavior.

Fintech's interconnected landscape and shared user base make this a persistent and scalable risk.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Require vendors to disclose third-party software dependencies—especially in file transfer, cloud, and messaging categories.
- Elevate scrutiny on vendors with APIs that integrate directly into transaction, customer service, or identity systems.

SOC Teams

- Monitor for credential stuffing attempts using breached credential datasets—especially across shared user platforms.

  Watch for anomalies tied to common productivity or cloud storage platforms, even when not flagged as malicious upstream.

Third-Party Risk Managers

- Include breach-enabling product categories in vendor onboarding questionnaires.
- Assess non-technical vendor relationships (e.g., legal, marketing) for privileged data access and fourth-party dependencies.

GRC Professionals

- Update procurement policies to require disclosure of vendor security controls for known high-risk enabler categories.
  Incorporate credential abuse scenarios into risk models —even when not tied to direct vendor compromise.

CREDENTIAL STUFFING AND THE FINANCIAL SUPPLY CHAIN

BEYOND THE BREACH: CREDENTIAL REUSE AS SYSTEMIC RISK

Credential stuffing attacks exploit a simple but widespread behavioral vulnerability: users often reuse the same credentials across multiple platforms. When attackers obtain valid email and password pairs—whether from phishing, infostealers, or public breaches—they can use automated tools to test these credentials across other services.

In a tightly interconnected fintech ecosystem, this means:

- A breach at one fintech firm can result in account compromise at another, unrelated company
- Platforms with no direct connection can still suffer customer loss, fraud, or reputational harm
- Attackers require no technical compromise of the second company—just a shared customer base and reused credentials

CASE INCLUSION AND JUSTIFICATION

SecurityScorecard included five credential stuffing campaigns in this report's breach dataset due to their scale and impact:

- These campaigns affected thousands of customer accounts per company.
- Victim organizations responded with customer notifications, incident investigations, and regulatory filings.
- The organizational burden was equivalent to that of a direct breach, despite no exploitation of internal systems.

Credential stuffing attacks differ from actual network breaches, but their operational consequences may have comparable consequences when executed at volume.

WHY CREDENTIAL STUFFING IS A SUPPLY CHAIN PROBLEM

Credential reuse links otherwise independent companies through shared customers. Attackers exploit this "behavioral overlap" as a bridge between services.

For example:

- A phishing campaign targeting users of **PayPal** may yield thousands of valid credentials.
- Those credentials are then tested against **Payoneer, Alipay**, or other digital wallet platforms.
- If users reused the same password, attackers gain access—without any vulnerability in the second company's systems.

This attack path:

- Requires no malware.
- Bypasses MFA if not enforced.
- Circumvents perimeter defenses.
- Spreads risk across vendors with overlapping user bases.

DETECTION CHALLENGES

Credential stuffing is difficult to detect in isolation. Unlike traditional attacks, it appears as legitimate login activity—albeit at abnormal volume or velocity. Attackers often distribute login attempts across:

- Multiple IP addresses.
- Geographic locations.
- Varying device signatures.

These tactics dilute signal and evade rate-limiting or IP blacklists unless companies:

- Monitor for credential reuse indicators.
- Aggregate authentication telemetry across vendors.
- Use breached credential databases for proactive defense.

STRATEGIC INSIGHTS BY ROLE

CISOs

- Treat credential stuffing not as a user error, but as a platform risk. Implement MFA and detection for reused or breached credentials.
- Require downstream vendors to monitor for leaked credential use and notify partners when targeting patterns are observed.

SOC Teams

- Integrate credential stuffing detection into SIEM logic using behavioral anomalies (e.g., login failure patterns, rapid device switching).
- Monitor dark web and breach data to preemptively block known credential sets.

Third-Party Risk Managers

- Ask vendors how they defend against credential stuffing. Require that customer-facing platforms implement IP velocity checks, MFA, and credential breach detection.
- Consider requiring notification when large-scale login abuse is observed using credentials not stolen from the vendor's own systems.

GRC Professionals

- Ensure compliance controls cover incident classification and reporting for credential stuffing—even if no internal system was compromised.
- Treat high-volume credential abuse as a breach-equivalent event in both reporting and risk posture.

RECOMMENDED SECURITY CONTROLS

OVERVIEW

This report has identified consistent, actionable patterns across the fintech sector:

- Weak points in application security and DNS hygiene
.
- Exposure through credential reuse and typosquatting.
- Technical and non-technical enablers of third-party breaches.
- Evidence of compromise across a small but meaningful subset of companies.

To address these realities, organizations must focus on a mix of preventative, detective, and vendor oversight controls—targeted at the specific gaps identified in the data.

PRIORITY CONTROLS BY RISK DOMAIN

1. Application Security

What We Saw:	Unsafe Subresource Integrity, exposed object storage, unsecured session cookies.
Recommendations:	• Enforce Subresource Integrity for all third-party scripts. • Require access controls for all object storage pools (e.g., AWS S3). • Set Secure and HTTPOnly flags on all session cookies. • Scan for use of HTTP in redirect chains. • Perform automated web asset scans at regular intervals.
Relevant CIS Controls:	• Control 4: Secure Configuration of Enterprise Assets. • Control 16: Application Software Security.

2. DNS and Email Spoofing Protection

What We Saw:	Missing SPF records, ineffective DMARC, spoofable domains.
Recommendations:	• Implement SPF with hardfail policy. • Pair SPF with enforced DMARC and DKIM. • Monitor for spoofing attempts via passive DNS and DMARC analytics. • Test vendor domains for SPF/DMARC coverage during onboarding.
Relevant CIS Controls:	• Control 9: Email and Web Browser Protections. • Control 14: Security Awareness and Skills Training.

3. Credential Protection and Abuse Prevention

What We Saw:	Compromised customer credentials, credential stuffing campaigns, typosquatting leading to phishing.
Recommendations:	• Enforce Multi-Factor Authentication (MFA) on all customer and admin interfaces. • Integrate known breached credential databases (e.g., Have I Been Pwned) into login workflows. • Rate-limit and behavior-analyze authentication attempts. • Monitor for typosquatted domains; initiate takedown where feasible. • Tag customer accounts accessed from known credential stuffing infrastructure.
Relevant CIS Controls:	• Control 6: Access Control Management. • Control 5: Account Management.

4. Patching and Vulnerability Management

What We Saw:	Delayed patching linked to breach risk; worst overall scores in companies with poor patch cadence.

Recommendations:

- Automate patch deployment for OS and application layers.
- Prioritize vulnerabilities listed in CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Monitor vendor response times to disclosed vulnerabilities.
- Require vulnerability disclosure programs for high-risk suppliers.

Relevant CIS Controls:

- Control 7: Continuous Vulnerability Management.
- Control 4: Secure Configuration.

5. Third- and Fourth-Party Risk Oversight

What We Saw:	41.8% of breaches were third-party; 11.9% fourth-party; high reliance on cloud, file transfer, and communication platforms.

Recommendations:

- Tier vendors by function and exposure—not just contract value
- Require vendors to disclose:
  - Recent breaches and root cause.
  - Technical dependencies (esp. file transfer, cloud storage).
  - Use of credential breach detection tools.
- Include fourth-party mapping and due diligence in vendor assessments.
- Require incident notification language that covers credential abuse and customer impact.

Relevant CIS Controls:

- Control 15: Service Provider Management.
- Control 17: Incident Response Management.

EMBEDDING CONTROLS INTO ORGANIZATIONAL PRACTICE

Security recommendations cannot be one-size-fits-all. They must be tailored by function, visibility, and responsibility.

CISOs

- Use this report's findings to recalibrate vendor scoring models and internal control audit focus.
- Drive investment toward controls that mitigate credential compromise and third-party vectors.

SOC Teams

- Integrate detection logic for SRI bypass, spoofed domains, session misconfigurations, and anomalous authentication.
- Monitor DNS records, certificate transparency logs, and cloud asset exposure.

Third-Party Risk Managers

- Ensure technical validation of vendor controls—not just policy or attestation review.
- Expand risk models to include fourth-party visibility and breach recurrence patterns.

GRC Professionals

- Align security audit checklists with findings from this report, including credential exposure, DNS protections, and cloud misconfiguration history.
- Incorporate technical signals into compliance scoring models and contractual enforcement language.



SUMMARY OF FINDINGS

The fintech sector shows strong cybersecurity posture overall. With a median score of 90 and the highest concentration of "A" ratings seen across any industry group, fintech firms have clearly invested in core security practices.

But ratings alone don't tell the whole story.

This assessment reveals persistent, measurable weaknesses that cut across even well-performing vendors:

- **41.8% of breaches originated from third-party relationships.**
- **Credential abuse is systemic**, affecting companies even without direct compromise.
- **Application and DNS misconfigurations** are the most common and impactful weaknesses.
- **Repeat breaches are predictive**—companies breached once are far more likely to be breached again.

Across all segments—Payments, Digital Assets, Business Process Solutions—critical issues continue to surface. Many are fixable. Some are avoidable. All are detectable.

OPERATIONALIZING THIS REPORT

To move from analysis to action, security leaders should use this report as both a benchmark and a roadmap. It is not just an industry snapshot—it is a tool for internal review, third-party evaluation, and risk-based decision making.

Use Cases:

Vendor Selection and Review

- Prioritize vendors with strong ratings and no recent breach history.
- Flag vendors with low scores in Application Security, DNS Health, or Patching Cadence.
- Ask for remediation evidence—not just policy documents.

Procurement and Contracting

- Include language requiring SPF/DMARC implementation, MFA, and credential breach monitoring.
- Define thresholds for mandatory incident notification—including customer-facing compromise patterns (e.g., credential stuffing).

Incident Preparedness and SOC Use

- Monitor for leaked credentials and typosquatted domains linked to your brand.
- Validate session cookie configurations, redirect chains, and DNS integrity.
- Track TOR, C2, and malware indicators—even at low volume.

Policy and Compliance Review

- Map findings to CIS Controls and NIST CSF alignment.
- Treat credential abuse and phishing impact as first-class breach events.
- Expand internal and vendor GRC models to include fourth-party risks and breach recurrence.

WHAT COMES NEXT: ACT WITH SCDR

This report confirms what many security leaders already know: strong ratings help define risk, but they don't eliminate it. Fintech's role in global finance is expanding—and so is the attack surface that comes with it.

Exposure is not just likely. It's built in.

To manage it, organizations need more than dashboards. They need detection and response—built for the supply chain. SecurityScorecard's Supply Chain Detection and Response (SCDR) operationalizes what this report reveals:

- Real-time telemetry across your third and fourth parties.
- Continuous monitoring of risk signals—not annual point-in-time reviews.
- Automation and intelligence to prioritize threats across vendors.
- Collaboration tools to push remediation, not just alerts.

SCDR turns breach data, score drift, and misconfiguration trends into action. It connects the dots between detection and accountability—so your team doesn't just see the risk, but stops it.

Every weak SPF record, every leaked credential, every exposed asset in this report is a reason to act. SCDR from SecurityScorecard is how you do it.



APPENDIX

A. METHODOLOGY

This report evaluates the cybersecurity posture of 250 leading fintech companies, selected for their global reach, industry influence, and operational scale. The companies span a wide range of financial technology segments, including payments, digital assets, neobanking, financial planning, and infrastructure providers.

Data Collection

All findings in this report are based on externally observable data captured through SecurityScorecard's global threat intelligence infrastructure. The following data sources and telemetry were used:

- **Security Ratings:** Ten-factor scoring framework, including Application Security, DNS Health, Patching Cadence, Endpoint Security, and others.
- **IP Reputation:** Evidence of malware infections, TOR participation, or command-and-control activity linked to company-owned infrastructure.
- **Credential Leaks:** Aggregated data from dark web sources, stealer logs, and open breach repositories over the past 24 months.
- **Typosquatting Domains:** Monitored and flagged based on DNS characteristics, lexical similarity, and activity linked to phishing infrastructure.
- **Publicly Reported Breaches:** Cross-referenced with third-party sources, including mandatory disclosures, media reports, and incident databases.

Analytical Scope

For each company in the dataset, SecurityScorecard analyzed:

- Overall cybersecurity rating and underlying sub-score trends.
- The risk factor in which the company scored the lowest.
- Specific technical issues that had the most negative impact.
- Number and nature of any publicly disclosed breaches.
- Evidence of malware infections or compromised systems.
- Number of exposed credentials and associated typosquatting domains.

Third- and Fourth-Party Breach Classification

Breaches were classified as third-party if they resulted from a compromise of a direct business partner, vendor, or service provider. Fourth-party breaches involved vendors of vendors or indirect exposure through shared infrastructure. Credential stuffing campaigns affecting large volumes of customers were included when the impact on the organization mirrored a traditional breach in scope and response.

B. REFERENCES

The following datasets, tools, and internal methodologies supported the research and analysis in this report:

- SecurityScorecard Cybersecurity Ratings Platform.
- SecurityScorecard IP Reputation and Threat Intelligence.
- Global Third-Party Breach Report Series (2023–2024).
- Internal breach correlation model based on historic rating and incident data.
- Industry-specific rating benchmarks: S&P 500, healthcare, insurance, federal contractors.
- External breach notification databases and public reporting.

To see how SecurityScorecard helps organizations detect, prioritize, and respond to cybersecurity risks across fintech ecosystems—including third- and fourth-party exposures, credential abuse, and misconfigurations—visit SecurityScorecard.com

