

BEYOND THE SIEM YOU KNOW:

WHAT FINTECH TEAMS NEED IN 2025



The new reality for Financial technology (Fintech) security

Fintech runs at transaction speed. Payments clear in seconds, trading never stops, and APIs blur the line between action and attack. Fraud is keeping pace.

ACCORDING TO IBM'S 2024 COST OF A DATA BREACH REPORT, FINANCIAL INSTITUTIONS FACE THE SECOND HIGHEST BREACH COSTS OF ANY SECTOR.

AVERAGING
\$6.08
million per incident

COMPARED TO
\$4.88
million per incident
globally

Once the breach occurs, it takes

168 days
to detect

51 days
to contain

LEAVING ATTACKERS WITH MORE THAN
7 months
OF ACCESS TO SENSITIVE DATA. *

In this environment, a breach is not only a technical failure. It means stolen identities, lost savings, and broken trust. The margin for error is measured in seconds.

The attack surface keeps widening with every new integration, partner, and product launch. Regulators are raising the bar with stricter mandates and more frequent audits.

When detection systems hit ingestion caps or rely on delayed queries, Fintech teams are not just behind. They are exposed.

Traditional security tools weren't built for the speed, scale, and real-time demands that define modern financial services. This is the moment when the conversation about SIEM (Security Information and Event Management) must change.

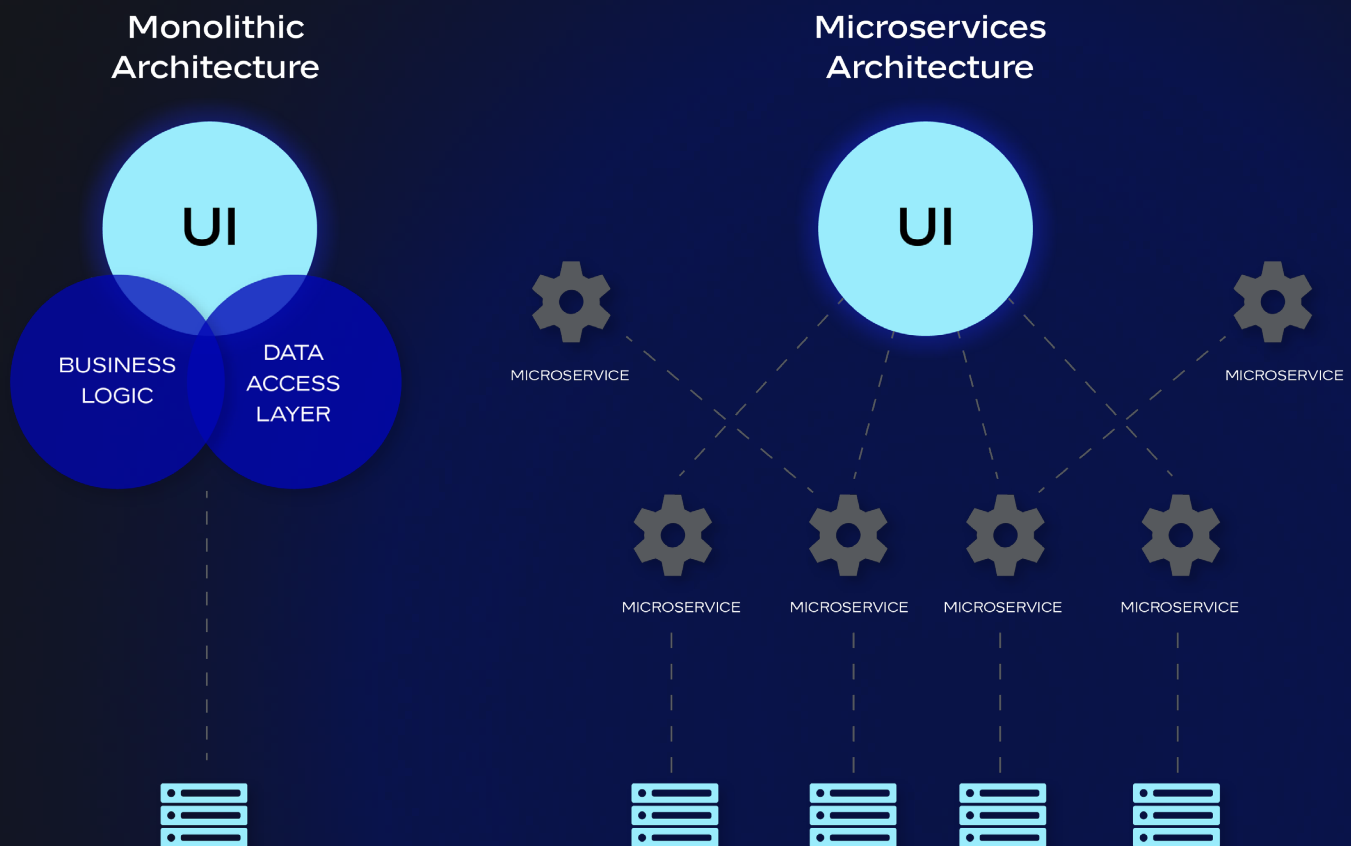
*Source: Neontri,
["Fintech Security Trends in 2025"](#)

The technical needs of a SIEM have changed

Most Fintech companies still rely on SIEMs built for a different era. Logs were collected in one place, searched when something looked suspicious, and stored for audits. That model was slow and compliance-first. It worked because threats moved more slowly then, too.

That world is gone.

Today, Fintech runs on high-speed transactions, cloud-native systems, and constant change. Attackers move just as fast, often using AI to push ahead. Traditional SIEMs can't keep up with the pace of modern business.



Here's what that looks like in practice:

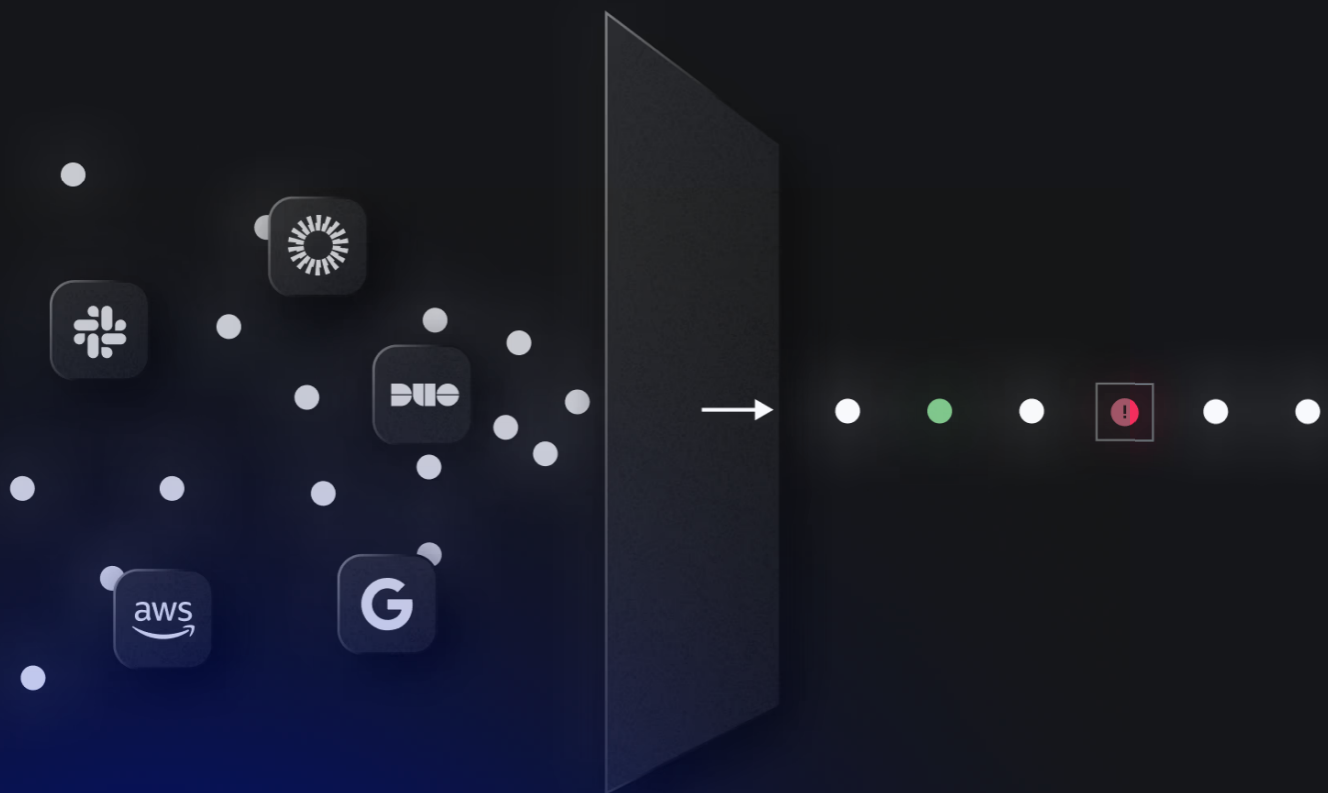
- Scale limits leave critical data out, creating gaps for attackers to exploit.
- Sole reliance on delayed queries means incidents surface only after damage is done.
- Static rules can't evolve as fast as new attack methods.
- Rising costs force trade-offs on which data to monitor, leaving critical gaps in visibility.

The result is a widening gap between how fast Fintech operates and how slowly security stacks respond. In this space, that gap isn't just a weakness. It's an open door for attackers.

What real-time detection at scale looks like

Fintech attacks don't happen in sequence. They break across cloud, identity, and business systems at the same speed customers trade, transfer, and transact.

With real-time detection, common log sources like AWS, Okta, Google Workspace, and custom apps are analyzed the moment they're ingested. Signals are correlated instantly so threats stand out as they happen. Instead of relying only on scheduled queries, attacks surface in real time.




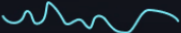







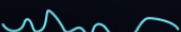
Detection logic is Python-based, versioned, and easily tested against production data. When new attack patterns emerge, rules are tuned and deployed as fast as engineers push code.

The result is a security posture that moves as fast as the business with complete visibility, immediate response, and investigations focused on real threats instead of false alarms.

Detection-as-Code: Engineering-led security

Traditional SIEMs lock detection rules inside rigid systems that make dynamic and version-controlled updates impossible. In Fintech, that pace leaves too much room for attackers. Detection-as-code changes the game by treating detections like software.

Rules are written in Python so they can handle complex, business-specific logic instead of relying on generic patterns. Every update is tracked in version control, creating a clear history of what changed, why, and by whom.

Detection name	Severity	Data Source	Alert Trends
 Root Account Access Key Created	C	AWS	
 AWS Root Account MFA	M	AWS	
 Okta Login Without MFA	H	Okta	
 Log4J Exploit IOC Search	C	Zscaler	
 GitHub Authentication Method Changed	M	GitHub	

Changes are tested before they go live. This prevents false positives from overwhelming analysts and keeps alert quality high. The workflow mirrors how engineering teams already build and ship code, making collaboration between security and engineering natural and fast.

With detection-as-code, security teams can adjust rules as quickly as threats evolve and tailor them to the company's unique environment, keeping detection relevant and specific to their needs.

Compliance at full speed

In Fintech, trust is built by stopping threats before they cause damage and proving to regulators that your defenses meet the highest standards. The challenge is doing both without slowing down security operations.



Panther's AWS-native architecture and detection-as-code model keep teams audit-ready at all times. Every rule is versioned, changes are tracked, and AI-assisted investigation threads are preserved, creating a permanent record for investigators and auditors.

Access controls are designed for security teams rather than limited to engineers, ensuring sensitive detection data is governed

appropriately without delays. Compliance frameworks such as PCI DSS and SOC 2 map directly to Panther workflows, making it possible to meet requirements and maintain rapid incident response.

The result is verifiable proof that meets Fintech compliance standards while enabling effective detection and response at full speed.

Panther + AWS in Action: Varo Bank

Varo Bank's security team was weighed down by an ELK stack that drained engineering hours yet produced low-value alerts. They needed a cloud-native SIEM that eliminated time spent on maintenance, supported their everything-as-code vision, and delivered meaningful detections from day one.

Solution

Panther's managed SaaS on AWS eliminates infrastructure overhead entirely. Native integrations connect key sources like AWS, Okta, Google Workspace, and custom logs, with scalable pipelines that make adding new sources fast and repeatable. With detection-as-code, the team tunes, tests, and iterates Python-based logic on their schedule, not an engineering backlog. This engineering-led approach keeps detection evolving as quickly as attacker tactics.

Impact



SECURITY ENGINEERING TIME
REFOCUSED ON DETECTION
AND RESPONSE



HIGHER-QUALITY ALERTS WITH
FEWER FALSE POSITIVES



CENTRALIZED VISIBILITY AND
IMPROVED AUDIT READINESS

**"PANTHER HITS THAT SWEET SPOT OF BEING A TOOL
AND HAVING ALL THESE USEFUL FEATURES, BUT IT'S
ALSO A FRAMEWORK... THAT'S WHAT MAKES
IT GENUINELY DIFFERENT."**

— JEREMY MILL, SENIOR MANAGER OF SECURITY
ENGINEERING, VARO BANK

Varo transitioned from a maintenance-heavy legacy stack to a cloud-based SIEM that operates at the speed and complexity required for modern Fintech teams.

Best practices for 2025 Fintech detection

Pull in all critical data

Bring in logs from AWS, Okta, Google Workspace, payment platforms, trading systems, and custom apps, so nothing slips through the cracks.

Rely on cloud scale

Analyze data in real time, at full volume, without slowdowns or caps.

Write and manage detections as code

Use versioning, testing, and fast updates so rules keep pace with attackers.

Bake in compliance from the start

Keep audit records and change history as part of daily work so reviews are always ready.

Modern SIEM built for the future of Fintech

Fintech moves fast, and so do today's threats. Traditional SIEMs, built for a compliance-only era, can't keep pace with the scale, complexity, and speed of today's sophisticated attacks. Every delay is an opening for adversaries to strike.

AI has the potential to sharpen detection and accelerate response, but it only works when built on complete, timely, and accessible data. Too many SIEMs fall short, leaving critical gaps.

Panther and AWS close those gaps with real-time detection, complete visibility across cloud and application activity, engineering-led control over detections, and built-in compliance readiness. This is how Fintech teams stay ahead of threats and audit-ready every day.

See it in action. Visit the Panther + AWS Sales Hub to book a demo today.

