

Guide

Director's Guide to Resilient Fintech Infrastructure

Fintech platforms depend on systems operating in real time and at massive scale. When those systems fail, the effects spread quickly:

- A failed authentication service can interrupt transactions instantly
- API abuse can expose fraud systems before security teams identify the source
- Traffic spikes that once caused slow page loads can now disrupt customer-facing financial workflows entirely

The board does not care whether the problem started in security, infrastructure, or delivery. They care that critical business services stay available and resilient. Regulators increasingly expect the same level of operational resilience from financial services organizations.

Infrastructure teams are feeling that pressure directly. APIs now sit behind nearly every customer interaction. AI-driven traffic is increasing unpredictability across production environments. Security leaders are being asked to tighten governance while engineering teams continue pushing for faster deployment cycles.

Most teams are already stretched thin. They are managing fragmented telemetry, growing attack surfaces, distributed services, compliance reporting requirements, and rising expectations around incident response simultaneously.

[Fastly's recent research](#) found that many CISOs are now being held accountable for environments they do not fully control. That gap between responsibility and visibility becomes harder to manage as fintech systems grow more distributed and interconnected.

This pressure is changing how fintech organizations evaluate infrastructure.

The following five considerations are becoming central to platform and security decisions across the industry.

1

Can the platform protect APIs without slowing deployment cycles?

Most fintech platforms now operate as API businesses. Authentication systems, payment flows, fraud tooling, mobile applications, customer dashboards, and partner integrations all depend on APIs communicating continuously across distributed services.

Every API introduces another dependency and another potential point of failure vulnerable to credential abuse, scraping, automation, and fraud activity.

Team priorities do not always align cleanly:

- Security teams need visibility into authentication traffic and suspicious behaviour
- Engineering teams need to release features quickly
- Infrastructure teams need systems that remain stable during traffic spikes and attack events

Legacy security tooling often creates friction because static rules require continuous tuning as applications evolve. Security teams end up spending time maintaining detection logic instead of investigating actual threats. Many security teams rely on complex regular expressions (regex) to create and maintain detection rules, which can be difficult to write and update. Fastly developed [SmartParse](#) for its [Next-Gen WAF](#) to reduce that dependency and make it easier to identify malicious requests without maintaining large collections of regex rules.

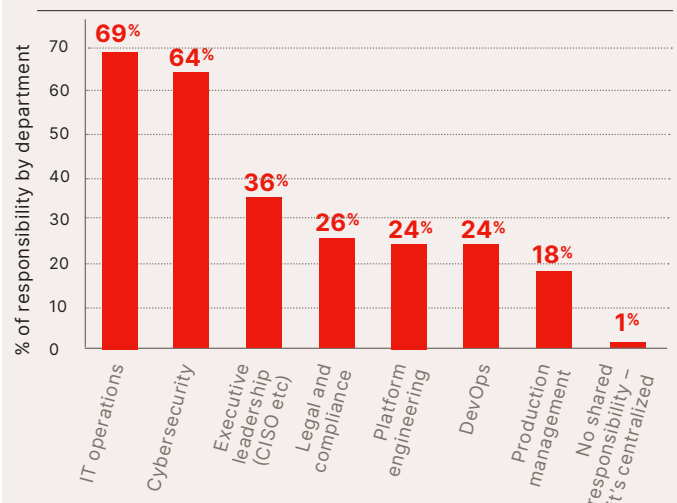
Teams are also dealing with alert fatigue. As alert volumes increase, teams spend more time validating noise and less time responding to real issues. False positives can interrupt legitimate customer activity during login or checkout flows.

RVU, operator of leading UK comparison brands including Uswitch and Money, needed to maintain a consistent security posture as it expanded through acquisitions. After implementing Fastly's WAF across its portfolio, RVU established a secure layer of protection for all brands while standardizing operations for performance, experience, and compliance. Because Fastly's WAF is integrated into the edge platform, RVU was able to strengthen security without introducing significant performance impact while simplifying configuration and management.

Questions infrastructure leaders should ask:

- How is API discovery handled?
- Can authentication abuse be detected behaviourally?
- How quickly can policies be updated globally?
- Does protection require ongoing manual tuning?
- How easily does security integrate into CI/CD workflows?

When it comes to cybersecurity, everyone has a part to play



Authentication requests, fraud inspection, bot mitigation, personalization logic, API processing, and feature flag evaluation all compete for origin resources simultaneously.

That workload adds up quickly. As traffic grows, latency increases during peak transaction periods. Infrastructure costs rise, and deployments become harder to manage safely. Small failures create larger downstream effects because so many systems depend on the same services.

In fintech environments, even small delays can affect transaction completion rates, customer trust, and fraud exposure. During traffic spikes or attack events, overloaded origin systems can quickly become operational bottlenecks.

Fintech organizations are benefiting from platforms such as Fastly that help them shift away from architectures that depend heavily on centralized origin processing. Depending on their technical, operational, and compliance requirements, organizations may run workloads in cloud, on-premises, or hybrid environments. Teams can execute routing logic, caching policies, request handling, and

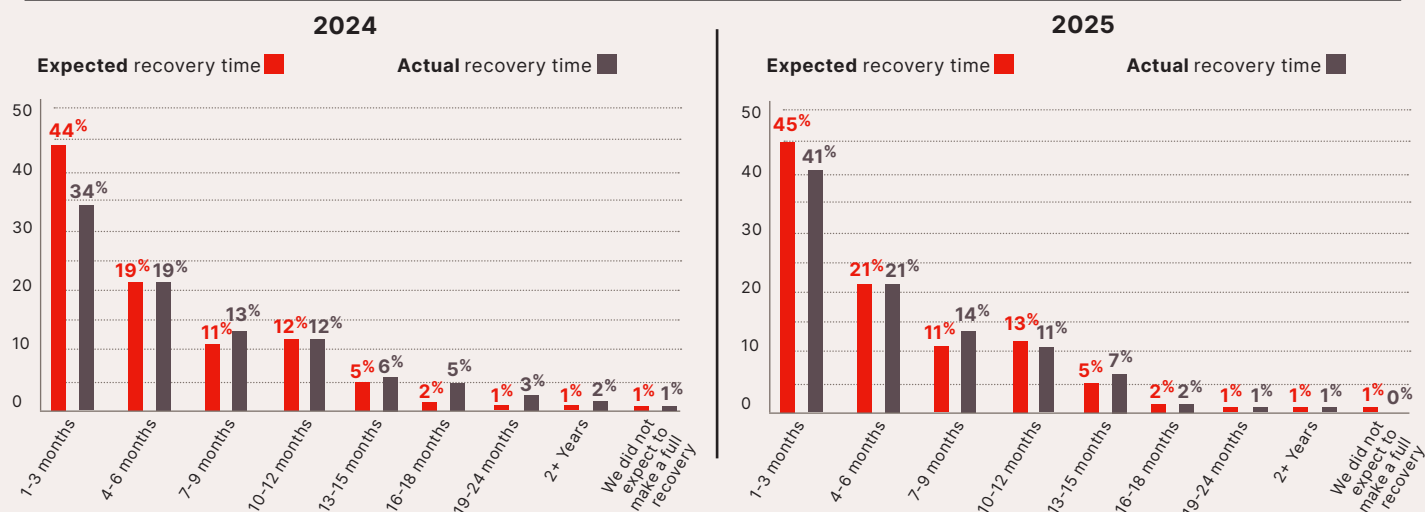
security enforcement closer to users instead of routing every request back through centralized infrastructure.

Questions infrastructure leaders should ask:

- How much traffic still depends on origin processing?
- Can API traffic be cached intelligently?
- How quickly can configurations be deployed globally?
- How much dependency remains on origin systems?
- Can infrastructure changes be made without external support involvement?

RECOVERY TIME FROM SECURITY ATTACKS

Recovery expectations are getting more realistic



Many fintech organizations still struggle to answer basic questions quickly during active incidents.

- Which systems are exposed?
- Which APIs are affected?
- Where is sensitive data flowing?
- Can affected services be isolated immediately?

Organizations lack complete visibility into what exists across their environments and how systems connect together under real-world conditions.

Security telemetry often lives in one platform, while API monitoring sits somewhere else. In some cases, APIs are not being monitored at all, or teams are unaware of shadow APIs that have been deployed outside standard governance processes. Teams end up stitching information together manually during incidents while customer-facing services remain under pressure.

Executive scrutiny adds another layer of pressure. Infrastructure and security leaders are expected to provide clear reporting around:

- Attack activity
- Incident timelines
- API exposure
- Resiliency risks
- Compliance posture

That becomes difficult when telemetry is fragmented across multiple vendors and disconnected tools. For many security leaders, the larger problem starts before incidents occur.

RVU, which operates several financial comparison platforms across the UK, streams Fastly telemetry directly into BigQuery so teams can analyze traffic, block rates, and security events in real time. According to RVU's infrastructure team, standardized integrations helped simplify reporting and operational analysis.

Questions infrastructure leaders should ask:

- How easily can telemetry be streamed and analyzed?
- Do security and infrastructure teams share the same operational data?
- How quickly can incidents be investigated?
- Does observability extend across APIs and edge environments?
- Can reporting support both technical and executive stakeholders?



Finance

Finance averages 54 breaches a year. Phishing still worries **39%** of organizations, and data breaches concern **42%**, but the killer statistic is **\$442,232**. That's the average increased annual infrastructure cost from AI scraping alone, and it's the highest across all sectors. Perhaps that's why generative AI worries **41%** of financial institutions. Only tech companies are more anxious about it.

Does the platform simplify infrastructure or create more coordination overhead?

Many fintech security teams are not struggling because they lack tools. They are struggling because operational complexity is growing faster than teams can realistically manage. Every new service, vendor, API, detection rule, and compliance workflow increases coordination overhead across already overloaded teams.

Infrastructure teams increasingly do not want:

- Separate vendors for security and delivery
- Complex rollback procedures
- Manual policy management workflows
- Infrastructure changes requiring lengthy escalation chains

They want systems that fit naturally into engineering workflows and can be updated safely without creating additional operational overhead.

Compliance pressure adds another layer of complexity. Many fintech organizations spend large amounts of time assembling audit evidence, policy records, incident documentation, and governance reporting across fragmented systems. That work rarely scales cleanly. One recurring frustration infrastructure teams describe is how difficult it still is to make small changes safely. In some environments, deploying new edge logic or traffic policies still involves lengthy deployment cycles or external support requirements.

Vendor consolidation is also becoming a larger priority for security teams. Managing separate WAF, bot management, DDoS, observability, and API protection vendors creates coordination overhead during both day-to-day operations and active incidents.

RVU's engineering teams highlighted Fastly's programmability as a major advantage because developers could write custom VCL directly at the edge instead of waiting for vendor-side limitations or workarounds. The company also used Fastly as a standardization layer across acquired brands, helping teams reuse code, redirects, configurations, and edge logic across multiple environments instead of rebuilding workflows from scratch each time.

Questions infrastructure leaders should ask

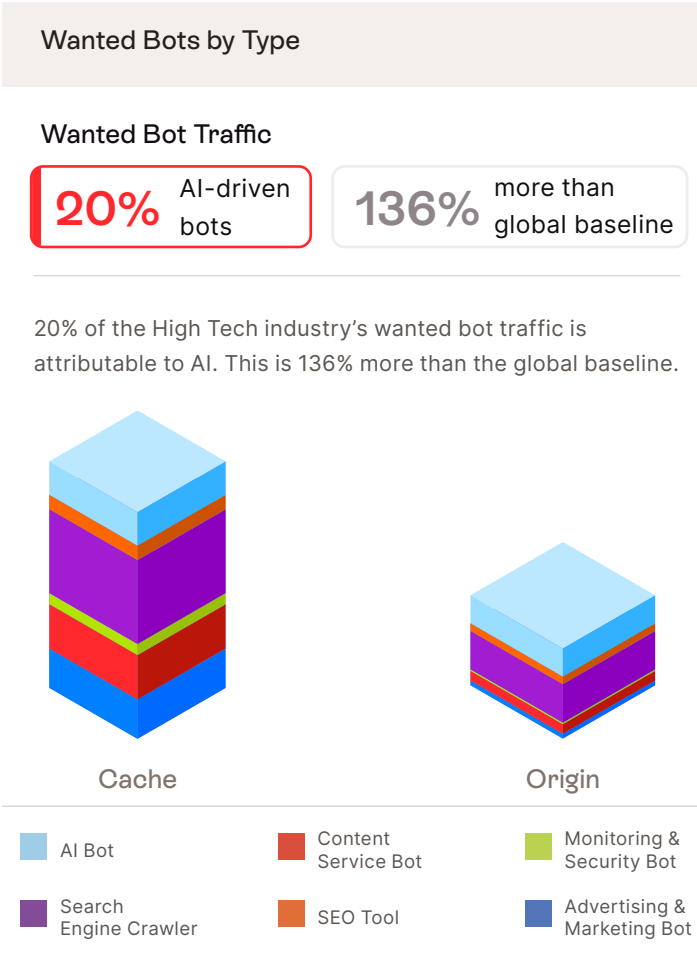
- How easily can deployments be automated?
- Does infrastructure integrate into existing developer workflows?
- How quickly can policies be updated globally?
- How much ongoing tuning is required?
- Does the platform reduce vendor sprawl?

5

Is the platform prepared for AI-driven traffic and automated abuse?

Fintech infrastructure teams are already dealing with the effects of AI-driven traffic, even when they are not deploying AI systems directly.

AI-assisted scraping, credential attacks, automated reconnaissance, and bot-driven abuse are increasing request volumes across financial platforms. Attackers can now test credentials, probe APIs, generate synthetic traffic, and adapt behaviour faster than many manual security processes can respond.



At the same time, AI-assisted commerce and agentic systems are introducing additional APIs, integrations, and services that security teams must monitor and secure. Every new AI-connected system expands the attack surface.

Most executive teams are not asking organizations to slow AI adoption down. They are asking security leaders to maintain governance and visibility while adoption

accelerates. That creates pressure across infrastructure and security teams simultaneously.

Many security teams already feel overloaded. They have not been able to hire their way out of alert fatigue, coordination bottlenecks, and expanding infrastructure complexity. AI-driven automation may reduce some manual work while increasing attack sophistication at the same time. Fastly's research on AI-first organizations found that many security teams are struggling to maintain visibility and governance as AI adoption moves faster than internal operational processes can adapt.

Traditional security approaches struggle in these environments because they rely heavily on static rules and centralized enforcement models that adapt slowly to changing traffic behaviour.



Questions infrastructure leaders should ask

- How is automated traffic identified?
- Can bot behaviour be analyzed in real time?
- How much AI-driven traffic is reaching origin infrastructure?
- Can mitigation happen at the edge?
- How quickly can teams respond to changing traffic patterns?

Conclusion

Fintech organizations are operating in environments where customer experience, security, governance, and transaction continuity are tightly connected. The pressure on infrastructure teams is not slowing down while regulatory scrutiny is increasing.

Many organizations are discovering that adding more tooling does not necessarily improve resilience. In many cases, it increases coordination overhead, operational complexity, and response friction across already overloaded teams.

Fastly works with fintech organizations to help reduce operational complexity across security, delivery, and edge infrastructure while improving visibility, resiliency, and deployment speed.

To learn how Fastly can help your team simplify infrastructure operations, strengthen API protection, and reduce operational overhead, [contact us today](#)