

THE PAYMENTS COMPANY THAT ALMOST BECAME A HEADLINE

How a fast-growing payments company in one of the world's most targeted industries confronted the limits of its own security, and found a way forward before the breach that everyone feared could happen.

This company moves money. Not in small amounts. Millions of transactions flow through its infrastructure every day: digital wallets, payment gateways, point-of-sale terminals, e-commerce rails. It operates under a central bank license, which means regulators are watching. It operates in a growth market, which means threat actors are watching too.

The security team was talented but small. And somewhere along the way, a realization set in that the team's leadership could no longer ignore: they were managing what they could see, but they had no real idea what was building outside their walls.

Cybersecurity leaders are facing a difficult reality: the threat landscape is expanding faster than most security teams can scale. According to IBM's 2025 X-Force Threat Intelligence Index, cybercriminals increased the use of infostealer-delivering emails by 84% in a single year, reflecting a broader shift toward faster, more automated, and increasingly difficult-to-detect attacks. At the same time, FS-ISAC's Navigating Cyber 2025 report found that heightened cyber threats are testing the operational resilience of financial institutions worldwide, driving organizations to adopt more proactive and intelligence-driven security strategies. For the first time in 19 years, Verizon's DBIR shows exploitation of vulnerabilities, not stolen credentials, as the top way breaches begin (31% vs. 13%). At the same time, the median time to fully remediate known exploited vulnerabilities has increased from 32 to 43 days, leaving organizations exposed for longer.

For organizations operating critical financial infrastructure, this creates a growing challenge. Protecting what happens inside the environment is no longer enough. Security teams must also understand the threats developing outside it, often before those

threats become active attacks. The question is whether organizations can identify emerging risks quickly enough to act.

THE QUIET CRISIS NO ONE WAS TALKING ABOUT

In financial services, the breach rarely announces itself. It does not show up as a blinking alert on a dashboard. It shows up months later, in a forensic report that traces a compromise back to an indicator of compromise that was never flagged, a threat actor that was already known to the intelligence community, a campaign that had hit three other organizations in the same sector before it reached this one.

The security team at this payments company understood this reality, but lacked the infrastructure to act on it.

Their workflows were reactive. Their visibility was inward-facing. They monitored their own environment with discipline, but threat actors do not live inside an environment until they already own it. The intelligence about who was coming in, why, and how lived outside the company entirely, and the team did not have the bandwidth to chase it.

"They feared the unknown," as one member of the account team later described it. Calling it a failure of will would miss the point entirely. The architecture had never been built to look outward.

The financial sector has long been the most targeted vertical in cybersecurity. Payment infrastructure sits at the intersection of personal data, transaction volume, and regulatory exposure.

When a breach occurs, the damage fans out across operations, reputation, regulatory standing, and customer trust simultaneously. The cost calculation extends far beyond incident response.

For a company trying to become the defining payments platform in its market, with an entire value proposition built on security and seamless experience, the gap between what they knew and what was happening beyond their perimeter had quietly grown into an existential exposure. The leadership team had started losing sleep over it.

THE PROBLEM WITH HOW MOST TEAMS RESPOND

When security leaders confront this kind of visibility gap, the instinct is to hire, specifically more analysts or more researchers to build a dedicated threat intelligence function. Grow the capability organically, staff it up, and bring the outside picture in-house.

That instinct is reasonable. It is also expensive, slow, and in most markets, nearly impossible to execute. Skilled threat intelligence practitioners are among the scarcest resources in the security industry globally. In emerging markets where talent competition is fierce and security headcount is a luxury, the hiring path simply does not lead anywhere.

This company was not going to triple its security team; the business did not allow for it and the market did not supply it. Even if it had, the fundamental architecture problem would have remained: a team doing manual threat research is a human-speed operation in an environment where adversaries today are moving at machine speed. The old operating model produced alerts at human speed. The new operating model has to produce governed decisions at machine speed.

A better managed threat intelligence solution was clearly needed. The harder question was whether they could operationalize it without resources they did not have.

A DIFFERENT KIND OF SOLUTION

The answer, it turned out, required rethinking the architecture rather than expanding the headcount.

Anomali Managed Intelligence as a Service (MlaaS), powered by ThreatStream Next-Gen, brought the outside picture in as enriched, contextualized, actionable signal delivered through a single platform, rather than raw intelligence dumps that required analysts to synthesize manually. The world's largest threat intelligence repository, fused with the company's own telemetry. Indicators of compromise correlated against their environment automatically. Threats aggregated, deduplicated, and surfaced with the context that turned a data point into a decision. Intelligence is the foundation everything else stands on, not a stage to move past: full-fidelity intelligence, curated and operationalized, gives every decision complete context.

The small security team needed to see more, know more, and act faster using the capacity they already had. Growing the team was beside the point. The Anomali Managed Intelligence model was built precisely for this constraint: deliver the intelligence program without requiring the intelligence program team.

The solution's approach addressed the deeper problem as well. The gap between intelligence discovery and operationalization, the window in which a known threat becomes an active incident because nobody connected the dots in time, is where most breaches actually live. That gap closed. Threat advisories became enforced controls. IOCs became active defenses. Intelligence that had previously existed only in external feeds began operating inside the payments company's security workflows within minutes of ingestion.

Three competitors were considered. The evaluation was rigorous. But the factors that ultimately decided the outcome were not price or feature matrix comparisons alone. The payments company needed a partner with a local team, a committed customer success model, and a solution that could grow with

them as their security posture matured. The roadmap ahead mattered as much as the capability available today. That vision is a ladder the customer climbs stage by stage, from recommendations, to actions that require human approval, to autonomous action, governed at every rung and never granted wholesale.

WHAT CAME NEXT

The deal closed in three months. The deployment delivered what the security team had been searching for: relevant threat intelligence, operationalized, without adding the headcount that the business could not support.

The metrics tell part of the story. Across similar deployments in financial services, organizations have reported 90% reductions in critical incidents, 60% improvements in CTI management, and incident response SLA improvements of 2x or more, and 30% of attacks mitigated before they execute. Analyst time shifted away from manual triage toward genuine investigation. The specific figures vary by deployment; what matters is the magnitude of impact, which is significant no matter which way you slice it.

But the outcome for this payments company is more fundamental than any single metric. They stopped fearing the unknown. The threat landscape had grown more dangerous, not less. What changed was that for the first time, the security team could see what was building outside their walls before it arrived inside their walls. For a licensed financial institution, the goal is not only speed but decisions it can defend to its management, its board, and its regulator.

In financial services, that is the margin between a breach that becomes a footnote and one that becomes a headline everyone in the industry reads.

This company intends to be in the former category. Anomali is built for exactly that: governed decisions at machine speed, defensible by design.

Concerned your organization might be one blind spot away from becoming the cautionary tale that your peers cite in their board presentations? Set up a confidential 1:1 meeting with Anomali to get the details behind this story.

[Ready to operationalize your threat intelligence?](#)
[Schedule a confidential conversation with Anomali.](#)

SCHEDULE A MEETING