ANOMALI

FROM INTELLIGENCE OVERLOAD TO CONFIDENT ACTION: HOW A FAST-GROWING FINTECH BUILT THE SECURITY DECISION CAPABILITY ITS REGULATOR DEMANDED

A regulated digital payments company faced a choice every FinTech CISO now confronts: stay buried in data, or build the intelligence capability to make fast, defensible security decisions. By deploying Anomali's Intelligent Unification Layer, it gained the governed decisioning platform its central bank regulator required—and positioned itself for the next phase of growth.

In the world of digital finance, speed is everything, and not just for transactions. When a threat actor moves, the window between detection and damage can close in hours. Yet for many of the FinTechs reshaping how the world pays, stores, and moves money, the security operations center looks less like a command post and more like a newsroom during a breaking story: alerts flooding in from every direction, analysts buried in feeds, and the genuinely dangerous signals lost somewhere in the avalanche.

For one fast-growing digital wallet and payments company —serving millions of customers and operating under the watchful eye of a central bank regulator—that was precisely the problem. And the stakes of getting it wrong were rising fast.

> Financial services had the highest median ransom demand of any industry in 2025 at $3 million, a 50% increase from $2 million in 2024, according to Sophos.

The Pressure Cooker

The company had done the right things. It had invested in threat intelligence feeds, multiple ones, in fact, casting a wide net across sources to ensure comprehensive coverage of the threat landscape. On paper, this looked like a robust security posture. In practice, it was delivering a lot of data but not a lot of decision-making insight.

Security analysts were spending hours each day manually sifting through a torrent of overlapping, unfiltered intelligence. Not every feed spoke the same language, and not every alert was relevant to their specific environment. The result was a team bogged down in data management rather than threat response—exactly the wrong side of the equation for a company processing high volumes of financial transactions.

The financial sector has become the most targeted industry on the planet.

According to Kroll's 2024 Data Breach Outlook report, the financial sector accounted for 27% of all breaches handled (up from 19% just a year earlier), making it the most attacked industry globally. These threats are targeted, patient, and sophisticated.

The company's exposure was compounded by its regulatory environment. As a regulated digital bank operating under the oversight of its central bank, it was subject to formal Cyber Threat Intelligence (CTI) requirements, including mandatory standards for how it collected, processed, and acted on threat information. Failing to meet those requirements was a security risk as well as a compliance risk with direct business consequences, including significant financial penalties and reputational damage that could erode customer trust and destabilize its operating license. The pressure was real. Something had to change.

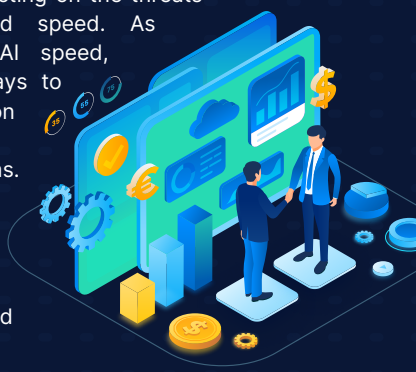
> When your analysts are spending hours correlating data between systems instead of acting on intelligence, you're not running a security operation. You're running a data management problem.

The Intelligence Problem Has a Name: Noise

Alert fatigue continues to exhaust even expert teams across enterprise cybersecurity. A 2024 study by Hack the Box found that 84% of cybersecurity professionals experienced burnout—with 89% citing being overworked as a primary cause. The financial toll is staggering: medium to large organizations in the United States lose more than $626 million annually in productivity due to stress and fatigue among security staff.

A 2025 SecurityScorecard analysis found that almost 42% of breaches at top FinTech companies originated from third-party vendors, meaning that the intelligence a security team needs to monitor extends far beyond its own perimeter.

The real bottleneck, however, was acting on the threats they found with confidence and speed. As adversaries began operating at AI speed, compressing attack chains from days to minutes, the gap between detection and decisive action became the defining vulnerability for security teams. Manual SOC workflows were never designed for this pace. For FinTechs processing high volumes of financial transactions under regulatory scrutiny, that gap had direct business consequences.



Finding the Signal

After evaluating its options, the company deployed Anomali's Intelligent Unification Layer—the entry point into the Anomali Security Decision Engine. Rather than replacing the existing stack, it sat on top of it, fusing intelligence directly into every alert and event so that analysts could work from a single, prioritized picture with context and relevance scoring already built in. The requirement was not simply to aggregate data. It was to create the governed decisioning capability that the security team—and the regulator—needed.

SCHEDULE A MEETING