RAPID7

CUSTOMER STORY

OUTNUMBERED? NEVER OUTPACED: HOW SOCS TOOK COMMAND WITH RAPID7

SECURING THE FINANCIAL BACKBONE WITH ONE PLATFORM

Industry	Company Size
Finance	Mid-Market

Pearl Data Direct (PDD) is a FinTech company and subsidiary of LuLu Financial Holdings, operating across multiple countries with over 250 physical locations and a mobile app for money transfers. As the software and infrastructure provider for LuLu's portfolio, PDD is responsible for processing high-volume financial transactions, managing sensitive customer data, and meeting strict regulatory compliance in the banking sector.

What changed

PDD faced two primary challenges: being a high-value target due to the nature of handling financial flows, and stringent regulatory requirements from central banks demanding rigorous security controls. Midhun Kumar, Head of Infrastructure and Cloud Operations, recognized that their existing defenses lacked unified visibility, and wanted a scalable solution with real-time alerting, compliance support, and automation.

The Rapid7 MDR experience

Pearl Data adopted Rapid7's next-gen SIEM, automation, and application security solutions, to deliver comprehensive detection, automation, and app security. With next-gen SIEM agents deployed on all endpoints, the team gained the ability to see alerts in real time and correlate data across endpoints, cloud operations, and network activity. The SOC analysts could instantly investigate a machine, collect DNS logs, processes, and cloud events in a unified view.

Through our automation solution, the security team automated responses: for example, blocking malicious IP addresses across firewalls or applying hash blocks across endpoints with a single click. Integration between Rapid7's products and existing security tools made these workflows seamless. With application security tied into the DevOps pipeline, code commits automatically trigger scans, and vulnerability gating is enforced at deployment time, reducing human bottlenecks.

Within days of deployment production was provisioned, showing the scalability and flexibility of the platform. Midhun appreciated the pricing model tied to assets, which made costs predictable and fair for a global environment.

> "With the InsightIDR [next-gen SIEM] implementation we have agents deployed on all the endpoints, so I can see all kinds of alerts in real time... the SOC analysts, with a few clicks, can investigate the machine ... see cloud activity ... all correlated together."
>
> **Midhun Kumar, Head of Infrastructure and Cloud Operations**

RESULTS AT A GLANCE

- Real-time alerting and correlation across endpoints, cloud, and network
- Automated responses via integrated workflows (block IPs, block hashes)
- Application security scans tied to deployment pipelines (code gating)
- Predictable asset-based licensing model
- Significant time savings (one workflow saved 11 days in one month)

> "I would recommend the capabilities of the Insight [platform] solution, the integrations and all the scalability. Plus, Rapid7 is very cost effective ... And of course there is the strong partnering relationship that Rapid7 maintains with the customer."
>
> **Midhun Kumar, Head of Infrastructure and Cloud Operations**

Built for what's next

With Rapid7's platform, Pearl Data shifted from reactive to proactive defense. The unified view across operations, automation of critical response tasks, and integrated app security make them resilient in a high-risk financial environment. As Midhun notes, the improved security posture and time savings give his team the breathing room to focus on innovation and strategic growth.

READY TO OUTPACE EVERY THREAT?

See how Rapid7's AI-powered SIEM helps SOCs adapt faster, cut through noise, and command with confidence.

LEARN MORE   REQUEST A DEMO

Exciting News: The next-gen SIEM functionality described in this case study is a core component of the recently announced Incident Command, which adds Attack Surface Management to provide SOC analysts with complete visibility into the entire threat attack surface.

ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

Command Platform | Exposure Management | Attack Surface Management | Vulnerability Management | Cloud-Native Application Protection | Application Security | Next-Gen SIEM | Threat Intelligence | MDR Services | Incident Response Services | MVM Services

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free - start your trial at **rapid7.com**