RAPID7

CUSTOMER STORY

Industry
Finance

Region
Americas

Company Size
Mid-Market

Products
Managed Detection & Response, Managed Service VM

LEAN, UNDERFUNDED, AND A SPRAWLING ATTACK SURFACE – NOW SECURE WITH RAPID7 MDR

OVERVIEW

It's a financial services firm with employees around the world – mostly brokers and traders – handling 3,500+ global institutions and corporate clients. The volume and sensitivity of transaction data is immense – primary points of attraction for attackers and key drivers putting the financial sector at the center of 20,000 cyberattacks and $12 billion in losses over the past 20 years.

The firm prefers to keep names under wraps, but wanted to share its valuable story – starting with a two-person cybersecurity team and a program that was nowhere.

Fortunately, they're the two right people. One is a former Special Forces Operator, and the other had a long tenure in financial services as well as time spent with a Managed Security Services Provider (MSSP). They split CISO responsibilities and got to work.

The former Special Operations CISO spoke to us about one of the natural tensions that comes with the job.

"I'm a cost center. Traders and bankers make the money, and they look at me as lighting it on fire."

He said his economic reality isn't terribly unique: he has to be bigger and better than his budget would ever be. "Anybody in security can say, please give me more money and more people," he said. It's a matter of "what you can do with what you got."

To have any chance at an effective in-house SOC, he'd need at least an engineer, an analyst, and probably more. He quickly understood that a trusted MDR partner was the only viable path.

THE FINANCIAL SECTOR HAS SUFFERED MORE THAN $12 BILLION IN LOSSES OVER THE PAST 20 YEARS.[1]

1 Advisen cyber loss data and IMF staff calculations

+

3,500

GLOBAL INSTITUTIONS & CORPORATE CLIENTS

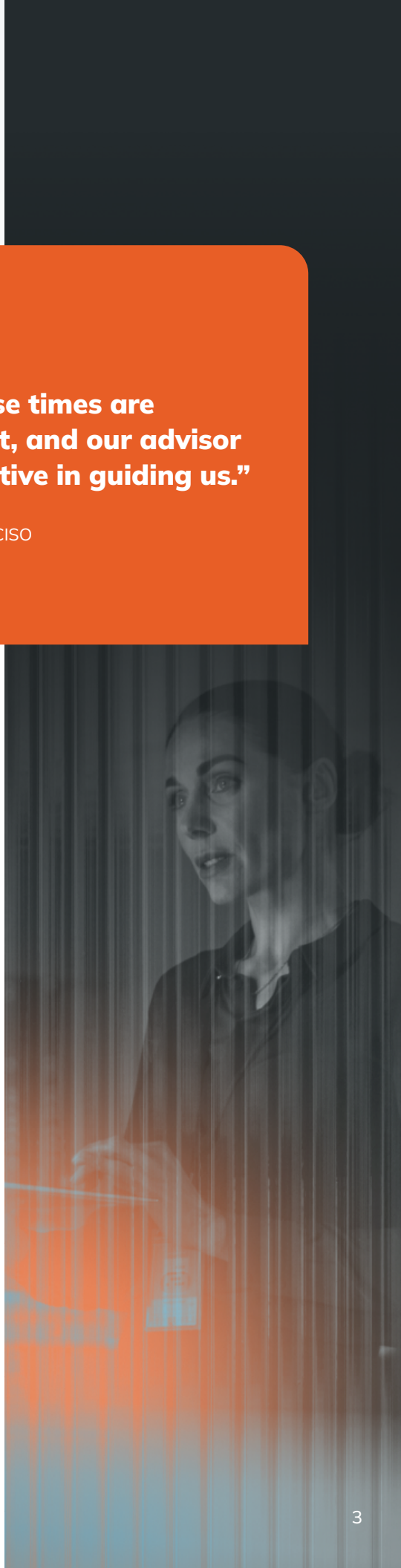
RAPID7 MDR HAD A STRING OF UNIQUE COMPETITIVE ADVANTAGES

One of the big draws to Rapid7 was its unlimited data ingestion, longer data retention, and unlimited incident response. Most MDR providers only keep data for a month, which isn't enough to meet the stringent transparency and compliance needs of financial services. Rapid7's standard 13-month retention gave them confidence they'd have the data when they needed it. "If our legal team had its way, they'd want indefinite retention," the company joked. With Rapid7, they didn't have to worry about hitting limits on data or response when it mattered most.

> **"Response times are excellent, and our advisor is proactive in guiding us."**
>
> Anonymous, CISO

The firm quickly eliminated MDR providers that do not give visibility into their technology. The CISO wanted meaningful collaboration and Rapid7 was best positioned to deliver on that. Their next-gen SIEM and XDR solution could be leveraged by the firm's in-house security team – as small as it was and would stay – but also served as the team's window into the Rapid7 SOC, giving direct line of sight into alerts, investigations, and outcomes that wouldn't be possible with "black box" MDR providers.

Integration with CrowdStrike wasn't just a backup plan - it was a critical part of the firm's security strategy. Since they relied on CrowdStrike for endpoint protection, it was essential that their MDR provider had full visibility into that telemetry. With Rapid7's extended SOC coverage for third-party tools, the MDR team continuously monitored CrowdStrike logs, ensuring no threat went unnoticed. "We tested it with the SOC team, and it works," the CISO explains. This deep integration gave the firm confidence that Rapid7 wasn't just reacting to incidents but proactively delivering defense in depth and comprehensive response across their entire security ecosystem.



THE RIGHT TOOLS AND PROCESSES WERE IMPORTANT, BUT THE PEOPLE MATTERED MOST

Having a dedicated Cybersecurity Advisor has proven its role in the firm's long-term success. "Response times are excellent, and our advisor is proactive in guiding us." Acting as a direct conduit to the Rapid7 SOC, the Cybersecurity Advisor ensures the firm gets more than just alerts – they get proactive guidance, strategic insights, and a partner who deeply understands their security needs. This hands-on support means the firm isn't just reacting to threats but staying ahead of them with expert advice tailored to their environment.

"I've managed a lot of tools and resources, and Rapid7 has consistently been either the best or right at the top in terms of customer relations and support. We get a team that truly understands what we need," the CISO says.

With Rapid7 MDR in place, he and his team have peace of mind and operational efficiency. Instead of being buried in Level 1 security alerts, they can focus on strategic initiatives like incident response planning, security training, and program development. "Having two teams—ours and Rapid7's—means I can sleep at night."

The in-house team is, in its own estimation, underfunded and understaffed for the security maturity it has actually achieved. "If we can get the results," he says, "then our management at a financial services firm is going to be really happy."

Outperforming the budget. Rapid7 is there for that.

> **Rapid7 has consistently been either the best or right at the top in terms of customer relations and support. We get a team that truly understands what we need"**
>
> Anonymous, CISO

View more success stories.

CUSTOMER STORIES

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/trial/insight