RAPID7

CUSTOMER STORY

Industry
Finance

Region
Americas

Company Size
Mid-Market

Packages
Exposure Command Advanced, Surface Command and Managed Threat Complete Advanced

FROM OUTSOURCED TO IN-HOUSE: HOW AMERICOR BUILT A PROACTIVE, CONTINUOUS, AND TRUSTED SECURITY PROGRAM WITH RAPID7

AMERICOR

OVERVIEW

Americor is an A+ rated debt relief company that guides people in serious distress back to stability and resilience.

A few years ago – with company growth accelerating, acquisitions underway, and the business expanding into new markets – Americor brought on fractional CISO, Daniel Akiva. He took security from rudimentary to innovative with Rapid7. The company transformed security operations from manually reconciling data across a fragmented ecosystem, to having it done for them, automatically, freeing their valuable time for more important, outcome-driven work.

The plan: score some wins, then win trust

Originally, Americor used an MSSP. "Over time," Akiva recalls, "it became clear we weren't getting the depth of coverage or the necessary level of collaboration with DevOps and IT." The friction and the blind spots across their hybrid, multi-cloud ecosystem and increasing concern of the "unknown" inspired a bold move: bringing security in-house.

Americor had become comfortable with the outsourced solution, but Akiva advocated for increased visibility, deeper integration, rather than fragmentation - especially with respect to vulnerability identification and remediation. This was hindering security efforts.

He needed a strategic security partner to provide tailored guidance and scalability as the business grew. Additionally, Americor has a lot of critical workloads in data centers, which many vendors fail to support/address. Having one platform that works seamlessly across multiple cloud environments and hybrid/data centers was an important requirement

Americor's leadership agreed, but were also looking to reduce current security spend by an ambitious 15%!

+

$3 BILLION IN TOTAL DEBT RELIEF

CONSOLIDATION AND COLLABORATION CHANGED EVERYTHING

Akiva overhauled the company's toolset and internal structure. He standardized on Rapid7, not just for its breadth but for its ability to centralize telemetry and address risk and misconfigurations across their entire infrastructure, cloud, and SaaS environments.

"We wanted more than just tools," he says. "We wanted a partner that could move at our speed and do most of the manual work for us, that way our time can be better spent driving true outcomes and reflecting to leadership what our attack surface is comprised of, identify and confirm with them what is accepted risk, and how we are reducing exposures that fall outside of our organization's established risk appetite. "

> **We wanted more than just tools. We wanted a partner that could move at our speed and do most of the manual work for us, that way our time could be better spent driving true outcomes"**
>
> Daniel Akiva, CISO

What followed was a transformation – not just in technology, but in trust.

Akiva built a lean but focused security team that partnered with IT, DevOps, legal, and compliance groups. He eliminated silos by positioning security as a catalyst for innovation, showing how every team now had instant visibility into every asset across the enterprise and the vulnerabilities associated with their operations. Within weeks of deploying Rapid7, the team uncovered unauthorized access patterns, surfaced misconfigurations, finally gained visibility into their multi-cloud environments, and identified gaps that had flown under the radar for years.

The narrative shifted. Security wasn't a roadblock – it was essential.

THE ATTACK SURFACE MAY DEFY CLEAR DEFINITION, BUT NOT CONTROL

Americor has a distributed workforce with over 1,600 employees. "You don't have just offices, we have remote employees, and people located around the world," Akiva explains. "If I were to define a modern attack surface, it's any endpoint, any system, really anywhere data resides that belongs to the company, anywhere users are logging into using corporate credentials. The question becomes how do you tie those together in some meaningful way? What's actually happening there"

The combination of Exposure Command and 24/7 Managed Detection and Response (MDR) monitoring has transformed the work and outcomes – connecting proactive risk reduction with rapid threat response.

Exposure Command provides direct visibility into real-time vulnerability context, prioritizing threats that pose the greatest risk – not just those that trigger alerts.

Akiva gave an example, “we noticed there were several users who were connecting from places we were entirely unaware of. We found teams in Russia that were using an unsanctioned VPN. Because of Rapid7’s ability to identify this to us, we are now implementing a company approved VPN to reduce the risk of unsanctioned access to proprietary data.”

Since Rapid7 doesn’t charge on data ingestion, Akiva reflected on how critical this was in his decisioning, “One of the main reasons we went with Rapid7 over other platform competitors, is how many native integrations were included in the platform. You have so many connectors into the platform for third party tools, it made onboarding a lot easier and we were able to see the platform’s value immediately.”

With Rapid7’s universal agent, Akiva highlighted, “we’re now getting up-to-date understanding on vulnerabilities, and have the right platform that gives us the tangible evidence and justification to drive the necessary change and evolve” Akiva says. And when an incident does occur, Rapid7’s MDR team detects and helps shut it down in minutes.

“Rapid7 was pretty easy to deploy in comparison to other agents. EDR providers are really good at killing processes, but we have to tune it so it’s not killing processes in our production environments. Getting the Rapid7 agents deployed allowed us to see a tremendous amount of information instantly out of the underlying assets without being disruptive to productivity. This makes it a lot easier to go to engineers with evidence and drive healthy collaboration cross-functionally. I see the Rapid7 agent as complimentary to best-in-breed EDR for a true defense in depth approach”

Akiva continues, “When you have workloads with little-to-no security telemetry, like production workloads containing PII, you have to think of risk in relevant terms. Controls in place at the user/employee levels worked well for us. We never had that level or degree of control in our cloud environments and the teams accessing them.”

Rapid7’s Exposure Command, “helps tie together our previously fragmented attack surface and define what it truly is, what our assets are comprised of and the existing vulnerabilities/gaps in coverage to take action on it.”

Today, Americor has a continuous, unified approach to security with complete visibility into what was previously unknown. Akiva and the Americor team were able to reduce costs, hire three full-time employees, and operate with a rare level of transparency, expert 24/7 SOC support, and pricing predictability that only Rapid7 offered.

As the company grows into new verticals and markets, security is up front, built in, never bolted on. The board sees the ROI, not just in risk reduction, but in resilience. And the fractional CISO is an indispensable advisor with a dedicated seat at the table—and a clear vision for what’s next.

“We’re not just reacting anymore. We’re building ahead of the business. That’s where security belongs.”

Command and control. Rapid7 is there for that.

> **“Getting the Rapid7 agents deployed allowed us to see a tremendous amount of information instantly out of the underlying assets without being disruptive to productivity.”**
>
> Daniel Akiva, 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