RAPID7

CUSTOMER STORY

Industry
Finance

Company Size
Enterprise (Large)

Products
Managed Threat Complete—Ultimate

Customer website
AAA Northeast

HOW AAA NORTHEAST WINS THE 24/7 BATTLE TO PROTECT ITS MEMBERS

Threats evolve faster than security teams can blink. According to Rapid7's 2024 Attack Intelligence Report, 53% of new widespread threat vulnerabilities were exploited before software producers could implement fixes. This attack landscape is exacerbated by the expansion of AI and a consistent shortage of resources. It's challenging even for the most capable security teams, and the team at AAA Northeast is no exception.

AAA Northeast serves almost seven million members across six states. In addition to world-class 24-hour roadside assistance, members have access to a range of specialized products, including auto, home and life insurance; a full-service travel agency; competitive loan rates; and exclusive discounts on everyday purchases and driver training programs. As a member-centric organization, AAA Northeast is committed to maintaining a reliable, secure system to deliver these services.

7 MILLION
MEMBERS ACROSS SIX STATES

53% OF NEW WIDESPREAD THREAT VULNERABILITIES WERE EXPLOITED BEFORE SOFTWARE PRODUCERS COULD IMPLEMENT FIXES. [1]

1 Rapid7's 2024 Attack Intelligence Report.

The AAA Northeast IT Security team had a highly skilled in-house SOC who faced the same challenges most security teams know too well:

- **Juggling too many monitoring tools.** The previous approach was to adopt best of breed for every single solution, but managing many platforms requires extra training and expertise to ensure everything is well configured.
- **Finding off-hours coverage.** Bad actors don't keep regular schedules, so team members had to respond to incident issues outside of their working hours.
- **Wasting time on false positives.** The program was reactive. Because they had to investigate every potential incident, they had less time to work on longer-term projects to enhance the program, such as reviewing and going deeper into existing controls.

> **"We quickly expanded with Rapid7 because we were getting the right support and the right performance from their solutions. The services are easy to integrate, the breadth is huge, and our experience has been tremendous."**
>
> Gaël Frouin, AAA Northeast
> Director of IT Security

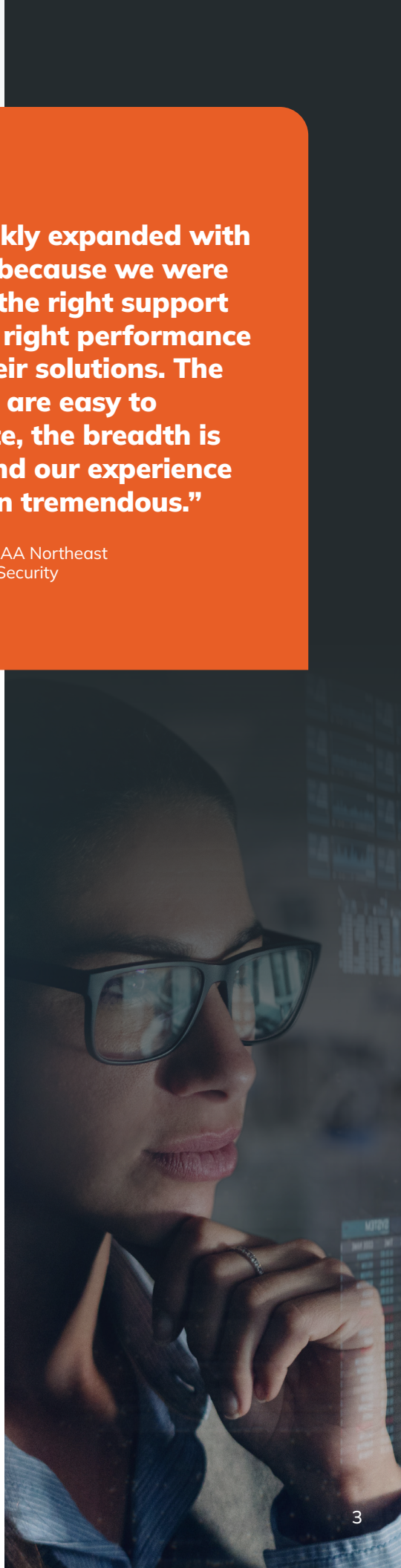
AAA Northeast found Rapid7, which addressed these concerns and offered integrated tools to detect and respond to threats. When Director of IT Security Gaël Frouin joined, he went even further, expanding their ecosystem to add Rapid7's Managed Detection & Response (MDR) service. Rapid7 MDR combines advanced protection of every attack vector, expert support and strategic guidance, and unlimited incident response—ensuring wider coverage and a more proactive, resilient approach.

"We quickly expanded with Rapid7 because we were getting the right support and the right performance from their solutions," Gaël said. "The services are easy to integrate, the breadth is huge, and our experience has been tremendous."

CYBERSECURITY THAT NEVER SLEEPS

Attacks often happen on nights, weekends, and holidays, when coverage tends to be lower. It's no wonder security leaders lose sleep, worrying something might slip through the cracks.

The Rapid7 SOC, as part of MDR, provides the assurance and confidence Gaël and team need to rest easy. "Knowing that Rapid7 is monitoring our environment 24/7 has helped the team to relax a bit more," Gaël said. "Now they can focus on those times when there's something critical to jump on, avoiding the alert fatigue that burns teams out," he said.



False positives used to drain the team's time and energy, but that's no longer an issue. Powered by AI, Rapid7's SOC automatically triages and prioritizes alerts and auto-closes false positives with a 99.89% success rate. Threats are automatically contained, so teams know exactly what to address. They also have access to a robust detection library and the ability to customize detection with guidance from their dedicated cybersecurity advisor. That efficiency allows Gaël and his team to be more effective. "Over the past couple of years, we've worked hard to augment our operations," Gaël said. "Rapid7 helps us limit distractions and respond faster to what's really suspicious."

Another improvement comes from increased visibility. Visibility is everything in security, and Rapid7's next-gen SIEM and XDR, InsightIDR, gives AAA Northeast complete insight into their security posture. Through the platform, the team can see what the Rapid7 SOC is monitoring, identify trends, and track threats as they emerge. This enhanced transparency not only strengthens their posture but also fosters greater collaboration and confidence in the outcomes delivered by the SOC.

EXTRA EYES AND INSIGHTS FROM A TEAM THAT'S SEEN IT ALL

Outside expertise goes a long way when protecting customer data. For Gaël's team, Rapid7's consultancy is absolute gold. "Rapid7 provides us with different ideas and recommendations, as well as a broad view of global security trends," Gaël explained. "Their advice helps us to refine and validate our internal practices."

Their strategic cybersecurity advisor provides ongoing insight, guidance, and support. This advisor has become a sounding board for the team while also sharing the latest threat intel, lessons learned from other customers, and advice on how to handle incidents or investigations. "We don't just have to rely on our expertise; we have a valuable external perspective that gives us confidence we're doing the right thing and going in the right direction," Gaël said.

Another win? The smart integration and consolidation of tools. Rapid7 MDR's seamless third-party integrations make it easy to extract and isolate threats while advanced threat intelligence targets the risks most relevant to AAA Northeast—ensuring the team is continuously ready for whatever threat emerges. And when the inevitable happens, Rapid7 integrates the leading open-source DFIR application, Velociraptor, for targeted threat hunting and deep forensic analysis. "Instead of dispersing our talent across many different platforms, we've concentrated our security tools and skillsets, which improves productivity and is key to being able to grow," Gaël added.

With the right advice and tools, Gaël's team has breathing room to tackle more big-picture projects. Engineers and analysts are free to focus on tasks with higher value, which have further reduced vulnerabilities.

> **"Instead of dispersing our talent across many different platforms, we've concentrated our security tools and skillsets, which improves productivity and is key to being able to grow."**
>
> Gaël Frouin, AAA Northeast Director of IT Security

LESS TIME EXTINGUISHING FIRES, MORE TIME TO EXPAND

True ROI in security is often invisible. Sometimes, the proof of a successful security program is that nothing happens. But for Gaël and his team, the value of Rapid7 is clear. Finely-tuned detections and AI-powered alert triage from an expert SOC reduces their workflow, allowing their internal resources to go further.

“Rapid7 ensures our security efforts are prioritized correctly,” Gaël said. “Without their efficient tools and services, we wouldn’t have been able to grow both the depth and scope of our security program the way we have. They’ve helped us reach our highest potential.”

A big part of their success comes from their relationship with the Rapid7 team. “Rapid7 is a key trusted security partner,” Gaël said. “They’re not just here to sell you something. They want you, your organization, and your security program to succeed.”

It’s easy to prove value to the board through quarterly reports that detail how many attacks Rapid7’s MDR service has caught. Add third-party validation from Gartner and a loaded cabinet of industry awards, and Gaël knows they’re in the best hands. With almost seven million people to protect, that confidence is priceless.

Rapid7 is a key trusted security partner. They’re not just here to sell you something. They want you, your organization, and your security program to succeed.”

Gaël Frouin, AAA Northeast Director of IT Security

Secure your end-to-end ecosystem with Rapid7 Managed Detection & Response.

LEARN MORE

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/try/insight