CUSTOMER STORY

RAPID7

US Signal

Adds Rapid7 Platform and Managed Services to Protect Its Customers' Networks

Products

- InsightVM
- Managed Detection & Response
- InsightAppSec
- InsightConnect

Industry

- Communications & Media

Size

- Enterprise (Mid-Size)

Overview

The Company

US Signal is the largest privately held data center services provider in the Midwest. The company provides industry-leading data center technologies, cloud solutions, and managed services to help companies transform their IT operations and meet the ever-changing technology and business needs. The key to US Signal's ability to deliver "total" solutions is its 14,000-mile secure fiber network with access to over 225 data centers and POPs, Tier 1 peering relationships, and metro rings in strategic markets. It's what makes US Signal one of the few companies that can develop comprehensive IT solutions that minimize downtime and latency, and ensure reliability, speed, and security.

The Challenge

US Signal's major security concern is protecting customers' networks. "We're both an internet service provider and a cloud-hosting provider," states Nick Defoe, director of information security. "Seven of the top ten healthcare systems in Michigan are customers of ours, in addition to the largest mental health provider in western Michigan, many managed service providers (MSPs), and numerous financial institutions. So, we have out-sized security needs."

Doing security well for customers means paying attention to a range of threats, large and small. As with many companies, phishing is a major concern. As is the accelerating pace of vulnerability discovery and the required patching and mitigation of vulnerabilities."That seems to be something that's accelerated over time," explains Defoe. "It just seems to keep coming faster and faster."

US Signal also ensures compliance with various security frameworks and regulations, including SOC 2, PCI and HIPAA. "We maintain high levels of compliance to ensure we are doing what's needed to keep our company and our customers' data safe."

Unfortunately, the vulnerability management software they were using before Rapid7 couldn't keep pace with US Signal's evolving environment. "The previous product was not particularly cloud-friendly," noted Defoe. "It required a lot of on-premises infrastructures to get coverage into all of our various environments. Because of that complexity, it was a lot more challenging to manage our vulnerability assessment program. That's when we started looking at other providers."

The Solution

US Signal replaced its existing vulnerability management platform with Rapid7 InsightVM.

Two years ago, US Signal replaced its existing vulnerability management platform with Rapid7 InsightVM. One year later, they added the Rapid7 Managed Detection and Response (MDR) service, which includes access to InsightIDR, Rapid7's SIEM/XDR. US Signal had worked with several SIEM tools over the past three years but wanted a cloud-based tool, so they can easily collect data from endpoints no matter where they are, and not have to manage the infrastructure on-premises.

"Once we switched to the Rapid7 platform, we found that the ability to collect vulnerability metrics via a more cloud-friendly approach greatly improved our ability to assess all of our systems," states Defoe. "As a part of our defense in depth strategy, we enforce network segmentation between our enterprise and production services environments. Being able to assess those environments in real time while maintaining segmentation between them is important to us."

Value Right Out-of-The-Box

A key factor in Defoe's selection of Rapid7 was the quality of the Rapid7 Insight Agent and how it operates in a cloud environment. "We can use the Rapid7 Insight Agent to do assessments in a more cloud-friendly and remote worker-friendly way. When we evaluated the MDR service, leveraging the Insight Agent was turnkey, so we were able to onboard with MDR very quickly. The Insight Agent became even more valuable when, because of its dual role in both vulnerability management and detection and response, we had log collection instantly from all of our hosts since the agent was already in place."

"The deployment of MDR was super easy compared to our previous tool," Defoe says. "All you have to do is install the agent. We turned the Insight Agent on to collect data for MDR, within a matter of minutes, we were seventy-five percent done. The Insight Agent provides excellent telemetry. We very quickly went from nothing to the POC providing real security value. The other thing that was just a huge relief to us is that the alerts we get out of the MDR service are much more accurate than what we saw from our previous SIEM."

"The Insight Agent became even more valuable when, because of its dual role in both vulnerability management and detection and response, we had log collection instantly from all of our hosts since the agent was already in place

Nick Defoe, Director of Information Security

Engaging All Teams in Vulnerability Management

Another key difference with Rapid7 InsightVM is the ability for Defoe to get other team's directly involved in using the platform for vulnerability management. "We've got at least five different teams that have responsibility for their own systems, including corporate IT, security operations, software development, cloud engineering and our facilities team," explains Defoe. "Using the dashboard interface, we've been able to build out the reporting for each individual team to get the high-level overview of where they're at and what they need to do to keep up with vulnerability management. Getting these disparate groups all into one platform where they can see what they need to do for vulnerability management has been critical to our success."

Defoe holds a weekly vulnerability management meeting with all the teams to review the upcoming issues they are seeing, the critical vulnerabilities each team needs to expedite patching of, and the overall status for each team. "It's part of our vulnerability management policy that we follow certain requirements. Everything is tracked and reported to our auditors and our executive security team. Vulnerability management is a critical part of what we do here at US Signal.

Expanding the Capacity of The SOC

Defoe also manages a 5-person SOC which includes an automation engineer, a security engineer and three analysts. They handle incident review, vulnerability management, security testing and pen testing along with email phishing and user education. Although the US Signal Security Operations Center does respond to critical security events 24/7, the team relies on Rapid7 MDR, with its follow-the-sun SOC model to enhance their decision making and responsiveness. "Having those eyes on glass 24/7 with MDR, to be able to raise and escalate alerts that are of critical importance around the clock is a big relief. The reduced alert volume certainly helps us sleep better, too. We're not flooded with false-positive alerts day in and day out like we were previously. Having the Rapid7 MDR SOC as a backstop is definitely very helpful."

"The user interface for MDR - InsightIDR - also is a lot better than our previous SIEM," Defoe says. "Before we would have to drill down two levels to get to the alerts we were trying to review and close. We had such a volume of alerts they got buried in this weird user interface and we would actually miss alerts. Now, we get much higher quality alerts right at the top of the queue."

1.2T

Weekly Security Events

RAPID7

In the coming year, Defoe will be focusing on automation using Rapid7 InsightConnect. "We really want to double down on our automation efforts, so that we're making sure that we continue to scale our capabilities faster than we're having to scale the number of people that are here on our team."

When a strong security team, like the one at US Signal, has the right security tools in place, things have a way of becoming more predictable and less three-alarm fire. "All of the alerts that we've gotten out of the Rapid7 MDR service over the past few months have been either security testing or legitimate activity. We haven't had anything that would classify as a major security incident."

In the end, Defoe's security approach is simple and straightforward. "It's important that our organization has the right people to meet our security demands, but also that we have the right tools, solutions, and services in place to assist us - which is something we're constantly evaluating. We are setting ourselves up for success when it comes to managing ongoing vulnerabilities, detecting and responding to anomalous behavior, and identifying weaknesses that might expose us and our customers to risk."

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 attackers methods. Trusted by more than 10,000 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

PRODUCTS

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

CUSTOMER SUPPORT

Call +1.866.380.8113

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