Experity Relies on Rapid7 Managed Services to Scale Security Operations

Managed AppSec, Managed Detection and Response

TABLE OF CONTENTS

In 2019, the two largest urgent care Electronic Medical Records (EMR) companies in the country came together to form Experity, a dynamic Health Information Technology company. With the merger came more employees in more locations working to develop and support Experity's comprehensive urgent care operating system. Today, Experity provides integrated technology and services solutions to more than 5,700 on-demand healthcare practices, urgent care centers, diagnostic testing centers, and primary care centers nationwide. The company is growing quickly as it works towards its mission to power the patient-centered healthcare revolution.

Rapid7's got the market cornered in terms of managed services. We now lean on MDR to vet alerts and tell us if they're seeing unusual activity from a user. The majority of the time when we get an alert, it's already handled by an engineer.

- Carl Stern, Director of Information Security

The Challenge

The rapid expansion of personnel, office locations, software and services as a result of the merger created unique challenges for the security team. "We've got a small team and we're charged with a fairly substantial mission to protect the company from loss events of any kind," said Carl Stern, Director of Information Security. This need for business continuity and standardization fueled the Experity team's search for a provider that could help them manage security operations and build resilience in their security program. "Which is where Rapid7 managed services comes into play," explains Stern. "Without Rapid7 managed services we would probably need to triple or quadruple the size of our team just to get the coverage we need."

Stern was tasked with building a security team and enhancing the caliber of the security tools at their disposal. "The company had been using a Managed Detection and Response (MDR) platform but it became clear to me that while it addressed a need at the time we implemented it, the solution didn't really roll with all the changes. For example, it only monitored network and server activity and not endpoint activity. We wanted to be able to monitor desktops and laptops because nine times out of ten, that's where companies get into trouble -- from a user clicking on something they shouldn't."

Prior to the merger, most employees were based in one office. So, if Stern saw activity from a user, he knew the user and what they should be doing. With Experity's new scale, the security team needed a platform to vet alerts. "We have so many more employees and contractors, so if we see alerts or activity from these users, we don't know if that's normal or not," explained Stern. "That's a pretty unique challenge for us."

Stern began looking for an MDR and vulnerability management solution that could monitor all activity and offer a user-friendly and actionable dashboard. "I wanted a company that had the right product and provided a managed service, because at the time it was just me and there was no way one person could monitor traffic 24 hours-a-day. And I wanted to be able to come in in the morning and look at a single pane of glass and see what had happened over the previous 24 hours and if there was anything I should be concerned about."

The Solution

Experity found its answer in Rapid7, purchasing MDR for incident detection and response, Managed AppSec to enhance their application security, and InsightVM for vulnerability scanning. Through activity monitoring, dynamic application security testing, and advanced vulnerability management analytics, Experity can now automatically assess, understand, and respond to risk across the entire IT infrastructure.

"Rapid7's got the market cornered in terms of managed services," stated Stern. "We now lean on MDR to vet alerts and tell us if they're seeing unusual activity from a user. The majority of the time when we get an alert, it's already handled by an engineer. I know that if an alert gets to us and Rapid7's MDR team is asking us questions, I'm confident telling my SecOps team to stop what they're doing and address it immediately."

Meeting Regulatory Compliance Standards

These advanced security capabilities have proven helpful for identifying and squashing malicious behavior and ensuring compliance with regulations such as HIPAA and HITRUST. "In one of our solutions, all user accounts are now managed in Active Directory, and all of a sudden we were seeing thousands and thousands of users that were clients. Rapid7 is extremely helpful in that regard, alerting us if there is anomalous behavior that has the potential to put a client's credentials at risk."

Cutting Through The Application Security Clutter

As Experity's portfolio grew, Stern looked for a robust solution to provide vulnerability management insights across their web applications which the development teams had been managing. Rapid7's InsightAppSec, the technology behind Managed AppSec, provides all the capabilities they need with the added benefit of offering a managed service. "InsightAppSec has helped us solidify our inventory of web apps. We can see where our apps live, and essentially we have a place where we can work without impacting the production environment," explained Stern. "That's pretty big for us."

Stern also noted that Rapid7's Managed AppSec provides validation and context that allows his team to focus on what is critical. "If we managed application security tools internally, we'd see hundreds of alerts and have to parse through and figure out what's what. Managed AppSec is a lot more manageable than having a static Excel sheet or a PDF of a hundred things to look into."

Rapid7's team also meets directly with the Experity developers that are responsible for remediation. "That's huge," stated Stern, "because it eliminates the 'lost in translation' issue, where the findings get communicated to my team. My team takes notes. My team goes to the developers. Developers ask questions. We try to answer, but we might be getting some of it wrong. And so we cut that part out. That's been great too."

Rapid7 Managed AppSec customers have access to view the underlying InsightAppSec dashboards as part of their service subscription, a popular value-add and differentiator for Experity's security team. "With a lot of other managed services, it's a black box and you only see a portion of what's going on in your environment," said Stern. "I like that although Rapid7 is a managed service, we still have full access to a dashboard for greater visibility. Our Rapid7 Security Advisor will also email me to let me know about interesting findings. It's more of a human connection."

I like that although Rapid7 is a managed service, we still have full access to a dashboard for greater visibility. Our Rapid7 Security Advisor will also email me to let me know about interesting findings. It's more of a human connection.

- Carl Stern, Director of Information Security

Gaining The Peace Of Mind To Focus On What's Next

"With the breadth of responsibility we have, there are so many things we need to be doing beyond just looking at environmental alerts," said Stern. "Knowing that we have a 24-hour MDR SOC doing that for us is great. I'm finally able to focus on the big picture and plan the direction of our program instead of getting bogged down in the minutia of each alert. My team can focus more of our energy on our operations project work, and policy and audit work, which is a bear, especially when you're talking about things like HITRUST certifications. We've made a lot of progress in maturing our policy and audit program thanks to an incredible team,and part of that success is due to our partnership with Rapid7."

A Partnership Built For The Future

The relationship with Rapid7 has given Experity's security team greater confidence in their ability to scale as the company expands. "One of the things I love about Rapid7 is that they're constantly evolving and improving their products, just like Experity continues to grow and be the market leader in urgent care EMR," said Stern. "At Experity, one of our core values is "Team First", and I'm fortunate to work with an extraordinary team, and Rapid7 is an extension of that. Rapid7 has been a real partner, staying with us and supporting us through this whole process."