RAPID7

Chemung Canal Trust Company

Rapid7 Provides Confidence and Credibility
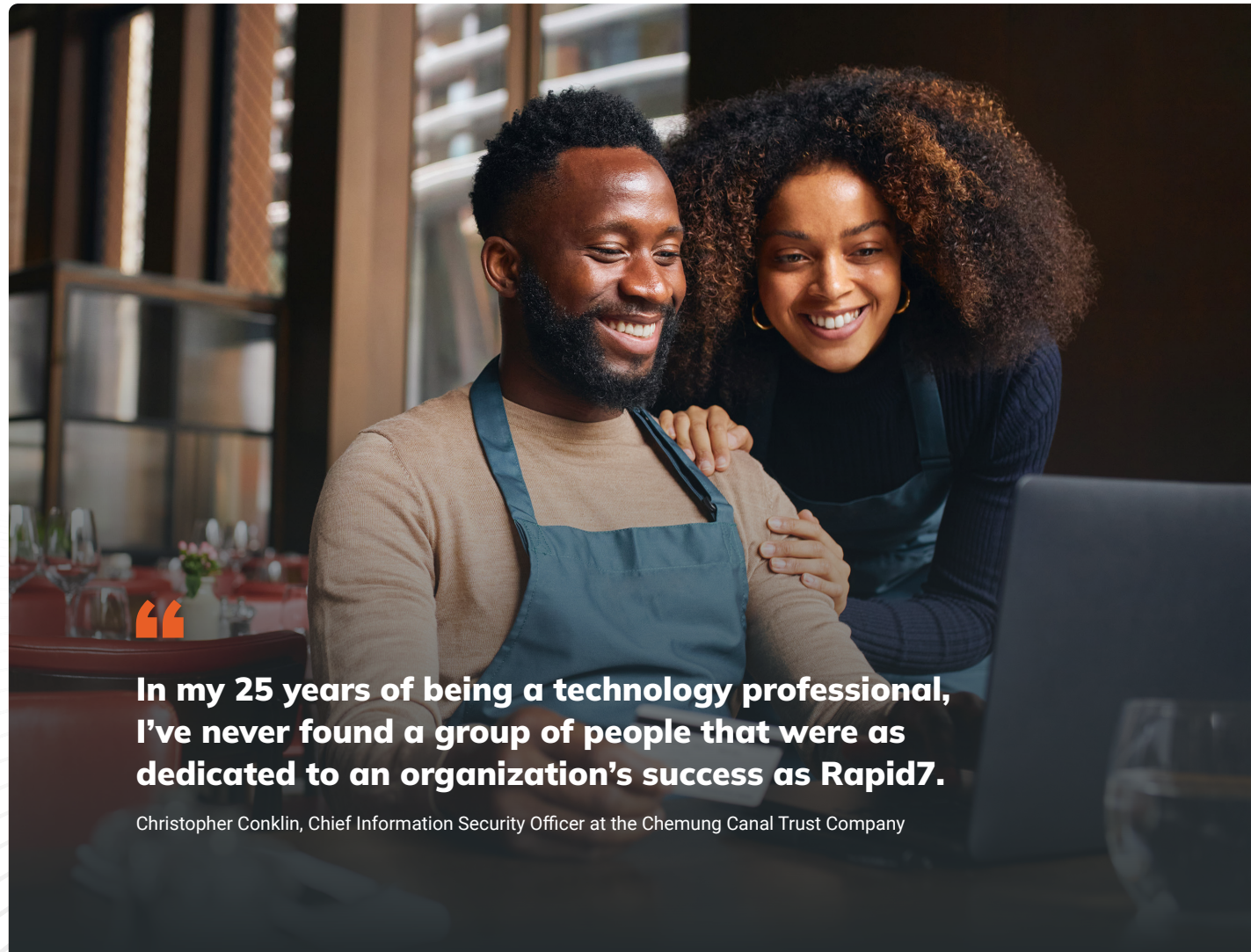
Industry
Finance

Region
Americas

Products
InsightVM, MDR, Security Advisory Services

Size
Mid-Market

" In my 25 years of being a technology professional, I've never found a group of people that were as dedicated to an organization's success as Rapid7.

Christopher Conklin, Chief Information Security Officer at the Chemung Canal Trust Company

Overview

Company

Since 1833, Chemung Canal Trust Company has provided continuous, progressive financial and credit services to south central New York State. Only two years earlier, the first steam-propelled locomotive made its initial trip from Albany to Schenectady; stage coach lines were still big business; the Chemung Canal had just opened; and the Erie Railroad was still a dream. The company's mission is to remain a strong and independent financial services organization creating value for shareholders, clients, employees and the communities where they do business, while maintaining the highest standards of business ethics.

Challenge

Christopher Conklin is the Chief Information Security Officer at the Chemung Canal Trust Company (CCTC) in Elmira, New York, where he oversees the work of two information security analysts. They signed with Rapid7 over a year ago after deciding they needed more visibility into their information architecture to best fulfill their core mission. Rapid7's InsightVM and InsightIDR have empowered them to do so efficiently, quickly, and easily.

Solution

Virtually as soon as they signed on with Rapid7's InsightIDR platform, CCTC was able to quickly establish a baseline of known activity and highlight any anomalies, such as failed authentication attempts and potential lateral movement. "It was very easy for us to create custom alerting for activity we felt important to monitor like account deletions, nslookup commands and inactivity on specific log sources," he recalled.

According to Conklin, the built-in detection rules that Rapid7 provides are phenomenal, but his team was particularly pleased that they were able to create specific rules tailored to their organization. "The logging capabilities are very, very robust," he explained. "It really helps give visibility into risk from a single pane of glass that we might otherwise miss."

"We had considered some other security tools, but we felt they were inferior to what Rapid7 could offer," divulged Conklin. "We had a vendor selection process where we vetted Rapid7 against other competitors. But Rapid7 came out well above and beyond its competitors due to its ease of use and the scope of the visibility with regard to strengths and weaknesses. The time it took to implement was very, very short. We were up and running within a few hours."

Conklin didn't hesitate to delve into specific examples, honing in on the visibility of their vulnerabilities. "We thought we had a good handle on our vulnerabilities. But InsightVM's scanning agents showed us existing vulnerabilities that we had to address," he listed. "From a day-to-day perspective, when we're in there, everything is seamless and just works well together. If we're looking at a vulnerability, we can see how it relates to a detection. If we're looking at a detection, we can see how it relates to a vulnerability. That helps us prioritize things before we address them. That means we can accurately chart our course day-to-day."

> **"**
>
> **We thought we had a good handle on our vulnerabilities. But InsightVM's scanning agents showed us existing vulnerabilities that we had to address...**
>
> Christopher Conklin, Chief Information Security Officer

Confidence and Credibility

Another benefit of Rapid7 for CCTC has been greater trust in their findings, knowledge and conclusions. "In most complex organizations, there's not always a particular person or a group that knows everything," mused Conklin. "But we were able to leverage our investment in Rapid7 to become an authority. We were able to be sure we understood what was going on in our organization and identify some things that were previously unknown."

According to Conklin, Rapid7 provided credibility and confidence in their observations and findings. "Instead of going around and double-checking all of these different data sources (authentication sources, netflow information, endpoint activity) and wondering how they align with each other, Rapid7 provides a much more holistic, clear depiction of what's going on in our environment. And we trust that depiction," he explained.

Prolific Patching

InsightVM has saved CCTC several hours a month when it comes to patching. "The product helps highlight what your true pain points are versus what you think your pain points are, so we were able to save a lot of time," Conklin shared. One of those time-saving opportunities were Remediation Projects for vulnerabilities that posed CCTC the highest security risk. Once created, these projects help IT teams target specific patching measures and maximize the return on their patching efforts.

"Rapid7 also has a host of dedicated and well-experienced professionals just a phone call away, so if you don't really understand it or you're confused by which metrics you should really go after, you can consult with them and they will help you build your program," he recommended. "So, that's something that we did early on. We consulted with them to ask, Look, we think we have a good understanding of what we should be tracking for metrics and what we might expect to reduce, but what's your perspective? And they were very, very helpful."

> **"**
>
> **The product helps highlight what your true pain points are versus what you think your pain points are, so we were able to save a lot of time...**
>
> Christopher Conklin, Chief Information Security Officer

Dynamic Detection

When asked about his favorite features of Rapid7, Conklin identified the platform's willingness and ability to improve its detection rules. "When new threats come out -- and they're always coming out – we typically have the same concerns. What's our reaction time? How quickly can we scan for them? If it's in our environment, how quickly will the detection rules be updated?"

Fortunately, Rapid7 updates detection rules and scanning agents frequently. Conklin is even able to review them on weekly calls with his customer service team – and he is impressed at how quickly those are updated. "It provides a lot of leverage. Maybe somebody on our executive team is reading an article and they see a topic. They often reach out to us, and we're already well-positioned, thanks to Rapid7, to address those concerns," he beamed.

"

They're very, very committed to helping organizations succeed.

Christopher Conklin, Chief Information Security Officer

Customer-Centric

Conklin's biggest concern when looking for a cybersecurity platform was that, after buying a product, his team would be left to fend for themselves. But he quickly learned that he had no need to worry about that. "In my 25 years of being a technology professional, I've never found a group of people that were as dedicated to an organization's success as Rapid7," he enthusiastically revealed, even referring to his customer service advisor as an extended member of his team.

"Everybody at Rapid7 is very quick to help. They're always checking in, touching base. It's not a set-it-and-forget-it mentality; there's a constant synergistic dialogue," he described. "They're very, very committed to helping organizations succeed. The technology and the processes and detection rules and all that, they're great. But really it's the staff that make it such a value-add proposition for organizations like ours."

View all of our customer success stories.

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 attacker methodology. Trusted by more than 11,000 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

CONTACT US

rapid7.com/contact

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

6