RAPID7

Industry
City Government

Region
Americas

Size
Small

Products
Managed Threat Complete

BEYOND CITY LIMITS:
A LEADING U.S. MUNICIPALITY TRUSTS RAPID7'S MDR FOR 24/7 SECURITY

SECURING A MIDWEST CITY'S CRITICAL INFRASTRUCTURE

In the western Colorado region, a prominent city in the Midwest plays a pivotal role — not just as a municipality but as a leader in managing regional infrastructure. Under the watch of the Chief Information Security Officer (CISO), the city's IT department oversees a vast range of services, from parks to critical infrastructure like water systems and waste management. Yet, with a small security team, the demands of keeping the city's systems safe from cyber threats have grown significantly. This Midwestern hub needed a trusted partner to help manage and secure its sprawling digital infrastructure. Rapid7 became that partner.

THE CHALLENGE

Managing Security with a Small Team

As the sole dedicated security personnel, the CISO had long recognized the growing complexity of the city's digital infrastructure and the increasing cyber threat landscape that came with it. Protecting essential services like fire response and waste management meant there was no room for gaps in security. The CISO knew that having real-time visibility across the city's systems was crucial to preventing potential threats from going unnoticed.

"I've always wanted some sort of log management solution," the CISO recalls. However, managing a wide array of security appliances, correlating data from multiple sources, and ensuring the city's safety with limited resources posed a considerable challenge. This was especially crucial, given that they were responsible for essential services like fire response and waste management, which are critical to the daily functioning of the city.

When the Log4j vulnerability made headlines in 2021 and directly impacted the city systems, it became the turning point. "I would have been able to see this if I had something in place," the CISO said of the vulnerability that plagued security professionals for months.

+

This incident underscored the need for a robust, centralized solution to gain full visibility into the city's infrastructure and quickly respond to emerging threats.

+

The demands of keeping the city's systems safe from cyber threats have grown significantly.

THE SOLUTION

A Unified Approach to Managed Detection & Response and Vulnerability Management with Rapid7's Managed Threat Complete

The CISO evaluated several options but was ultimately attracted by Rapid7's comprehensive managed security solutions. Starting with Managed Detection and Response (MDR) and later expanding to Managed Threat Complete, which broadened their MDR coverage to include vulnerability management, the CISO found that Rapid7's offerings aligned perfectly with his vision of security.

For a small team like the CISO's, the benefits of a managed solution went beyond just monitoring. The 24/7 coverage with Managed Threat Complete allowed the city to respond to incidents, even during off-hours. As the CISO puts it: "It's crucial to have that ability to actively respond to an incident if I'm not available." He highlighted a particular incident where Rapid7's quick alerts enabled him to disable an employee's compromised email account before it could cause significant damage.

"
One of the big things that stood out to me was the ability to see what's going on in the environment. With other providers, I wouldn't have had that visibility. Rapid7 gave me access to monitor and address concerns before they escalated into critical issues."

Chief Information Security Officer (CISO)

THE BENEFITS

Proactive Defense and Comprehensive Support

Through Rapid7's suite of solutions, the CISO and his team gained crucial time back, focusing on strategic work instead of being bogged down by manual processes. The integration of Rapid7's Threat Command added an extra layer of defense by monitoring external threats and dark web activity. "We have highly visible officials, and it's important to know what's being said about them and what data might be exposed," the CISO said.

The collaborative approach between the CISO and the Rapid7 team also became a key advantage. "Sometimes I just don't have the time to write queries or analyze data in depth. But with Rapid7, I have a team of experts who can handle that for me. It feels like I'm no longer a one-person team," the CISO said. This partnership has allowed this Midwestern city to stay ahead of cyber threats while freeing up valuable resources for other projects.

> **"**
>
> **I have a team of experts who can handle that for me. It feels like I'm no longer a one-person team."**
>
> Chief Information Security Officer (CISO)

THE IMPACT

A Trusted Partnership for the Future

Since implementing Rapid7's solutions, the city has drastically improved its security posture. By leveraging tools like InsightIDR for managed detection and vulnerability management, the CISO can now preemptively address vulnerabilities before they become real issues. This proactive approach has helped the municipality not only react faster to incidents but also prevent them from happening in the first place.

"

Rapid7 allows me to balance managed services with visibility, I can log in, see what's going on, and act quickly if necessary. It's the perfect blend of managed service and hands-on control.

Chief Information Security Officer (CISO)

"

By helping this city protect essential services like fire response and waste management, Rapid7 plays a crucial role in safeguarding the community's digital infrastructure.

+

With Rapid7 as a trusted partner, the city can focus on what matters most – serving its people. Rapid7 is here for that.

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.

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/try/insight