



CUSTOMER STORY

Industry

Services

Region

Americas

Company Size

Mid Size

Package

Managed Threat
Complete Advanced

**NAVIGATING COMPLEXITY:
HOW MANAGED THREAT
COMPLETE SECURED A
SOUTHWEST TRIBE'S
DIVERSE OPERATIONS**

OVERVIEW

Comprehensive risk management and 24/7 threat coverage with Rapid7's Managed Threat Complete

In the Southwest Colorado region, a technology services provider delivers IT solutions that support tribal governments, businesses, and essential services. To enable these operations, a dedicated technology services provider delivers critical IT solutions, supporting services, economic development initiatives, and multiple business entities. With a mission to provide secure, high-quality, and timely technology solutions, the technology services provider's IT team plays a key role in enabling its clients to remain agile and innovative.

The Vice President of IT Security, oversees the protection of this vast infrastructure, which includes enterprise applications, network infrastructure, and telephone systems. With over 25 years of cybersecurity experience, their role is to ensure the security of critical tribal systems, including healthcare, business operations, and essential government functions.

Enter Rapid7's Managed Threat Complete—a service that brought together 24x7 threat monitoring, vulnerability management, and incident response under a single subscription. For the Vice President of IT Security, it was the exact solution their team needed to secure this vast digital landscape.



With the tribe's diverse ecosystem, from government operations to healthcare and casinos, we needed a partner that could cover every angle, Managed Threat Complete gave us 24x7 coverage and streamlined our approach to threat detection and response."

Vice President of IT Security

A GROWING SECURITY CHALLENGE

When the Head of IT Security joined the technology services provider, the security landscape was a patchwork of tools and manual processes. Their team struggled to keep up with threat detection and response while using legacy tools that just couldn't scale to meet the tribe's needs. Running security 24x7 with a small team was quickly becoming an untenable situation.

"We were doing this in-house with a small team and some cobbled-together tools," they recall. "It was exhausting, and there was no way it could scale given the complexity and size of our environment."

With critical operations running around the clock, it became clear that a more robust solution with automation capabilities was

necessary. The tribe needed a comprehensive approach to threat detection and response, vulnerability management, and incident response, to ensure consistent protection.

TURNING TO RAPID7'S MANAGED THREAT COMPLETE

The IT VP knew their team needed more than just another tool—they needed a trusted partner. After evaluating several providers through a series of proof-of-concept (POC) trials, they chose Rapid7's Managed Threat Complete (MTC), an all-encompassing solution for detection and response. MTC provides comprehensive security with Managed Detection and Response (MDR) for 24x7 monitoring, threat hunting, and proactive response, alongside InsightIDR for advanced SIEM capabilities and InsightVM for vulnerability management.

The speed of deployment and the effectiveness of the Managed Threat Complete solution were game changers for the technology provider's team.

MTC not only provided around-the-clock threat coverage but also included additional critical services, like unlimited incident response and proactive risk scoring, helping the IT security team secure their environment from all angles..

EXPANDING THE SECURITY LANDSCAPE WITH SURFACE COMMAND

As tribal organizations and businesses continue to expand their technology infrastructure, the IT security team is excited to implement Rapid7's Surface Command. This next-generation solution will give the team unprecedented visibility into both internal and external attack surfaces, eradicating blind spots and improving their security posture.

"Adding Surface Command will be a big step forward for us," the Vice President of IT Security says. "With the ability to monitor both



Rapid7 was different from the start. The time to value was critical—we were able to get the service off the ground quickly, and the existing agents we had already deployed made it seamless."

Vice President of IT Security



internal and external assets and eliminate shadow IT, we'll have even greater control over our environment and faster response times when threats emerge."

Surface Command is designed to unify the entire asset inventory, providing full context around potential exposures and enabling faster, more effective responses to emerging threats. With this proactive approach, the IT security team will be able to pinpoint

A KEY PARTNER IN SECURING CRITICAL INFRASTRUCTURE

Rapid7's MDR service quickly proved its worth by providing real-time threat detection and response. With a small team, they relied on Rapid7's global security operations center (SOC) to provide the 24x7 monitoring and response that their team simply couldn't maintain.

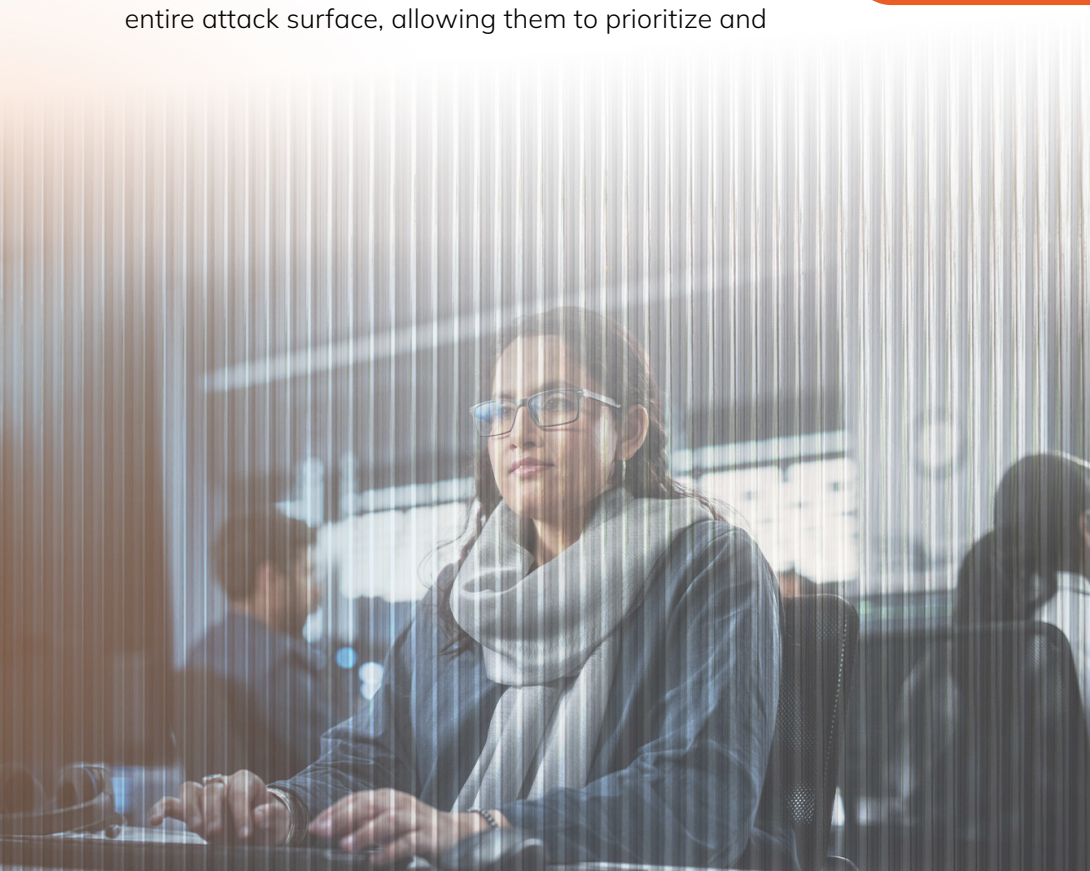
"Rapid7 is like having an extension of my team. We know that if something happens, we're going to get a call, and our guys are rested and ready to handle escalations," says the Vice President of IT Security.

The vulnerability management also improved dramatically with the introduction of InsightIDR. The IT security team now had a clear view of their entire attack surface, allowing them to prioritize and



My team can sleep at night knowing Rapid7's SOC is watching over everything."

Vice President of IT Security



“One of the great things about InsightIDR is its ability to detect impossible travel scenarios. We’ve caught compromised credentials multiple times where a user logged in from Colorado and then from London within minutes—that’s not possible,” they note.

REDUCING RISK AND ENHANCING RESILIENCE

With Rapid7’s solutions in place, the IT security team was able to streamline threat detection and response, reduce vulnerabilities, and enhance the tribe’s overall security posture. They even saw a reduction in cyber insurance premiums, thanks to the improved security measures.

By delivering 24x7 protection, shrinking their attack surface, and increasing visibility, Rapid7 has helped tribal enterprises and organizations stay secure and resilient. Rapid7 is here for that.



Partnering with Rapid7 has allowed us to reduce risk across all our operations—from healthcare to oil and gas to government services. It’s also helped me work with our underwriters to lower premiums and increase coverage.”

Vice President of IT Security



**View more
success stories.**

CUSTOMER STORIES



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