RAPID7

CUSTOMER STORY

Industry
Education

Region
Americas

Products
InsightIDR,
InsightVM,
InsightConnect

FROM RANSOMWARE TO RESILIENCE: HOW BLUE VALLEY SCHOOLS SECURED ITS FUTURE WITH RAPID7

OVERVIEW

Blue Valley Unified School District in Kansas encompasses more than 23,000 students and 3,100 staff and teachers across five high schools, nine middle schools, and 21 elementary schools. The district has a long-standing commitment to integrating technology into its curriculum, operating as a 1:1 enabled district where students have access to personal devices as early as kindergarten. Beginning in sixth grade, these devices travel between school and home, creating a dynamic but challenging security landscape. Ensuring a safe and secure learning environment for students is paramount, with all online activities protected through a cloud-based filtering system.

In August 2019, Blue Valley faced a wake-up call that no IT team wants: a full-domain ransomware breach. For a district responsible for tens of thousands of users across 55 sites, the attack underscored an urgent need for a dedicated cybersecurity strategy.

Enter Evan Nichols, Blue Valley's first-ever Cybersecurity Engineer. Having started on the district's support desk before moving into systems engineering, Evan was tapped to lead the charge in securing the district's vast, tech-heavy environment. A problem-solver at heart with deep technical expertise, he took point on selecting and implementing the tools necessary to transform Blue Valley's security posture.

"I actually picked Rapid7 for this environment," Nichols said. "A lot of that has to do with it being right-sized and the best possible fit for us. We don't have a lot of warm bodies, we don't have a lot of people trained as SOC analysts or engineers, so we needed a platform that could do a lot of the heavy lifting."

> **I actually picked Rapid7 for this environment. A lot of that has to do with it being right-sized and the best possible fit for us. We don't have a lot of warm bodies, we don't have a lot of people trained as SOC analysts or engineers, so we needed a platform that could do a lot of the heavy lifting."**
>
> Evan Nichols, Cybersecurity Engineer

A DISTRICT IN THE CROSSHAIRS

With one-to-one device programs starting as early as eighth grade and an open-ended approach to technology, Blue Valley faced unique challenges. Schools are prime targets for cybercriminals due to perceived resource constraints, and in 2019, attackers explicitly sought out Blue Valley as one of the largest districts in the state.

“Our biggest threats are always going to be ransomware and phishing,” Nichols explained. “K-12 education is a high target because the expectation is that we have shoestring budgets and a lack of manpower, and cybercriminals bank on that.”

Compounding the challenge was visibility—or the lack thereof. “It comes down to getting a 1,000-foot view with only a small team,” Nichols said. “The biggest challenge is avoiding alert fatigue and making sure we get pertinent data to the top immediately.”

A SMARTER, MORE AUTOMATED APPROACH

To combat these challenges, Blue Valley implemented the Rapid7 Platform, starting with InsightIDR for detection and response, InsightVM for vulnerability management, and InsightConnect for security automation.

“We needed a way to consume all of the events in the environment, and we landed on InsightIDR because there wasn’t a huge cap on the events we could bring in,” Nichols said. “When we looked at other cloud SIEM solutions, we would’ve been priced out really quickly. The only other option would’ve been to roll it all ourselves, which would mean a lot of on-premises storage and management overhead.”

> “
>
> **We needed a way to consume all of the events in the environment, and we landed on InsightIDR because there wasn’t a huge cap on the events we could bring in. When we looked at other cloud SIEM solutions, we would’ve been priced out really quickly. The only other option would’ve been to roll it all ourselves, which would mean a lot of on-premises storage and management overhead.”**
>
> Evan Nichols, Cybersecurity Engineer

Blue Valley was up and running with **InsightIDR in less than a week**—a crucial factor for a team that needed to move fast. “The Rapid7 platform was really easy to deploy,” Nichols noted. “It’s good at drawing to the surface the data that a security practitioner wants to see. I don’t have to search very far to understand what’s happening.”

AUTOMATION THAT ACTUALLY LETS YOU SLEEP AT NIGHT

A major force multiplier for Nichols' small team has been **InsightConnect**, which automates critical security workflows, helping reduce alert fatigue and response times. "We can sleep easily," Nichols said. "Between 5:30 PM and 6:30 AM, we have tailor-made workflows that account for the things that would otherwise keep us awake at night."

Blue Valley also relies on **custom parsing and log event sources** that integrate seamlessly with the Rapid7 platform. "With some products, you have to do a lot of upfront legwork to make sense of logs," Nichols said. "Rapid7 already cares about the same event sources that we do, which makes it easier to get useful insights right away."

THE RESULTS: NIGHT AND DAY

The impact of implementing Rapid7 solutions has been profound. Blue Valley reduced its **datacenter risk score from 70 million to 1.2 million**, a testament to its improved vulnerability management strategy.

"We went from no patching strategy at all to a structured approach that our leadership now fully supports," Nichols said. "The ransomware event was almost a blessing in disguise—it forced us to quantify our risk, and now we have the executive buy-in to enforce maintenance windows and proactive security."

> **We went from no patching strategy at all to a structured approach that our leadership now fully supports. The ransomware event was almost a blessing in disguise—it forced us to quantify our risk, and now we have the executive buy-in to enforce maintenance windows and proactive security."**
>
> Evan Nichols, Cybersecurity Engineer

Meanwhile, **50% or more of Blue Valley's security alerts are now automatically handled by InsightConnect**, reducing manual workload and enabling the team to focus on higher-priority initiatives.

"We're shipping in half a billion events a day to Rapid7," Nichols said. "The ability to see everything happening in our environment and know that we can take immediate action—without needing a massive security team—is game-changing."

A TRUSTED PARTNER FOR THE FUTURE

Beyond technology, Nichols emphasized the human side of Blue Valley's partnership with Rapid7. "Of all the companies I've worked with, Rapid7 seems to be the least siloed internally," he said. "With IBM, you never talk to the same person twice. With Rapid7, I've continuously worked with the same people the entire time."

Looking ahead, Blue Valley is already thinking about the next phase: penetration testing to further validate its improved security posture. "We say we're confident in what we've built, but now we're pushing to have Rapid7 do a pen test so we can prove it," Nichols said.

For a district tasked with keeping 23,000 students safe—both physically and digitally—Rapid7 has become an essential partner in its security journey. Rapid7 is here for that.

> **"**
>
> **Of all the companies I've worked with, Rapid7 seems to be the least siloed internally. With IBM, you never talk to the same person twice. With Rapid7, I've continuously worked with the same people the entire time."**
>
> Evan Nichols, Cybersecurity Engineer

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/trial/insight