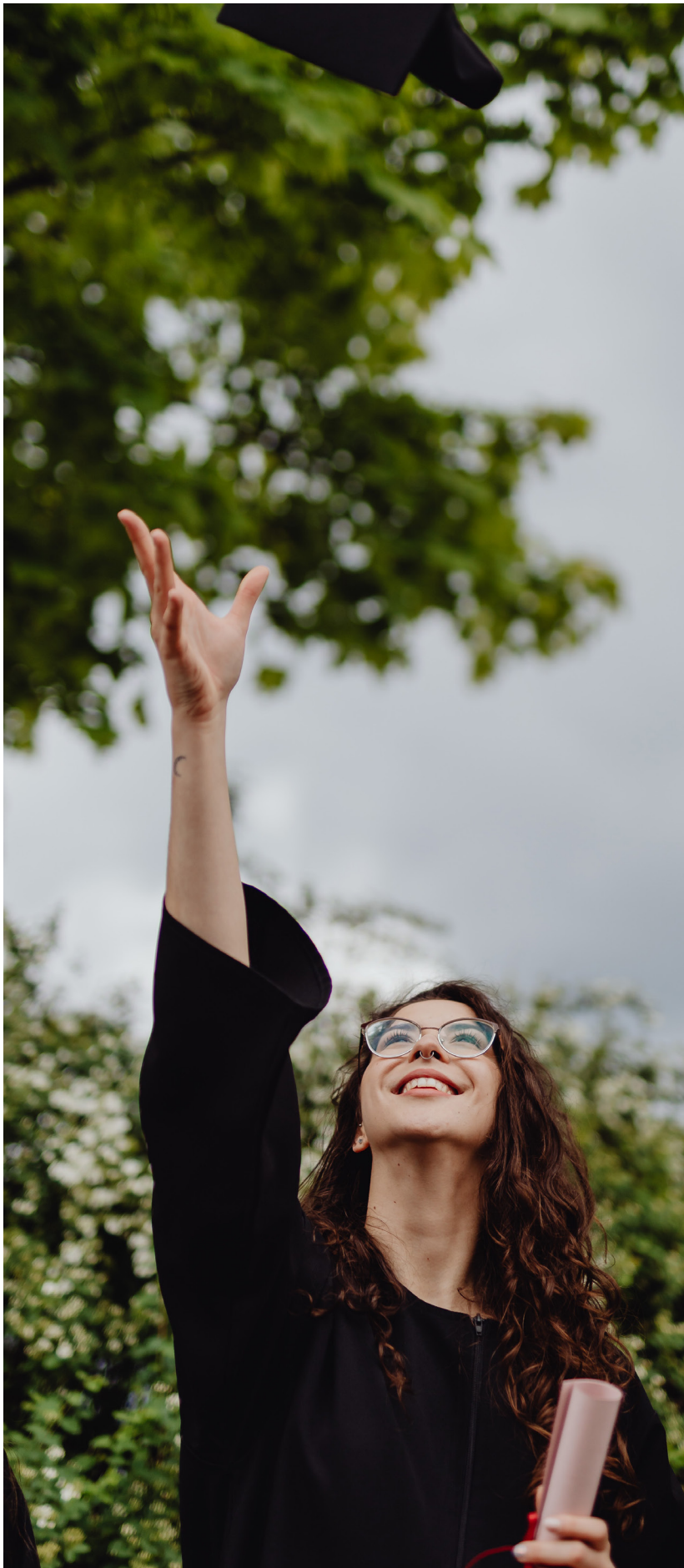
CUSTOMER STORY

Blue Valley School District

Partners with Rapid7 to Empower their New Security Team



Products

- InsightVM
- InsightIDR
- InsightConnect

Industry

- Education

Size

- Enterprise (Large)

Overview

The Company

Blue Valley Unified School District in Kansas encompasses more than 23,000 students and 3,100 staff and teachers spread over five high schools, nine middle schools and 21 elementary schools. The district has a long-standing commitment to ensuring the use of technology as an integral part of district curriculum and instruction. Blue Valley Schools is a 1:1 enabled district, which means that beginning in kindergarten, there is one device available for each student and beginning in 6th grade those devices go back and forth between school and home - an environment challenging enough to give any security professional serious pause.

Equally important, Blue Valley Schools is committed to providing safe learning environments for students. All district devices and activities students perform online are protected through a cloud-based filtering system 24/7. This means students can learn anytime, anywhere and always experience the same level of digital safety when on district devices, whether they are in the classroom, on the bus, or at home.

The Challenge

In August of 2019 Blue Valley was the target of a successful ransomware attack and after fortunately mitigating the attack immediately undertook a top to bottom security assessment of its vast application and network infrastructure. Cybersecurity engineer Evan Nichols was Blue Valley's first cybersecurity engineer and is the department's resident expert. In this article, Evan highlights the key security challenges the school district faces.

RANSOMWARE

Ransomware attacks will always be at the top of the security team's threat list, notes Nichols. "Our biggest ongoing threats are the entry points for phishing. The perception is that public school districts have shoestring budgets and lack manpower and cybercriminals bank on that. Our district was targeted in 2019 because we are one of the largest districts in the state and it was just days prior to the start of school."

VISIBILITY

"It comes down to being able to get a 1,000-foot view on things with only a small team of people to look at what we're pulling in," explains Nichols. "The biggest challenge is avoiding things like alert fatigue and making sure we get pertinent data to district administration immediately."

STAFFING

Nichols also acknowledges that many school districts are not able to make the level of investment in staffing and software that is needed to deal with the demands of today's cybersecurity environment. "A lot of public K-12 environments don't have the manpower to do what is required to run a full-blown security stack. Or they may rely on open-source tools that require a lot of attention; but that also requires staffing hours and expertise which a lot of school districts don't have."

The Solution

Implement the Rapid7 Insight Platform

Nichols first step was to implement the Rapid7 Insight Platform, including InsightIDR for detection and response, InsightVM for vulnerability management and InsightConnect for automation. "I chose the Rapid7 Insight Platform because It was the right size and fit for us," states Nichols. "We're dealing with massive amounts of data, but we don't have a lot of warm bodies. And we don't have a lot of people trained as SOC analysts or engineers. We need the Rapid7 platform to do a lot of the heavy lifting for us."

"We started with detection, because you don't know what else you're going to need until you assess. And, we were able to get up and running with Rapid7 InsightIDR in less than a week. It was really easy and quick to deploy in our environment." Blue Valley also usesInsightVM to scan data center assets as part of its goal of shifting to a zero-trust model. "InsightVM gave us the ability to move there with confidence."

Today, Blue Valley Schools has three professionals continuously training in all things cybersecurity , a lean, but highly effective security team. The Rapid7 Insight Platform is providing them with the big-picture and deep visibility they need to oversee and protect their challenging environment. "The Insight Platform is good at drawing to the surface the data that we want to see," Nichols says. "I don't have to search very far to see what's happening. That's because the searches in InsightDR are really easy to navigate and tailor around our environment. Also, it's easy to save and call back to queries."

"We are monitoring a little bit of everything. The foundational sources for InsightIDR are one thing entirely, and that feeds the user behavior detective analytics models InsightIDR provides. On top of that, we have tons of custom parsing and log event sources that we're able to do a lot faster than we would be able to with other products. A lot of the upfront legwork was already done by Rapid7 because Rapid7 cares about the same security and IT event sources that we do."

"Rapid7 came prepared with the answer to our manpower problem by way of InsightConnect," continues Nichols. "It really helps with our manpower shortage problem because you can throw all of your alerts into a central workflow system. Before it was really hard for us to act and respond at scale. InsightConnect has empowered us to do a lot of our incident response in an automated way. And by us, I really mean me. Because early on I was the only one handling incident response."

> **"I chose the Rapid7 Insight Platform because It was the right size and fit for us. We're dealing with massive amounts of data, but we don't have a lot of warm bodies. And we don't have a lot of people trained as SOC analysts or engineers. We need the Rapid7 platform to do a lot of the heavy lifting for us."**
>
> Evan Nichols,
> Cybersecurity Engineer

Nichols and his team were impressed with the easy Rapid7 setup. "It's really great between InsightIDR and InsightConnect. You can bring anything to the table and it's fine. It's really easy to set up and get going. We have a Cisco product for network traffic analytics. It consumes all of the flow data and we generate alarms and behavior threshold alerts out of it. Then we pump that into InsightIDR and we're able to respond more automatically by leveraging InsightConnect."

The Benefits

"When we looked at other cloud security solutions with comparable breadth and depth, we would've been priced out of our budget pretty quickly. With the Rapid7 Platform we get a lot of capabilities for the money. The other platforms would have been too complex for our small team to operate on a daily basis. The only other option would've been to do it all ourselves with open source software. Which would have meant a lot of on-premises storage and systems, which equals a lot of costs. And then you have to consider the human capital to manage it. That's an entire environment you must oversee. Those are things that steered us in the direction of InsightIDR and the broader Insight Platform."

Going with Rapid7 has helped the Blue Valley Schools team manage their workflows more effectively. "We can rest and sleep easily between the time we leave the office until we return the next day because we have tailor-made workflows to account for things in our environment that would otherwise keep us awake at night. We knew that we needed a way to gather all the events. We landed on InsightIDR because there was not a cap on total events or data storage."

"Rapid7 helped us meet all our goals. We have all the visibility we need. We have tuned up all the detection analytics and data sources. I'm confident in what we have put in place with Rapid7," concludes Nichols.

RAPID7

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 attackers methods. Trusted by more than 10,000 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

CUSTOMER SUPPORT

Call +1.866.380.8113

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