Customer Story

STAMUS NETWORKS

Center Grove Community Schools

Enhance Security with Stamus Network Detection and Response

Center Grove Community School Corporation is a public school system that serves the residents of White River Township in Johnson County, Indiana, located 20 minutes south of Indianapolis.

Center Grove's staff of more than 1,100 is dedicated to the education of about 8,500 students in grades Kindergarten through 12. The district is the 32nd largest in the state, operating six elementary schools, two middle schools, and one high school.

The IT department at Center Grove manages a variety of technology assets, including a one-to-one device program for students consisting of both iPads and Chromebooks. The district uses a variety of educational services and programs that are a mix of self-hosted and cloud-based offerings, according to Jaime Pereda, Director of Infrastructure Technology at Center Grove Community School.

Pereda, a certified education technology leader (CETL), is responsible for overseeing a team of 10 that provides technology support to the entire district, managing network infrastructure and networked systems and working in cross-functional teams to find ways to incorporate the latest technology as useful learning tools in the classroom.

SNAPSHOT

Organization type: Public School System

Location: Johnson County, Indiana (USA)

Staff: 1,100

Students: 8,500

Technologies: iPads, Chromebooks, self-hosted and cloud-based apps; hyper-converged server infrastructure

Top challenges: Improve network visibility and real-time threat notifications

Solution: Stamus Network Detection and Response (Stamus NDR)

The district has been incorporating more hybrid solutions for its operations, upgrading outdated building systems with the latest technology to be fully connected. Access control and camera systems are being upgraded as well for a fully automated system that will be managed from a campus Emergency Operations Center shared with the local sheriff and fire department.

"These systems are accessible via cloud access from anywhere but can still be managed locally if needed" Pereda says. "Our paging systems have the ability to be integrated as well, for fast alerting in case of lockdown or other emergencies."

Center Grove has an on-site data center that houses a hyper-converged server infrastructure along with a few remaining stand-alone servers, which are required for some student applications. The IT staff uses laptops and iPads and classrooms are equipped with interactive TVs and audio systems.

The district is spread out across eight miles, and the main campus connectivity contains the core of its network infrastructure. It uses an Internet service provider (ISP) fiber ring to deliver connectivity to the most distant buildings. In all, two ISPs provide 10Gb of available bandwidth to students.

Like other educational institutions, Center Grove has made cyber security a major priority.

> *With our IT department being relatively small, we rely on our IT staff to implement best security practices from top to bottom. Each staff member has a role in protecting/securing our environment. Building technicians are hands-on with endpoints, making sure the latest BIOS and security patches are applied, running anti-virus scans if suspicious activity is detected.*
>
> - Jaime Pereda, Director of Infrastructure Technology at Center Grove Community School

System administrators monitor suspicious network and account activity, and examine logs for recent changes to systems. The organization uses next-generation threat prevention and anti-virus software, and a network detection and response tool.

CHALLENGES

One of Center Grove's biggest challenges is spreading awareness to staff and students about the importance of digital citizenship and cyber security—especially at a time when so many people are working from home at least part of the time.

Educational institutions can be easy targets for cyber attacks, Pereda says. Staffers have limited free time outside of the classroom for extensive training on indicators to look for, such as phishing emails, suspicious files, or links.

There can also be a lack of understanding about the sensitivity of the students' personally identifiable information to which they have access. "And if the staff are compromised, then that data most likely will be as well," he says.

"Our IT department works hard to block the potential threats and security risks every day while onsite. But with the majority of our devices going home daily, that opens the door for potential risk vectors."

"Our IT department works hard to block the potential threats and security risks on a daily basis while onsite," Pereda says. "But with the majority of our devices going home daily, that opens the door for potential risk vectors."

The district provides nearly 9,000 students with devices that they can bring to and from school. "With students, the risk is higher as they are just beginning to grasp the concept of having their own technology device, and are oblivious to potential threats or dangers and are easily tempted to click on a link or install video game software that is really malware," Pereda says. "Containing and minimizing the attack surface for these threats can be challenging."

The district had been using a managed security service provider (MSSP) for the monitoring and detection of network activity and threats. Prior to signing on with the MSSP, the district had practically no visibility into the activity on its network. The service required an onsite appliance that was tapped into the district's network to inspect traffic. Information was relayed back to the district's IT via email or Web portal."

But the MSSP was expensive, especially considering the district's limited resources for security technology. In addition, the security service did not fit especially well with Center Grove's technology goals.

"With the service we would receive one or two notifications a month, and some would be delayed as many as 24 hours after the event took place," Pereda says.

The district began researching other solutions that would enable the IT team to get these notifications in real time and have access to the underlying data any time. Such a solution "would increase our security posture, while at the same time educating us about these threats, as we are the ones here every day and most familiar with our network," Pereda says.

SOLUTION

The district in February 2020 deployed Stamus Security Platform (with the Stamus NDR package). The platform from Stamus Networks is an advanced network detection and response (NDR) solution that exposes threats against critical assets, enables rapid response, and mitigates an organization's risk.

The team was able to quickly evaluate the Stamus Security Platform and knew right away that it was a great fit. The platform monitors network traffic, event data from an enhanced Suricata intrusion detection system (IDS), real-time network security monitoring (NSM), and organizational context that's processed by an advanced analytics engine.

One of the IT team members, systems administrator Brian Cooper, "suggested we look into Stamus Networks, as we knew we wouldn't be renewing our service contract with the MSSP," Pereda says. "He had been working on piecing together a security stack from a previous project, and is always pro-actively looking into utilizing open source tools that will help make our IT department more efficient and not break the bank."

Stamus Security Platform is a turnkey network threat detection and response system for organizations with small IT staff who need to meet compliance objectives, whose environment does not lend itself to endpoint detection solutions, and who want an easy

to-deploy system that operates like a smoke alarm, alerting them only when they are faced with serious and imminent threats.

"With the Stamus Networks solution, we gain that visibility into our own network and can actively monitor activity and threats as well as be proactive when irregularities are found," Pereda says. "We monitor this daily and have notifications set up for the highest fidelity threats. We send the data to a dashboard on display in our IT building. The Stamus Security Platform allows us to track down possibly dangerous clients on our network and remediate."

In addition, Stamus Security Platform shifts network threat hunting from a traditional alert-driven model to an asset-centric approach. This allows analysts to more clearly understand the threat impact and speed up incident response.

Unlike typical NDR systems, Stamus Security Platform is easy-to-deploy, provides notification only when urgent and imminent threats are detected, and delivers easy to understand results with detailed supporting evidence.

"With the Stamus Networks solution, we gain that visibility into our own network and can actively monitor activity and threats as well as be proactive when irregularities are found"

OUTCOME

The Stamus Security Platform provides the school system with complete network visibility and insights into its security posture, giving the organization the ability to quickly detect and respond to incidents and mitigate risk.

"We are able to visualize and provide data to the entire IT department daily in real time, as well as report during meetings," Pereda says. The IT team has weekly Friday meetings, where the team shares relevant information from the week. These gatherings help educate those on the team with less knowledge about how an intrusion detection system works, or who are just getting started in IT.

"Being able to educate our team as a whole on the importance of cyber security and decreasing incident response time has been valuable."

The technology has enabled the school system to have a more accurate sense of serious and imminent threats than it did before. "By comparing the threats identified by Stamus

to outside reports of recent cyber security trends, we are able to corroborate the threat events, so we know the information we are seeing come in is accurate," Pereda says.

With Stamus Security Platform, Center Grove has been able to reduce the number of network security events it needs to investigate, by filtering based on relevant indicators and using custom policies set to alert based on the severity of a threat in our specific environment. "These are then automatically sent out to specific team members to investigate and remediate," Pereda says.

Given the success of the technology deployment, Pereda says he is extremely likely to recommend Stamus Networks to a colleague.

> *The recent major updates to the basic platform and the introduction of Stamus Security Platform have shown that Stamus is really dedicated to steadily improving the solutions. As a customer, that is very reassuring, especially when dealing with network security. The Stamus team has been very helpful from the beginning and continues to stay in touch with us on the latest updates.*
>
> - Jaime Pereda, Director of Infrastructure Technology at Center Grove Community School

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com