SECURITY IN THE TIME OF COVID-19: HOW OPEN SYSTEMS' MDR ENABLED CSN TO CREATE A SECURE AND EFFECTIVE REMOTE LEARNING EXPERIENCE

The College of Southern Nevada (CSN), a public college with multiple campuses, was already in the midst of its security transformation when COVID-19 restrictions were imposed. This made the move all the more urgent.

"Failure is not an option when it comes to ensuring the security of the 37,000+ students and 2,500+ faculty and staff remotely logging into our systems," says Chief Digital Experience Officer (CDxO) Mugunth Vaithylingam.

> Both teams knew exactly what was ahead of us and jumped in together and got to work.
>
> **Mugunth Vaithylingam,** CSN CDxO

WHY CHANGE?

- Increase in unsecured endpoints due to remote learning and working
- DIY security not cutting it

THE NEW REALITY

- Unified solution: SASE SD-WAN + Microsoft Azure Sentinel + MDR
- 24x7 SOC

WHY IT'S BETTER

- Direct 24x7 detection, investigation, and remediation of threats
- No budget stress
- Ability for IT to focus on student, faculty, and staff technology experience

With the changing threat landscape and severity of attacks, the CSN IT team was spending a lot of time and focus in a firefighting mode to keep the CSN community safe and secure. Due to the complexity of all the cybersecurity solutions they were using, it had become hard to hire, train, and retain security professionals who could manage and administer the network. Says Vaithylingam, "It was a budgeting nightmare, and I was never confident that we were as secure as we should be."

CLOSED DOORS DON'T STOP SECURITY THREATS

After committing to exit the DIY cybersecurity business, Vaithylingam found Open Systems to be the perfect partner. For similar costs, the college would gain a best-in-class SASE (secure access service edge) solution that includes secure SD-WAN and MDR (managed detection and response) that would work seamlessly with its Microsoft Azure Sentinel SIEM. All this would be supported with expertise and technology that previously seemed out of reach.

"Open Systems comes in and replaces all the hardware and manages it," explains Vaithylingam. "Their 'eyes on glass' are level-3 engineers with a collective 500+ years of experience. If anything goes wrong, they can triage it immediately and/or co-manage it with the CSN team."

The tight integration of the Secure SD-WAN and MDR is the key to responsiveness. Rather than sending threat alerts to the already overtaxed IT team at CSN to manage, Open Systems can directly respond to threats in real time, 24x7, based on an incident response plan.

CSN signed its contract with Open Systems the day before travel bans were announced in March 2020. Vaithylingam recalls, "Open Systems came in at a time when CSN's IT team had to support the college's faculty and staff who were now working from home while concurrently deploying the MDR service. Working together, the teams were able to conduct a fully remote implementation, including Secure SD-WAN. Within a few months, all legacy hardware had been replaced, solutions were baselined, and the entire setup prepped for a full launch of the SASE and MDR service." Remarkably, even after adapting to this new scenario, the timeline stayed intact.

"Both teams knew exactly what was ahead of us and jumped in together and got to work," says Vaithylingam.

During implementation they prioritized Endpoint Detection and Response (EDR) to protect all endpoints as soon as possible – a particularly important issue because more people were using personal equipment on unsecured networks. It was a smart move. Within a few weeks, the Open Systems team found suspicious activities that would have not been caught by CSN's prior security operation.

CASCADING BENEFITS DURING COVID-19

Tighter Security, Better Budgets

As CSN approaches its first full semester of remote learning, the IT team needs all possible resources to ensure the infrastructure and online learning applications function correctly.

> I can finally sleep through the night knowing I won't have to beg my CFO for money to buy another point security product.
>
> **Mugunth Vaithylingam,** CSN CDxO

Knowing CSN is now shielded from unexpected security costs, "I can finally sleep through the night knowing I won't have to beg my CFO for money to buy another point security product."

Vaithylingam also has gained peace of mind that Open Systems' state-of-the-art hardware, automation, 24x7 detection and response, and team of security analysts can provide the stringent cybersecurity his institution needs – especially as threats proliferate. In a recent survey, 92% of respondents noted an increase in malware since the pandemic began.[1]

Creating a stable, resilient environment is key in a time of rapidly changing dynamics. Now, instead of worrying about undetected security breaches and a surging security budget, Vaithylingam can breathe easy knowing security is taken care of and his team is freed up to focus on delivering the best learning and working experience for its community.

[1] ZDNet, "COVID-19 fuels cyber attacks, exposes gaps in business recovery," July 21, 2020

Open Systems is a groundbreaking cybersecurity company delivering an experience way beyond expectations. Our obsessive care for our clients' businesses has led us to reinvent how cybersecurity is delivered to fit today's mobile, cloud-based world. Our team, based in North America, Europe, and Asia, consistently provides crazy good cybersecurity to leading organizations all over the world.

Learn more at **open-systems.com** | Approved for public use.