Ontinue

CUSTOMER STORY

College of Southern Nevada Takes Strategic Security Approach with Ontinue

Each day at the College of Southern Nevada (CSN), the state's largest college with more than 30,000 students and multiple campuses, Chief Experience Officer (CxO) Mugunth Vaithylingam acknowledges that cybersecurity incidents are not just a threat, but an inevitability. Even casinos in Las Vegas, where CSN is located, recently made headlines over cyberattacks generating staggering losses, highlighting the need for a more proactive approach. Criminals don't discriminate; they continue to target more than organizations teeming with high rollers, with schools and colleges collectively suffering 1,600 days of downtime due to ransomware attacks, with an average breach costing $4.54 million in 2022. [1]

Cybercriminals are opportunistic and educational institutions have valuable personally identifiable information (PII) and research data. Additionally, they often run on outdated technology with countless, often unsecured endpoints. This reality made Vaithylingam's job nearly impossible — until he found the right security services partner.

"Our team was spending a lot of time and focus in a firefighting mode to keep the CSN community safe and secure," says Vaithylingam. "Due to the complexity of the cybersecurity solutions we were using, it had become hard to hire, train and keep qualified security professionals. Additionally, DIY had become costly and difficult to manage."

During an internal technology audit, Vaithylingam found some security products hadn't been fully implemented, optimally configured or updated. Many of these were reaching their end-of-life. Worse yet, visibility and detection of potential threats couldn't be relied upon – especially not at the level of best-in-class security operations centers

College of Southern Nevada
Investing in Our Future. Students First.

Motivators

- Unable to keep up with threat alerts
- Difficult to hire qualified security staff
- DIY security solutions not optimized well
- Needed 24/7 threat coverage

Solution

- Managed extended detection and response (MXDR) service
- 24/7 SOC
- Unified solution under Microsoft A5 Security license and Defender for Endpoints

Business Outcomes

- Unified solution provides access for immediate, 24/7 threat remediation
- Augmented Microsoft Sentinel data with human-powered threat investigation
- Increased collaboration via Microsoft Teams
- Increased detection coverage with use cases in CSN's Sentinel instance
- Maximized Microsoft Security investment
- Updated architecture to follow Microsoft best practices
- Avoided attacks through offensive threat hunting
- Customized incident response plan
- Combined automation and SOC saves equivalent of 3.5 full-time engineers while increasing protection and stability

About CSN

Founded in 1971 and located in Las Vegas, Nevada, the College of Southern Nevada is a multi-campus community college offering more than 150 degrees and certificates in 70 academic programs, including healthcare and IT. The college educates 30,000 students and specializes in two-year degrees and workforce development for high-demand careers or transfer to a university.

(SOC) that combine automation and artificial intelligence (AI) with the intuition of veteran security engineers for comprehensive 24/7 monitoring. With the budget constraints of a public college, it is impossible to meet these standards without the economies of scale that SOC as a Service can provide.

"I was never confident that we were as secure as we should be," Vaithylingam said, acknowledging that the CSN IT team had no way to tell what was slipping through the cracks.

Rapid response without a rapidly increasing budget

With the college's data and reputation on the line, Vaithylingam wasted no time in searching for a solution to the college's security management and cost issues. He found a savior in Open Systems for their SASE and what is now Ontinue ION for managed extended detection and response (MXDR) – at a price that fit his budget.

With the Ontinue ION MXDR service, CSN was able to outsource its entire SOC to Ontinue for far less than it would have cost the college to build one internally. When CSN first engaged with Ontinue, the company was a division of Open Systems, which also provided the Secure SD-WAN for CSN — and today, the two companies are both able to offer better service to customers through dedicated teams. Ontinue engineers can provide immediate threat response, based on a preapproved incident response plan, which saves time and, potentially, damage. ION is also built on the Microsoft Sentinel SIEM, which helps customers like CSN optimize their investments. Ontinue's AI-powered MXDR — which aligns well with CSN's own AI strategy —offers CSN increased localization through both human and artificial intelligence based detection, strong collaboration between security provider and local IT, all with the specialization of Microsoft, whom the college was already deeply invested in.

"The Ontinue ION Cyber Defense Center team's 'eyes on glass' are level-3 engineers who are seasoned incident responders," says Vaithylingam. "If anything goes wrong, they can triage it immediately or co-manage it with the CSN team. I strongly believe that no educational institution should be managing their own security operations centers." There are significant cost savings, as well. Today, the ION Cyber Defense Center saves CSN 183 hours of work each week.

> "By partnering with Ontinue, CSN is saving the equivalent of 3.5 full-time engineers each week."

Mugunth Vaithylingam
CxO
CSN

This is based on a volume of 1 billion events generated through CSN's environment. This is achieved through the combination of automation and work the Cyber Defenders in the ION Cyber Defense Center take on to investigate, triage and threat hunt on CSN's behalf.

"By partnering with Ontinue, CSN is saving the equivalent of 3.5 full-time engineers each week," says Vaithylingam.

With Ontinue ION providing stability by protecting students and faculty at the college's campuses, Vaithylingam and his IT team are able to focus on projects that help drive student and faculty learning and enablement.

Goodbye tactical response, hello strategic security.

The teams have developed incident response plans so that CSN can determine the exact level at which it wants its IT personnel to be involved. This means that the institution maintains the level of control it is comfortable with, while leveraging the expertise, technology, and scope of a highly developed partner. Now, years after the initial implementation CSN is all-in on Microsoft Security. With Microsoft Sentinel, Ontinue provides 24/7 service far beyond threat recognition and alerts. Its security analysts research threat alerts, provide reports that augment the raw Microsoft Sentinel SIEM data, and can immediately remediate network threats – even if they originate outside of the network.

Vaithylingam is happy with the results. By getting out of the tactical side and simplifying management of cybersecurity operations with Ontinue ION, his team can focus on other ways to reduce threats, such as governance and educating the CSN community on best practices.

[1] Malwarebytes Labs, "The 2023 State of Ransomware in Education: 84% increase in attacks over 6-month period," June 5, 2023

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats. Continuous protection. AI-powered Nonstop SecOps. That's Ontinue.