SUNY Old Westbury Enhances Office 365 Security with Cisco's Cloud Email Security

One of 64 campuses of the State University of New York (SUNY), Old Westbury prides itself on the diversity and accomplishments of its faculty, staff, and student body, as well as its longstanding commitment to academic innovation, access, and social justice. Established more than 50 years ago on Long Island – just 20 miles from the center of Manhattan – the college has matured into a regional institution of higher education that has consistently been ranked among the most diverse liberal arts colleges in America by U.S. News and World Report.

As the college begins its next 50 years, it remains dedicated to providing continued access to education that is of the highest quality, responsive to student needs and demands, and forward-thinking for the people and communities it serves. For Milind Samant, SUNY Old Westbury's Director of Information Technology Services and Information Security Officer (ISO), technology is the common thread that enables these objectives, but it must be secure and scalable to keep up with an expanding user base.

Executive summary

Customer name:
State University of New York (SUNY), College at Old Westbury

Size:
Nearly 4,400 students and 300+ full- and part-time faculty

Industry:
Higher Education

Location:
Old Westbury, Long Island, NY

“Cisco Cloud Email Security with AMP helps me sleep better at night. I don’t have to stay up expecting an email from the C-level folks or VP asking ‘Is this email legit?’ or ‘Should I open this attachment?’ since CES is managing all that for us.”

Milind Samant
Director of Information Technology Services and Information Security Officer (ISO), SUNY Old Westbury

Increased reliance on cloud-based email

With enrollment on the rise and a growing population of students, faculty, and staff, Mr. Samant and his team were looking for innovative ways to support secure collaboration, a new Go Green initiative, and students’ expectations for instant access to information, anytime from anywhere. “We began to rely on our email system more and more to address each of these challenges and our system was becoming overburdened,” says Mr. Samant, ISO.

Prior to going green, the communications options were personal email and regular “snail” mail which kept email volumes down. “Now any official communication between the university and students, faculty, and staff is through the official SUNY email system based on Microsoft Office 365 – everything from financial aid notices to course schedules and grades,” says Mr. Samant. “Going green more than doubled the volume of email – every alert and notification is now communicated through email – and it has to be fast and reliable. For example, students want to be notified by email immediately if there’s a balance on their account and they want access to that information on their mobile device and laptops.”

With an increase in email volume, came an increase in spam and other threats that use email as an attack vector. “Despite the email security in Office 365, the system wasn’t as secure as we would have liked, particularly given the volume and type of information we needed to communicate – much of which includes Personally Identifiable Information (PII),” explains Mr. Samant. “A lot of bad messages were getting through and our service desk was getting calls that involved malicious URLs, zero-day exploits, and cases of ransomware infections.”

When they began to see spoofed emails targeting specific high-level people in their administration, the ISO knew they were facing serious risks and needed to augment their email security. “Office 365 provides us with a great email platform, but we needed more robust security capabilities for the cloud-based email solution” Mr. Samant explains. “We chose Cisco Cloud Email Security because it provided enhanced email protection against constantly increasing risks, but also because it integrates seamlessly with Office 365. Combined it’s a win-win... we get the email platform we need to better handle our increased email load, plus the robust security we need to protect that platform.”

Enhanced security solution

SUNY Old Westbury followed a methodical process to evaluate their options to boost security for Office 365, considering research from Gartner and Forrester, looking at the top five players in email security, comparing features, and then narrowing down to three solutions that they thought would be a good fit for the unique needs of a university. Licensing and pricing were also critical to their decision.

"Licensing models based on mailboxes aren't a good fit for us since students or faculty may be away for a semester or longer," says Mr. Samant. "On average we have more inactive mailboxes than a typical enterprise and we don't archive as we know students will often be coming back within a year, so per mailbox licensing doesn't work for us. Cisco's licensing model is a perfect solution for higher ed. What you pay is based on the amount of traffic that is being passed through – what you actually use vs the number of users."

The Director of ITS at SUNY OW wanted a fully cloud-based solution to better align with the cloud-based email platform. "Since our email system is in the cloud we wanted to make sure our email security solution was in the cloud as well. We didn't want any ties to the on-prem network because we don't want to route the email traffic to come to our on-prem datacenter only to be routed back out to the cloud." explained Mr. Samant.

Based on the initial assessment, Mr. Samant and his team decided to look at Cisco more closely and setup a Proof Of Value (POV).

"During the POV everyone from Cisco was just terrific – from the initial setup where the sales engineer Rose and our account manager Cindy were very generous with their knowledge and provided us assistance throughout the evaluation – and the experience stuck with me," says Mr. Samant. "We saw that Cisco Cloud Email Security could be deployed quickly and would give us the protection we needed, for example defending against business email compromise and eliminating risk from spoofing. The solution includes checks and balances to let legitimate messages through and flags emails that could be forgeries so we can warn users of potential risks. And because of the way it is licensed, we could save money and make it a priority for the upcoming year."

Advanced threat protection

Milind Samant and his team were able to get started with Cisco Cloud Email Security quickly and tailor the solution to their environment. "The ease of setup and daily admin and overhead is really negligible and the GUI really reduces the learning curve," notes Mr. Samant. "Once you spend a few hours you are pretty much ready to go and the amount of control and customization you have really stands out. With Office 365 you have very limited basic level control over the emails that are getting into end users' mailboxes. When you complement Office365 with CES you get the advance capability of managing emails using policies and rules.

"Cisco Cloud Email Security has allowed us to become proactive rather than reactive – there is no comparison"

Evan Kobolakis,
CIO and AVP of Information Technology Services, SUNY Old Westbury

You can let the good email reach the SUNY OW folks and at the same time quarantine any suspected email for three minutes or three hours to better detect, remediate, and remove—the options are just tremendous."

In addition to the team's own custom signatures, Cisco Cloud Email Security is continuously updated with built-in threat intelligence provided by Cisco Talos. "The intelligence from Talos does an awesome job of sanitizing emails before they even arrive. Our SMTP gateways that were previously overworked are now working less," says Mr. Samant. With Cisco Advanced Malware Protection (AMP) as part of their Cisco Cloud Email Security solution, email-based attacks like spear phishing, ransomware, cryptoworms, and other sophisticated attacks are no longer a problem. "Cloud Email Security with AMP helps me sleep better at night. I don't have to stay up expecting an email from the C level folks or VP asking 'Is this email legit?' or 'Should I open this attachment?' CES is managing all that for us."

The Director of ITS and ISO further explains, "AMP notifies users of financial scams with a header and message in the email alerting the user that this looks like a potential fraud email. The message then automatically goes to the proxy server where it is checked and either prevents access or allows access if it is clean."

Spam is a growing problem for every organization and SUNY Old Westbury is no different. "On average we receive 412,000 emails every day – not to mentioned the ones that our Cisco email security solution automatically blocks that we don't even know about," Mr. Samant shares. "Of these 412,000 emails, 266,000 are classified as spam and blocked and even more are classified as commercial and blocked – so 75% of emails we receive are bad emails!"

AMP also helps combat zero-day exploits. "We still use the security built-in to Office 365 as a first layer of defense, but at one point a zero-day got through," explains Mr. Samant, ISO. "With AMP we can now receive retrospective alerts, quickly quarantine emails for further inspection, and then release or block them based on information from Talos global threat intelligence."

This level of intelligence and automation is important for Mr.Samant and his small team. "Cisco Cloud Email Security has definitely reduced the time/man hours required for management," says Damian Obara – Systems Engineer and Office365 Administrator at SUNY Old Westbury.

"I don't have a separate security person on my team who can spend time every day looking at reports, logs, and IP blacklists. When we were comparing features we wanted a solution that is adaptive based on what is going on at a global level. If something bad is happening somewhere else in the world, Cisco Talos updates our email security without requiring a lot of time on our part," adds Mr. Samant, ISO.

With Cisco Cloud Email Security and AMP, Mr. Samant and team have gained much needed visibility and control. "We now know what is going on so we can have control," says Mr. Samant.

"Cisco Cloud Email Security with AMP has allowed us to become proactive rather than reactive – there is no comparison," adds Evan Kobolakis, CIO and AVP of Information Technology Services, SUNY Old Westbury.

A cloud-based future

As SUNY Old Westbury looks to the future they are considering Cisco Data Loss Prevention to further reduce the risk of confidential information falling into the wrong hands given the amount of network and email traffic that contains PII. They are also evaluating Cisco Umbrella, a secure internet gateway that provides a first line of defense against bad domains, URLs, IPs, and files – blocking malicious connections before they are even established. "Now that we have strengthened our email security, we also have to look at better protection against network attacks and Cisco Umbrella just makes sense as a next step," says Mr. Samant.

Moving to the cloud can be a formidable undertaking but Mr. Samant shares some words of encouragement: "The question everyone always asks is: 'How do we secure a cloud-based solution?' I had these same concerns, but when I looked at Cisco it didn't seem that we needed to do much – just deploy, tweak, and monitor. Cisco has built solutions with best practices applied. It's more turnkey so we can get the protection we need and not worry about daily administration and management overhead."

Products and services

- Cisco Cloud Email Security
- Cisco Advanced Malware Protection (AMP)

C36-739233-00 06/17