



Case Study

industry: Education
problem: Security

Mazu Profiler Delivers A+ Security to CUNY

About CUNY

The City University of New York (CUNY) was founded in 1847 and comprises 23 institutions: 11 senior colleges, six community colleges, the William E. Macaulay Honors College at CUNY, the Graduate School and University Center, the CUNY Graduate School of Journalism, the CUNY School of Law at Queens College, the CUNY School of Professional Studies, and the Sophie Davis School of Biomedical Education. The University serves more than 231,000 degree-credit students and 230,000 adult, continuing and professional education students.

CUNY's network supports these 461,000 students in 23 colleges as well as more than 30,000 faculty and staff located in the five boroughs of New York City. The network topology is an ISP model and the colleges attach to the shared ISP network, which is managed centrally. Each college is responsible for managing and protecting its own internal network infrastructure and applications. As a result, CUNY has 20 IT operating environments with 20 CIOs, 20 information security managers, and 20 network directors. Carl Cammarata, CUNY's CISO, is responsible for overseeing security across the entire university.

CUNY views security technology as an enabler to furthering the mission of university, which is teaching, learning and research. If a technology doesn't help or if it impedes the university mission, they don't buy it.

With Mazu Profiler™, CUNY can quickly identify and understand network activity allowing IT teams to make intelligent and targeted security decisions. This enables CUNY to create a safe and functioning network without compromising academic freedom, a major business requirement for academic institutions.

Challenges

CUNY had four key challenges:

- **Build a cohesive security program and organization.** Cammarata was challenged to build a security community at CUNY that previously didn't formally exist. He began by building relationships with college and central administrative executives and getting a standards-based security plan formally approved. Although the college security managers are his central point of contact for college-specific security matters, he maintains strong working relationships with the CIOs and college administration for strategic and funding decisions.
- **Improve ability to proactively address security issues.** University network environments pose unique challenges for security teams. Thousands of students connect to the university network every day and hundreds of servers are maintained by non-technologists. There is no easy way to know if these devices are securely maintained. This lack of control places university security teams at a severe disadvantage. CUNY needed to gain a better understanding of the integrity of its networks. Specifically, they needed help to proactively identify potential issues and to isolate problem situations more quickly.
- **Understand what was going on in the network to improve their security posture and to make further security technology investment recommendations.** Substantiating security investments based on sound real-time information enables university decision makers to support the security team's technology recommendations and to positively reinforce the approved security plan.
- **Balance protection of private information while at the same time supporting academic freedom.** "It is critical for us to balance a secure network environment with one that does not restrict academic freedom," said Cammarata. "An open and accessible network is a business requirement for CUNY and therefore just as important to our IT program as security. We needed to proactively identify potential security issues and more quickly isolate problem situations without disrupting or limiting usage of the network and applications by our college community."

“The GUI is the best GUI I've ever seen in my life ... the ease of immediate use is beyond description.”

— Carl Cammarata, CISO

The stakes were high: a new security program, the university's first CISO, and CUNY's first substantial investment in security technology. "Because we were starting to build the security program and connect the security community, we needed a quick, solid win to back up our justification for the investment and to establish us as a reputable and reliable organization," said Cammarata. "We needed a win that would also result in a more team approach to furthering future security standardization."

The Mazu Profiler Solution

Cammarata had experience with Mazu Profiler in a previous job and immediately saw what it could do for CUNY to help them understand what is going on in the network, where the "hot spots" were, and what needed to be addressed.

CUNY deployed 20 standard Mazu Profilers and nearly 50 Application Sensors across their 20 IT operating environments. Cammarata credits the success of the six-month deployment largely to Mazu's commitment to ensuring success and proactive help to ensure that CUNY implemented the technology appropriately. "I put my trust in Mazu Networks and they exceeded my every expectation," said Cammarata.

Results

Better information for better decision making. With Mazu Profiler providing information on what network activity is normal versus abnormal, the CUNY security team can be more proactive. According to Cammarata, prior to Mazu Profiler, they never had access to this kind of detailed information on network behavior; they can now make educated decisions about potential security issues. Mazu Profiler also adds intelligence and corroboration to data coming from other security technologies in CUNY's program such as intrusion detection systems and end point integrity solutions. Mazu Profiler also helps dilute claims of "false positive" from those on the receiving end of an incident report.

Security and academic freedom. Mazu Profiler enables CUNY to assess the behavior of network traffic flowing into and out of the college networks and understand what kind of traffic is flowing. This enables them to support academic freedom — they don't monitor the content of the traffic — but they do have the information they need to sustain the availability and integrity of the network from a security perspective.

Reduced number of security incidents. Mazu Profiler has helped identify servers and workstations that have become infected with malicious code or are being used in a manner not consistent with university security practices. CUNY tracks security events through their incident response protocol and, since deploying Mazu Profiler about a year ago, they've observed approximately 75 percent reduction of security events. Most of the reductions are the result of improvements in how servers and desktops/laptops are managed, such as applying security patches, using secure configurations, and maintaining current levels of anti-virus protection. The continual reporting of these former problem areas to the security technologists has underscored the need to maintain device integrity, whether or

not the device is maintained by a capable technologist in the IT department or elsewhere in the college. This was a problem not so easily solved given the open nature of the academic environment, but the data provided by Mazu Profiler was indisputable.

Better incident response. Mazu Profiler has also helped significantly reduce the time it takes to understand and respond to potential security situations. The insight into unusual network behavior they get from Mazu Profiler enables them to be more proactive and mitigate situations before they get out of control. The response time to security situations has been improved by more than 50 percent.

Eliminate rogue internal scanning. Many of the CUNY Colleges have degree programs and curriculum in the Computer Sciences. Many students are taught vulnerability assessment scan and penetration testing techniques, but targeting anything outside of a lab environment is inappropriate. In some cases, technologists have initiated scans that were not authorized, run at inappropriate times, or were too broadly configured. CUNY has been able to quickly identify unauthorized scans and significantly reduce their occurrence from an insider perspective.

Improve network management policies. In some cases, the history of security events has led to changes in the way CUNY manages its networks. For example, new email servers now require pre-approval. Before Mazu Profiler, rogue email servers contributed to CUNY's spam email profile on the Internet. Now, new email servers require approval and CUNY's spam profile is greatly improved.

Better technology investment decisions. With the success of the Mazu Profiler and the unification of the CUNY security team, additional security technology investments can now be quickly approved in areas such as vulnerability management, security event management, end point integrity technology, and network diagnostic tools. CUNY has also made sizable investments in security technologist training and security awareness programs for all students, faculty, staff and executives.

CUNY began seeing benefits from Mazu Profiler immediately. After several days of the Mazu sensors collecting data on their network, CUNY could see potential trouble spots on the network. Cammarata easily learned how to use the GUI and how to run reports. The GUI's ease-of-use enabled CUNY to start seeing the benefits right away. "The GUI is the best GUI I've ever seen in my life," said Cammarata. "I've never picked up the manual on it. And I'm not an engineer; I'm not a technical hands-on person. I'm more senior management, but when I want to use it to check up on things, I can do so. It doesn't take a rocket scientist to use it. I barely attended the multiple training sessions that Mazu gave us here, but I'm still able to use it and understand it. The ease of immediate use is beyond description."

Mazu Networks

125 CambridgePark Drive
Cambridge, MA 02140
Tel (617) 354-9292
Fax (617) 354-9272
www.mazunetworks.com