Education Security: Infoblox Protects the Network That Hosts City University's Curriculum

The Solution
- BloxOne™ Threat Defense

The Results
- Proactive, SaaS subscription-based cloud security to defend against malware
- Flexibility to accommodate CityU's fluctuating installed base
- Better visibility into and reporting of malicious activity and behavior

Education Security: Infoblox Protects the Network That Hosts City University's Curriculum

City University of Seattle, also known as CityU, has designed its dynamic operational model with the serious working adult in mind. Research indicates that the primary reasons why students choose CityU are that it provides convenience, flexibility, and an adult learning environment that includes relevant, online programs that fit their working schedules. The school bears the essential responsibility

The Customer

City University of Seattle, also known as CityU, is a private, not-for-profit institution of higher learning based in Seattle, Washington. It enrolls more than 6,000 students worldwide on its campuses and online. Established in 1973 to provide higher education primarily for working adults, the school has since expanded worldwide and negotiated partnerships with other educational institutions to offer relevant certificate and degree programs.

The Challenge

Like thousands of other large organizations, City University experienced a potentially disruptive ransomware attack on its network. The school immediately identified a need to implement a more robust security solution to proactively protect its students, faculty, staff, and visitors from becoming victims of malware and data theft. It needed a solution that would scale to meet the needs of the fluctuating school population and enable its IT team to be able to monitor and report on browsing activity to detect and remediate threats automatically and more efficiently.

"In this day and age there is way too much ransomware, spyware, and adware coming in over links opened by Internet users. The Infoblox cloud security solution helps block users from redirects that take them to bad sites, keeps machines from becoming infected, and keeps users safer."

Ron Washburn,
Senior System Administrator and Network Engineer for
City University of Seattle

to provide robust security to protect its sensitive, personal, and academic data and devices within in its globally distributed network.

CityU provides an international distribution of 28 locations, including satellite campuses that are located in Canada, China, the Czech Republic, Greece, Mexico, Slovakia, Switzerland, and Vietnam. Its curriculum includes subjects as diverse as business administration, education, accounting, computer systems, criminal justice, forensic IT, project management, psychology, various technologies, and more.

City University's IT team initially managed its entire network in-house and supported its curriculum with an internally managed Blackboard learning system. It now hosts a significant portion of its online research access, educational management systems, HR, and finance plat-forms with various external vendors. The CityU IT team links these outlying sites back to the campus domain via tunnels. Each campus has a computer lab with its own domain controller, print server, and wireless infrastructure

on site. This new setup allows students to work locally or remotely with online access to central resources. The cloud-based system is streamlined, and gives students, faculty, and staff access and uptime with minimal IT staffing requirements.

Ransomware Attack Reveals Need for More Robust Data Protection

City University identified a need to protect its devices and sensitive data when it experienced a potentially damaging and expensive ransomware attack on its network. An administrative assistant went to a seemingly legitimate educational website and downloaded a PDF that, unbeknownst to her, was infected with ransomware. The ransomware easily bypassed the school's antivirus software. The planted code went to the assistant's map drive where the assistant had read/write access; she used her permissions to copy the files, encrypt them, and delete the originals.

After recovering from this ransomware attack, City University began to work with Infoblox to bring its network security to the next level. The solution it chose enabled the university to protect its devices, users, and data worldwide with a more elastic, subscription-based means for automated monitoring and reporting of malware and other malicious activity on its network.

Implementing Infoblox SaaS Cloud Security Solution for Automated Monitoring and Reporting

The CityU IT team ensures that all students, faculty, staff, and online visitors have easy, secure local and remote access to all of its online resources. It does so by monitoring and reporting on all sites that users visit, and indicating whether any online activity qualifies as malicious. The process of monitoring and reporting must be automated and efficient to be able to immediately identify any potentially malicious sites or online behavior. It must also work automatically to prevent any malicious attacks, which could lead to potential expensive network downtime, brand damage, or disputes among users, Human Resources, or even law enforcement.

To obtain the next level automation it needed, City University worked with Infoblox to implement a new subscription-based BloxOne Threat Defense Cloud solution alongside its other Infoblox deployment. With BloxOne Threat Defense Cloud, CityU was able to replace its 17-year-old Windows Proxy that depended on a SQL box and two Windows 2003 servers. This legacy solution had resulted in a cumbersome, slow, and ineffective monitoring and reporting process that lacked security and automation.

Through the advanced security and automation capabilities of BloxOne Threat Defense Cloud, City University is now well equipped to prevent future ransomware and other malware infections from taking place on its network.

Ron Washburn, senior system administrator and network engineer at City University, says "In this day and age, there is way too much ransomware, adware, and spyware coming in over links opened by Internet users. Infoblox's SaaS subscription-based cloud security solution helps block users from redirects that take them to bad sites, keeps machines from becoming infected, and keeps users safer."

City University and its IT team are now able to monitor and report on all potential malicious Internet destinations and behaviors automatically, and thus far more efficiently and more securely, from the cloud.

A Customized Licensing Solution Licensing to Meet CityU's Unique Requirements

City University had several key requirements in wanted from a new solution. It needed to avoid having any infrastructure on the premises, to move IT to the cloud, and to protect students, faculty, and staff at the device level. A SaaS subscription-based solution met these requirements.

In designing the solution, the Infoblox team worked diligently to deliver the flexibility that the school's innovative operational model demands. City University's network is extremely dynamic in volume, time, traffic destinations, and the transient nature of the user community. Dozens of individuals arelikely to use any of the 400 devices in the school's computer labs on any given day.

The Infoblox team arranged for a customized licensing model that would be tied to the workstations rather than the users. "The licensing scheme works well for us," says Washburn, "and will work well for other organizations [such as satellite campuses] that have multi-user machines."

Infoblox and CityU Maintain a Trusting Relationship as Long-Time Partners

City University has been working with Infoblox for over a decade to help manage its core network and DNS. When the need to elevate to more robust, cloud-based security arose, the City University IT team initially talked extensively with several vendors to identify its options. "We came full circle back to Infoblox," says Washburn, "because what Infoblox offers is how we want to use and manage our DNS. I needed a way to manage my network in logical components where each part of the network serves a particular business need. That type of flexibility should not add complexity or cost. With Infoblox I can put in as many zones as I want and there's no IP limit. The Infoblox system serves DNS for all the different domains that we own and points our students where they need to go." Both Infoblox and City University will also continue to benefit from a trusting and strong working relationship. Infoblox looks forward to helping City University protect its devices, users, and data from attacks and threats.

For More Information

Learn more about how you can prevent ransomware and other types malware from disrupting your network, and how you can protect your network devices in the cloud. Visit our website or start your free trial of BloxOne Threat Defense Cloud today.