plixer
International

Scrutinizer™
NetFlow & sFlow Analyzer

Plixer International Case Study

Bloomington Public Schools

Scrutinizer Helps Bloomington Public Schools Pinpoint and Stop a Virus.

The educational mission of Bloomington Public Schools is to assist, challenge, and enable each student to develop into a productive and constructive citizen in a global society. The individual student is the emphasis of the educational program.

BLOOMINGTON

Through a curriculum which stresses critical thinking, problem solving, and the enhancement of communication and computational skills, the District's education programs respond to varying learning styles and learning abilities while instilling within the student the notion that learning is fun, meaningful, and has a purpose.

The Challenge

The Bloomington Public Schools' network is somewhat unique. With approximately 98% virtual traffic, Systems Administrator Jason Radford equates the public school network to the Wild West, unlike modern corporate environments which tend to have straight and narrow paths. The IT Department services technology needs across 10 sites for three primary groups: students, teachers, and faculty. With the multi-directional traffic and with the laws governing student cyber safety, the ability to monitor and trace network activity is vital. Within months of obtaining Plixer International's Scrutinizer NetFlow & sFlow Analyzer software, Bloomington Public Schools had an urgent opportunity to use it.

A user contacted the IT Department complaining of suspicious PC behavior. The user's web browser wasn't responding and was causing many unrequested pop-ups. IT staff dispatched a technician who confirmed the machine was infected with a virus called "AV2009" which wasn't caught by the anti-virus software they had been using. The virus was reaching out to specific botnet websites and was sending email to further propagate itself. In a short time, the virus infected over 100 machines.

The Solution

Upon discovering the nature of the virus, Radford immediately suggested using their new Scrutinizer NetFlow monitoring software to pinpoint it. From their centralized data center location, Radford's team created filters in Scrutinizer for SMTP and specific subnets trying to hit known botnet sites. In less than an hour, they isolated every single infected machine and dispatched IT SWAT teams armed with a Scrutinizer report. "Before enabling NetFlow and Scrutinizer, we had very little visibility," Radford explained. "There is no question that it would have taken a lot longer to catch every infected computer without Scrutinizer."

The Benefits

Radford's IT team uses Scrutinizer on a daily basis to verify that connection thresholds aren't exceeded, and to provide overall metrics for bandwidth utilization to traffic anomalies. Their primarily virtual processes rely on internet connectivity in all fields, from classroom instruction to food service operations. Online video streaming requires large amounts of bandwidth- not just for the 50 security cameras in each building, but also for educational instruction through video sites like YouTube. NetFlow analysis allows the IT Department to not only pinpoint traffic that is prohibited by school policy, but it also allows the team to increase bandwidth for accessing permitted sites for legitimate educational needs. "Visibility is everything to us so that we can correct problems on our network," Radford said.

The Bloomington Public Schools System pushes the envelope with educational network traffic configuration. They serve 9,000 students in 10 separate locations for Pre-Kindergarten through high school. These locations are interconnected through a Metro TLS Ethernet network then linked to a central data center with an all-Cisco network. The Bloomington School system was the first school district in the nation to get a Cisco Nexus 7000 switch and a Cisco UCS server.

Few schools have this type of infrastructure and primarily virtual nature. Radford stated this type of setup allows multiple points of entry which demand tools to ensure security. "The Scrutinizer product has changed our processes. It lets us drill down to any type of traffic, anywhere on the network, so we can quickly provide answers to what is going on and why."