Blue Coat Secure Web Gateway Helps Texas Children’s Hospital Control Web 2.0 Applications and Protect against Malware

A safe and productive Internet experience is priority at Texas Children’s Hospital, one of the premier pediatrics hospitals in the United States. Texas Children’s Hospital is renowned for its treatment of congenital heart disease, cancer, diabetes, asthma, HIV and premature babies, among many other specialties. The hospital is ranked nationally in U.S. News & World Report’s list of America’s Best Children’s Hospitals.

Clinicians, administrative staff and medical equipment at this Houston-based hospital rely on a high-performance, secure Internet connection in countless ways to help deliver quality pediatric care, support clinical research and communicate with other healthcare professionals, patients and their families. With Internet connectivity essential for electronic medical records, billing systems, diagnostic systems, informatics and many other key healthcare applications, Texas Children’s Hospital must ensure that its 8,000+ workers can use the Web productively and without concerns about inappropriate and malicious Web content.

Control, Protection and Productivity

The hospital had long used Web filtering to protect against unwanted and malicious Web content, but as the hospital’s Internet traffic volumes rose, the Web filtering product couldn’t keep pace. In particular, filtering outbound Internet content was stressing the hospital’s firewalls. Plus, the Web filtering product was often slow to categorize new sites, leaving the hospital at risk from malware.

The IT team at Texas Children’s Hospital set out to find a high-performance Internet gateway solution that would effectively protect employees from inappropriate content and malware. IT sought an appliance solution so it could free its firewalls from the burden of filtering outbound Internet traffic. The hospital also wanted to add another layer of malware protection for its desktops as part of its layered-security approach.

“We chose Blue Coat for the price, functionality and the ease of implementation,” said Kevin Kujawa, data security architect at Texas Children’s Hospital.

Optimize Application Performance and Web Security

Texas Children’s Hospital deployed Blue Coat’s Secure Web Gateway solution, including ProxySG, ProxyAV, WebFilter and Reporter.

Blue Coat ProxySG protects users and networks from Web threats, phishing and other attacks. The appliance also accelerates application performance for files, email, Web, SSL and rich media applications. ProxySG significantly reduces bandwidth with leading compression, byte caching and object caching technologies.

Blue Coat WebFilter blocks malware and filters content according to strict policy controls. WebFilter is continuously updated by the WebPulse community watch cloud defense that detects malware and provides reputation and Web content analysis. WebFilter provides over 7 billion ratings per day for over 70 million users around the world.

Blue Coat ProxyAV delivers advanced malware detection at the Web gateway. It performs inline threat protection and malware scanning of Web content at the gateway, which protects users from viruses, Trojans, worms, malware and other malicious content. Texas Children’s uses Kaspersky antivirus software with ProxyAV. It chose a different antivirus engine for the Web gateway than it uses on its desktops as another layer of protection.

The Secure Web Gateway solution is deployed at the hospital’s primary data center as well as at a secondary location for redundancy. Inbound and outbound Internet traffic from employees and some medical systems is funneled through Secure Web Gateway.
Traffic is load balanced across the ProxySG appliances. "One ProxySG can handle 100 percent of the traffic, and we have about 8,000 users, but the load balancing gives us added performance," Kujawa said.

Malware Stopped in its Tracks

Texas Children's Hospital sidestepped potential performance and security issues that could have arisen from the "Here You Have" email worm outbreak in the fall of 2010. The email enticed unsuspecting users to download malware with the theme of "here's the document I told you about." IT uses Secure Web Gateway to block potentially malicious file types, so if a user clicked on the link in the email, the malware wouldn’t be downloaded. "We had blocked malicious file types from the beginning, and it saved us," Kujawa said. "We were very happy that we had implemented file type blocking through Blue Coat."

Nor was the hospital affected by the spike of LinkedIn spear-phishing attacks in the fall of 2010. The phishing emails started coming in over a weekend, and the IT staff moved quickly to thwart the threat. "We were able to block those emails almost immediately, and we didn’t have any issues because no one could click on the link," Kujawa said.

The ability to control applications and bandwidth with Blue Coat has proven itself time and again, especially during popular events, such as the 2009 inauguration of President Barak Obama. Employees were encouraged to watch the event on televisions in the hospital’s break rooms, but so many people watched the video from their desks that the hospital’s firewalls were quickly overloaded and network performance was impacted.

The IT team moved quickly to cache the streaming media files on the ProxySG appliances. "Our ProxySG appliances could handle an 8:1 caching ratio for the video without any problem," said Kujawa. "It reduced traffic on the firewalls and allowed our other services to run."

Michael Jackson’s funeral, also in 2009, was a popular event with employees. "The Michael Jackson funeral cranked up our Internet utilization as high as we’ve ever seen it," he said. "Both of these events showed us the importance of having both the proxy and the cache."

Holding the Line on Internet Cost

Texas Children’s Hospital has been able to hold the line on Internet bandwidth growth by deftly controlling applications and fine-tuning access policies using Blue Coat. This level of control allowed the hospital to turn the tide on the escalating demand for Internet bandwidth.

"Since deploying Blue Coat, our Internet usage has remained constant in terms of traffic through our external routers. We’ve flat-lined," Kujawa said. "We’re holding down our cost on the Internet connection and on the utilization on the Blue Coat appliances themselves. That is a success."

The hospital has experienced a 57 percent savings on Internet bandwidth because of the compression, caching and control capabilities of ProxySG appliances. "We’re saving one-third of the cost of our Internet link," Kujawa said.

Controlling Streaming Media

Delivering audio and video securely and with a good user experience can be challenging, but it is a challenge that must be overcome. Rich media is an integral part of business today. For instance, Texas Children’s streams Radio Lollipop to patients’ rooms so children can enjoy games, art projects, storytelling and contests.

YouTube had long been one of the hospital’s major bandwidth-hungry applications, and the hospital did not scan video because of the performance impact. Yet the threat was rising with the growing number of Flash vulnerabilities. With the addition of Secure Web Gateway to the network, Texas Children’s could protect itself while delivering streaming media to employees.

"With the increase of live meetings and collaboration, you can’t automatically block streaming audio and video," Kujawa said. "You have to design around it to make it work."
"Our ProxySG appliances could handle an 8:1 caching ratio for the video without any problem, it reduced traffic on the firewalls and allowed our other services to run."

- Kevin Kujawa, Data Security Architect

A Collaborative Approach to Policy

Setting Internet access policies is collaboration between IT and Human Resources (HR). All users must follow the hospital’s Internet usage policy, and users are authenticated through Microsoft Active Directory before they may access the Web.

“We treat the Internet as an application,” Kujawa said. “With integrated Windows authentication on the browser, authentication is transparent for most users. We know from a non-repudiation standpoint that the person was actually responsible for the sites they were surfing.”

“When IS blocks sites, we look like the bad guys. We are here to support technology, not to dictate the policies that users will have. We codified our partnership with HR last year, and they determine which categories to block and can hold users accountable,” Kujawa said.

The hospital’s HR and compliance teams are the primary users of Blue Coat Reporter. Reporter gives managers visibility into Web-related user activity. Managers have customizable, at-a-glance dashboards and reports, along with intuitive drill down capabilities. Reporter provides visibility into Web traffic performance, trends, errors, security threats, bandwidth impact and streaming traffic levels.

Deciding which sites to block can be a grey area at times. For instance, social-media sites have both personal and business uses. When employees want to access such sites, they are presented with a green notification page, where they must acknowledge that they’re visiting the site for business reasons before the site is served.

After the LinkedIn attacks, the hospital decided to block all uncategorized sites. Previously, users attempting to access an uncategorized site were presented with a yellow warning page. “Blocking the unknown sites is a differentiating factor for us,” said Kujawa. “It puts more stress on the back end when a user needs to get to a site, but Blue Coat is pretty quick in categorizing an unknown site.”

“Blue Coat is good at categorization. We don’t get many sites that are uncategorized,” Kujawa said. If a user needs access to an uncategorized site, the user can email the service desk with the request. The service desk gathers the relevant information and submits it to Blue Coat for site review. “Blue Coat categorizes unknown sites quickly. If it’s an emergency, we have an exclusion list to temporarily permit access to that site,” he said.

Texas Children's Hospital is committed to excellence in pediatric patient care, education and research, and its pediatric outcomes are among the best in the nation. That excellence in healthcare is underpinned by strong security controls that give clinicians and administrators access to vast resources through Internet while protecting them against its ills.