Robust Cybersecurity Cures Endpoint Penetrations at Canadian Healthcare Company

CBI HEALTH GROUP

"The minute that we turned on Traps, the number of ransomware infections dropped to zero. We literally haven't had a successful CryptoLocker attack since we installed Traps."

Cameron Chojnacki | Infrastructure Manager | *CBI Health*

CBI Health Group
CBI Health Group is a privately owned leading Canadian healthcare company dedicated to providing an integrated approach to health management. The company's multidisciplinary team consists of about 10,000 clinical and support professionals, such as physiotherapists, occupational therapists, massage therapists, chiropractors, occupational physicians, family physicians, nurses, psychologists and dietitians. CBI Health has more than 240 offices and provides services to people in all ten of Canada's provinces.

Industry
Healthcare

Challenge
Protect sensitive patient health information and avoid remediation costs associated with successful network breaches

Solution
Palo Alto Networks® Next-Generation Security Platform to prevent ransomware and other cyberthreats from infecting personal computers, leading to lost productivity for users and IT staff.

Subscriptions
Threat Prevention, AutoFocus™ and Traps™

Appliances
PA-5020 (2)

Services
Palo Alto Networks Consulting Services

Results
- Eliminated ransomware infection from the network
- Devoted more IT time to innovation instead of remediation
- Lowered risk of data breaches
- Avoided lost user productivity caused by infections
- Gained deep visibility into the lifecycle of cyberattacks

Story Summary

As one of the leading healthcare providers in Canada, CBI Health depends on its infrastructure to connect more than 240 offices and thousands of mobile users to its primary data center, which contains all the company's data and applications. With so many possible entry points for cyberattacks, CBI Health needed to protect the data center from all kinds of threats. The healthcare firm chose the Palo Alto Networks Next-Generation Security Platform to perform that task because of the security company's reputation for innovation and quality.

CBI Health supports its users with a Citrix-based virtual desktop infrastructure (VDI). Thanks to the standard utilities in the Palo Alto Networks Next-Generation Security Platform, the healthcare firm now has visibility into user behavior as well as the threat lifecycle. When ransomware became a significant problem, CBI Health again turned to Palo Alto Networks to augment its existing platform with endpoint security. Since then, CBI Health has not had any successful ransomware (e.g., CryptoLocker) attacks. As a result, the infrastructure team spends less time on remediation and other routine security tasks, freeing up hours for innovative initiatives that improve overall security and strengthen compliance.

Blanketing Canada with Healthcare Services

CBI Health Group is all about wellness. The privately owned enterprise is one of Canada's leading healthcare organizations, with facilities in all ten provinces from Newfoundland and Labrador in the east to British Columbia in the west. The secret to CBI Health's growth lies in its comprehensive approach to patient care: the company's healthcare management experts develop a personalized care plan for each individual and coordinate the services of its top-notch staff of 10,000 professionals, from physiotherapists and occupational therapists to dietitians and home-care nurses. Reflecting a deep understanding of the family dynamics of wellness, CBI Health is pioneering a creative approach to autism care called Monarch House, where behavioral and speech specialists work closely with parents and guardians to develop a comprehensive treatment plan that meets the individual needs of the entire family.

In the healthcare industry, safeguarding every patient's personal health information (PHI) is a top priority. Unauthorized disclosure of PHI can have devastating consequences, including fines of up to $50,000 per patient record and irreparable damage to CBI Health's reputation and brand. To guard against such an event, all data and applications reside in the CBI Health primary data center, which is connected via secure VPN tunnels to more than 240 remote offices. The company's employees, including thousands of mobile workers, access the applications and information they need to do their job using Citrix® software running on thin clients, personal computers and smart devices.

Protecting Patient Information

To Cameron Chojnacki, infrastructure manager for CBI Health Group, all that incoming traffic creates opportunities for cyberattacks—and it's his job to ward off as many of those threats as possible. "We needed something that would look at everything coming into the data center, identify the threats, and eliminate as many of them as possible," says Chojnacki. "That's why we invested in the Palo Alto Networks Next-Generation Security Platform. It gives

"Palo Alto Networks has consistently innovated in the security marketplace in areas such as next-generation firewalls and endpoint protection. Others are now following their example, but Palo Alto Networks was first."

Cameron Chojnacki | Infrastructure Manager | *CBI Health*

us great cybersecurity and simplifies IT management." The company also subscribes to the Threat Prevention service to protect the network from advanced threats across all its ports and protocols.

Why Palo Alto Networks instead of a competitor? For Chojnacki, it's all about innovation and quality. "Palo Alto Networks has consistently innovated in the security marketplace in areas such as next-generation firewalls and endpoint protection," he says. "Others are now following their example, but Palo Alto Networks was first. When it comes to product quality, Palo Alto Networks sets the standard for the industry."

Keeping an Eye on VDI

The Citrix virtual desktop infrastructure (VDI) at CBI Health is absolutely critical to the company's business because it allows users to securely access applications and data without having to store the information locally where it might be lost or stolen. However, there was a downside to VDI: visibility. "We didn't know what sites our users were accessing on the Internet and therefore couldn't accurately assess the risk of infections from specific regions or countries," Chojnacki says. "Integrating the Palo Alto Networks Next-Generation Security Platform with our Citrix VDI allows us to have that level of visibility right out of the box using Content-ID™."

Being Held Ransom by CryptoLocker

Recently, CBI Health became the target of ransomware. This insidious virus masquerades as an ordinary email attachment that an unsuspecting user might innocently try to open. At that point, the damage is done: the ransomware (e.g., CryptoLocker) quickly encrypts all information on the user's computer and threatens to delete the information unless a ransom is paid.

In CBI Health's case, this kind of attack isn't a significant security threat, but it does have ramifications. "When we get a ransomware infection, we simply wipe the machine and restore the data from our backups," says Chojnacki. "However, that process takes a few hours of a technician's time and the user's productivity suffers at the same time."

When the average number of successful infections reached three per week, Chojnacki's team sat down to assess and solve the problem. "My team was anxious about where this was going," he says. "What if an IT user's machine got infected? With administrative access, the ransomware could potentially infect huge amounts of data. It could take a week or more to recover. We just couldn't take that risk."

Padlocking the Endpoint to Thwart Threats

Building on CBI Health's good experience with the Palo Alto Networks Next-Generation Security Platform, Chojnacki starting looking at Traps. "The philosophy just made sense to me," he says. "Why not stop threats right at the endpoint rather than clean up the damage? It's just another example of how Palo Alto Networks takes a fresh look at cybersecurity and comes up with an innovative solution."

The infrastructure team set up a Traps trial for a handful of users who had been experiencing the largest number of attacks. They were hoping to see a reduction in the number of ransomware infections but were unprepared for what happened next. "The minute that we turned on Traps, the number of ransomware infections dropped to zero," Chojnacki says. "A week later it was still zero. We literally haven't had a successful CryptoLocker attack since we installed Traps."

Chojnacki is impressed by the way that Palo Alto Networks uses crowdsourcing to improve the operation of Traps. "Even though we don't have a subscription to WildFire, we still benefit from the information there because of the way that Palo Alto Networks has architected Traps," he says. "When Traps finds a file it doesn't recognize, it checks with WildFire to determine if that file has already been encountered. If it's a known threat, Traps blocks it."

Unlocking Staff Time to Fuel Innovation

Based on the successful pilot, the infrastructure team deployed Traps for the entire data center. "The rollout was extremely easy," says Chojnacki. "It took just a few hours of tweaking. We had purchased three days of Palo Alto Networks Consulting Services and wound up using only one and a half for the Traps installation and knowledge transfer."

"Why not stop threats right at the endpoint rather than clean up the damage? It's just another example of how Palo Alto Networks takes a fresh look at cybersecurity and comes up with an innovative solution."

Cameron Chojnacki | Infrastructure Manager | *CBI Health*

Now that Traps is fully operational, CBI Health has reclaimed 8 to 10 hours of staff time a week that would have been spent on remediating the damage from ransomware. Instead, that time has been redirected to more productive uses. "My staff now spends more time on strategic tasks," says Chojnacki. "As a result, we're constantly coming up with new ways to improve security and compliance."

An unanticipated benefit of Traps is that Chojnacki doesn't have to focus on constantly updating the anti-malware software. "Traps catches virtually anything that eludes my other security components, so we can afford to wait on installing patches," he says. "That simplifies security management by giving me one less thing to worry about."

Focusing on the Threat Lifecycle

"Seeing is believing"–that's something that Chojnacki takes to heart. The Palo Alto Networks consultant showed him how to use AutoFocus to observe the entire threat lifecycle. Chojnacki watched in real time as a potential threat easily passed his antivirus software, only to be stopped by Traps. "That time I spent getting up to speed on AutoFocus was one of the most valuable exercises I've done in a long time," he says. "Just one session gave me lot of useful information in a very short time about the efficacy of our various security components and also confirmed just how effective Traps is compared to traditional signature-based security products."

Enjoying Peace of Mind

Chojnacki views the Palo Alto Networks Next-Generation Security Platform as much more than a security solution. "It's peace of mind," he says. "I can tell our executives that we have a stronger security paradigm than virtually anyone else in the industry. Because of our relationship with Palo Alto Networks, we spend more time coming up with ways to improve security, reliability and compliance, and less time just keeping the lights on."