The Heinz Endowments Regains Lost Productivity with Improved Security from Next-Generation Firewalls and WildFire™ from Palo Alto Networks®

BACKGROUND

The Heinz Endowments is a foundation based in Pittsburgh that develops solutions to regional, statewide, and national challenges. The organization's goals are to help southwestern Pennsylvania thrive economically, ecologically, educationally, and culturally—while advancing the state of knowledge and practice in fields such as philanthropy in general, and disciplines in five grant-making programs: Arts & Culture; Children, Youth & Families; Education; Environment; and Community & Economic Development.

PUBLIC OPENNESS COMES WITH RISK

The Heinz Endowments faces particular challenges when it comes to protecting its network. This is due to the foundation's need to be open in its external posture and public interactions. "We need grantees and the public to have access to our executives and staff, so we do some things that aren't best practice, like putting everyone's email address on our website," says Charlie Richardson, Director of Information Technology, The Heinz Endowments.

In addition, the foundation's 40 employees routinely scan documents and send and receive lots of emails with attachments, internally and externally. "A file marked 'Xerox' or 'PDF' usually gets opened," says Richardson. The foundation's staff also frequently interacts and shares documents with 30 interns and many grantees via Microsoft SharePoint. The organization also hosts a Microsoft IIS/SQL server that's not part of its internal network. All of this translates to elevated risk.

Richardson is the one-man in-house IT staff charged with keeping The Heinz Endowments' users and content safe, and the network running smoothly. "From hardware to software, I handle everything," he says. "Every technology has to improve how our employees work and interface with our grantees and the community at large."

The Heinz Endowments' incumbent security infrastructure featured two Cisco 5510 Adaptive Security Appliances (ASA). Its core applications include Microsoft Office 2010 and a grant-making program with a web-based version. Social media is not widely used.

THREAT RAMP-UP CAUSES SHUT DOWNS

A change in the volume and sophistication of threats caused The Heinz Endowments to reexamine its network security. "Over six to nine months, we saw a big increase in malware targeting us," says Richardson. "Previously, we'd seen obvious spam that tried to get our staff to open an attachment, but threats became more devious and clever and truly confused people about whether an email was real or not."

THE HEINZ ENDOWMENTS
Howard Heinz Endowment • Vira I. Heinz Endowment

ORGANIZATION:
The Heinz Endowments

INDUSTRY:
Non-profit

CHALLENGE:
- Gain visibility into network to improve security and safely enable application access.

SOLUTION:
- Palo Alto Networks PA-3020 and PA-200 next-generation firewalls, with Threat Prevention, URL Filtering and WildFire, for granular visibility of threats and better control of Internet applications, and Panorama for Centralized Management.

RESULTS:
- Improved security, with zero network infections since installation
- Lowered annual costs nearly $12,000 through device consolidation
- IT staff recovered 25 percent of time formerly spent on network security
- Increased application visibility and control
- WildFire stopped three malicious threats in first month that nothing else caught
- Enabled flexible application usage policy by user

paloalto NETWORKS®
the network security company™

"All I originally wanted was something to scan files as they come in and get rid of malware. But Palo Alto Networks gives me so much more. It lets me see the type of threat, its category, source IP and port, which port and server it's heading to - everything. It's given me back 25% of my time, which I used to spend answering questions from users about threats or fixing infected machines. Since installing Palo Alto Networks and WildFire, we've had no infections at all."

Charlie Richardson
Director of Information Technology
The Heinz Endowments

The biggest risks came from phishing scams. "Our staff handles so many attachments in emails, so something resembling a PDF would get opened, sending links to people internally and to the network, and infecting everyone. Threats were getting by our firewalls and to our endpoints."

This caused major headaches. "If an infection gets to our network it spreads really quickly because we share so many documents and things via Sharepoint, so we'd literally have everyone shut down and log off and be done for the day," says Richardson. This happened at least once a month, taking a toll on productivity. "Everyone had to unplug their computer and we'd spend all day and night cleaning out each workstation," says Richardson. "Sometimes an infection was so nasty we had to rebuild entire workstations."

The firewalls The Heinz Endowment had in place were unable to keep pace with the new threat landscape. "They were UTMs and didn't have the visibility to detect or analyze the threats that were getting through," says Richardson. He estimates he spent twenty-five percent of his time dealing with threats. "At least an hour a day was lost answering questions from users about spam, what they should or should not open and related issues," he says.

The Heinz Endowments needed more visibility into its network. "I thought there might be something to scan traffic at the packet level as it comes in the door to identify threats, match patterns, and not let users download anything malicious, versus only after it's on your machine," says Richardson.

VISIBILITY SOUGHT, BUT MUCH MORE DELIVERED

Richardson did some research. "Other security solutions can't drill down to the packet level to see if something is malicious," he says. "Then I came across Palo Alto Networks."

Palo Alto Networks next-generation firewalls safely enable applications, users and content through innovative, tightly integrated technologies and services. The firewalls determine an application's identity and classify it across all ports. Next, the application and user are assigned a safe enablement policy, which applies to all users and protects the network against all type of threats from the application—both known and unknown. The PA-3020 next-generation firewall protects datacenters, large enterprise Internet gateways, and service provider environments where traffic demands require predictable, high-speed next-generation firewall and threat prevention at throughput speeds of up to 2 Gbps.

"We requested a Palo Alto Networks PA-3020 firewall demo box and put it in parallel to our Cisco firewall," says Richardson. "Within hours we could see suspect traffic making it through the other firewall that Palo Alto Networks was identifying and wouldn't let through. That was very convincing." Every Palo Alto Networks firewall includes URL filtering, IPS, and Antivirus—all in one box.

Richardson planned to purchase two Palo Alto Networks PA-3020 firewalls. "I was going to sit them alongside the Cisco ASAs, not replace them," says Richardson. "But then I discovered Palo Alto Networks firewalls work seamlessly with our existing VPNs, which our offsite people use to tunnel in, so I decided to replace our primary firewalls and the smaller boxes for our offsite users as well."

All of The Heinz Endowments' traffic now runs in and out of Palo Alto Networks firewalls, which sit in its datacenter and run high availability. The foundation also purchased nine Palo Alto Networks PA-200s, which deliver visibility and control over applications, users, and content to enterprise branch offices. Panorama, from Palo Alto Networks, enables Richardson to easily manage the foundation's distributed network of Palo Alto Networks firewalls.

"WildFire caught three malicious email attachments that nothing else caught within the first month. It has been a lifesaver."

Charlie Richardson
Director of Information Technology,
The Heinz Endowments

WILDFIRE LIGHTS A FIRE UNDER THREATS

To further protect its network, The Heinz Endowments added a Threat Prevention subscription from Palo Alto Networks. The subscription provides integrated protection from a variety of network-borne threats including exploits, malware, dangerous files, and content. "The Threat Prevention subscription was doing a good job blocking a lot of malware, so I wasn't considering adding a 'zero day' malware subscription," says Richardson.

"My curiosity got the better of me, so I requested a trial of WildFire just to see if it would actually catch anything more," says Richardson. Palo Alto Networks' WildFire subscription provides the increasingly important ability to proactively identify and block unknown threats commonly used in modern cyberattacks. It extends the capabilities of Palo Alto Networks next-generation firewalls to identify and block targeted and unknown malware by actively analyzing it in a safe, cloud-based virtual environment.

"For the first few days there was no change or evidence that WildFire was doing anything, so I was fairly sure I didn't need it," says Richardson. "But a week into the trial I noticed a new piece of malware in my Inbox that had gotten past the Threat Prevention module and my third party anti-spam and antivirus product." The file was an imitation of a Xerox scanned email that contained a malicious payload within the attachment.

"Since we use Xerox scanners, I knew people would click on this email without a second thought," says Richardson. "Before I even had time to email our staff, Wildfire had forwarded the file to its cloud service, analyzed the results of opening the payload, deemed the file malware and began blocking it based on a quickly released dynamic update from the Wildfire service." Richardson purchased WildFire and is glad he did. "It caught an additional three malicious email attachment attempts that nothing else caught within the first month," he says. "It has been a lifesaver."

BETTER SECURED TO HELP OTHERS

The Heinz Endowments decision to replace its legacy firewalls with next-generation Palo Alto Networks firewalls has paid off. The foundation is able to interact with all of its constituents - including the public—in a safe and secure manner, while meeting the ever-evolving threat landscape.

"Before Palo Alto Networks, we often instructed everyone to stop working because of infections," says Richardson. "Since installing Palo Alto Networks and WildFire, we've had no infections at all. I can see exactly what is coming in and going on and what is suspicious."

Richardson is confident in the foundation's strengthened network security. "The Palo Alto Networks dashboard tells me way more than I ever knew before," he says. "I can see traffic and threats, URL filtering sees infections or attempted infections and identifies the specific machine involved, and I can see user logs and if anyone is downloading anything potentially harmful or disallowed. My system logs tell me the last time an IPSec tunnel was checked and if there is any problem with it in real-time."

The Palo Alto Networks' Application Command Center (ACC) is a tool Richardson appreciates. "It shows which activities are using bandwidth, who is doing something they shouldn't, if social media is being overused or not and more," he says. "With URL filtering I can see the exact categories of web pages being viewed without having to buy a separate web analytics box."

SAVING ON INFRASTRUCTURE MEANS MORE TO GIVE

"All I originally wanted was something that can scan files as they come in and get rid of malware—that's all," says Richardson. "But Palo Alto Networks gives me all these other functions that I love. It's a true threat management box and true gateway in that I can see everything that comes in and out. I know what kind of threat, its category, source IP, and port—and I can click on an IP and it'll tell me where it came from, which port and server it's heading to—everything. The visibility and level of granularity is tenfold what our previous security products delivered."

The comprehensive capabilities of the Palo Alto Networks next-generation firewalls are enabling The Heinz Endowments to consolidate devices. "Our other firewalls, and our IPS and SmartNet licenses, were expensive," says Richardson. "Getting rid of our incumbent firewalls and SmartNet licenses are saving us about $11,600 annually."

But it's not just money Richardson is saving. "Because I no longer spend an hour a day answering questions from users about threats or dealing with infected machines, I've gotten about 25 percent of my time back, which is the savings I most appreciate," he adds. "Now I can focus on training staff and on other projects, instead of on malware."

Palo Alto Networks support is solid. "They're very good, and even help with things that aren't their responsibility," Richardson says. He has nothing but praise for Palo Alto Networks firewalls. "It's everything needed for network security in a box," says Richardson. "I said 'this little thing does all this for this price?' It's shocking what you really get out of this little box."

paloalto NETWORKS®
the network security company™

4301 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com