Healthcare Provider Cures Persistent Cyberthreats With Advanced Endpoint Protection and Dynamic, Integrated Threat Intelligence

HealthPartners®

"We just have so many options for what we can do with all the different solutions Palo Alto Networks offers and how they all work together. It's kind of scary to think of what we didn't have before. This has been a real eye-opener."

Timothy Pearson | principal security analyst | *HealthPartners*

Industry
Healthcare

Challenge
Prevent malware, ransomware and advanced persistent threats from compromising network hosts and medical systems to ensure the availability and integrity of vital healthcare services and protected health information.

Solution
Palo Alto Networks® Next-Generation Security Platform creates an enterprise-wide barrier against cyberattacks and malicious exploits across endpoints, around the network perimeter, and deep in the network core.

Subscriptions
Threat Prevention, URL Filtering (PAN-DB), WildFire, Traps, AutoFocus, Panorama

Appliances
PA-5220 (6)

Results
- Stopped 100 percent of ransomware samples tested during proof of concept.
- Consolidated multiple systems onto one platform at half the cost of competitors.
- Blocked dozens of cyberattacks in the first year using integrated threat intelligence.
- Reduced PCI scope by securely segmenting PCI and non-PCI traffic in core network.
- Gained granular visibility and deeper insight into cyberthreat activity and point of origin.

Background
HealthPartners® is an award-winning integrated healthcare system based in Bloomington, Minnesota, with a team of 25,000 people dedicated to its mission to improve the health and well-being of members, patients and the community. HealthPartners provides clinical services as well as health plan financing and administration. It's the largest consumer-governed nonprofit healthcare organization in the U.S., serving more than 1.8 million medical and dental members. Founded in 1957 as a cooperative, HealthPartners runs a care system that includes a multi-specialty group practice of more than 1,800 physicians serving more than 1.2 million patients.

Summary
Faced with increasingly sophisticated, persistent cyberthreats, HealthPartners needed advanced endpoint protection as a first line of defense. The company's goal was to tie in endpoint protection with a firewall refresh it was initiating. However, to get all the next-generation security capabilities required in a sensitive healthcare environment, the organization would have had to invest in a huge amount of hardware from its firewall vendor. Instead, HealthPartners got the full breadth of security capabilities at about half the cost by moving to Palo Alto Networks Next-Generation Security Platform.

The move has provided HealthPartners with advanced endpoint protection on all its workstations and servers. It is natively integrated with threat prevention and shared threat intelligence to effectively stop cyberattacks before they can compromise network assets. HealthPartners has also been able to segment its PCI traffic more securely, reducing PCI scope and strengthening compliance. In addition, the organization now has deep visibility and insight into the origin and activity of malware and other exploits, enabling the security team to further strengthen its prevention strategy. The team can now insulate vital healthcare systems from attacks and exploits that could compromise patient care and hospital administration.

Stopping Cyberattacks at Every Endpoint

Imagine sitting in an exam room at a hospital, waiting to find out the result of an important test, but your doctor can't access it because the electronic medical records system has been corrupted with malware. It's a nightmarish scenario that the security professionals at HealthPartners make sure never happens. Preventive barriers exist at every point around the network perimeter and throughout the core data center with help from Palo Alto Networks Next-Generation Security Platform.

"We could clearly see the effectiveness in a real environment of the next-generation firewall using threat intelligence from WildFire based on information Traps was picking up. That gives us a good sense of security, knowing that intelligence is shared across the enterprise."

Joel Pfeifer | principal security analyst | *HealthPartners*

Like any healthcare organization, HealthPartners faces daily cyberattacks attempting to exfiltrate highly sought-after protected health information. The breadth of potential attacks is even greater for HealthPartners as both a care provider and health insurer. Because the threats continue to grow more sophisticated and stealthy, in 2016, HealthPartners took a fresh look at the "next-gen" firewalls it was using at the time. The verdict: the firewalls were no longer adequate to protect the enterprise.

After evaluating several major firewall vendors, HealthPartners chose Palo Alto Networks for the capabilities of its comprehensive Next-Generation Security Platform.

"To get the next-gen features we needed from our previous firewall vendor would have required a huge amount of hardware," says Timothy Pearson, a principal security analyst at HealthPartners. "Palo Alto Networks provided a complete platform of capabilities for about half the cost. Plus, we could consolidate not only the firewalls but also our IPS and web filtering systems from another vendor onto the Palo Alto Networks platform."

This integration will ultimately reduce costs for HealthPartners while providing completely integrated network security.

Joel Pfeifer, also a principal security analyst at HealthPartners, adds, "We were looking for a full package that provides an aggressive approach to identifying and stopping threats; not just detection, but also prevention, so we're not dealing with infections and trying to remediate them afterwards. A key part of that is advanced endpoint protection, ideally integrated with the firewalls. With their Traps offering, that made Palo Alto Networks a perfect fit for us."

Pfeifer put Traps™ advanced endpoint protection through a battery of tests to validate that it was the best choice. The results were unequivocal.

"During the proof of concept, Traps dominated everything else I tested," Pfeifer says. "The local static analysis shut down all the malware I ran through it. I was encrypting a lot of ransomware samples, effectively creating zero-day variants, and Traps stopped 100 percent of them."

Pfeifer didn't see the same level of protections from other vendors he tested. "I had a fully compromised host on the first try," he says. "The dynamic analysis with WildFire was also very successful and consistently stopped all the threats I threw at it. And it returned full reports within five [minutes], just as advertised. One of the competing systems took two days."

Shared Threat Intelligence Preempts Exploits Enterprise-Wide

HealthPartners encircled its enterprise with a rock-solid layer of security. Palo Alto Networks Next-Generation Security Platform, with next-generation firewalls, Traps, and WildFire® cloud-based threat analysis service was deployed to nearly 30,000 workstations and more than 2,000 servers. This allows the organization to protect applications, users and content from known and unknown cyberthreats across seven hospitals, its insurance business, and approximately 100 other locations.

"We had excellent support [for our Traps deployment] from Palo Alto Networks," Pfeifer says. "The few issues that did arise were addressed very quickly. With the first ticket I submitted, which was low priority, I got a call back within eight minutes. That's unheard of with any of our other technology vendors."

Pfeifer has been impressed with the Traps interface and the detailed insights it provides.

"It's very intuitive and fast, with useful information I can use to see what's going on," he says. "In the case of an attack, I can clearly identify what kind of attack, all the details of what the malware is doing, post-detection events – it's all very straightforward and logical."

Since having Traps in place, HealthPartners has effectively stopped more than 100 cyberattacks from compromising its systems.

"We can clearly see the effectiveness in a real environment of the next-generation firewall using threat intelligence from WildFire based on information Traps was picking up," notes Pfeifer. "That gives us a good sense of security, knowing that intelligence is shared across the enterprise."

Prevention of Known and Unknown Threats

Working in tandem with Traps, the next-generation firewalls bring a powerful preventive capability across the entire enterprise. Previously, HealthPartners had both an edge firewall and

"Because of the consistency and high percentage of true positives we get from the Palo Alto Networks platform, we have the confidence now to automate. We could take advantage of information the Palo Alto Networks platform provides and automate threat mitigation. That's something we've never had the opportunity to do until now."

Joel Pfeifer | principal security analyst | *HealthPartners*

core firewall that served double duty, separating the corporate network from the DMZ and PCI traffic. As Pearson points out, this created a compliance nightmare.

"Regulators don't like to see a firewall sharing a configuration that could touch PCI and non-PCI traffic," he says. "One of the really awesome things about switching to Palo Alto Networks is we could divide up the PA-5220 into two virtual systems. So, we're running a PCI [virtual system] and a DMZ [virtual system], which keeps the policies completely separated and reduces our PCI scope."

This approach effectively prevents a constant barrage of high-, medium- and low-priority cyberthreats from penetrating the network while giving the security team a level of network visibility they've never seen before.

"We're stopping the threats and then have the granularity to trace down where they're coming from," Pfeifer says.

Pfeifer points out that AutoFocus™ contextual threat intelligence service plays a key role in giving him deep visibility into threats. AutoFocus allows him to look up an IP address or a hash to determine if the organization has seen it on an endpoint or at the perimeter, or throw in a certain tag to see if Palo Alto Networks has seen it before.

Pearson adds, "We just have so many options for what we can do with all the different solutions Palo Alto Networks offers and how they all work together. It's kind of scary to think of what we didn't have before. This has been a real eye-opener."

Real-Time Insights Through Splunk Integration

In addition to the range of next-generation security capabilities and tools, Pfeifer has created some custom applications that integrate data from the Palo Alto Networks platform with Splunk®. This enables greater opportunities for ad hoc analysis, with real-time visibility into things like PowerShell® code executed across HealthPartners network assets.

Pfeifer explains, "I use the Splunk analysis to execute ransomware delivered via PowerShell to see how Traps stopped the malicious payload and how it's handled in the firewalls. I have a single pane of glass that's live when I'm testing malware to gain full visibility into the entire attack chain, and uncover any potential gaps we may have in our security. Splunk works great with Traps and the Palo Alto Networks firewalls. They're super flexible and dynamic."

Intelligent Security Administration Relieves Frustration

To streamline managing the security landscape, the HealthPartners team relies on Panorama™ network security management. Panorama provides a centralized resource for managing static rules and dynamic security updates, saving time and ensuring consistency enterprise-wide.

"Panorama makes administration of multiple firewalls so easy," Pearson says. "It gives you the information you need to figure out what's going on across the whole Palo Alto Networks platform." He goes on to say that, from a compliance standpoint, Panorama gives a single policy push that is easier to monitor instead of tracing back to individual firewalls. "It definitely reduces a lot of frustration, while giving us so much more information and insight," he says.

The future looks bright in security strategy for HealthPartners, thanks to the strong abilities of the Palo Alto Networks platform.

"There are a lot of exciting opportunities that we haven't had before," Pfeifer says. "Because of the consistency and high percentage of true positives we get from the Palo Alto Networks platform, we have the confidence now to automate. We could take advantage of information the Palo Alto Networks platform provides and automate threat mitigation. That's something we've never had the opportunity to do until now."