Case study

Loyola University Chicago prevents harmful network intrusion with HP TippingPoint

University protects its global network from malicious attacks and malware with HP TippingPoint Next-Generation Intrusion Prevention System

Industry
Higher education

Objective
Strengthen network security against malicious attacks and malware infections

Approach
Deploy HP TippingPoint Next-Generation Intrusion Prevention System, HP TippingPoint Security Management System, and HP TippingPoint Threat Digital Vaccine service

IT matters
- Improved visibility of network devices and traffic to maintain highly trusted state
- Successfully contained infiltration of notorious CryptoLocker malware
- Simplified management with easy creation of security policies and automatic digital vaccine updates

Business matters
- Identified and contained approximately 160 malware infections, preventing widespread disruption to the university
- Blocked 77 million attacks in just two months thanks to more granular, broadly encompassing filters from DVLabs, ensuring protection of the university community and IT
- Strengthened protection of dynamic academic environment through quick assessment of new devices and implementation of appropriate security policies prior to on-boarding

LOYOLA UNIVERSITY CHICAGO
Preparing people to lead extraordinary lives

"I have the utmost confidence that if something malicious enters our network, TippingPoint is blocking it."

– Brett Weston, Information Security Administrator, Loyola University Chicago

With tens of thousands of devices on its global network, Loyola University Chicago needed a highly reliable intrusion prevention system to block malicious attacks and quickly contain infected devices. The university deployed HP TippingPoint Next-Generation Intrusion Prevention System (NGIPS), which blocks as many as two million attacks per week. TippingPoint NGIPS also successfully contained a potentially devastating infection of CryptoLocker, preventing the malware from spreading across its network. With automatic updates from HP Digital Vaccine Labs (DVLabs), Loyola has the utmost confidence that its network and devices are securely protected.

Loyola University Chicago is one of the largest Jesuit institutions in the United States, with nearly 16,000 students and campuses worldwide. With each student bringing on average 4.5 devices to campus, the university's IT department faces an enormous daily challenge to protect tens of thousands of devices from becoming infected and spreading viruses or malware across its global network.

One of the university's primary objectives for enterprise security is to maximize visibility on its network—to track devices and monitor traffic to quickly identify potential threats. To do that, Loyola relies on HP TippingPoint NGIPS.

Brett Weston, information security administrator for Loyola University Chicago IT Services, says, "We evaluated TippingPoint against other offerings in the market, like Palo Alto, and TippingPoint is so much more polished and powerful than those other solutions. We also have strict separation of duties between the network management team and information security. Because TippingPoint is a dedicated device, inline on the network, we're able to maintain the necessary separation. That was a big selling point."

Stops malware in its tracks

Loyola deployed three TippingPoint NGIPS devices at its network edge, configured to protect against signature-based attacks. The NGIPS automatically blocks traffic identified as malicious and enforces policies to contain malware or viruses should a device become infected. An essential element in blocking malicious flows before they hit Loyola's network core is HP TippingPoint Threat Digital Vaccine (ThreatDV), a subscription reputation security service that disrupts malware activity.

Loyola's TippingPoint solution was put to the test when the CryptoLocker malware began attacking networks in 2013. To prepare for a possible attack by CryptoLocker—which encrypts all the data on a device, rendering it useless unless a ransom is paid—Loyola leveraged the HP TippingPoint DVLabs team, which provided the necessary filters within 48 hours. The university immediately enabled the filters on TippingPoint NGIPS with policies customized to automatically kick an infected device off its network. Because CryptoLocker infiltrates a network as an email attachment, there was no way to stop it—but with TippingPoint, Loyola had a powerful way to contain it.

"We ultimately had about 150 devices infected by CryptoLocker," reports Weston. "TippingPoint contained all of them immediately, which really spared us from a nightmare scenario. If the malware had spread across our network, it would have essentially shut us down. Instead, we stopped CyptoLocker in its tracks. And the security intelligence provided by ThreatDV pointed us right to 'patient zero' so we could quickly identify the infected devices and get them cleaned up."

With TippingPoint NGIPS, Loyola has stopped approximately 160 such malware infections from spreading across the university. On average over the last three years, the ThreatDV service has blocked 80 million threats per year. However, with potential threats on the rise, DVLabs has been developing more granular, more broadly encompassing filters that have enabled Loyola to block 77 million attacks in the last two months alone.

"We're confident HP is doing everything possible to ensure our protection against malicious attacks," Weston remarks.

Protection against foreign attacks

Most recently, Loyola implemented the geo-filtering capabilities of TippingPoint NGIPS to block IP addresses originating or traveling to certain countries other than the U.S. Geo-filtering is specifically applied to the university's Payment Card Industry (PCI) environment to limit bad traffic and keep this critical credit/debit card payment network secure against foreign attacks.

"Implementing the geo filter based on IP address was easy," says Weston. "It only took about two minutes to create the filter and implement it in 'permit and notify' mode. We wanted to watch the network behavior for the first month and then decide what to block. Now we're in 'block' mode and it is working like a charm."

Customer at a glance

HP Solution

- HP TippingPoint NGIPS
- HP TippingPoint Security Management System
- HP TippingPoint Threat Digital Vaccine service

Detailed reporting guides security strategy

Loyola also takes advantage of the HP TippingPoint Security Management System (SMS), which provides global visibility of the protected network, as well as extensive security policy control and reporting. Using the SMS, Weston has created a number of custom reports around compliance for the university's PCI environment. The SMS also provides daily reports of every filter that's triggered to identify the number, type, frequency, and source of attacks. With geo-filtering, the SMS reports also list the top origins for foreign-based attacks.

Weston comments, "The reports have helped us demonstrate to upper management the value of our security investments, and that gives us credibility when we request funds for additional technologies. The reports also help us scope how we posture new devices coming onto our network."

Under the rules of academic freedom, Loyola allows nearly any device on its network. However, before a new type of device is on-boarded, Weston identifies the exact configuration of the device and pulls a report of all current digital vaccine definitions from the SMS. "That way we know exactly what threats TippingPoint will prevent, map them to the operating environment and applications running on the device, and set up that device with the most appropriate security policies," he explains.

Set-it-and-forget-it management

An important factor in keeping up with a constantly changing threat environment is having protection that simply works without a lot of hands-on management. TippingPoint has proven to be very easy to set up and configure. In fact, when DVLabs pushes out updates, a number of filters turn on automatically.

"With HP TippingPoint, it's mostly just 'set it and forget it,'" asserts Weston. "I spend maybe an hour a week on administration. It's the simplest product our office manages, which frees up a lot of time to focus on other important projects. And I have the utmost confidence that if something malicious enters our network, TippingPoint is blocking it."

Learn more at
hpenterprisesecurity.com

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-5898ENW, November 2014