CASE STUDY

THREATX

GHX Trusts ThreatX to Secure and Optimize the Performance of the Largest Footprint in Healthcare Supply Chain

GHX

ABOUT GHX

GHX is a healthcare business and data automation company that provides a cloud-based supply chain technology exchange platform as well as solutions, analytics and other services. GHX brings together more than 4,100 healthcare providers and 600 manufacturers and distributors in North America, and another 1,500 providers and 350 suppliers in Europe through its exchange. These customers rely on smart, secure healthcare-focused technology and comprehensive data to automate their business processes and make more informed and timely decisions. The exchange processes about a million orders every day.

The company also operates web-based SaaS applications that enable customers to look at catalog data, validate contract pricings, and negotiate with trading partners. The data at the heart of these applications is sensitive and subject to government and industry regulations such as HIPAA, PCI-DSS and GDPR.

THE CHALLENGE

- Eliminate the burdens of an on-premises, rule-based WAF
- Provide stronger security assurance to customers and prospects

People throughout North America and Europe who go to a hospital or clinic for healthcare services are likely to be the indirect beneficiaries of GHX services. In many cases, the medical supplies in the facility –from tongue depressors and scalpels to knee joint implants – are the result of an order that came through GHX's systems. The company essentially manages the order supply chain across 800,000 different trading partner relationships through its base exchange. Two dozen or more ancillary SaaS applications support the GHX ordering systems.

AT A GLANCE

Customer:
Global Healthcare Exchange (GHX)

Industry:
Healthcare Supply

Challenge
The cost and complexity of operating and maintaining the company's traditional, on-premises firewall was costly. GHX also needed to provide customers and prospects stronger security assurance.

Solution
ThreatX Intelligence Web Application Firewall (WAF) and Managed Service

Results

- Implemented a kill-chain based managed service that effectively monitors for and prevents application security threats 24x7x365.
- Extended the internal security team with expert support from the ThreatX Security Operations Center (SOC), thus avoiding the expense of additional in-house security professionals.
- Acquired threat and attack intelligence to proactively support SecOps in near-real-time.

Given the company's broad market reach, the assurance of uptime and security of all the applications is critical to healthcare providers who rely on GHX to automate their business processes. About five years ago, Sloane Stricker, Chief Information Security Officer and VP of Operations and Infrastructure, began to lead a transformation to modernize the GHX technology platform and reallocate the company's time and resources. The goal was to transition from a 1990's style architecture based on a "do it all ourselves" data center to a hybrid approach where many infrastructure services could be cloud-based.

The company's WAF was a top priority in the transition process, according to Stricker. "We had a firewall appliance that we bought, installed and configured. Then we had to operate it, maintain it, and stay on top of the correct updates. The cost and level of effort to run it ourselves was significant. We knew there was a better solution out there."

> "When I look at ThreatX as a managed service, not just as a toolset, they have allowed us to stay on top of security.
>
> - Sloane Stricker - CISO and VP of Global Operations and Infrastructure, GHX

A second issue for GHX was passing their audits and providing the right assurances to customers. "As a technology company, we must attest to our customers in written agreements that our operations are secure. This often involves completing lengthy questionnaires detailing our security practices, and if we can't do that, we can't get their business," says Stricker. "This was a real challenge when we operated our own on-premises security devices, largely due to the complexity of managing extensive rules and keeping up to date with threat detection measures."

THE SOLUTION

GHX signed on to do a proof of concept project with ThreatX for a solution involving a managed service of their cloud- based WAF. "We had a complex application environment," according to Stricker. "The biggest hurdles we had were our network topologies, we had infrastructure as a service with AWS along with our own data centers, and real complexity in how our applications and our web front end were configured. ThreatX worked with us to reconfigure things to pass all our traffic through a third party and measure the latency." The team did extensive testing of the configuration to make sure good traffic wouldn't get backlisted, and to help demonstrate the visibility that the ThreatX iWAF provided that GHX didn't have before.

"ThreatX sent their experts to work side by side with us and they had people on call when we had questions. They helped us see not just security threats but also traffic patterns to help us ensure everything was configured correctly. We couldn't take a chance that any legitimate customer traffic would be blocked inadvertently," says Stricker. "The ThreatX solution is a living part of our network that is going to provide so much more than a traditional web application firewall does."

Following a successful PoC, GHX bought into the managed service for the ThreatX iWAF, and the solution has been in place for more than two years. The ThreatX Security Operations Center provides alerts and threat intelligence pertaining to suspicious activity or actual attacks.

The threat intelligence is a real plus for GHX—it's something they weren't getting before deploying the WAF. Stricker's security team uses the information to look more broadly at what kind of suspicious activity they have and to stay on top of it in near-real-time. The intelligence feed from ThreatX is based not only on events that are internal to the GHX environment, but also external to the network, across and even beyond ThreatX's entire customer base.

> “ I've been able to avoid the headcount expense of a security engineer that would be tasked with reviewing events, looking at the attack intelligence, and staying on top of everything.
>
> - Sloane Stricker - CISO and VP of Global Operations and Infrastructure, GHX

The GHX security team is in regular communication with the ThreatX SOC, at least twice a month if activity appears to be normal, and more often if there are higher level alerts or concerns of an attack. The SOC has essentially become an off-payroll extension to Stricker's security team. "I've been able to avoid the headcount expense of a full security engineer that would be tasked with reviewing events, looking at the attack intelligence and staying on top of everything," he says.

THE BENEFITS

» Eliminates the ever increasing operational burden of maintaining an, on-premise, rule-based WAF including concern around a single point of failure

» Elevates the company's overall security posture through a broader, proactive security operations program

» Shortens and improves the sales cycle by providing security assurance for customer master agreements

GHX now routes a high percentage of its web application traffic through the ThreatX WAF in the cloud, which allowed the company to decommission its old firewall. "One of the biggest benefits of this solution is that we no longer have to run the firewall ourselves, or deal with the licensing, the growth in throughput, and the annual true-ups of the usage contract," says Stricker. "We no longer worry about having a single point of failure of a critical piece of our security." The threat intelligence feed from ThreatX helps bolster the company's broader security program. "We have recently embarked on a program around SecOps – security operations – similar to DevOps," says Stricker. "Before we had ThreatX, we would look at our reports in a reactive, firefighting mode when there was suspicious activity or a real attack.

No one would do analysis and look at what was trending in terms of threat intelligence to try to get ahead of threats. Now we have these reports that give us meaningful, real-time intelligence and we can build that into our security programs to become proactive. This allows us to tell our customers that we are protecting our websites and we are actively looking for threats that may or may not be in our environment. The reports provide us a lot of assurance there."

The protections and assurance delivered by ThreatX provide a real business advantage for GHX. "We have a lot of sensitive data going back and forth across our systems," explains Stricker. "Our customers have to have InfoSec agreements as part of our master agreements with them. This includes our SOC reports, PCI attestations, and now, assurances of GDPR compliance. With our customers and prospective customers, we have to complete very lengthy security questionnaires, and there are entire sections that ask questions like, 'How do you do your firewall? How often do you review logs? How often do you look at threats? When was your last incident? When was your last malicious attack?'" "If we can't answer those questions, we won't get their business," Stricker says. "When I look at ThreatX as a managed service, not just as a toolset, they have allowed us to stay on top of security. Now I can answer those questions a lot more confidently and we can move the sales process along. Once these customers are in production with us, they have assurances that they are running on this secure platform. I can't understate the value this delivers to our company."

THREATX

www.threatx.com | +1 888.303.5580 | info@threatx.com

ABOUT THREATX

Using a unique kill-chain approach, ThreatX's Intelligent Web App solution provides real-time threat detection and neutralization in a highly adaptable, cloud-based architecture. With dynamic, progressive and automated behavior profiling, ThreatX delivers a holistic view of all threats, attack vectors, and targeted application vulnerabilities, all in an easy to understand, risk-based view of threat intent.

TRY THREATX TODAY
www.threatx.com/free-trial