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

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 pricing, 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. 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.”

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: A Next-Gen WAF and Managed Service Expertise from Threat X

GHX signed on to do a proof of concept project with Threat X for a solution involving a managed service of their cloud-based iWAF. “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. Threat X 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 blacklisted, and to help demonstrate the visibility that the Threat X iWAF provided that GHX didn’t have before.
"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."

- Sloane Stricker, CISO and VP Global Operations and Infrastructure, GHX

"Threat X 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 Threat X 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 Threat X iWAF, and the solution has been in place for more than two years. The Threat X 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 iWAF. 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 Threat X is based not only on events that are internal to the GHX environment, but also external to the network, across and even beyond Threat X’s entire customer base.

The GHX security team is in regular communication with the Threat X 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 Threat X iWAF 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 Threat X 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 Threat X, 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 Threat X 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 Threat X 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 understated the value this delivers to our company."

**Confidently Secure Your Web Apps with Threat X**

Using a unique kill-chain approach, Threat X's Intelligent Web Application Firewall solution provides real-time threat detection and neutralization in a highly adaptable, cloud-based architecture. With dynamic, progressive and automated behavior profiling, Threat X 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.

Schedule your personalized demo at: [https://threatx.com/demo](https://threatx.com/demo)
A Fundamentally Different Approach to Web Application Threat Protection

The Challenges of Today's Web Application Environments

The complexity of modern, hybrid cloud and heterogeneous technology environments combined with an ever-evolving threat landscape creates a large and dynamic attack surface for almost any organization. Furthermore, "next-gen" rule, signature, and anomaly detection-based web application firewall (WAF) solutions are missing the most critical, high-impact attacks because they lack contextual information on the attacker itself. As a result, security teams are armed with limited intelligence from their current tools to address an increasing volume of sophisticated attacks.

An Attacker-Centric Web Application Security Solution

Threat X's next-generation web application firewall addresses the gaps left by other WAF's. Instead of focusing solely on the applications themselves, Threat X focuses on the attacker. By tracking their progress through the kill-chain, and combining and corroborating multiple indicators of suspicious activity, Threat X is able to build a progressive risk profile of threat intent. The result is deep visibility into the varying attack types and techniques, as well as the target vulnerabilities in your application environment.

Threat X has transformed web application protection with a highly effective and accurate threat mitigation solution that reduces false positives without the constant tuning of rules and signatures:

- Precise detection and neutralization of even the most sophisticated, high-impact attacks (SQLi, XSS, OWASP)
- Comprehensive and accurate views into risk and vulnerability levels
- Significantly lower operational burden and cost
The Threat X Platform

How it Works

1. A kill-chain based approach classifies suspicious behaviors and associated risk
2. IP Interrogation uses javascript injection, cookies, and forms to validate suspicious users and build attacker profiles
3. Deception overlays customer applications with bait URIs, headers, and forms to lure attackers into disclosing their intentions
4. Shared threat analytics correlates attack patterns and techniques across multiple customers and applications
5. Threats are blocked in real-time based on a configurable risk score, instead of rules

Combined Bot, DDoS, CDN, and WAF in a Rapidly Deployable Cloud-Native Solution

Threat X is purpose built for the hybrid-cloud, is application agnostic and deploys in hours via docker containers. This means you can be in blocking mode within 1-2 days vs. 4 weeks, as is common with other next-gen WAF’s. Threat X also integrates WAF, Bot, DDoS and CDN into one solution so customers can realize immediate protection for all their apps against OWASP and zero-day attacks. These features, combined with Threat X’s 24/7 monitoring and managed service, enables highly proactive threat response for any organization.

Trusted by Global Enterprises

“The real business benefit for us, first and foremost, is the level of protection that Threat X provides to our web applications...Next would be the ability to provide this protection across all our services with very little overhead. Using Threat X moves us forward without impacting our team’s constrained resources.”

- Senior Director of Information Security, BMC Software

Ready to see what a next-gen WAF should really do?

Take the next step. Start your free trial today and see how easy it is to enable comprehensive, unparalleled protection for your application environment from today’s advanced threats.

Learn more about Threat X and connect on Twitter and LinkedIn.

Start your free trial
https://info.threatx.com/free-trial

Contact Us

Threat X Inc.
info@threatx.com
+1 888-303-5580

© 2018 Threat X, Inc.
BMC Software Relies on Threat X to Protect Its Vast Portfolio of Enterprise Applications and Websites Across a Multi-Cloud Environment

About BMC

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises, including 92 of the Forbes Global 100.

The company provides hundreds of software products serving functions such as IT service management, data center automation, performance management, virtualization lifecycle management and cloud computing management. Increasingly, these products are offered as Software-as-a-Service delivered from numerous cloud hosting services. Practically every BMC customer has a web presence into various BMC software solutions.

The Challenge

- Support a multi-cloud initiative for BMC's high-volume applications
- Eliminate traditional security toolsets deployed on a per-provider basis
- Protect the brand and sensitive information by securing external facing applications and API integrations
- Support rapid deployment and validation of WAF configurations with minimal application downtime
- Satisfy legal requirements on embargo country compliance

BMC Software is the premier provider of IT management solutions to enterprise organizations around the world. Founded almost 40 years ago, the company has helped tens of thousands of customers operate, manage, and optimize their computing environments, from the IBM mainframe era of the 1980's to the diverse mobile and cloud computing environments of today.
BMC has developed industry leading, SaaS-based versions of many of their products, delivering them to customers through various cloud hosting environments. BMC has some of the largest enterprises in the world running mission-critical applications on their cloud services and the company website, BMC.com is an important brand and solution evaluation platform. To protect these web applications and services from external threats and attacks, BMC had made investments in traditional security toolsets; however, these tools simply could not effectively support and protect the company’s innovative and rapidly evolving cloud application portfolio. Applying these tools as point products on a one-off basis was too costly from both a budgetary and a people perspective. A better solution was needed.

“Our forward-thinking, multi-cloud initiative demands that we are able to support the use of different service providers and hosting solutions,” says Joel Bruesch, Senior Director of Information Security at BMC. “My team very much needed a standardized, best-in-class solution that could scale and work everywhere. We can’t cobble together 10 different application security solutions and still end up with a technology portfolio that we can protect and manage. It would grow exponentially and be totally unsustainable, given the size of our support team.”

Bruesch says that the complexity and the limitations of the other solutions, namely rule and signature-based approaches, were quite a resource strain on his team. It was difficult to provide the protection they wanted by continuing to utilize the legacy tools. “The old tools did not support a path forward for us, whereas Threat X really diminished the need for internal resources to secure our cloud services with a high level of threat protection,” he says.

**The Solution**

BMC was attracted to the Threat X SaaS-based Web Application Firewall for several reasons. “A behavior-based approach to security was very compelling for us. Threat interactions are monitored, and Threat X enables us to automatically identify and block potentially malicious and suspicious behavior. We don’t have to specify the conditions or rules like we would in any other WAF because the Threat X solution continuously learns from what it observes,” says Bruesch.

Another selling point was that Threat X enabled BMC to optimize its cost structure and the service levels they were trying to achieve. “Our existing investments in security were not something we could leverage for our new multi-cloud model,” says Bruesch. “For any company that is going to take a multi-cloud approach, there are financial drivers behind that, and any security organization that doesn’t have a reference architecture to support their traditional capabilities in a multi-cloud world is going to get crushed. We put in a significant effort to reassess our capabilities.
across the board to make sure they were going to fit into that future, and Threat X suited our requirements quite well.”

BMC started with a proof of concept test (PoC) of the Threat X SaaS-based WAF and managed service. Threat X engineers worked closely with the BMC Security Operations Center (SOC) team to configure the solution. According to Bruesch, “Threat X has a lightweight, but highly effective PoC process and it was a was a success by every measure. It gave us the confidence to move forward with Threat X and proceed with protecting our largest website. The set up required very little in the way of time and resources, and the support and responsiveness we got from Threat X has been world class.”

The Benefits

Unparalleled Protection
As of this writing, BMC has had the Threat X web application firewall and managed service in place for about a year. “The real business benefit for us, first and foremost, is the level of protection that Threat X provides to our web applications,” says Bruesch. “Next would be the ability to provide this protection across all our services with very little overhead. Using Threat X moves us forward without impacting my team’s constrained resources.”

Complete Visibility
Threat visibility has been another important benefit of using this solution. “With Threat X, we get a level of visibility into our threat landscape that we’ve never had before, and we share it with the business unit (BU) stakeholders. Their traditional view of security has been that it’s cumbersome and introduces more complexities than it does benefits. Threat X has changed that perception by giving us the ability to easily show the value of this solution to the BUs. For example, we can show the specific vulnerabilities that are being targeted for attack. Armed with that knowledge, the BU leaders are now driving the adoption of Threat X into the cloud product and services they are responsible for. That’s very uncommon for security solutions, in general. It helps us support our mission of putting very accurate protection around all of our customer-facing products and services.”

Active Prevention
Bruesch says they have experienced secondary benefits they hadn’t specifically anticipated as part of the adoption of Threat X. The experienced Threat X SOC team closely monitors activity and can identify where an attack is originating. The SOC then proactively alerts the BMC security team to recommend custom rules needed to whitelist legitimate application behavior.
Accurate Blocking
In one instance, BMC was able to detect and mitigate a bot-based attack that was focused on generating traffic overhead on its main website. The excessive activities could have impacted performance and put BMC at risk of significant overhead costs with its content management provider. "Threat X picked it up and we were able to provide a cost avoidance for one of our business units," says Bruesch. "Additionally, Threat X helps us to satisfy a legal requirement for blocking embargoed country traffic to our applications and websites without adding additional maintenance or cost."

Executive Level Analysis
Threat X sends regular reports, which arm BMC with metrics on the attack types, source countries, top application targets, and more. "It has been incredibly useful for us to show our internal clients the sheer volume of attacks that our web assets get, and which ones are most vulnerable," says Bruesch. "It's an eye-opener for the business units that haven't yet incorporated Threat X protection on their products. These metrics speak for themselves and help to sell the service internally."

Confidently Secure Your Web Apps with Threat X
Using a unique kill-chain approach, Threat X's Intelligent Web Application Firewall solution provides real-time threat detection and neutralization in a highly adaptable, cloud-based architecture. With dynamic, progressive and automated behavior profiling, Threat X 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.

Start your free trial of Threat X: https://threatx.com/free-trial

Contact Us
+1 888 303 5580
info@threatx.com
www.threatx.com