BMC Software Relies on ThreatX to Protect Its Vast Portfolio of Enterprise Applications and Websites Across a Multi-Cloud Environment

bmc

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.

AT A GLANCE

Customer:
BMC Software, Inc.

Industry:
Information Technology Management

Challenge
Protect BMC's critical business and portfolio applications and websites distributed globally across a hybrid-cloud environment.

Solution
ThreatX SaaS-Based Web Application Firewall as a Managed Service

Results
» Delivered extensive visibility and insight to the business units on the volume and types of attacks across critical web and cloud apps, helping to drive smart optimization decisions, reduce the threat the threat landscape, and meet legal requirements.

» Met the need to protect and scale across a growing number of applications and cloud platforms, without increasing headcount.

» Aligned the BMC and ThreatX SOC teams to monitor the health of BMC's application environment, and share best practices and critical threat intelligence.

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.

> " My team very much needed a standardized best-in-class solution that could scale and work everywhere."
> - Joel Bruesch, Senior Director of Information Security at BMC

"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 ThreatX 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 ThreatX SaaS-based Web Application Firewall for several reasons. "A behavior-based approach to security was very compelling for us. Threat interactions are monitored, and ThreatX 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 ThreatX solution continuously learns from what it observes," says Bruesch.

Another selling point was that ThreatX 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 ThreatX suited our requirements quite well."

BMC started with a proof of concept test (PoC) of the ThreatX SaaS-based WAF and managed service. ThreatX engineers worked closely with the BMC Security Operations Center (SOC) team to configure the solution. According to Bruesch, "ThreatX 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 ThreatX 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 ThreatX has been world class."

> " The real business benefit for us, first and foremost, is the level of protection that ThreatX provides to our web applications."
>
> - Joel Bruesch, Senior Director of Information Security at BMC

THE BENEFITS

Unparalleled Protection

As of this writing, BMC has had the ThreatX 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 ThreatX provides to our web applica- tions," says Bruesch. "Next would be the ability to provide this protection across all our services with very little overhead. Using ThreatX moves us forward without impacting my team's constrained resources."

Complete Visibility

Threat visibility has been another important benefit of using this solution. "With ThreatX, 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. ThreatX has changed that perception by giving us the ability to easily show the value of this solution to the BUs. For exam- ple, 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 ThreatX 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 ThreatX. The experienced ThreatX 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 overage costs with its content man- agement provider. "ThreatX picked it up and we were able to provide a cost avoidance for one of our business units," says Bruesch. "Additionally, ThreatX 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

ThreatX 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 ThreatX protection on their products. These metrics speak for themselves and help to sell the service internally.

SRC CYBER SOLUTIONS LLP

THREATX

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com   🐦 f in

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

CALL TO ACTION
www.srccybersolutions.com/contact-us