CASE STUDY

Dynamic Cloud Security Enables Global Training & Enablement Group To Focus on Business Transformation

Fortinet is a Fortune 500 network security company that prides itself on leveraging technology to improve efficiency. An important team within the Fortinet Global Training & Enablement group, the systems development team designs, develops, and manages the custom web applications underlying Fortinet's award-winning training and certification programs. Like many lean teams with ambitious goals, the systems development team leverages a combination of off-the-shelf commercial and open-source solutions as building blocks. Using the open-source learning platform Moodle and the secure open web analytics platform Matomo for analytics, combined with three Atlassian commercial applications—Jira for project management, Bitbucket for version control, and Confluence for documentation—enables the team to focus on delivering cost-effective and highly scalable training applications.

> *"This application is absolutely critical to our business, so we decided to roll out FortiGate VM next-generation firewalls and FortiWeb web application firewalls. These enterprise security solutions alleviated concerns that open-source code tends to raise."*
>
> – *Tristan Roscoe, Systems Development Manager, Global Training & Enablement, Fortinet*

Details

Customer: Fortinet

Industry: Technology

Location: Sunnyvale, CA

DevOps Introduces New Security Challenges

Until Fortinet started down the path to open its Network Security Expert (NSE) certification program to the public, the Global Training & Enablement group used a Software-as-a-Service (SaaS)-based learning management system (LMS). The Global Training & Enablement group knew this change would greatly expand the number of users of the LMS, and licensing costs for the SaaS-based solution were poised to skyrocket to more than $1 million per year.

Tristan Roscoe, systems development manager for the Fortinet Global Training & Enablement group, led the charge to reevaluate the technologies underlying the SaaS platform. As the company prepared to extend the NSE program, Roscoe elected to transition to an open-source learning platform, which completely eliminated per-user licensing costs and saved hundreds of thousands of dollars in software licensing costs. This advantage, however, did not come without risk. "Even though we see more widespread adoption of open-source software, concerns with open source remain," Roscoe says. Specifically, Roscoe and his team were troubled with the fact that small upgrade windows are provided before vulnerabilities are made public. "And this doesn't include new vulnerabilities that are unintentionally introduced in some future product update," Roscoe adds.

Roscoe and his team planned to run their custom, Moodle-based learning platform in Amazon Web Services (AWS). As AWS embraces a shared responsibility model, Roscoe knew that security needed to be a top priority. "Even when security practices are robust, DevOps processes can sometimes introduce new vulnerabilities," Roscoe says. Here, the systems development team needed to ensure that the mission-critical learning platform would be protected, and that vulnerabilities would be addressed before reaching production. Yet, at the same time, they needed to do so without sacrificing code quality, performance, or time to market for delivery of new features. "A dynamic cloud security approach is a requisite when dealing with DevOps, and a traditional security approach simply would not work for us," Roscoe states.

DevOps Demands Dynamic Cloud Security

The systems development team turned to FortiGate VM, a next-generation firewall (NGFW) that provides protection parallel to that of a physical appliance but in a virtual machine (VM) form factor. They also deployed FortiWeb web application firewalls (WAFs) in AWS. "WAFs are the primary tools that DevOps teams typically use to address vulnerabilities in the applications they develop," Roscoe explains.

As the Fortinet learning platform and other internally developed systems evolve, the FortiWeb WAF alerts the systems development team of any suspicious behavior it detects. Moreover, by incorporating application learning, FortiWeb minimizes false positives, optimizing efficiency while achieving effective protection. This ensures that the security layer does not slow down speed to market for upgrades to Fortinet training systems.

"This application is absolutely critical to our business," Roscoe says. "So, we decided to roll out FortiGate VM next-generation firewalls and FortiWeb web application firewalls. These enterprise security solutions alleviated concerns that open-source code tends to raise."

Today, the systems development team uses EC2 instances, one each for an application server, FortiGate NGFW, and FortiWeb WAF—along with EC2 Auto Scaling and RDS relational databases. Managing these systems in the public cloud saves Roscoe's team from hardware deployment and maintenance. It also makes redundancy possible. "The instances spin up in different Availability Zones," Roscoe explains. "That removes a single point of failure for our systems. If any of the VMs goes down in one availability zone, traffic is routed through the other availability zone."

While this approach works well, it also consumes a lot of management time for Roscoe and his team. "We need to focus our energies and time on application development," Roscoe observes. "Time managing the security environment takes away time that we can spend on activities that add value back to the business and to learners on our learning platform." Indeed, he estimates that managing the security infrastructure takes one full-time equivalent (FTE) for his staff of four developers. "The time it requires to manage security tallies up quickly—particularly time on evenings and weekends," he adds.

It also requires specialized skills. "You really need to wear two hats and know what you are doing, because there are differences between managing a FortiGate in the cloud versus on a rack in the data center," Roscoe says. "As a group within a security company, we are fortunate to have technical expertise available to us; however, with FortiWeb WAF we don't need to rely on those resources and can be a lot more hands off, which allows us to focus on application development. "

Business Impact

- Projected one FTE will be reclaimed for development work, equating to a 25% productivity gain
- Hundreds of thousands of dollars in cost savings due to ability to use secure open-source code
- $2,400 cost savings via reduction in outbound data transfer and inclusion of CDN capabilities
- Upwards of $100,000 in annual cost savings by moving from WAF VM to WAF SaaS model

Solutions

- FortiGate VM
- FortiWeb VM
- FortiWeb Cloud WAF-as-a-Service

"FortiWeb Cloud WAF-as-a-Service helps get security out of the way of development. We are a web team, and we want to focus on building our web applications. This product allows us to do that."

– *Tristan Roscoe, Systems Development Manager, Global Training & Enablement, Fortinet*

WAF-as-a-Service Improves Efficiency and Business Agility

To minimize the amount of time spent managing the security solution, the systems development team decided to move to FortiWeb Cloud WAF-as-a-Service (WaaS). The platform provides the same multilayered and correlated approach as FortiWeb WAF appliances or VMs. It also protects web applications from threats, including the OWASP Top 10, and incorporates FortiGuard Labs threat-intelligence services for identifying both known and zero-day threats. At the same time, the cloud-native SaaS-based environment minimizes the amount of time Roscoe and his team spend managing the security hardware or software infrastructure.

"FortiWeb Cloud WAF-as-a-Service is a great solution for a small team like ours," Roscoe observes. "We are able to partially offload security responsibilities and focus on application development." Currently, the systems development team is still in the process of testing and rolling out the solution. "The starting point is to have traffic flow through FortiWeb Cloud WAF-as-a-Service to all our applications with block mode disabled," he continues. "We will monitor the logs while we perform regular tasks in all our applications in order to appropriately configure the SaaS WAF. We are very pleased with the initial results."

Reaping the Rewards of the SaaS-based WAF

Roscoe expects that his team will reclaim one full-time employee for development work—which equates to as much as a 25% improvement in productivity—once the transition to FortiWeb Cloud WaaS is complete. This is a huge win for smaller agile teams—equating to a significant productivity gain. Roscoe also expects it to reduce costs. Because they no longer have to provision VMs to run their security, it will significantly lower cloud compute and maintenance costs. "Moreover, we currently pay for Amazon CloudFront content delivery network (CDN) to route web traffic worldwide," Roscoe says. "These capabilities are included in the FortiWeb Cloud WAF-as-a-Service at no extra charge, which will lower our costs by as much as $2,400 annually."

In addition to the above, once FortiWeb Cloud WaaS is rolled out across all six of the applications Roscoe's team supports, the cost savings will multiply. "We currently spend around $20,000 annually per application using the WAF VM," he explains. "We'll save upwards of $100,000 annually with FortiWeb WAF-as-a-Service."

Leveraging the SaaS WAF will also make it easier to expand the team's solution set as needed. "This approach increases our ability to put new applications out there," Roscoe says. "FortiWeb Cloud WAF-as-a-Service helps get security out of the way of development so that security is not a blocker but rather an enabler of innovation. We are primarily a web development team, and we want to focus on building our web applications. This product enables us to do just that."

February 1, 2020 5:53 AM

570835-0-0-EN

D:\Fortinet\Case Study\Fortinet Web Applications\cs-dynamic-cloud-security-V2-212020-553AM