CASE STUDY

Fortinet Migrates Its Website to AWS, Protected by Its Own WAF-as-a-Service

Websites are the primary way that companies interact with their customers digitally, and global corporations typically have multiple web properties to support different business units, functions, and geographies. Fortinet is no exception, with a U.S.-focused primary website at www.fortinet.com, dozens of country-focused localized sites, and sites providing support, education, threat intelligence, and more.

Like many large and small organizations these days, Fortinet chooses to host its main website on a public cloud platform rather than on-premises. "Not only do we avoid the expense and hassle of building and maintaining the infrastructure ourselves, but we also make a more efficient use of resources because we pay according to our actual traffic—rather than having to have excess capacity on hand for occasional traffic spikes," explains Jayden Ye, a security engineer at Fortinet who manages security for Fortinet internet properties.

Bolstering Protection for the Main Website

Fortinet built the current infrastructure two years ago when the company migrated the main website to Adobe Experience Manager (AEM) running on Amazon Web Services (AWS). During the design process, the web team explored options for protecting the site with a web application firewall (WAF). Fortinet uses its own network and security solutions when possible, so the team considered three possibilities: two on-premises solutions—one as an appliance and one as a VM—and FortiWeb Cloud WAF-as-a-Service for AWS.

"Deployment literally took just a few minutes, compared with anywhere from a half day to two days when we were testing the on-premises form factors."

– *Jayden Ye, Security Engineer, Fortinet*

Details

Customer: Fortinet, Inc.

Industry: Technology

Location: Sunnyvale, California, USA

Solution

FortiWeb Cloud WAF-as-a-Service for AWS

The team did extensive testing with the on-premises options and FortiWeb Cloud. "We tested from several perspectives: performance, management, cost-effectiveness, and protection," Ye remembers. "In the end, the FortiWeb Cloud solution was the clear winner in all four areas."

FortiWeb Cloud WAF-as-a-Service for AWS is a full-featured WAF that uses the same comprehensive approach to security as other FortiWeb form factors, including the monitoring of IP reputations, protocol validation, and protection against distributed denial-of-service (DDoS) attacks and other application attack vectors. FortiWeb Cloud WAF-as-a-Service is deployed in the same AWS region as the application it protects—unlike other WAF form factors that make this difficult. The result is low latency, less expensive intraregion bandwidth rates, and simplified compliance.

Realizing Immediate Benefits

Ye and his colleagues benefited immediately from operational efficiencies enabled by the WAF-as-a-Service form factor. "Deployment literally took just a few minutes, compared with anywhere from a half day to two days when we were testing the on-premises form factors," Ye reports. "We also save around an hour per month of staff time previously spent dealing with integration issues with AWS. With the WAF in the same AWS region, everything is seamlessly integrated."

Another operational benefit is that no staff time is required for maintenance of the WAF infrastructure and hardware. "With other websites that we host on-premises, we had one system issue and two firmware upgrades that consumed more than 10 hours of staff time in a period of one year," Ye reports. "The WAF-as-a-Service form factor eliminates this hassle."

Efficient use of resources is another benefit of the WAF-as-a-Service model. "We still host some websites on-premises with an appliance form factor protecting them," Ye explains. "These sites have an average CPU and memory utilization rate of around 20% to 30%, to allow for spikes in traffic. The other 70% to 80% represents wasted capacity—and ultimately wasted funds. With WAF-as-a-Service, we pay for the capacity we use, and we do not have to spend time with capacity planning."

Deploying a WAF directly on AWS also brings a more streamlined approach to high availability—which makes for a much less expensive solution. "With a hardware WAF, an organization ideally needs three appliances—two to mirror at the main data center for high availability and a third at another site for disaster recovery," Ye relates. "Deploying the WAF-as-a-Service on AWS means that we pay for just one service and avoid the power and maintenance costs of managing one on-premises. Plus, we do not have to replace hardware when it reaches end of life. Not having to deal with hardware saves us significantly from a total-cost-of-ownership (TCO) perspective."

Fortinet's web team also benefits from rapid access to new features and functionality that are being added to FortiWeb. "We receive enhancements almost every week, and we do not have to do anything to take advantage of them," Ye says. "With the on-premises form factors, firmware upgrades come once every several months, and they must be installed—which involves scheduled or unscheduled downtime for the site."

On the subject of enhancements, Ye is impressed by the speed with which the Fortinet team has managed new feature requests—including a critical enhancement to the solution's support of content delivery networks (CDNs). "They turned that one out in a couple weeks," he recalls.

Finally, Ye and his colleagues are pleased with the flexibility of the cloud-based WAF in scaling for future growth. "We are looking to expand the AWS deployment to all our country-based sites in the near future, and we are looking at potentially migrating other web properties after that," Ye describes. "Since AWS has regions all over the world, we can deploy FortiWeb Cloud in every region where we have a web property—and realize the same benefits we are seeing with the main site. We will also see the same efficiency and performance improvements in the regions as we are seeing now at headquarters."

Business Impact

- Up to 15x reduction in deployment time—less than one hour compared with up to 15 hours with on-premises form factors
- 12 hours of staff time saved annually dealing with integration issues with AWS
- 10 hours of staff time saved annually in maintenance of WAF infrastructure and hardware
- Efficient use of capacity—paying for exact usage versus having 70% to 80% idle capacity on hand for traffic spikes
- High availability and disaster recovery provided seamlessly via SaaS versus the need to purchase three appliances for on-premises form factors
- Weekly enhancements with no installation required versus the need to install firmware upgrades once every several months
- Flexibility to expand globally using different AWS regions

"We receive enhancements almost every week, and we do not have to do anything to take advantage of them. With the on-premises form factors, firmware upgrades come once every several months, and they must be installed."

– *Jayden Ye, Security Engineer, Fortinet*

FORTINET

www.fortinet.com

September 11, 2019 6:26 PM

478485-0-0-EN

D:\Fortinet\Work\2019\September\091119\cs-fortinet-migrates-website-aws