SOLUTION BRIEF

Implement Scalable Security for Ecommerce Apps and Achieve PCI DSS Compliance with FortiWeb Cloud

Executive Summary

As ecommerce grows to become 11% of consumer transactions, securing ecommerce web applications is essential.[1] Additionally, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is a leading cybersecurity priority, as it is required in order to process payment card data. For many organizations, the most sustainable method of achieving both web application security and compliance with PCI DSS requirements to protect web applications against exploitation is deployment of a web application firewall (WAF).

FortiWeb Cloud enables organizations to achieve flexible, scalable, and affordable security for its web applications. Cloud-based protection means that security can be enabled, disabled, and scaled based upon business needs, decreasing total cost of ownership (TCO). Integrated machine learning (ML) decreases operational expenditures (OpEx) by automating rule tuning and decreasing false-positive detections, enabling security teams to focus on protecting the organization against ongoing threats.

43% of organizations deploy their WAF in Detect/ Alert Only mode.[3] Unless alerts are responded to immediately, this does not meet PCI DSS compliance requirements.

Introduction

Because websites handle so much sensitive and protected personal data, website security is essential to maintaining strong cybersecurity and regulatory compliance. Protecting a website against exploitation, ensuring that cardholder data is protected in accordance with regulations, and maintaining business continuity in the face of distributed denial-of-service (DDoS) attacks requires deploying security at every level of the web application deployment infrastructure.

It is not enough to focus security efforts on identifying and remediating vulnerabilities in code developed in-house, as web applications can also inherit vulnerabilities from third-party dependencies. For example, ecommerce websites are often built on top of content management systems (CMSs) such as WordPress or Joomla. These CMSs receive frequent updates that offer new capabilities; however, these same updates can also include vulnerabilities that could cause a breach of sensitive cardholder data.

Additionally, these platforms often offer plugins providing specific functionality, but that could also contain vulnerabilities. For example, WooCommerce, a WordPress ecommerce plugin, included a cross-site scripting (XSS) vulnerability reportedly that could allow injection of malicious code into a payment page.[2] Sites often use dozens of these plugins, each developed by a different third party.

FortiWeb Cloud is a comprehensive web application and application programming interface (API) security solution that identifies and blocks attempts to exploit these and other vulnerabilities. Suitable to organizations of all sizes, it provides a scalable, cloud-based option for achieving website and API security and regulatory compliance.

Achieving Compliance with PCI DSS

PCI DSS is a data protection regulation created by the major payment card brands to ensure that merchants and services providers are properly securing cardholder data. The regulation is divided into 12 main requirements, with a number of sub-requirements under each.

PCI DSS Requirement 6.6 aims to reduce threats to cardholder data by ensuring that merchants and service providers are correctly managing vulnerabilities in their web applications. It offers two options for compliance: application code reviews or deployment of a WAF.[4]

Complying with PCI Requirement 6.6 via code review means that an organization is committing to review every piece of code included in an application prior to release. As development teams transition to DevOps practices, this can be difficult or impossible, as code may be released on a daily, or even hourly, basis. Additionally, these reviews should include inspection of the web application's third-party and open-source dependencies; the average web application has over 1,000 dependencies.[5]

Deployment of a WAF such as FortiWeb Cloud, on the other hand, can not only meet compliance needs for PCI DSS Requirement 6.6 but also provide other benefits to an organization. FortiWeb Cloud protects an organization's web applications against a range of real-world threats, not only those listed in the OWASP Top 10 but also DDoS, and zero-day attacks.

Applications secured with FortiWeb also benefit from threat intelligence provided by FortiGuard Labs, enabling the identification and mitigation of the latest threats. This threat intelligence includes information regarding the latest web application vulnerabilities, bots, suspicious URL patterns, and data-type patterns. This elevates the organization from simply attaining PCI DSS compliance to maintaining sustainable security for their web infrastructure and customer payment card data.

FortiWeb Cloud Built-in Security Modules:

- Security Rules
- Client Security
- Access Rules
- Bot Mitigation
- DDoS Prevention
- Advanced Applications
- API Protection
- Account Takeover
- Application Delivery

Scalable, Flexible Deployment Model

Offered as a service on Amazon Web Services (AWS), Google Cloud, and Microsoft Azure, FortiWeb Cloud can be configured and activated within minutes. It reduces the time and effort associated with virtual machine (VM) management, software updates, and redundancy planning—enabling security teams to focus on more strategic threat protection. As a cloud-based WAF, FortiWeb Cloud eliminates the capital expenditures associated with the acquisition and deployment of a physical appliance.

FortiWeb Cloud also offers all the elasticity and cost-effective deployment options organizations expect from cloud services. FortiWeb provides the same level of protection to a single web application handling terabytes of data as it does to multiple smaller applications with much smaller data volumes. Because FortiWeb has built-in support for multitenancy and single-pane-of-glass visibility, the security team can manage applications centrally from a single console. Or, they can assign visibility and control privileges for individual applications to the application owners.

FortiWeb Cloud services can be easily scaled up and down to meet the current security needs of an organization's web applications. If, for example, an ecommerce site launches a limited-time promotion, the WAF can scale to handle the increased traffic volume associated with that promotion and rapidly return to normal after the promotion is complete.

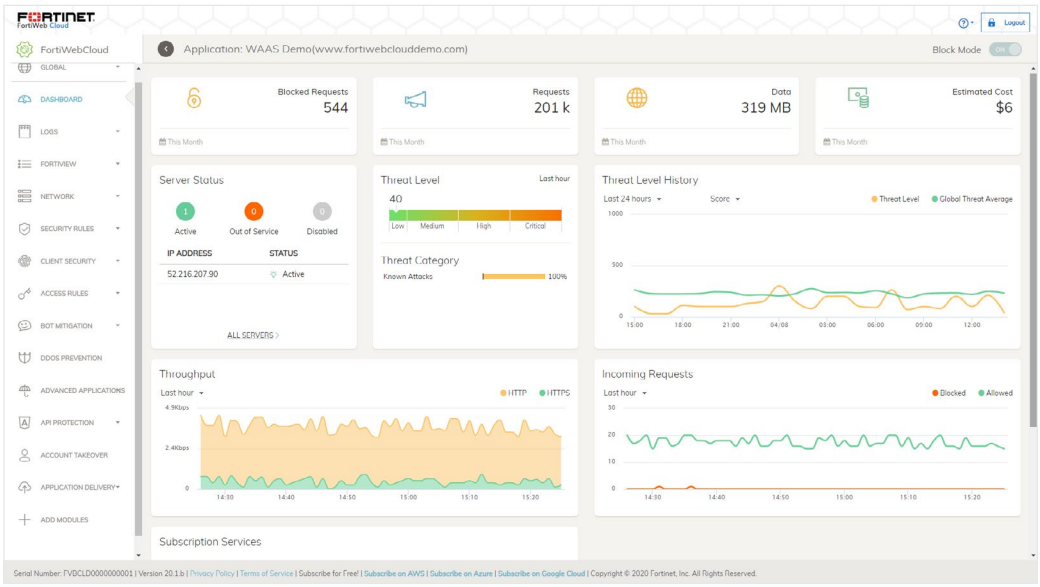

Figure 1: Management pane for FortiWeb Cloud.

Machine Learning Simplifies WAF Management

WAFs use rules to identify whether a user request to a web application is benign or malicious. The rules are based on the structure of the application and how users typically interact with it.

When a WAF-protected web application changes, the WAF rules must be updated as well. This "rule tuning" ensures that legitimate requests pertaining to the new functionality are not flagged as malicious and blocked by the WAF. Rule tuning after each code update creates a significant burden on development teams as they transition to DevOps practices and update code on a daily basis, or even more frequently.

To reduce this burden, FortiWeb Cloud offers ML-based anomaly detection, which can detect and block malicious content without requiring explicit rules. The ML process in FortiWeb Cloud consists of multiple stages. In the first stage, known threats, such as those matching IP blacklists or known malware signatures, are identified and blocked. Then, anomaly detection is applied to differentiate known benign traffic from anomalies. Finally, in-depth analysis is applied to anomalous requests to determine whether or not they include malicious content.

In addition to enabling automated rule updates, this process dramatically reduces false positives since detected anomalies are subjected to in-depth analysis in a sandboxed environment. This enables security teams to focus their time and effort on investigating and responding to true threats rather than manually triaging and removing false-positive alerts.

Two-thirds of organizations spend over 40 hours per week responding to WAF alerts.[6] FortiWeb Cloud uses ML to provide nearly zero false positives, decreasing security team workload.

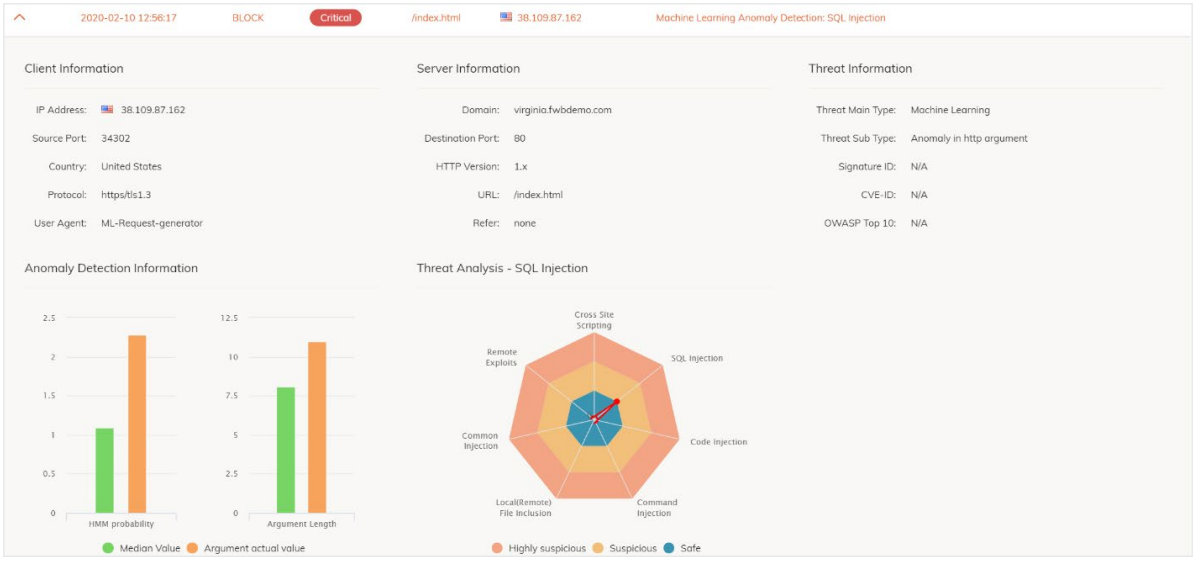

Figure 2: Example of an attack detected using machine learning.

Conclusion

PCI DSS compliance is essential for organizations processing payment card data, and the velocity of code changes accelerates as development teams adopt DevOps practices. FortiWeb provides a flexible, affordable, and scalable option for protecting web applications that enables security architects to both meet PCI DSS compliance requirements and protect their web presence against real-world threats.

[1] "Quarterly Retail E-Commerce Sales 4th Quarter 2019," U.S. Department of Commerce, February 19, 2020.

[2] Zhouyuan Yang, "WordPress WooCommerce XSS Vulnerability – Hijacking a Customer Account with a Crafted Image," Fortinet, March 4, 2019.

[3] "The State of Web Application Firewalls," Ponemon Institute, May 2019.

[4] "Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified," PCI Security Standards Council, April 15, 2008.

[5] Rui Ribeiro, "Enterprise Web Security: Risky Business," Dark Reading, November 5, 2019.

[6] "The State of Web Application Firewalls," Ponemon Institute, May 2019.

April 17, 2020 11:21 PM

622731-0-0-EN

D:\Fortinet\Solution Briefs\blue solution briefs\FortiWeb for PCI Compliance\sb-implement-scalable-security-for-ecommerce-apps-V1-4172020-1119AM