SOLUTION BRIEF

FortiWeb and Qualys

Web Application Vulnerability Scanning and Virtual Patching

Virtual patching is a great method to protect applications until they can be permanently fixed by developers. Qualys and Fortinet offer an integrated solution that scans applications for vulnerabilities with Qualys Web Application Scanning (WAS) and protects them with Virtual Patching on the FortiWeb Web Application Firewall (WAF). Once a vulnerability is discovered, it's protected by FortiWeb instead of issuing disruptive emergency patches or worse, waiting weeks or even months for the developers to deploy a new release while the application sits unprotected.

FortiWeb's virtual patching uses a combination of sophisticated tools such as URLs, parameters, signatures, HTTP methods, and others to create a granular rule that addresses each specific vulnerability discovered by Qualys WAS. With this multi-faceted approach to rule creation, FortiWeb minimizes the possibility that a scanner-based rule will trigger false positives and won't impact overall WAF performance.

Virtual Patching won't take the place of the traditional application development process, however it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application code, such as with legacy, inherited, and thirdparty applications, FortiWeb's virtual patching can provide a permanent security solution for vulnerabilities.

Solution Benefits

Using FortiWeb with Qualys WAS gives organizations:

- Fewer disruptions due to emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed
- Reduced risk of exposure to threats between the time a threat is discovered until it is fixed by developers
- Protection for legacy, inherited, and third-party applications where development fixes aren't an option or are impractical
- More stability in application security patches as developers have more time to properly fix code vs. issuing emergency patches that haven't had time to be fully tested
- Minimized false detections based on accurate and verified web application firewall alerts by Qualys WAS
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by Qualys WAS
- Additional flexibility and granular management of FortiWeb's Web Application Firewall policies based on scanning results
- An enhanced solution that exceeds PCI DSS 6.6 compliance standards

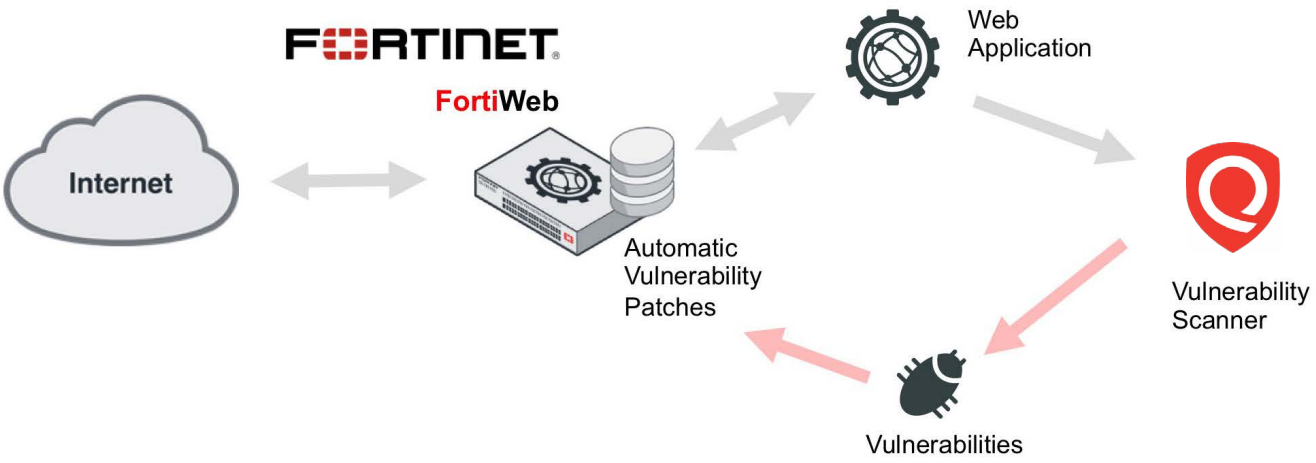

Figure 1: Qualys was scan results are imported into FortiWeb; then FortiWeb Virtual Patching automatically creates new rules to protect against newly discovered vulnerabilities.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses.

Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Learn more at www.qualys.com.

June 20, 2019 1:06 AM

D:\Fortinet\Solution Brief\FA\GREY Solution Briefs\FA - SB - Fortinet Qualys\FA - SB - Fortinet Qualys

429123-A-0-EN