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 third-party applications, FortiWeb’s virtual patching can provide a permanent security solution for 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 without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. More than 280,000 customers worldwide trust Fortinet to protect their businesses. Learn more at www.fortinet.com.
Qualys Web Application Scanning (WAS) is a cloud service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection. The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to secure a large number of websites. It proactively scans websites for malware infections, sending alerts to website owners to help prevent black-listing and brand reputation damage. Built on the world’s leading cloud security and compliance platform, Qualys WAS frees you from the substantial cost, resource, and deployment issues associated with traditional software products. Known for its fast deployment, ease of use, and unparalleled scalability (scan thousands of web applications), Qualys WAS is relied upon by leading companies around the world.

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.