



FortiWeb and WhiteHat Sentinel

Web Application Vulnerability Assessment and Virtual Patching

Virtual patching is a great method to protect applications until they can be permanently fixed by developers. WhiteHat and Fortinet now offer an integrated solution that scans applications for vulnerabilities with WhiteHat Sentinel and then protects them with FortiWeb's Virtual Patching. 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 WhiteHat Sentinel. 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.

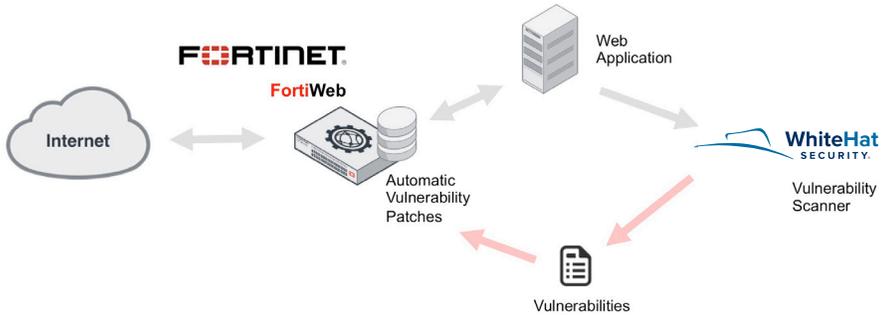
Virtual Patching won't take the place of the application remediation process, however it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application code,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

Using WhiteHat Sentinel to uncover application vulnerabilities provides industry-leading accuracy and false positive avoidance in web application threat assessments. FortiWeb complements Sentinel with granular application protection rules that take the imported vulnerability results and provide immediate mitigation with the same level of accuracy. This granular virtual patching is able to maintain application security until the development teams are able to fully deploy permanent fixes in the application code. It can also extend the windows between security patches to minimize disruptions to the organization and its users.

About Fortinet

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments - be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at <http://www.fortinet.com>, the Fortinet Blog or FortiGuard Labs.





WhiteHat Sentinel scan results are imported into FortiWeb then FortiWeb Virtual Patching automatically creates new rules to protect against newly discovered vulnerabilities.

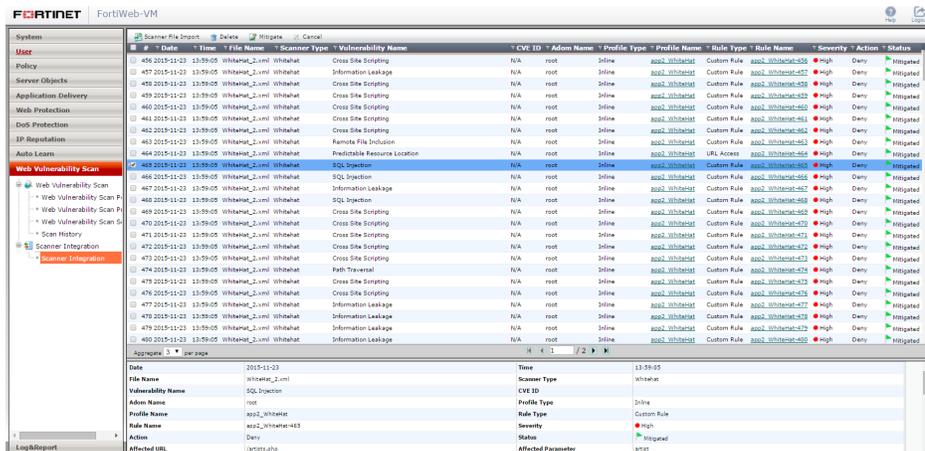
Benefits

Using FortiWeb with WhiteHat Sentinel gives organizations:

- Less 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 WhiteHat Sentinel.
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by WhiteHat Sentinel.
- 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.

About WhiteHat Security

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites – including sites in highly regulated industries, such as top e-commerce, financial services, and healthcare companies. For more information on WhiteHat Security, please visit www.whitehatsec.com.



FortiWeb's deep integration with WhiteHat Sentinel gives you increased user and traffic visibility and provides protection from web application threats.



GLOBAL HEADQUARTERS
 Fortinet Inc.
 899 Kifer Road
 Sunnyvale, CA 94086
 United States
 Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
 905 rue Albert Einstein
 Valbonne
 06560, Alpes-Maritimes,
 France
 Tel: +33.4.8987.0500

APAC SALES OFFICE
 300 Beach Road 20-01
 The Concourse
 Singapore 199555
 Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
 Paseo de la Reforma 412 piso 18
 Col. Juarez
 C.P. 06600
 México D.F.
 Tel: 011-52-(55) 5524-8428