

SOLUTION BRIEF

FortiWeb and IBM Security AppScan

Web Application Vulnerability Scanning and Virtual Patching

Virtual patching is an excellent method to protect applications until their vulnerabilities can be permanently fixed by developers. IBM and Fortinet now offer an integrated solution that scans applications for vulnerabilities with IBM Security AppScan and then protects them with FortiWeb's virtual patching. Once a vulnerability is discovered, it is 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 IBM Security AppScan. With this multifaceted approach to rule creation, FortiWeb minimizes the possibility that a scanner-based rule will trigger false positives and won't impact overall web application firewall (WAF) performance.

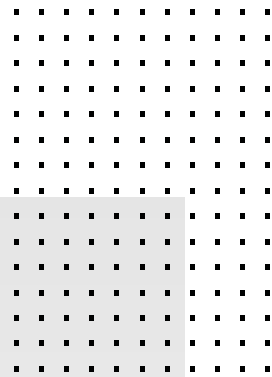
Virtual patching won't take the place of the traditional application development process; however, it can create a secure bridge between the time a vulnerability is discovered and the time a software release is issued to address it. In cases where it may not be possible or practical to change the application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

Solution Description

Comprehensive Web Application Security With FortiWeb

Using an advanced multilayered and correlated approach, FortiWeb provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats. At the heart of FortiWeb is an artificial intelligence (AI)-based detection engine that uses machine learning to identify requests that stray from normal patterns and takes action to protect applications from known and unknown.

Using IBM Security AppScan to uncover application vulnerabilities provides industry-recognized accuracy and false-positive avoidance in web application threat assessments. FortiWeb complements IBM Security AppScan 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.



Joint Solution Components

- Fortinet FortiWeb
- IBM Security AppScan

Joint Solution Benefits

Using FortiWeb with IBM Security AppScan 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 IBM Security AppScan
- More accurate FortiWeb reporting and identification of attempts to exploit vulnerabilities discovered by IBM Security AppScan
- 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



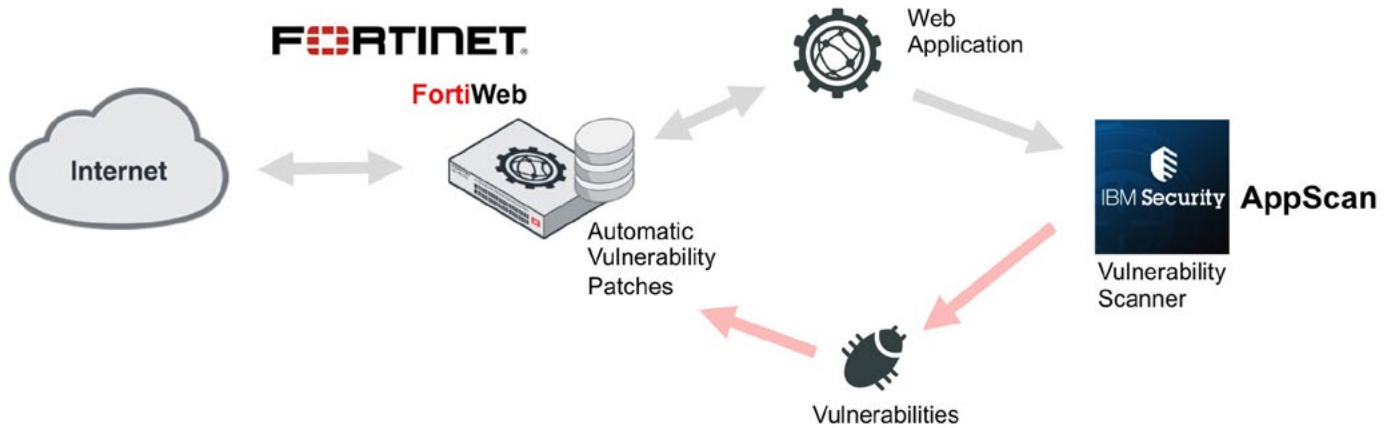


Figure 1: IBM Security AppScan scan results are imported into FortiWeb; then FortiWeb virtual patching automatically creates new rules to protect against newly discovered vulnerabilities.

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 IBM Security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research and development organization and delivery organization. For more information on IBM security, please visit: www.ibm.com/security.



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.