WhiteHat Sentinel and F5 ASM

Integrated Web Application Firewall Solution

Websites are today's target of choice, one that attackers are exploiting for immense financial gain. They are the gateway to a wealth of corporate information and yet, nine out of ten websites have at least one serious vulnerability that can put that data at risk. Add the dynamic nature of the Web, custom code and the multiple stakeholders involved in website management, and the complex nature of website security becomes readily apparent.

WhiteHat Sentinel brings website security under control by finding and fixing vulnerabilities before hackers do, enabling corporate security and development teams to focus on remediation and attack prevention. For any company conducting business on the Web, WhiteHat Sentinel is the ideal solution to ensure the security of customer and corporate data, maintain regulatory compliance, and safeguard brand integrity.

What is WhiteHat Sentinel

WhiteHat Sentinel is the only website vulnerability management solution that enables organizations to address all website vulnerability issues with accuracy and confidence. A Web-based subscription service, WhiteHat Sentinel combines advanced proprietary scanning technology with expert analysis, allowing customers to identify, prioritize, manage and remediate website vulnerabilities as they occur. This comprehensive approach gives all parties a clear view into the organization's website security posture in an easy-to-manage, cost-effective manner.

Closed-Looped System

Integration between Web application scanners and a Web application firewall (WAF) has been attempted before without success. The primary reason for its failure was due to the number of scanner false positives that would overwhelm WAFs. No fully automated tool is capable of the level of accuracy to safely create WAF rules. These implementations not only slowed down a WAF's performance, but also blocked other business critical traffic from accessing a website. The fix was too broad and couldn't distinguish good traffic from bad, rendering it ineffective and potentially dangerous.

Now WhiteHat Sentinel can directly configure policies on a WAF to protect against vulnerability exploits (e.g., cross-site scripting, SQL injection) that were found during the scanning process. This makes the process simpler for the end user — find the problem, then fix the problem with the click of a button. This integration makes "virtual patching" a reality.

F5's open iControl® API provides the integration between WhiteHat Sentinel's industry-leading website vulnerability management service and F5 BIG-IP® ASM's (Application Security Manager™) award-winning WAF.

The integrated solution brings the entire industry to a new level of website protection—with extreme accuracy and efficiency. Customers have been waiting for a solution that delivers on the promise of rapid identification and immediate mitigation of vulnerabilities. The WhiteHat /F5 alliance makes complete website security simpler than ever for security professionals and developers.

Total Website Security ::

The linkage between WhiteHat Sentinel and BIG-IP ASM completes the loop from vulnerability checking and detection to remediation of specific vulnerabilities using the BIG-IP ASM remediation process. The end result is total website security:

- *Increased protection via the rapid identification of website vulnerabilities, with minimal false positives*
- *Highly targeted vulnerability remediation (virtual patching)*
- *Simplified management:*
  - *WhiteHat filters and validates the data to provide only actionable results*
  - *WhiteHat continually updates and refines its vulnerability information to stay on top of the latest attack vectors*

A critical component of the Sentinel Service is to require WhiteHat Security Operations Team to verify the accuracy of every identified vulnerability, creating a highly precise vulnerability database for specific website's. As a result, the

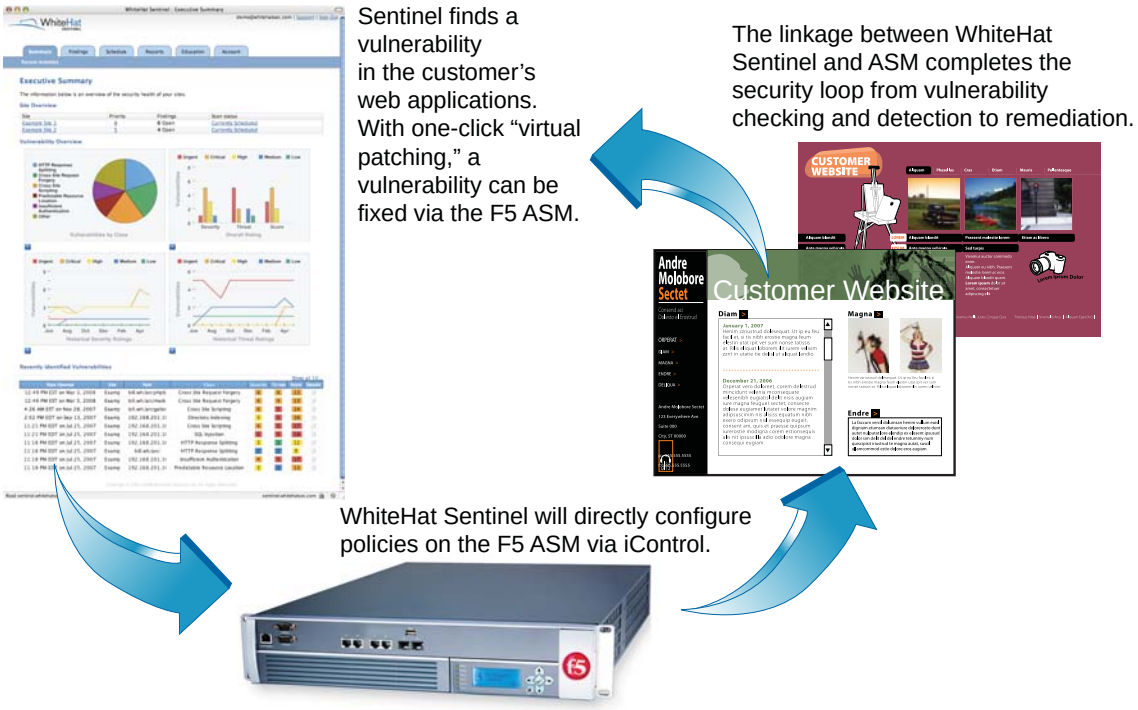
WAF rules generated are "laser focused," and as such, enable companies to use their WAFs in block mode without the fear of blocking good traffic. (Currently, companies rarely use their WAFs in block mode for this very reason.)

Through the F5 iControl API, WhiteHat Sentinel will be able to directly configure policies on the BIG-IP ASM product to protect against vulnerability exploits (e.g., Cross-site Scripting, SQL Injection) found during the scanning process.

Customers can apply a "virtual patch" to their site immediately, mitigating the current risk and then addressing the root issues as time and budgets allow.

PCI Compliance

Satisfy the requirements of PCI DSS Section 6.6 with an F5 ASM / WhiteHat Sentinel integration. This solution exceeds the recommendations of Section 6.6 by providing application scanning and code review by an application security specialist (WhiteHat) and installing a WAF in front of Web-facing applications.



F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
(206) 272-5555 Voice
(888) 88BIGIP Toll-free
(206) 272-5556 Fax
www.f5.com/info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Voice
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932 582 000 Voice
+44 (0) 1932 582 001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Voice
+81-3-5114-3201 Fax
info@f5networks.co.jp