

WhiteHat Sentinel Satellite Appliance – Datasheet

Web Application-Layer Assessments Behind the Firewall

WhiteHat Security has introduced the Sentinel Satellite Appliance to address the Web application vulnerabilities found on internal websites, applying the benefits of the WhiteHat Sentinel Service for public-facing Web applications, and delivering them behind the firewall. The Satellite Appliance complements the Sentinel Service to deliver a complete vulnerability management solution across the entire lifecycle of internal and external Web applications.

The Satellite Appliance enables the Sentinel Service to securely assess internal websites using the same rigorous and iterative methodology of scanning, verification and custom testing that WhiteHat Sentinel uses for public-facing Web applications – same methodology, same approach – consistently reporting internal findings alongside external vulnerabilities in the Sentinel Web interface.

Cost Effective, Customer Controlled

The purpose-built Sentinel Satellite Appliance is delivered as an easily accessible rack-mountable server, that strategically resides behind the firewall, typically inside a customer demilitarized zone (DMZ).

With the Satellite Appliance deployed inside the network, the Sentinel Service can be delivered through a secure, encrypted tunnel between the customer-designated internal servers and the WhiteHat Security Operations Center.

The Satellite Appliance is a one-time cost that protects the internal network through many years of Sentinel Service subscription renewals.

Minimal Installation Requirements

The pre-configured Sentinel Satellite Appliance installs in a network in minutes, smoothly integrating inside even the most dynamic internal environments. Successful installation of the Satellite Appliance requires the following basic conditions:

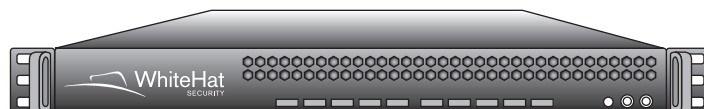
- 1U of rack space
- A 120V/20A power connection
- The Satellite Appliance must be able to connect to the Satellite Controller through the Internet and must be connected to a network that can access the designated internal Web servers
- The Satellite Appliance must be able to obtain a network address via DHCP

Features

- 1U form factor for easy rack mounting
- Pre-configured to work out of the box as a plug-and-play device
- Flexible deployment in the network
- Encryption ensures that the Satellite communicates only with WhiteHat Operations. No inbound connections are ever made to the Satellite
- IP address rewriting prevents network service conflicts
- Flexible configuration to survive network updates

Benefits

- Quickly discover vulnerabilities earlier in the SDLC by assessing staging and QA platforms prior to production deployment of new code
- Thoroughly assess intranet Web applications for weaknesses that could compromise sensitive data if exploited
- Look for flaws in the design and architecture of internal Web applications, and recommend remediations against internal threats



Assuring Secure Assessments

With the Sentinel Satellite Appliance, the need for administrators to open inbound ports in a firewall to connect to the WhiteHat Security Operations Center is eliminated.

All Satellite Appliances connect outbound to a Controller in the WhiteHat Security Operations Center. Each Controller can manage as many as 8,000 Satellite Appliances. The Controller configures each Satellite Appliance on connection, and then acts as a router between the Satellite Appliance and the WhiteHat Sentinel Service.

All communications between the Controller and the Satellite Appliance occur on an encrypted SSH channel. No sensitive vulnerability data is stored on the Satellite Appliance.

- **Secure Connection:** *Once deployed and powered on, the Satellite Appliance configures its network card via DHCP and seeks an SSH connection to the Controller. The Controller's host key is verified, and then the Satellite Appliance provides its tunnel key.*
- **Authentication:** *The Controller looks up the Satellite Appliance's authentication credentials and designates the servers to assess. The Controller assigns virtual IP addresses to the servers, allowing the Satellite Appliance to connect to those addresses as if they were the servers themselves. Extensive IP address rewriting assures that addresses on networks managed by the Satellite Appliance cannot come into conflict.*
- **Association:** *The Controller listens for connections from Satellite Appliance, associates the received tunnel key with a specific Satellite Appliance, and starts the Satellite Appliance server application with the Satellite Appliance name. This application*

determines the servers managed by its Satellite Appliance, then begins the negotiation phase of the connection.

- **Negotiation:** *The Controller communicates to the Satellite Appliance which servers should be assessed. Once both sides acknowledge the negotiation, they each bring up routes in preparation for the transmission phase.*
- **Transmission:** *The transmission phase simply transports packets from one side of the link to the other, rewriting the addresses on each. Transmission persists until one side of the connection terminates, at which point the process starts again.*

The Controller also provides DNS, enabling the WhiteHat Sentinel Service to use hostnames to access virtual IP addresses for name-based virtual hosting.

Multiple Deployment Options

The Sentinel Satellite Appliance supports deployment in a number of security postures. See the Deployment Guidelines for WhiteHat's best-practice recommendations for deployment in a QA Environment.

Comprehensive Support Services

Support for the Sentinel Satellite Appliance is available from the WhiteHat Security Operations Center. Support needs, including hardware replacement, may be met by e-mail or telephone.

About WhiteHat Security, Inc.

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of website vulnerability management services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company's flagship service, is the only solution that incorporates expert analysis and industry-leading technology to provide unparalleled coverage to protect critical data from attacks. For more information about WhiteHat Security, please visit www.whitehatsec.com.



WhiteHat Security, Inc. | 3003 Bunker Hill Lane, Suite 220 | Santa Clara, CA 95054 | 408.343.8300 | www.whitehatsec.com

Copyright © 2008 WhiteHat Security, Inc. | Product names or brands used in this publication are for identification purposes only and may be trademarks or brands of their respective companies.

12.13.07