WhiteHat Sentinel Dynamic & Imperva SecureSphere Integration

Integrated Application Security

There is not always enough time or resources to patch a web application at the time a new vulnerability is found, and assessing large numbers of applications on websites can be overwhelming when hundreds of vulnerabilities are discovered. Additionally, in some cases it may not be practical to remediate every finding due to issues with legacy code, third-party integrations, or other inherited limitations.

Virtual patching is one way to address these vulnerabilities, mitigating the risk until the developers can patch or re-design to prevent exploitation. The integration of WhiteHat Security's Sentinel Dynamic™ continuous scanning and risk assessment combined seamlessly with Imperva's SecureSphere™ web application firewall (WAF) addresses this gap in remediation. With virtual patching, organizations can design and implement code fixes on their own schedule, eliminating the need for emergency outages to fix and protect.

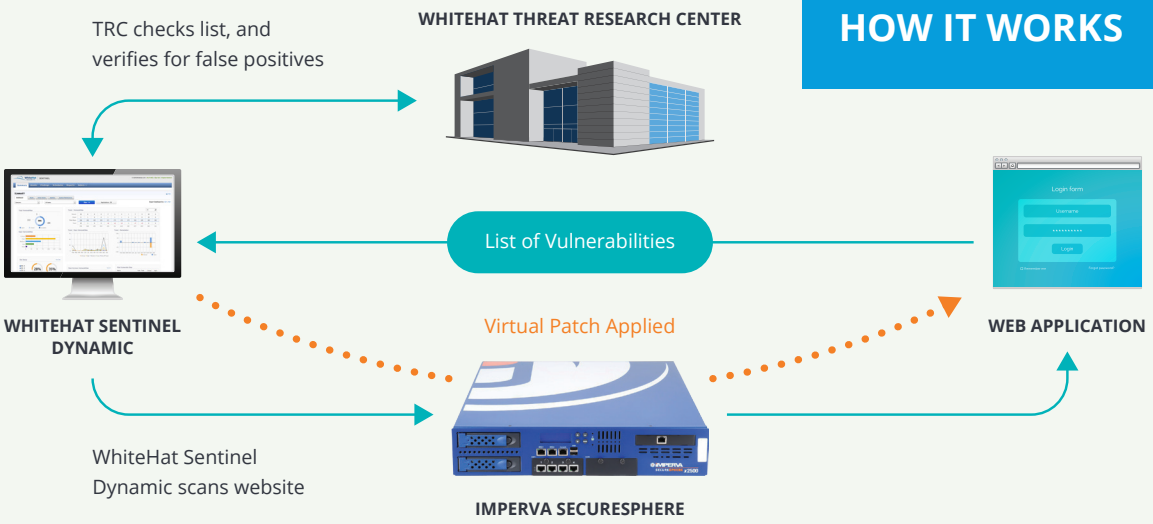
WhiteHat Sentinel assesses web applications for vulnerabilities using the most accurate vulnerability assessment analysis available – verifying all results to virtually eliminate false positives. Working with SecureSphere's proven ability to block attempts to exploit vulnerabilities in production, your organization is protected from malicious application-layer attacks.

Virtual patching cannot replace application remediation, but it can help your organization provide immediate mitigation and keep you more secure.

KEY BENEFITS

- Simplified management via web interface
- Real-time vulnerability mitigation and blocking via automated behavior modeling
- Scalable to fit any number of websites and scanning frequency
- Transparent deployment and ultra-high performance
- Protection for legacy and third-party web applications where development will be slow to implement change
- Centralized management and compliance reporting

HOW IT WORKS



1. WhiteHat Sentinel scans the application, finds a list of potential vulnerabilities, and sends the list to the Threat Research Center (TRC)
2. The TRC security experts verify the list, and return it to Sentinel, which pushes unique vulnerabilities to SecureSphere
3. SecureSphere creates a virtual patch for the application, blocking any exploitation of the vulnerability
4. Sentinel re-tests the vulnerability to ensure that remediation is in place, completing the security loop

SecureSphere Controls

SecureSphere patented Dynamic profiling technology, and automatically builds a model of legitimate behavior and maps to application changes over time.

- Accurate protection against web application attacks
- Reputation-based security to stop automated threats
- Pre-defined and custom correlation rules block multi-stage attacks
- Transparent deployment and high performance
- Centralized management and reporting

Looking Forward

Application security is a process best addressed throughout the software development lifecycle. It's important to develop a comprehensive remediation process that addresses risk analysis, long-term code remediation, and the education to understand best practices in securing web and mobile applications alike. A virtual patch is well suited to address a particular threat vector, however the highest long-term benefits involve fixing the vulnerable code, and should remain a strategy for developers and management alike.

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 15 years. Combining technology with the expertise of our TRC team, we deliver solutions to our customers that reduce their risk, lower their costs, and decrease the time it takes for them to develop and deploy secure applications and websites.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com