WhiteHat Sentinel Dynamic and Web Application Firewalls

The WhiteHat Sentinel Dynamic and Web Application Firewall (WAF) integration provides users with a highly integrated and secure solution for identifying and mitigating web application vulnerabilities in a manner that is fast, safe and cost effective.

WhiteHat Security Sentinel Dynamic

WhiteHat Security Sentinel Dynamic is a software-as-a-service platform that combines automated web application assessments via the Sentinel scanner with the manual verification of our Threat Research Center (TRC) providing near zero false positives. Our scans are production safe and run continuously so web applications remain safe regardless of how frequently changes are being made. Once the Sentinel scan is complete, our team of experts provides ongoing verification of all vulnerabilities identified by the Sentinel scanner. Sentinel Dynamic streamlines the remediation process for unparalleled efficiency and vulnerability coverage.

Fixing Vulnerabilities Takes Time

The remediation of vulnerabilities is not an easy process. Often times, it takes days, weeks or even months before the vulnerability gets remediated. In many cases, the vulnerability may not be remediated at all if the security team does not have the capacity or if it is not practical to change the application code, particularly with legacy, inherited and third-party applications. So what happens to an organization that is left vulnerable to attack for long periods of time? What options do they have to ensure that their data is secure until the teams have the resources to remediate the identified vulnerabilities properly or until new software is released?

In all too frequent situations like these, Web Application Firewalls (WAFs) are the ideal solution to protect applications until developers can remediate or until new software is released.

Sentinel Dynamic and WAF Integration

Web Application Firewalls (WAFs) set security policies that instantly block attempts to exploit vulnerabilities in production environments. Emergency patches can be disruptive to developers and the rush to fix can limit a developers ability to properly test fixes before implementation. Alternatively, waiting for deployment of new releases leave the applications unprotected and vulnerable to exploitation. WAFs protect vulnerabilities as they are discovered, allowing developers to prioritize their remediation efforts and to design and implement code fixes based on their schedule. Once a member of the WhiteHat Security TRC verifies a vulnerability, the customer or their WhiteHat Partner can implement the appropriate WAF configuration changes. Additionally, several WAF vendors leverage WhiteHat's API's to automate a majority of the virtual patching process.

While this won't take the place of the application remediation process, it does provide a temporary solution to ensure security between the time a vulnerability is discovered via Sentinel Dynamic and manual verification, to the time new software is released or until proper fixes can be tested and implemented.

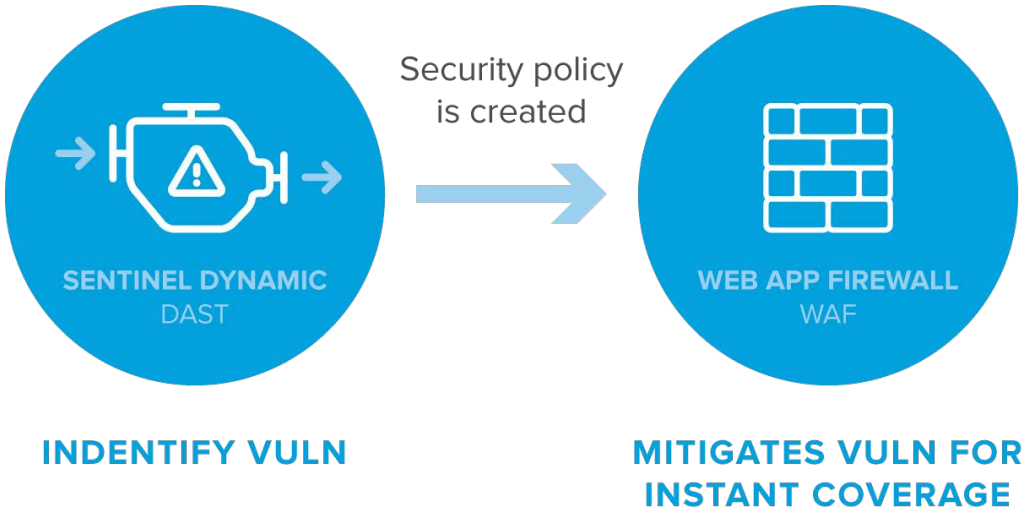
Benefits

Identify Vulnerabilities with Sentinel Dynamic

- Near zero false positives with manual verification of all vulnerabilities by the Threat Research Center
- 24/7 direct access to the engineer who identified the vulnerability
- Cloud based platform with no hardware or scanning software to install
- Unlimited, continuous and concurrent assessments for an always-on risk assessment
- Automatic detection and assessment of code changes to web applications
- Scalable to fit any environment and assess thousands of websites simultaneously
- Integrates into existing infrastructure with little to no disruption
- Exceeds the requirements for the application security of PCI DSS 3.1

Mitigate Your Risk with Dynamic WAF Integration

- Accurate and verified WAF alerts by WhiteHat Sentinel
- Lower cost and less disruption to production with emergency fixes
- Reduce risk of exposure to threats from the time a vulnerability is identified until it is fixed by developers
- Achieve protection for legacy, inherited and third-party applications where remediation is not an option or is impractical
- Gain assurance that remediation efforts are fully vetted rather than issuing emergency patches that haven't been thoroughly tested



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.

WhiteHat SECURITY

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com