

# Simple Identification And Remediation: F5 and WhiteHat Integrate Web Application Assessment and Defense Technologies

## Abstract

On March 10, 2008, F5, a leader in application delivery, and WhiteHat Security, an innovator in application security assessment, announced they would be partnering to create an integrated Web application assessment and firewall technology. This product integration will incorporate WhiteHat's Sentinel assessment technology and F5's ASM attack blocking technology into a single solution. The partnership will allow customers to conduct both assessment and remediation of Web application vulnerabilities through a single management interface. This capability is in high demand as most enterprises are in dire need of not only accurate security assessments of their applications, but of more simple methodologies for remediating vulnerability findings.

## Background

Web application security has moved to the forefront of many organizations' security strategies. Not only are Web applications a serious gateway for incidents that result in heavy costs to organizations, they are also the targets of new compliance standards. The Payment Card Industry Data Security Standard (PCI DSS) in particular is one of the most prescriptive security compliance measures that call for specific measures in Web application security. Unfortunately, PCI DSS requirements are flawed. PCI DSS gives organizations the option of determining the best way to ensure application security through automated assessment or through the implementation of a Web application firewall. This is not an apples-to-apples comparison between technologies. In fact, the two technologies are more complementary than the either-or choice the PCI standard would suggest.

---

*Unfortunately, attempts at combining the strengths of Web application assessment and Web application firewall technologies have previously been marred by major weaknesses in assessment engines.*

---

Web application firewalls can put a measure of defense directly in-line in a readily deployable form factor—but without an assessment technology, they may not be intelligent enough to remediate specific application risks as fully as possible. Conversely, Web assessment technologies can be more accurate in identifying risks, but proper solutions typically require a great deal of resource delegation and time to implement, which can introduce significant costs as well as delays in remediation exposures. Adoption of either of these two technologies individually will leave a gap in the security posture of an organization and most likely create cost inefficiencies in strategies trying to fill those gaps.

It is for these reasons that the integration of Web application firewalls and automated Web application assessment is so logical. Unfortunately, attempts at combining the strengths of Web application assessment and Web application firewall technologies have previously been marred by major weaknesses in assessment engines. False positives in particular have caused a great deal of headaches in these attempts at integration. These false positives fool integrated firewall technologies into believing serious flaws exist where they do not. This “miseducation” often blocks necessary application functionality that may be critical to the business.

Therefore, all the assessment findings must be verified before being implemented into a Web application firewall blocking methodology. Of course, this negates the cost efficiencies of integrating the two technologies in the first place.

---

*F5 has long driven towards the goal of enhancing application firewall intelligence through efforts such as the recent release of their iControl API and the creation of community Web application firewall rules for standard applications such as Microsoft's Outlook Web Access (OWA).*

---

## Event

It is for these reasons that F5 and WhiteHat Security have partnered to create an effective integrated Web application firewall and assessment solution. Integrating assessment intelligence with Web application firewall technologies is important to creating effective security for dynamic Web applications whose vulnerabilities are often as complex as the functionality of the application itself. F5 has long driven towards the goal of enhancing application firewall intelligence through efforts such as the recent release of their iControl API and the creation of community Web application firewall rules for standard applications such as Microsoft's Outlook Web Access (OWA). Partnering with WhiteHat introduces an approach to assessment integration very different from other formidable market competitors. WhiteHat manually verifies automated application vulnerability assessment findings to gain a deeper understanding of some of the issues noted by the assessment and determine some of the vulnerabilities the automated assessment may have missed.

This distinctive competitive differentiator allows WhiteHat to produce far less false positives than any other application security assessment vendor. This is particularly important in automated vulnerability remediation as it ensures the availability of protected Web applications and all of their functions. This stands in stark contrast to other attempts among application security vendors to integrate automated remediation with application firewalls. In these previous efforts, the application assessment engine did not utilize vulnerability scans that were nearly as accurate as those produced by WhiteHat, often resulting in application downtime when critical aspects of protected Web applications were disrupted.

## Key Ramifications

The partnership between F5 and WhiteHat Security to deliver integrated Web application assessment and vulnerability remediation drastically simplifies a previously difficult manual task. Even organizations having mature application security strategies have found it difficult to create efficiency in their risk mitigation process. This is primarily due to the fact that firewall technologies are only as good as their understanding of the dynamic applications that they protect. By integrating the two technologies, customers are now capable of simply clicking a button to effectively educate their firewalls in order to remediate difficult security issues that may have previously taken months to mitigate.

This is a key development in the realm of application security. It introduces an integrated solution that creates accuracy and efficiency across two functions where gaps have slowed the adoption of Web application security solutions for a long period of time. The integrated F5 ASM and WhiteHat Sentinel solution could remove these roadblocks and allow organizations to enhance their security posture immediately upon implementation of the solution. This is in stark contrast to the many months that previously went into configuring firewalls and tweaking remediation strategies.

## EMA's Perspective

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts have long held the view that application security strategies must be comprehensive to be effective. While compliance standards such as PCI DSS may have misunderstood the necessity of integrating both vulnerability assessment and attack blocking technologies, F5 and WhiteHat did not. The integration of these two solutions is without a doubt one of the most powerful singular approaches to Web application security.

EMA believes that adopting the F5-WhiteHat solution will allow organizations to identify and mitigate the security risks their applications face in a much faster, more effective manner. However, the utilization of a Web application firewall is of course no substitute for the practice of secure coding. When security risks appear, Web application firewalls

should be used as an immediate remediation technique, but not as a replacement for deploying securely coded applications. The organization committing to Web application deployment must also commit to assuring that applications are securely developed and maintained—or face the ever-increasing risk of exploit to applications that may be critical to the business. An integrated Web application firewall and vulnerability assessment methodology complements such a strategy, but does not—nor can it—replace it.

Regardless, the working integration of a Web application firewall and security assessment is an important application security enabler, and the challenge raised by the partnership of F5 and WhiteHat makes it likely that other application security vendors will attempt to follow suit to create a more intelligent attack blocking solution. However, without WhiteHat Security's distinctive model that also includes manual testing in their standard offerings as a method for the removal of false positives, competitors will be challenged to create equally effective solutions, making it highly likely that the ASM-Sentinel integration will be unrivaled for quite some time.

---

*While compliance standards such as PCI DSS may have misunderstood the necessity of integrating both vulnerability assessment and attack blocking technologies, F5 and WhiteHat did not. The integration of these two solutions is without a doubt one of the most powerful singular approaches to Web application security.*

---