

HP Application Security Center

Web application security across the application lifecycle

Solution brief

HP Application Security Center helps security professionals, quality assurance (QA) specialists and developers facilitate the security of the Web applications across the enterprise, reducing overall risk of new and operational applications while saving time and money by addressing vulnerabilities across the complete application lifecycle.

Application security is more important than ever

As more mission-critical business processes and customer connections take place on the Web, effective application security is increasingly critical for organizations. IT is being asked to develop new Web applications at a break-neck pace, and security threats are on the rise.

Back when Websites did little more than make static information available, hacking was rare—usually done by attention seekers who wanted to show off their skills. However, with the shift of business-critical

applications moving to the Web and containing sensitive information, hacking has become profitable. Organized criminals are making a big business of stealing, selling, and exploiting Web applications for private information and data. And even though organizations have invested heavily in network firewalls and intrusion detection systems (IDS) to protect themselves, Web applications extend beyond these secure perimeters and hacker activity is often impossible to distinguish from activity by legitimate users.

In addition to rising threat levels, businesses face new challenges. There is more code to secure and less time to secure it, and security resources are limited. The shift to Web 2.0 has created a greater attack surface by pushing business logic and data to the browser. Hackers have developed new techniques and are finding new ways of penetrating applications each passing day. And the recent shift toward applications in the cloud gives IT organizations yet another perimeter to worry about.

A recent study from SANS Institute, a computer security training company, found that attacks against Web applications constitute more than 60 percent of the total attack attempts observed on the Internet.¹ Yet despite the enormous number of attacks and widespread publicity about these vulnerabilities, most Website owners fail to scan effectively for common flaws, according to the study.

It's time for a new approach

Raising the priority of security testing is only the first step. IT organizations have to follow up by taking a new approach to application security testing—a proactive approach that extends across the application lifecycle, across the entire organization and combines the power of both static and dynamic testing.

Since more than 80 percent of vulnerabilities are found within the source code of the application rather than the Web server or application configuration, the traditional practice of having a siloed security team test finished Web applications and report vulnerabilities to development teams needs to be replaced by security testing that spans the whole application lifecycle. Development teams, QA teams, and security teams have to work together. And the business needs a sophisticated, scalable, enterprise-wide application security program.

HP application security center: All the ingredients for application security success

A good security program involves people, processes, and technology, and HP Application Security Center takes all three into consideration. HP Application Security Center includes a comprehensive suite of software, professional services, and SaaS solutions to help improve your overall application security program as well as the security of each application. HP offers three software products that can be used separately or together to test Web applications and manage your overall security program; HP Assessment Management Platform, HP WebInspect, and HP QAInspect. HP also has key integrations with third-party niche vendors such as Fortify Software.

HP Assessment Management Platform

HP Assessment Management Platform (AMP) is the industry-leading enterprise application security solution for managing the complexities of today's Web application security programs. HP AMP software gives CSOs, business managers, security professionals, QA and development teams the ability to extend and scale their Web application security programs across the complete application lifecycle, gain an enterprise-wide view, and increase return on investment (ROI) by making informed business decisions.

HP WebInspect

HP WebInspect software is an award winning Web application security assessment solution designed to thoroughly analyze today's complex Web applications. It delivers fast scanning capabilities, broad assessment coverage, extensive vulnerability knowledge, and accurate Web application scanning results.

HP QAInspect

HP QAInspect software enables QA professionals to incorporate fully-automated Web application security testing into overall test management processes without the need for specialized security knowledge and without the risk of missing aggressive product release deadlines.

HP Application Security Center also helps organizations to manage and report compliance status of their applications in regards to relevant industry regulations, such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and payment card industry (PCI) standards.

More than 2000 organizations rely on HP Application Security Center to secure their Web applications.

¹ SANS Institute, "The Top Cyber Security Risks," September 2009.

Figure 1. HP Assessment Management Platform



Figure 2. HP WebInspect

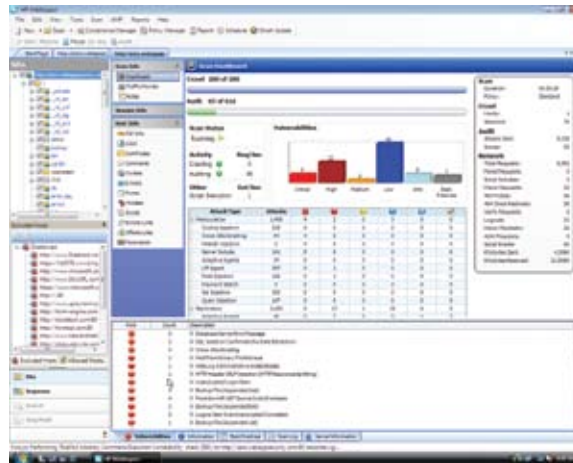


Figure 3. HP QAInspect

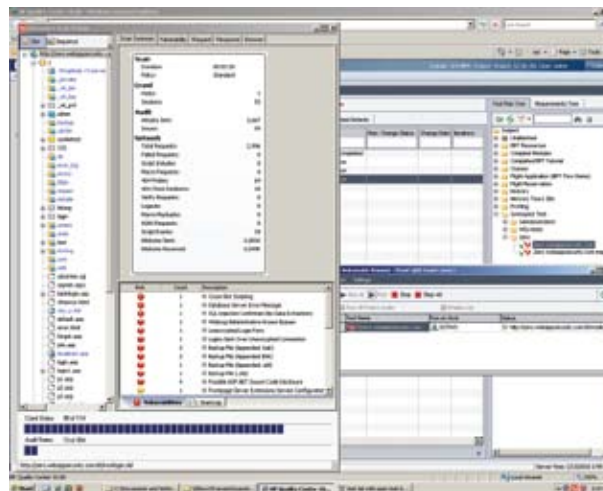
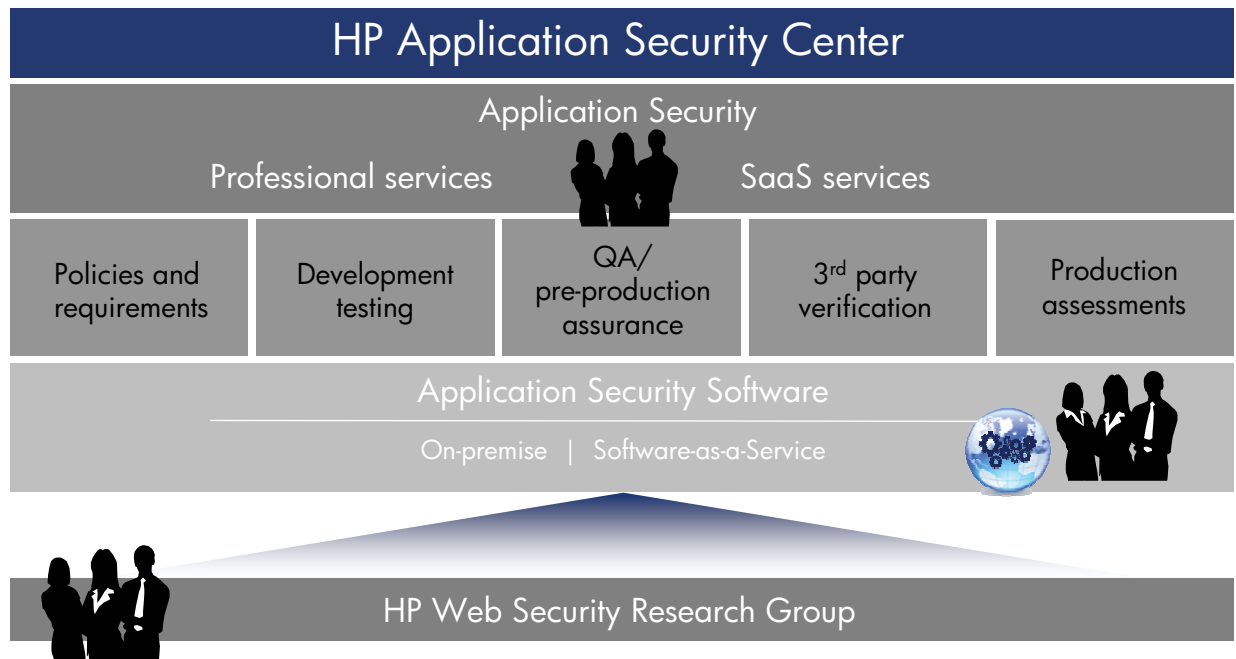


Figure 4. HP Application Security Center brings people, processes, and technology together to support a complete, effective application security program.



Adding value across the organization

HP Application Security Center software provides an effective end-to-end Web application security solution that brings together security professionals, developers, and QA professionals across the enterprise to build and deliver secure applications.

Security professionals

Security professionals protect enterprise Web applications and reduce the risk of malicious attacks from hackers, who are constantly finding new ways to exploit applications. They also demonstrate the state of Web security and regulatory compliance.

Today's security professionals perform these functions for an overwhelming number of applications,

vulnerabilities, and users around the world. They must identify critical applications, maintain a holistic risk-management view, and give numerous stakeholders visibility into the state of application security across the enterprise. And they must scale their assessment processes across the enterprise and throughout the lifecycle to developers, QA teams, other security professionals, and the business managers who own the applications.

This has prompted many organizations to strive for proactive application security programs that find vulnerabilities early in the lifecycle to avoid the excessive costs associated with fixing defects in production applications. Such programs require sophisticated software for coordinating global teams to manage and mitigate application risk.

HP WebInspect

HP WebInspect is easy-to-use, extensible and accurate Web application security assessment software. Many security professionals begin their application security testing programs with HP WebInspect, which enables both security experts and security novices to identify critical, high-risk security vulnerabilities in Web applications and Web services. HP WebInspect is a highly interactive tool that allows for an in-depth analysis of an application. IT addresses the complexity of Web 2.0 and identifies vulnerabilities that are undetectable by traditional scanners. And it supports today's most complex Web application technologies with breakthrough testing innovations, including simultaneous crawl and audit (SCA) and concurrent application scanning, resulting in fast and accurate security assessment.

HP Assessment Management Platform

HP AMP fully addresses the complexities of today's Web application security programs. After using HP WebInspect for a short time, security professionals often find the need to scale their program to test the rapidly growing number of Web applications and perform tests more frequently. HP AMP provides a scalable, automated solution that allows security penetration tests to be managed, scheduled, executed, and reported. HP AMP also helps IT security easily extend security testing across the application lifecycle into non-traditional security teams like QA and development.

HP AMP supports an advanced global security program that allows multiple participants to get the application security information they need and participate in the assessment and remediation process, while letting security professionals maintain centralized control of both the tools and data. It provides a Web-based interface for a consolidated global view, supporting multi-user lifecycle collaboration and control of application security risk throughout the enterprise and helping organizations make informed security business decisions.

Developers

Developers are under intense time pressures and are not security specialists. They are increasingly relying on security products to help them identify security defects during development to eliminate the time and expense of patching security defects in later stages. The following HP Application Security Center solutions offer options for developers to help ensure the security of their Web applications either dynamically, statically, or a combination of both (hybrid). The solutions are flexible to support whatever development methodologies (that is, Agile, Waterfall) your organization may use.

HP Assessment Management Platform

Development organizations can use HP AMP to conduct dynamic security testing of applications, targeting exploitable security defects. The platform conducts comprehensive tests for all Web applications, regardless of the language in which they are built, and includes flexible reporting capabilities, including full remediation solutions and knowledge sharing with security experts. Developers can easily execute a security test, or security teams can schedule a test to run after each build.

Fortify 360 Source Code Analyzer (SCA)

The HP Software & Solutions collaborative partnership with Fortify Software enables IT organizations to leverage the industry's best-of-breed static and dynamic security testing solutions. Fortify SCA provides root-cause identification of security vulnerabilities in source code that can be reported into HP AMP to give users a real-time dashboard view of application security scanning efforts enterprise-wide. Security vulnerabilities discovered with Fortify SCA can also be tracked within HP Quality Center.

QA professionals

Security defects need to be managed and tested for any other software defects. It is imperative that application security be built into the QA process to reduce the risk of missed release dates or worse, security vulnerabilities making it into production.

QA teams need security products that augment their automated tests, minimize impact on time pressures, fit their existing methodologies, and integrate into their environments.

HP QAInspect

HP QAInspect seamlessly integrates into an organization's overall quality assurance processes, providing an automated application security testing solution within HP Quality Center. QA teams can help identify security defects earlier in the application lifecycle. HP QAInspect reports on vulnerabilities in a way that QA professionals can understand by delivering concise, prioritized lists of vulnerabilities and thorough vulnerability descriptions. Analysis results yield detailed information on possible types of attacks, including cross-site scripting (XSS) or structured query language (SQL) injection.

HP WebInspect

HP WebInspect provides the ideal solution for advanced QA security testing professionals.

It provides the agility, in-depth analysis and interaction that advanced professionals require. HP WebInspect's integration with HP Quality Center and IBM Rational ClearQuest allows you to track and manage your security defects consistently with other software defects.

HP Assessment Management Platform

HP AMP's automatic scheduling capability lets QA teams schedule and execute regular Web security tests with minimal impact on their time. The platform also includes comprehensive reporting capabilities that help QA teams share information and security policies with development teams and security professionals.

HP Web Security Research Group

All HP Application Security Center software is backed by the HP Web Security Research Group, a team made up of the industry's leading security researchers, dedicated to being at the forefront of Web application vulnerability discovery and innovation. Made up of acclaimed authors and spokespeople, this team does extensive research that not only provides the latest innovations in Web application vulnerability assessment, but also regular and timely updates to all HP Application Security Center products through the HP SmartUpdate function.

HP application security software as a service (SaaS)

HP SaaS enables you to lower your up-front cost and risk. HP SaaS can help you establish a security program or provide turn-key security assessment services to augment your security program, so that you can start mitigating your security risks immediately. Extensive HP experience in SaaS delivery gives you a level of safety and maturity unmatched in the industry. With over nine years of experience, HP has learned that successful SaaS involves much more than simply hosting the software. A named technical account manager becomes part of your team, assists in customizing the solution to your needs, and helps to make sure that you get the most out of your investment in Web application security.

For more information on HP SaaS visit: <https://saas.hp.com/>

A complete solution

Comprehensive training

HP provides a comprehensive curriculum of both computer-based and instructor-led Application Security Center courses. These offerings provide the training you need to realize the full potential of your HP application security solutions and achieve better return on your investments. For more information about these and other educational courses, visit: www.hp.com/learn

Contact information

To find an HP Software & Solutions sales office or reseller near you, visit: www.managementsoftware.hp.com/buy

HP Services

Get the most from your investment

HP Services can help you build an application security center of excellence (COE) with a dedicated team, consolidated tools, and standard processes. HP Services offers methodologies, a maturity model, content bundles, blueprints, process descriptions, implementation templates, product content, user adoption tools, function descriptions, implementation utilities, and much more.

Our Application Security Center COE Service consists of:

- A strategy workshop to brainstorm challenges and develop a roadmap
- An application security strategy service for developing the solution blueprint and business case
- An enablement service for the pilot installation
- A roll-out service for deployment

Whether you need an incremental approach of staged improvements in a small organization or division, or a top-down approach for building a COE framework across your enterprise, HP Services can give your IT staff best practices for implementation, configuration, and integration.

For an overview of HP software services, visit: www.managementsoftware.hp.com/service



Get connected

www.hp.com/go/getconnected

Get the insider view on tech trends, alerts and HP solutions for better business outcomes

Technology for better business outcomes

To learn more, visit www.hp.com/go/securitysoftware

© Copyright 2007, 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA1-5368ENW Rev. 1, February 2010

