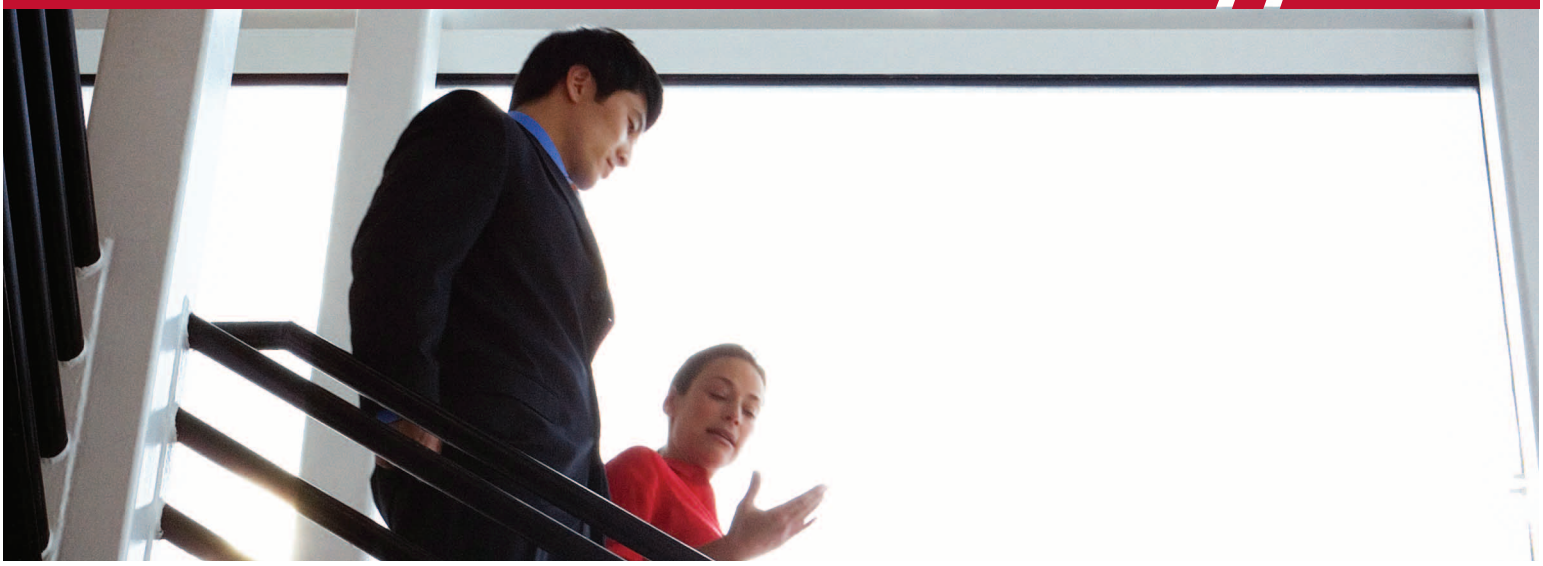
HP security assessment technology

Solution brief

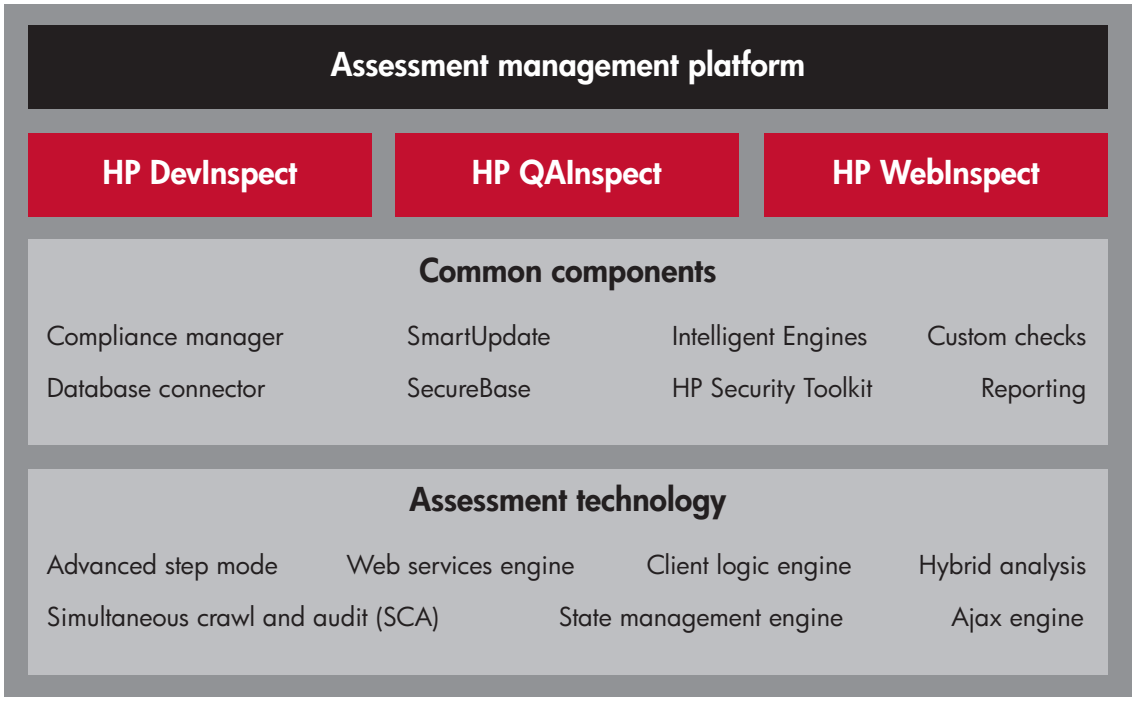


HP Application Security Center software products thoroughly analyze today's complex web applications built on emerging Web 2.0 technologies. They deliver fast scanning capabilities, broad assessment coverage and accurate web application scanning results.

How web application security has changed

Traditional application security scanners perform well when discovering vulnerabilities in some of the more mature web technologies, such as Hypertext Markup Language (HTML) and Common Gateway Interface (CGI), but they lack the intelligence required to scan emerging Web 2.0 technologies, such as Ajax, Simple Object Access Protocol (SOAP), service-oriented architecture (SOA), Rich Site Summary (RSS) and Atom, as well as more dynamic technologies, such as JavaScript and Flash. Legacy web application scanners are simply not designed to navigate and interpret today's web applications with active content, mandatory two-factor authentication and other advancements. Simply put, traditional scanners cannot see the entire application. As a result, traditional scanners fail to discover exploitable security vulnerabilities that exist in the more dynamic and complex regions of modern web applications. This results in an unacceptable level of false negatives.

HP Application Security Center products and assessment technology
Sophisticated assessment technology is embedded in all of the HP Application Security Center software products, providing you with accurate results.



Common components

Reporting
The reporting system lets you customize reports through configuration options and template-driven reports. Standard reports include security auditor, quality assurance (QA) and developer-focused reports as well as numerous sorting and filtering options. Output formats include PDF, HTML, Microsoft® Office and XML.

Database connector
HP Application Security Center products are built on Microsoft SQL Server technology, providing a centralized database for large data storage, easy access to information and high-performance analysis, reporting and processing of security data.

Intelligent Engines
Using a structured, logic-based approach to analyzing applications, the patent-pending Intelligent Engines technology customizes attacks based on each web application's behavior and environment. This results in an automatic penetration test that produces few false positives and finds more vulnerabilities than ever before.

SecureBase
With more than 5000 unique web application specific vulnerabilities, threats and security checks, the security vulnerability database is a comprehensive and accurate knowledgebase. Our hands-on, consulting experience for application penetration testing, combined with extensive research, lets us keep the database current, resulting in daily updates. SecureBase is tuned to work with our Intelligent Engines technology, providing you with accurate results.

SmartUpdate
When new vulnerabilities are published, we build smart adaptive checks to detect those vulnerabilities and make them immediately available for you to access through the SmartUpdate feature. You should also contact HP about new vulnerabilities you may find. The combination of our research team and SmartUpdate can make new capabilities available to you within 24 hours of their initial discovery.

Custom checks
All of our products let you develop custom checks using our custom check wizard. Advanced users can create custom agents written in C#, using our rich scan engine API.

What we check for

Our assessment technology includes pre-built security policies for more than 20 laws, regulations and best practices and checks for the following vulnerabilities:

Data injection and manipulation attacks
- Reflected cross-site scripting (XSS)
- Persistent cross-site scripting (XSS)
- Cross-site request forgery
- SQL injection
- Blind SQL injection
- Buffer overflows
- Integer overflows
- Log injection
- Remote File Include (RFI) injection
- Server Side Include (SSI) injection
- Operating system command injection
- Local File Include (LFI)

Sessions and authentication
- Session strength
- Authentication attacks
- Insufficient authentication
- Insufficient session expiration

Server and general HTTP
- Secure Sockets Layer (SSL) certificate issues
- SSL protocols
- SSL ciphers
- Server misconfiguration
- Directory indexing and enumeration
- Denial of Service (DoS)
- HTTP response splitting
- Encoding attacks
- Windows 8.3 file name
- DOS device handle DoS
- Canonicalization attacks
- URL redirection attacks
- Password autocomplete
- Cookie security
- Custom fuzzing
- Path manipulation—traversal
- Path truncation
- Ajax auditing
- WebDAV auditing
- Web services auditing
- File enumeration
- Information disclosure
- Directory and path traversal
- Spam gateway detection
- Brute force authentication attacks
- Known application and platform vulnerabilities

Assessment technology

Simultaneous crawl and audit
Patent-pending simultaneous crawl and audit (SCA) technology achieves faster, more accurate results by combining the application crawl and audit phases into a single fluid process. By conducting these activities in parallel instead of sequentially, scan times are reduced by 50 percent or more. Additionally, scans are refined based on real-time audit findings, resulting in a comprehensive view of the entire web application attack surface.

State management engine
The state management engine authenticates every scan. It can address multiple, simultaneous threads operating independently as different users or acting together as a single user session. If a state is lost, the state management engine pauses all scan activity, re-establishes a connection, reauthenticates and then continues the assessment.

Client logic engine
Web 2.0, Ajax, Flash and JavaScript have created rich and complex web applications that require advanced security testing. Capable of processing applications using a complex mix of these technologies, the client logic engine provides an accurate, automated assessment.

Ajax engine
The Ajax engine provides the capabilities necessary to analyze and assess Ajax-based applications and discover vulnerabilities. We work closely with customers and prospects to identify various Ajax programming styles and to support unique Ajax approaches.

Advanced step mode
Our security assessment technology includes capabilities that integrate directly into your web browser for advanced manual scanning. For advanced users who want extra control during their assessment, our advanced step mode functionality lets auditors precisely control what is audited and when. Auditing simultaneously with users or after they have completed their individual analysis, the advanced step mode crawls and audits even the most complex sites.

Hybrid analysis
HP DevInspect software, designed to simplify security for development, performs both black-box testing and source code analysis for accurately and precisely identifying root causes of security vulnerabilities in source code. HP DevInspect can identify web application and web services security vulnerabilities with high confidence.

Web services engine
The web services engine lets you analyze, assess and discover vulnerabilities in web services-based applications.

Advanced authentication management
Intelligent automation eliminates the complexities of authentication even with applications that use advanced technologies, such as two-factor authentication or Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs). HP Application Security Center software can authenticate secure web applications and detect when re-authentication is required, providing your applications with full coverage.

Compliance manager
HP Application Security Center software includes advanced compliance reporting and testing tools. The software supports major laws, regulations and best practices with more than 20 common compliance templates, including policies such as Payment Card Industry (PCI) Data Security Standard (DSS), Open Web Application Security Project (OWASP) Top 10, Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). Additionally, we include a compliance editor that lets you modify or capture your existing IT security policies and translate them into automated test plans and reports that can be run and shared across the software products.

Compliance Pack

The Compliance Pack addresses the following best practices and legal regulatory initiatives:

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- North America Electric Reliability Council (NERC)
- Safe Harbor
- Payment Card Industry (PCI) Data Security Policy
- UK Data Protection Act
- Basel II
- ISO 17799
- OWASP top 10
- California SB1386
- Gramm-Leach Bliley Act (GLBA)
- Sarbanes-Oxley Act, Section 404
- 21CFR11
- NIST 800-53
- Director of Central Intelligence Directive 6/3 (DCID)
- California Online Privacy Protection Act
- Children's Online Privacy Protection Act (COPPA)
- Japan Personal Information Protection Act (JPIPA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)

A complete solution

Comprehensive training
HP provides a comprehensive curriculum of HP Software and IT Service Management courses. These offerings provide the training you need to realize the full potential of your HP solutions, increase your network optimization and responsiveness, and achieve better return on your IT investments.

With more than 30 years experience meeting complex education challenges worldwide, HP knows training. This experience, coupled with unique insights into HP Software products, positions HP to deliver the optimum training experience. For more information about these and other educational courses, visit **www.hp.com/learn**.

The smartest way to invest in IT
HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage and ultimately retire your HP solutions. For more information on these services, contact your HP sales representative or visit **www.hp.com/go/hpfinancialservices**.

Contact information

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

HP Services

Get the most from your software investment
HP provides high-quality software services that address all aspects of your software application lifecycle needs. With HP, you have access to standards-based, modular, multi-platform software coupled with global services and support. The wide range of HP service offerings—from online self-solve support to proactive mission-critical services—enables you to choose the services that best match your business needs.

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

To access technical interactive support, visit Software Support Online at **www.hp.com/managementsoftware/services**.

To learn more about HP Software Customer Connection, a one-stop information and learning portal for software products and services, visit **www.hp.com/go/swcustomerconnection**.

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

4AA1-5367ENW, October 2007

invent