

Sony standardizes application security

Implementing HP Application Security Center reduces security testing labor costs, boosts mean time to resolution



“By leveraging QALinspect and WebInspect during our development lifecycle, we’ve lowered the overall costs associated with bringing our applications up to compliance before we go into production.”

Erika Pecciotta, Executive Director of Enterprise Technology and Quality, Sony Pictures Entertainment

HP customer case study: Implementing standardized security tools and processes lowers application development costs, risk of security vulnerabilities

Industry:
Entertainment

Objective:

Standardized, uniform processes to more efficiently assess and address potential security vulnerabilities for web applications

Approach:

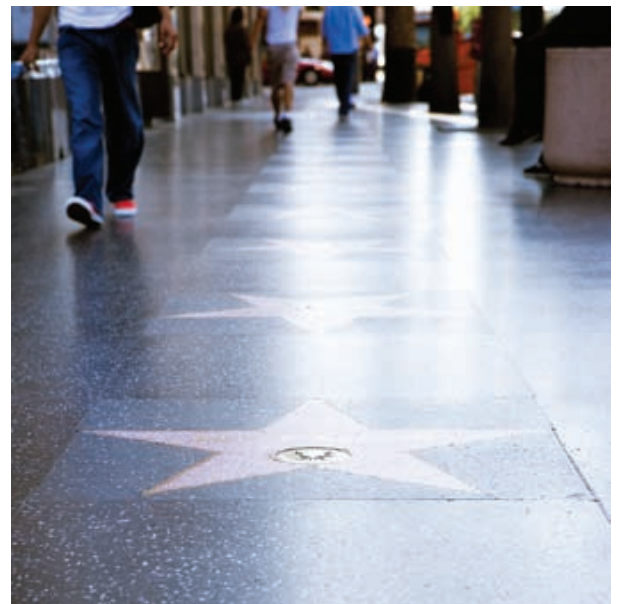
Create center of excellence and provide toolset to support testing standards

IT improvements:

- Integration with SecureBase ensures attack information and tests always current
- Less duplication of effort
- Greater awareness about security vulnerabilities
- Testing has less impact on development schedules

Business outcomes:

- Lower overall costs to bring applications into compliance
- Able to increase testing teams’ workload without adding staff, saving thousands in labor costs annually
- Vulnerabilities identified earlier in development, when corrections are less costly
- More testing now possible without adding staff, time
- Improved regulatory compliance
- Lowered mean time to resolution when vulnerabilities detected



Sony Pictures Entertainment (SPE), the multi-billion dollar subsidiary of Sony Corporation, knows the importance of implementing secure development and quality assurance policies to remove defects from its Web applications. But like many corporations with vast and dispersed application development teams, SPE lacked a uniform, enterprise approach to managing security issues within its development processes.

Instead, each SPE development team took its own approach. Furthermore, the teams vetted applications for flaws toward the end of their development processes. It was an unstandardized and inefficient approach, and as SPE accelerated its use of new and complex development tools and architectures, including SOA, .Net, and Java, the penalties for that inefficiency grew.

“It’s a partnership. It’s not just about IT security, and it’s not about inhibiting the business. What we’re doing is bringing to light the risks to our proprietary information. And we’re leveraging WebInspect and combining it with our expertise in system development lifecycles and overall quality assurance. WebInspect helps us to bring those two disciplines together.”

Erika Pecciotto, Executive Director of Enterprise Technology and Quality, Sony Pictures Entertainment



SPE needed a new framework and set of processes to manage security-related development issues—a framework that would comply with Sony Corporation’s global information security standards and policies, which address everything from physical security to secure software development.

“Any time we have an application that we know will manage personal information, we hit that application with WebInspect. And we can feel confident that the applications are compliant with these standards.”

Jeff Cox, Quality Assurance Security Engineer, Sony Pictures Entertainment

To do this, SPE put into place several competency centers designed to collaboratively share best practices within critical facets of its business, including quality assurance, security, systems architecture, and business analysis.

In addition, SPE implemented HP Application Security Center WebInspect™ and QALinspect™ software.

Point it and let it run

A crucial facet of SPE’s broader governance effort is the ability to identify any application security vulnerabilities and misconfigurations that might jeopardize both regulatory compliance and security. It’s a challenging task. The company’s development projects are led by some 25 different development groups that support eight business units; their applications support a range of critical business processing including everything from collaborative sales and marketing team efforts, to distribution, supply-chain management, and back-office ERP systems.

To manage these development initiatives, SPE needed Web application security and quality assurance tools that would scale, and that would enable everyone in the process—developers, quality assurance teams, internal auditors, and IT security groups—to seamlessly perform their respective roles.

SPE chose the HP software tools after performing a technical analysis to validate the software’s functionality, manageability, and ease of use. “We simply point WebInspect to any application and let it run,” notes Erika Pecciotto, Executive Director of Enterprise Technology and Quality, SPE. Another crucial advantage the HP solution offers is its integration with HP’s vulnerability database, SecureBase, which is kept up-to-date by HP Application Security Center’s research and development team. “Because of SecureBase, we feel confident that we always have the most current attack information and tests,” Pecciotto says.

“It’s amazing how surprised developers are when you first show them that the application they’ve developed contains serious vulnerabilities which, if not addressed, could expose sensitive information.”

Erika Pecciotto, Executive Director of Enterprise Technology and Quality, Sony Pictures Entertainment

SPE also cites the training, support, and long-term product roadmaps HP provides. “The learning curve and training required to use the HP solutions was minimal,” says Pecciotto. “And after spending time with HP’s executive leadership, we appreciate their vision and roadmap for their tools.”

Reduced overhead costs

Since implementing HP Application Security Center, SPE has incorporated its tools into every facet of its quality assurance and Web application development lifecycle. Applications are now vetted for vulnerabilities during development and QA, and then, on an as-needed basis, by the information security team to mitigate any potential risks once the applications are put into production.

"The learning curve and training required to use the HP solutions was minimal. And after spending time with HP's executive leadership, we appreciate their vision and roadmap for their tools."

Erika Pecciotto, Executive Director of Enterprise Technology and Quality, Sony Pictures Entertainment

By leveraging QALnspect and WebInspect during the development lifecycle, SPE has lowering their overall costs of bringing applications up to compliance before production. For instance, having a single, standardized solution reduces the risk of duplication of efforts during testing and QA procedures, which reduces overhead costs and improves productivity.

The tools have also helped SPE reduce costs associated with specific testing functions. For instance, by automating security testing, the company is able to increase its test teams' workload without adding more staff, thereby saving thousands of dollars in payroll costs.

Using the tools also helps SPE's development, quality assurance, and security teams collaborate more effectively—which also helps reduce the risks and costs associated with spotting vulnerabilities late in development, or in production.

"It's a partnership. It's not just about IT security, and it's not about inhibiting the business. What we're doing is bringing to light the risks to our proprietary information. And we're leveraging WebInspect and combining it with our expertise in system development lifecycles and overall quality assurance," says Pecciotto. "WebInspect helps us to bring those two disciplines together."

WebInspect has also helped SPE improve Web application security awareness across its development teams and IT management. "It's amazing how surprised developers are when you first show them that the application they've developed contains serious vulnerabilities which, if not addressed, could expose sensitive information," Pecciotto notes.

"The awareness part of the equation is key," she adds. "People previously believed that if they're inside the corporate firewall, and the application has a username and password for authentication, then the application is secure. WebInspect has brought a lot of visibility to the fact that if port 80 is open, everything coming through port 80 is suspect."

"Now, before any application goes live, we run WebInspect once again to not only make sure that it's secure, but also to demonstrate that the development teams have successfully mitigated their vulnerabilities."

Erika Pecciotto, Executive Director of Enterprise Technology and Quality, Sony Pictures Entertainment

SPE's next step is to leverage the momentum of this awareness to further improve the software development process. "As development and QA teams utilize its reporting features, WebInspect becomes

Customer solution at a glance

Primary applications

Web application development
security testing

Primary software

- HP Application Security Center
WebInspect™ and QALinspect™
software
- HP Quality Center

an integral educational tool,” says Peccioto. “It helps teach our people the discipline of self-assessment. We then have our teams validate those assessments, before they eventually go through internal audit.”

Another benefit of WebInspect is that it helps SPE maintain its fast-moving production schedule and make certain that its applications are in compliance. SPE’s financial systems must be are compliant with Sarbanes-Oxley; the company also needs to comply with a myriad of privacy laws from countries around the globe, including European Union Directive 9546, the various privacy laws of each EU member state, and laws throughout Asia and Japan. “Any time we have an application that we know will manage personal information, we hit that application with WebInspect,” says Jeff Cox, Quality Assurance Security Engineer, SPE. “And we can feel confident that the applications are compliant with these standards.”

Tight integration

SPE turned to HP QALinspect because of its tight integration with SPE’s crucial Quality Assurance tools, including HP’s Quality Center.

QALinspect helps streamline the entire security and quality assurance process, Cox explains. “Quality assurance testers can run security-based tests in addition to their functional and performance tests. And those results are integrated with HP Quality Center, so the application development teams will be able to track security defects within the same environment they track everything else,” he adds.

QALinspect also enables SPE to automate its Web application security testing directly from within the HP tools their QA professionals already know, which makes it possible to quickly develop secure applications at the lowest possible cost. Its ability to provide fully-integrated defect reports means security issues are highlighted alongside functional defects from within HP’s Quality Center and

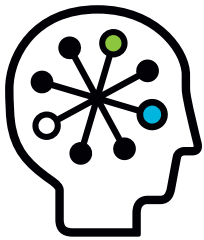
Defect Management modules. It’s this ability for QALinspect to tightly integrate with HP’s tools that greatly improve SPE’s security assessments toward the end of the development cycle. “And it helps QA and development teams to standardize the defect management process,” says Peccioto.

While QALinspect enables SPE to test for security defects throughout the development process—it helps SPE find and prioritize security vulnerabilities in every Web application, model specific usage scenarios during testing, and provide detailed information and remediation advice about any vulnerabilities uncovered—its ease of management mean comprehensive testing doesn’t slow down SPE’s project schedules or require new security expertise.

In fact, the software has allowed SPE to add an additional layer of security, Peccioto explains. “Now, before any application goes live, we run WebInspect once again to not only make sure that it’s secure, but also to demonstrate that the development teams have successfully mitigated their vulnerabilities,” she says.

The integrated risk management and quality assurance processes and procedures SPE is putting into place, with the help of WebInspect and QALinspect, is something security and compliance teams hope to emulate throughout the other Sony companies. It enables a Center of Excellence, a single point of visibility into security-related issues and a single view of the truth. This, in turn, helps minimize time to resolution when issues are discovered.

“The key for management has been our ability to gain visibility into the development and quality assurance processes, and express quality in terms of visibility into defects that need to be fixed,” says David Buckholtz, VP of Enterprise Technology and Quality, SPE. “The shared knowledge that’s generated across development, audit, and security teams is a model for the ways we will tackle all of our progress toward greater governance.”



Technology for better business outcomes

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

© 2009 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.

This customer’s results depended upon its unique business and IT environment, the way it used HP products and services and other factors. These results may not be typical; your results may vary.

4AA2-6406ENW, May 2009

