

Accenture and Symantec Security
Transformation Services

Application Security Services



High performance. Delivered.

In alliance with



Market pressures, increasing complexity, and a lack of generally accepted development practices are causing many organizations to deploy custom and commercial applications with inadequate security. Software vulnerabilities typically result from insufficient use of secure design methods and processes, coding errors, and inadequate testing and deployment strategies.

Vulnerabilities may translate into significant financial loss through increased software development and remediation costs and damage to the organization's reputation. Ultimately, applications without adequate security may affect the bottom line and lead to potentially devastating brand erosion and other market impacts. Consequently, it is imperative for organizations

to develop test plans and procedures to address application software security defects and implement new standards, methodologies, and development processes to minimize risk.

Accenture and Symantec Security Transformation Services provide a comprehensive suite of software development lifecycle (SDLC) services. Accenture and Symantec's joint Application Security Services offering provides a solution for repeatable and scalable development processes, drives the ability to reuse secure code, and enables the development of secure business applications. The result is that organizations are able to implement strategies to help mitigate risk and reduce the cost and complexity of deploying software security controls.

The Challenge

Application software programs that drive the global economy are increasing in size and complexity.

The probability that vulnerabilities exist in source code is nearly absolute. It is not a question of whether there are vulnerabilities, but rather of how many and how severe.

While completely secure code is prohibitively expensive to develop, the risks associated with less secure code can be managed to acceptable levels. This requires the deployment of balanced controls during the development and maintenance cycles based on a coherent software strategy and framework that integrates security principles into the relevant processes. For most organizations, this will require significant transformation of the existing SDLC to embed security processes and secure coding principles. But with mounting market pressures and the increasingly high cost of downstream remediation, many organizations see no other alternative than to "bake" security into the SDLC from the ground up.

Key Drivers

Market pressure

Competition and first-to-market pressure is driving software development at an accelerated pace. Application development plans may outstrip security initiatives, even as the requirements for security assurance are increasing.

Size and complexity

Software is becoming more complicated and modular, with the sheer size of the code base often preventing effective detection and remediation of vulnerabilities. Simultaneously, the integration of open-source and third-party software increases attacker knowledge of vulnerabilities while limiting developer control of source code.

Remediation costs

Remediation costs increase substantially for errors found at advanced stages of the development cycle, yet testing typically occurs only after the software release or during beta testing. Software remediation is laborious and expensive.

The Solution

Accenture and Symantec Application Security Services assist organizations with testing services and transformation of their software development programs. The desired end-state is a re-engineered SDLC, integrated with supporting technologies, operational practices, and management structures.

Services

The Application Security Services offering consists of four services that address the most common security needs across a broad spectrum of SDLC maturity levels. Each service is tailored to assist an organization to achieve step-wise gains, which transform development processes to effectively support and manage application software security.

1. Application Architecture and Design Review

Assesses an organization's application architectures, design practices, and implementation processes to identify and recommend improvements to minimize application vulnerabilities. Output includes a gap analysis, prioritized recommendations, and a high-level plan to mitigate risk areas.

2. Code Review and Analysis

Examines applications at the source-code level for existing vulnerabilities. Outcomes include detailed findings linked to specific lines of code, distilled findings pointing to systemic practices, triage recommendations for application portfolios, a high-level plan to mitigate risk areas, and knowledge transfer. Major activities include:

- Formulation of software development contractual acceptance criteria
- Black box and white box testing for application-level vulnerabilities
- Automated testing of code base
- Sampled and line-by-line code reviews
- Integration of automated scanning tools into the development environment
- Leveraging of assessment findings, if needed, to modify software standards and security policy
- Delivery of remediation plan and vulnerability details

3. Code Remediation

Executes code remediation plans for applications. Objectives for individual projects can be customized to include the appropriate combination of focused break/fix coding of selected modules within a single application, program management and oversight of in-sourced code remediation projects, or outsourcing of an entire application portfolio. Specific activities include:

- Competitively priced code remediation services
- Secure coding training and workshops for developers, testers, and managers
- Assistance with or complete project management of code remediation activities
- Assistance with or complete ownership of policy updates

4. SDLC Transformation

Transforms an organization's existing SDLC by embedding secure coding practices, including supporting technologies, operational processes, and management structures. The goal is to integrate secure code development and an effective framework to measure and manage associated risks. Activities include:

- Transformation of existing framework or creation of a new SDLC and associated frameworks
- Application architecture and design review
- Development process review
- Assistance with certification criteria
- Developer training for secure coding practices and management training for new secure development procedures

Benefits

- Establishes comprehensive security risk management processes and controls
- Improves the software design processes, coding practices, testing methods, and deployment strategies, which can lead to more on-time releases and fewer resources spent on logic flaws and bug fixes
- Helps reduce costs during testing and bug-fix phases by detecting errors in existing code earlier in the SDLC
- Builds an adaptable code development framework that is measurable, repeatable, and sustainable
- Develops more effective deployment strategies that create robust code and can lead to more on-time releases
- Increases understanding, detection, mitigation, and control of risk associated with software flaws
- Provides more effective management of the enterprise application portfolio to improve measurement and control of IT operational risk

Why Accenture and Symantec

Application Security Services is anchored by Accenture's extensive IT transformation track record and Project Management Office capabilities and is built upon Symantec's technology, experience, and tools.

Application Security Services offers an effective combination of tools and processes that leverage proprietary technologies, third-party assets, and an integrated methodology for application security testing and maintenance. The offerings feature independent third-party assessments, custom development work, and a portfolio of application outsourcing contracts, providing organizations access to distinctive services and assets, including:

- Integrated set of tools and processes that are based on the best of proprietary technologies and third-party assets
- Comprehensive application security lifecycle solutions, custom application development, and security assessments that leverage Accenture's expertise developed through years of outsourced application management operations
- World-class security experience with cost-effective global delivery models to provide security services that are robust yet economical to deploy
- Access to the Symantec application security knowledge base, which tracks vulnerabilities in 30,000 technologies, operating systems, and product versions from more than 4,000 vendors, and can automatically deliver timely security notifications worldwide¹
- Real-time intelligence on security threats and incidents gathered from Symantec's more than 40,000 sensors in 180 countries¹

- Ability to provide independent security services to effectively monitor and manage outsourced IT operations

Conclusion

Combining world-class security and system delivery strengths, Accenture and Symantec offer a complete SDLC service. The joint offering provides repeatability and scalability of methodologies and drives the ability to reuse secure code and develop secure business applications. Leveraging the best proprietary technologies and third-party assets, this offering helps organizations achieve step-wise gains and position themselves for transformation over time. Those most likely to benefit include Internet-facing service portals, business-critical application users, users with data protection requirements, and application outsourcing clients. Overall, the services can help reduce the total cost of ownership while strengthening an organization's application security posture.

Notes

1. Source: Symantec Internet Security Threat Report, 3/06.

Contact

To learn how your organization will benefit from Accenture and Symantec Application Security Services, contact:

Accenture

jesse.w.bowen@accenture.com

Symantec

security_transformation_services@symantec.com

The Accenture and Symantec Security Transformation Services Joint Initiative

Accenture and Symantec Security Transformation Services, a new global joint initiative, provides a comprehensive suite of security offerings for organizations grappling with the increasing complexity of managing and mitigating risk. Accenture and Symantec's primary objective is to help organizations reframe the way they think about information security. Delivering scale, experience and a diverse knowledge base with a global footprint, Accenture and Symantec are working in collaboration to provide a strategic and holistic set of end-to-end security offerings incorporating both company's services and products.

This joint initiative draws on the complementary strengths, expertise and experience of these two industry leaders, combining Accenture's broad industry experience driving high performance through acclaimed IT transformation and program management capabilities with Symantec's leading-edge technology, tools and security expertise.

Accenture and Symantec Security Transformation Services offerings enable organizations to swiftly and effectively respond to on-going information security challenges and threats.

Copyright © 2006 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

Copyright © 2006 Symantec
Corporation. All rights reserved.

Symantec and the Symantec Logo
are trademarks or registered
trademarks of Symantec Corporation
or its affiliates in the U.S. and other
countries. Other names may be
trademarks of their respective
owners.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills, and technologies to help clients improve their performance. With approximately 140,000 people in 48 countries, the company generated net revenues of US\$16.65 billion for the fiscal year ended Aug. 31, 2006.

www.accenture.com or
www.accenture.com/Security

About Symantec

Symantec is the global leader in providing solutions to assist individuals and enterprises assure the security, availability, and integrity of their information. Symantec provides a full range of services for assessing, architecting, implementing, supporting, and maintaining an enterprise's security, storage, and infrastructure software solutions. Symantec's global services organization also provides comprehensive maintenance, technical support, and educational services.

www.symantec.com