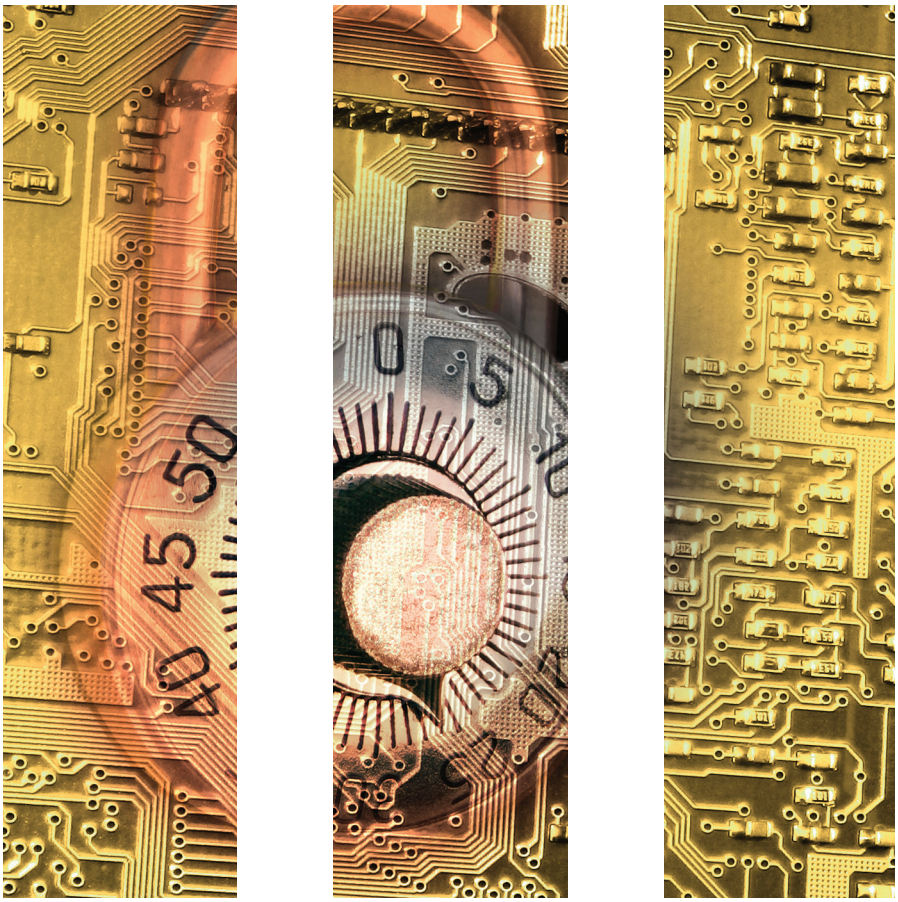
WHITE PAPER

Does Application Security Pay?

Measuring the Business Impact of Software Security Assurance Solutions



mainstay partners
making technology investments count

This study provides the evidence that information security executives need to communicate the business value of application security solutions in a language that matters to senior leadership.

Table of Contents

Executive Summary

The last decade has seen a dramatic shift in the way companies manage information security and protect vital data. In the past, businesses confronted the threat of cyber attacks and data breaches primarily by building firewalls and other "perimeter defenses" around their networks, but the threat has continued to evolve, and more criminals are hacking into applications that are running on a plethora of new devices and environments, including cloud, mobile, and social media.

As a result, the focus of threat protection is moving from securing the infrastructure to securing the software applications that businesses write and deploy. The shift has created a market for a new generation of products and services—known as software security assurance (SSA) solutions—that help companies uncover vulnerabilities in their code, effectively fix these defects, and produce software that is impervious to security threats.

In an effort to quantify the business value of SSA, Mainstay Partners studied 17 organizations that have implemented solutions from Fortify Software, a leading provider of SSA solutions. This study combined executive interviews, industry research, and benchmark analysis to identify, qualify, and quantify the full range of benefits that organizations are seeing from their SSA investments.

The study found that companies are realizing substantial benefits from SSA right out of the box, saving as much as $2.4M per year from a range of efficiency and productivity improvements, including faster, less-costly code scanning and vulnerability remediation and streamlined compliance and penetration testing.

Exponential increases in benefits, however, are being achieved by companies that deploy SSA in more comprehensive and innovative ways. These advanced deployments include embedding software security controls and best practices throughout the development lifecycle, extending SSA programs into critical customer-facing product areas, and leveraging SSA to seize unique value-generating opportunities. For these strategic companies, the benefits of software security solutions can add up to as much as $37M per year.

At a time when IT budgets are coming under closer scrutiny, chief information security officers (CISOs) say they are being called upon to justify SSA investments from a cost-benefit perspective. To that end, this study can provide the evidence needed for information security executives to communicate the business value of software security solutions in a language that matters to senior leadership.

THE BUSINESS CASE FOR SOFTWARE SECURITY

In our interconnected world, software is everywhere—not just in data centers or on desktop computers, but in mobile phones and all kinds of wireless devices and consumer products. Software resides on the Web and in the cloud, where businesses rely on software-as-a-service solutions (SaaS) for mission-critical business functions. For the executives we talked to, application security meant protecting the software that is running in all these environments and devices, and the business improvements of SSA were seen as extending to wherever applications were deployed.

These executives reported a number of significant operational and financial improvements from their SSA implementations. A selection of key performance improvements are shown in the table below.

By analyzing such improvements, we identified the following benefit areas for SSA-enabled organizations:

- More efficient and effective vulnerability assessment and remediation.
- Streamlined regulatory compliance and penetration testing efforts.
- Fewer security-related delays affecting the launch of new products.
- More favorable pricing of outsourced code development.
- Improved valuations of the software assets of merger-and-acquisition targets.

To estimate the financial impact of these benefits, we have relied on industry benchmarks and our own research to make assumptions about key variables such as labor costs, consulting fees, and the size and duration of remediation efforts.

In the sections that follow, we present the study's core findings, estimate the dollar benefits achieved by companies, and summarize the full benefit potential of comprehensive software security solutions. We conclude with a discussion of the "journey" that many companies take after implementing SSA solutions, and the best practices shared by the most successful SSA adopters.

Key Findings

- The full benefit potential of SSA solutions can reach $37M annually.
- Initial SSA deployments can create $2.4M in annual benefits.
- Average vulnerability remediation time fell from 1 to 2 weeks to 1 to 2 hours.
- Repeat vulnerabilities reduced from 80% to virtually zero.
- Organizations saved an estimated $44K in remediation costs per application.
- Companies reducing time-to-market delays saved an estimated $8.3M annually.

"Before we implemented Fortify, I wouldn't have used our own online shopping service. Software security is a critical differentiator for us. We wouldn't be in business without it."

Security Engineer, provider of card-based financial solutions

Performance Metric	Improvement
Vulnerabilities per application	From 100s to 10s
Average time to fix a vulnerability	From 1 to 2 weeks to 1 to 2 hours
Percentage of repeat vulnerabilities	From 80% to 0%
Compliance and penetration testing effort	From ~$500k to ~$250k
Time-to-market delays due to vulnerabilities	From 4+ incidents (30 days each) per year to none

KEY FINDINGS

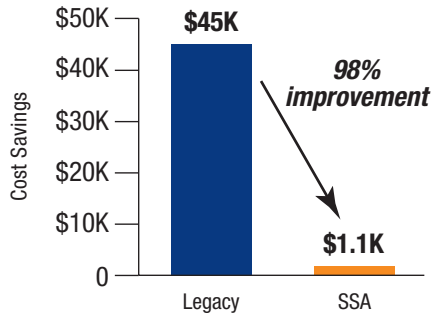
Faster Vulnerability Remediation

Across the board, companies adopting SSA solutions reported significant efficiency improvements in finding and remediating software security flaws. The executives we interviewed said that in the pre-SSA environment, vulnerabilities took an average of 1 to 2 weeks to fix. Slow remediation cycles were common because most defects weren't found until late in the development process, when remediation is time-consuming and expensive, and because organizations using penetration testing to detect flaws spent a significant amount of time tracking down defects in the source code.

Findings

- By introducing automated SSA technology and best practices, organizations reduced average remediation from 1 to 2 weeks to 1 to 2 hours.[1]
- Organizations saved an estimated $44K annually in remediation costs per application.
- For the average organization, these cost savings are estimated conservatively to amount to $3M per year.[2]

Remediation Cost Savings per IT Application



Streamlined Compliance and Penetration Testing

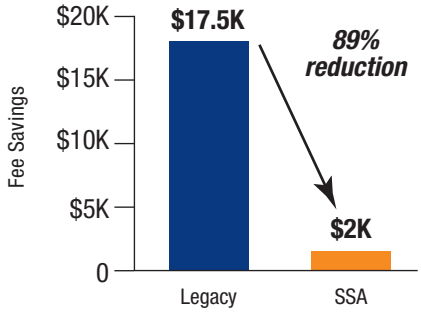
Most of the companies surveyed are facing tighter government and industry regulations for application security, particularly in new software standards in the financial services and health-care industries.[3] The extra development and auditing effort needed to comply with these standards can be costly, as are the potential penalties for non-compliance.

In our interviews, many executives said their SSA solution helped control costs by streamlining regulatory compliance projects that require meeting strict application-security standards. By configuring the SSA solution to address specific compliance mandates, for example, organizations quickly identified and ranked vulnerabilities according to severity. The solution also generates a report that documents these activities, creating an audit trail for regulators.

Finding

- The average organization adopting SSA saw its fees paid to compliance auditors fall by 89%—or about $15K annually.

Auditor Compliance Fee Savings



Energy Company Avoids Costly Fixes

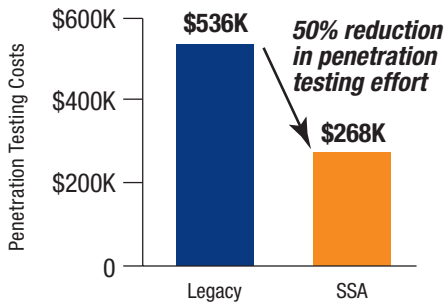
An energy company in the study is controlling costs by enforcing SSA best practices early in the development process. Since implementing Fortify, developers now conduct a threat analysis before writing code and scan applications before deploying them. By remediating vulnerabilities pre-production, the company dramatically reduced remediation effort and expense.

Similarly, after adopting SSA and instituting more rigorous code scanning and remediation processes—along with improved developer awareness and education—organizations found they consistently met quality standards, and thus could plan and focus their penetration testing better and reduce the overall effort required.

Finding

- The average organization achieved a 50% reduction in penetration testing efforts, translating into annual savings of more than $250K.[4]

Penetration Testing Costs



Avoiding Data Breaches

The threat of a major data breach can keep CISOs awake at night, and most are aware of the history of high-profile security failures that have damaged company reputations and resulted in millions of dollars in legal and PR fees, remediation expenses, lost revenue, and customer churn.[5]

Findings

- The average cost of a data breach is about $3.8M, or $204 per compromised record.[6]
- Companies can save an estimated $380K per year by adopting SSA solutions to avoid major data breaches. [7]

Avoiding Software Compliance Penalties

Businesses that fail to comply with industry standards for software security can face substantial penalties. In the payment card industry, for example, penalties can range from $5K to $25K per month. Moreover, when lost sales, customer churn, and remediation expenses are also factored in, the full cost of PCI non-compliance can be substantially more.[8]

Finding

- By ensuring compliance through systematic application security testing, companies can conservatively avoid approximately $100K in penalties annually.[9]

Pay-for-Performance Benefits

In an innovative use of software security technology, companies that outsource software development to partners are leveraging solutions from Fortify Software to drive cost-effective "pay for performance" programs. These companies garner savings and boost software quality by routinely checking for security flaws in the work of their development partners. Fortify scans incoming code for vulnerabilities and allows companies to adjust the fees paid to partners accordingly.

Finding

- Companies using SSA to screen and adjust the price of outsourced code can capture fee savings of about $100K annually while improving the overall quality of code delivered by development partners.[10]

"We went from taking between 60 and 100 hours to pass compliance testing to just 12 hours."

Consultant to CISO of an enterprise decision management company

Government Agency Finds 100 Times More Vulnerabilities

Deploying Fortify initially as a proof-of-concept in a small department, this public-sector organization saw adoption spread quickly when security scans of mission-critical software uncovered 100 times more vulnerabilities than were known before.

Faster Product Launches Boost Revenue and Margins

For companies that sell e-commerce and other commercial software, discovering security flaws late in the development life cycle can delay new product introductions (NPI) by weeks or months, putting revenue and market share at risk and adding millions of dollars in development costs. One software company in the study reported 3 to 5 product delays a year as a result of security defects that surfaced close to launch. Another company put revenue at risk when it discovered software vulnerabilities late in development, jeopardizing delivery of an online service to a major corporate customer.

By embedding SSA tools, training, and best practices in their product development process, these companies were able to minimize security-driven delays and speed product launches. Fewer product delays also helped control development costs at these companies, since they deployed more resources to code development rather than remediation.

Findings

- Companies can capture an estimate $8.3M of additional software revenue through a comprehensive SSA program to minimize product delays.[11]
- Companies can realize development cost savings of about $15M per year from SSA-driven reductions in product delays.[12]

Maximizing the Value of M&A Deals

Several companies in the study are extending the value of their software security solution by deploying it in strategic ways. One company, for example, is using Fortify to perform software security audits of acquisition targets that own core products critically dependent on software. The audit results become part of deal negotiations and can trigger price breaks if the target's core applications are found to have significant vulnerabilities. Not every company will take advantage of this kind of SSA deployment, but for a business depending on M&A activity to grow or innovate, the strategy can yield substantial business value.

Finding

- In the case of a company completing two $100M deals a year, using SSA to assess the software assets of prospective acquisitions can yield valuation benefits of approximately $10M.[13]

"The ROI we are seeing is incredible. In a year's time, we made up for the cost of implementation and we've all but eliminated time-to-market delays caused by security flaws discovered late in the development cycle."

Consultant to CISO of enterprise decision management company

Financial Services Firm Accelerates Time to Market

After implementing Fortify, this financial company uncovered thousands of previously unknown security flaws in its applications. By cleaning code early, the company is now avoiding remediation costs of around $1M per year, eliminating 100 hours of compliance testing per application, and avoiding product-launch delays—a benefit worth $7M–$8M annually.

REALIZING THE FULL POTENTIAL OF SSA

By pulling together the various benefit estimates above, we can begin to see the full potential of SSA to generate business value. As shown in the figure below, for companies able to exploit all of the opportunities for value creation, that potential can reach $37M annually. However, the benefits accruing to a particular company would necessarily vary according to its business profile, including its size, industry, and business strategy.

For example, only companies that sell commercial software (or that provide software-enabled products or services) are likely to gain the revenue and cost benefits from accelerating new product introductions. Similarly, only companies actively engaged in M&A activities can achieve the valuation benefits from SSA-enabled acquisition-valuation initiatives. In addition, not all of the estimated benefits should be understood as "hard savings" that directly impact the profit and loss statement. For example, benefits from avoiding costs—such as a breach remediation—may be considered "soft" because some organizations may never experience a breach event.

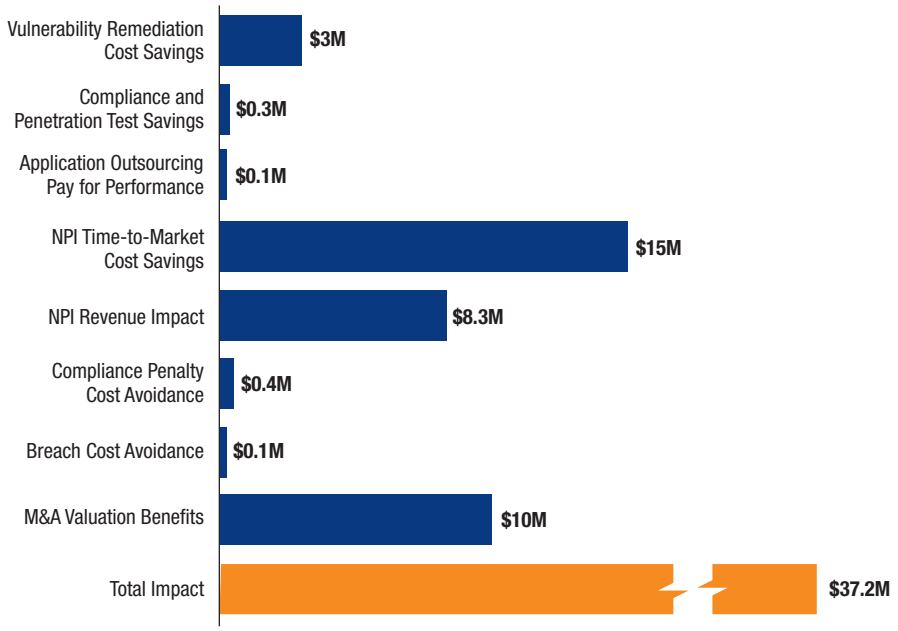
To estimate the expected benefits for an individual company, we recommend upfront research to establish key benchmarks for that organization. These would include the number of applications developed or tested per year, current time-to-fix cycles, and current developer costs, among other metrics.

An accurate benefit estimate will also include a time component. For example, while most of the companies in the study captured benefits within the first year of SSA deployment, many of the more significant benefits weren't realized until the second year, when companies had completed the organizational and process changes necessary to integrate SSA into a comprehensive software development life cycle (SDLC) program.

Global Food Products Company Gains Edge in M&A

Deploying Fortify initially to reduce risk, this food products company is now realizing significant benefits by cutting per-vulnerability fix time from a week to a few minutes and minimizing compliance assessment cycles. Furthermore, by using Fortify to measure the software security level of acquisition targets, the company is negotiating better pricing for M&A deals.

Total Annual Economic Value Potential for SSA[14]



THE JOURNEY TO STRATEGIC SSA

The companies we interviewed took a variety of paths to software security, and some have gone further than others in adopting a comprehensive approach to SSA, including instituting a formal SDLC program. The study identified three stages that organizations typically go through on the path to SSA maturity:

- **Explore.** These organizations deploy an SSA solution across a small number of applications (10–20) and developer teams as a proof-of-concept initiative.
- **Accelerate.** These organizations are moving beyond "toe-in-the-water" pilot programs and are actively incorporating threat detection and remediation techniques across key development teams and applications.
- **Optimize.** These organizations have embedded software security tools, processes, and training within a formal SDLC program. Many are also leveraging SSA solutions in innovative ways to generate additional business value and create competitive differentiation.

The study found that companies reported substantial efficiency gains and risk reduction right out of the gate—at the Explore and Accelerate stage—even before implementing a formal SDLC program. These organizations typically cut vulnerability fix times from 1 to 2 weeks to about 1 day, and saw repeat vulnerabilities drop from 80% to 20%. These operational improvements can lead to operating expense benefits valued at about $2.4 million, the study found.

Getting Over the Hump

An exponential jump in value, however, occurs when companies "graduate" to the Optimize level—that is, when they institutionalize and extend SSA tools and practices throughout the organization and begin to deploy SSA in innovative ways. As we showed above, the payback for some strategic organizations can be 10 times greater, or as much as $37M annually.

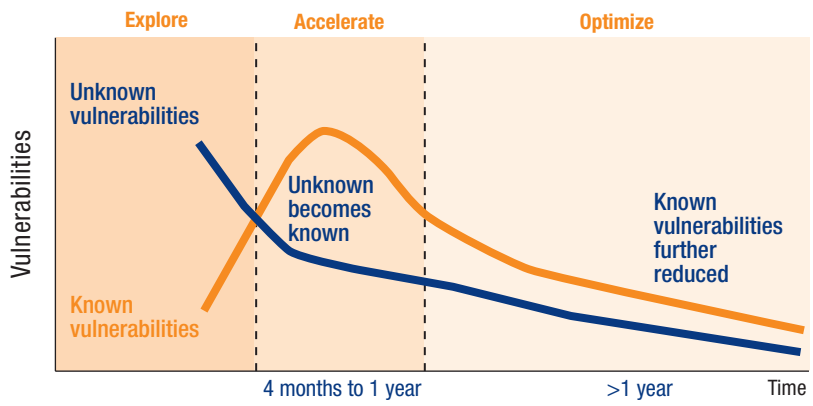
Getting to the Optimize level isn't always easy. During the first four months of an SSA implementation, executives say the number of known vulnerabilities explodes as hundreds or even thousands of previously unknown flaws in the code become known, as shown in the figure below. Getting over this initial "adoption hump" can be daunting. Developers confronting the sheer size of the threat can become caught in a reactive find-and-fix mode—although SSA tools that prioritize and automate remediation efforts can help lighten the workload.

The initial spike in known vulnerabilities can also have a positive effect, serving to spur adoption of SSA solutions across the organization as developers and stakeholders realize the magnitude of the security risk and agree on the need for a systematic solution. Over time, these organizations move beyond the reactive mode and begin proactively institutionalizing SSA tools and practices across development teams, usually as part of an SDLC program. As a result, these organizations learn to write secure code in the first place and encounter fewer and fewer vulnerabilities over time.

"We're buying companies all the time and we need to understand the security posture of the targeted company. By introducing software security as a parameter in deal valuations, we're gaining several million dollars in benefits every year."

CISO, global agriculture products company

Typical SSA Adopter Life Cycle



Furthermore, organizations implementing a full suite of SSA capabilities and practices find that software security solutions can quickly extend beyond software development teams and become a core part of IT operations. In data centers and communications hubs, IT managers are using advanced SSA solutions to monitor live applications and spot emerging vulnerabilities—in effect providing real-time threat protection.

Accelerating Adoption

Securing buy-in from senior IT leadership, including the CIO and the head of application development, is another key to successfully deploying a high-value strategic SSA solution. Without this commitment, there is little likelihood that organizations can realize maximum value from a strategic SSA deployment. To gain support from senior leadership, about 90% of the executives we talked to said that proving SSA's payback potential in the form of a business case or ROI assessment was critical.

Indeed, we found that the most successful SSA programs employed a set of best practices that helped organizations accelerate adoption and derive more value from their solutions. Combining people, process, and technology, these practices include:

People: Drive awareness of SSA by securing support from key stakeholders.

- Communicate the business value of software security to the board of directors.
- Set aggressive goals for applications and developer coverage in the first year.
- Invest in software security education and training.

Process: Drive vulnerability-prevention processes deeper into the development organization.

- Require code scans at strategic checkpoints in the development process—such as during nightly builds—before releasing applications to production.
- Rapidly integrate software security resources with development teams.
- Include software security performance as part of developers' job appraisals.
- Urge adoption of SSA practices by application development partners and track their compliance.

Technology: Integrate SSA into SDLC automation tools.

- Connect SSA tools to a bug-tracking database to improve time-to-fix.
- Integrate SSA solution with audit and compliance tools to accelerate compliance process and maintain audit trails.
- Systematically prioritize vulnerabilities to focus remediation plans and streamline remediation and penetration-testing activities.

Travel Services Company Innovates with SSA

After gaining immediate cost savings from more efficient vulnerability remediation, this company began measuring customer satisfaction with the security of its software products—in effect, using software security as a competitive differentiator. It is also using Fortify to scan code from third-party developers, ensuring high-quality deliverables and favorable fee structures.

CONCLUSION

As the security threat moves from computer-network intrusions to attacks on software applications running in multiple environments, the demand for software security assurance solutions is on the rise. But in a time of tightening IT budgets, security executives are facing increasing pressure to justify investments—even the relatively easy sell of software security—from a cost-benefit perspective.

As this study has shown, SSA solutions not only help companies minimize the risk of a successful cyber attack, but also offer substantial efficiency and productivity benefits that help control costs, speed software development cycles, and in some cases even boost revenue and asset values.

The study shows that organizations realized value from SSA solutions right out of the box just by accelerating vulnerability fixes and compliance testing. For other companies, the value of SSA solutions can be exponentially higher. These organizations are generating more business benefits by extending the solutions to more applications and teams, and by embedding security controls and best practices throughout the development lifecycle.

What should organizations look for in a SSA solution? Our review of 30 software security providers found that not all vendors offer the same functionality and services. When evaluating the options, organizations should look for an SSA value-maximizing solution that:

- Offers both deep remediation functionality and a breadth of supporting services.
- Provides support for cross-team collaboration—bringing information security teams, developers, risk officers, and auditors together in a coordinated effort.
- Seamlessly integrates with existing application life-cycle management (ALM) and development environments, shortening time to remediation.
- Provides in-depth guidance on how to correct each security vulnerability, thus accelerating remediation further.
- Offers robust governance capabilities, including the ability to define and communicate security policies and rules across the organization.
- Provides research on the latest threat trends and techniques, ensuring that teams are aware of all emerging threats.

For help in understanding the full potential of Software Security Assurance solutions in your organization, go to www.fortify.com/ssa-basics/overview/index.html. For information on Fortify 360 and other products and services from Fortify, go to www.fortify.com.

"Today, every developer is required to do a threat analysis before writing the first line of code. We've made software security an important part of their job description and performance review."

Manager, Information Protection, leading energy company

APPENDIX: RESEARCH INTERVIEWS

To more clearly understand the economics of software security, Mainstay Partners conducted more than 20 interviews with information security leaders, including 7 chief information security officers (CISOs) and 10 information security managers and directors. Seventeen private- and public-sector organizations were studied, spanning a cross-section of industries and geographic regions.

- **Industries studied:** financial services, high technology, transportation, services, healthcare, agriculture, and telecommunications
- **Regions:** North America, Europe, Asia Pacific
- **Company size:** $1–5B (30%), $5–25B (29%), >$25B (41%)

The interviews addressed various aspects of software security objectives, strategies, and implementation, along with the specific benefits of Fortify solutions. Data gathered from these in-depth interviews formed the basis for the business value estimates presented in the study.

END NOTES

[1] The reduction in remediation time is due to several factors, including SSA capabilities and practices that (1) pinpoint the exact location of a flaw in the code lines, (2) prioritize vulnerabilities to focus resources on the most critical flaws, and (3) provide guidance on how to correct each vulnerability.

[2] Estimate based on a conservative 10 vulnerabilities per application, and 67 critical applications.

[3] Mandates and standards commonly impacting application development projects include: the Payment Card Industry Data Security Standards (PCI DSS), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPPA), and North American Electric Reliability Corporation (NERC) standards.

[4] Assumes 50% reduction in penetration testing effort; legacy environment costs are based on an average of eight penetration tests per year at $67K per test.

[5] See "Top 10 Data Breaches and Blunders of 2009," *eSecurity Planet*: http://www.esecurityplanet.com/views/article.php/3863556/Top-Ten-Data-Breaches-and-Blunders-of-2009.htm.

[6] Fourth Annual U.S. Cost of Data Breach Study, Ponemon Institute, 2009.

[7] Assumes that the average company would experience a major data breach once every 10 years.

[8] Assumes that an average penalty period would last six months. Research indicates that penalties make up only 30% of the full impact of non-compliance ("Industry View: Calculating the True Cost of PCI Non-Compliance," Ellen Lebenson, CSO Online).

[9] Assumes a non-compliance period lasting six months. Average penalty periods range from 3 to 24 months.

[10] Assumes average fee discounts of 1% applied to annual outsourced development expenditures of $10M.

[11] Estimate assumes a $20B company earning 1.25% of its profit per quarter from new product sales; 50% of product introductions are assumed to benefit from SSA efficiencies, which help avoid an average of four critical vulnerabilities per product and 30 days of delays.

[12] Estimate assumes a $20B company incurring new product development costs equal to 3% of revenue; 50% of new products, or $300M in expenses, are assumed to be impacted by SSA efficiencies, which help avoid an average of four critical vulnerabilities per product and 30 days of delays; the resulting 5% productivity increase saves $15M in development expenses.

[13] Sample customer assumptions include: $20B customer, 10% new product revenue contribution; 50% first year margins; two-month product delay due to vulnerabilities; 500 critical/severe vulnerabilities; $3.8M cost per breach @ 10% probability; $200M in M&A @ 5% valuation benefits.

[14] Estimate assumes an average deal discount of 5% from SSA code analysis.

mainstay partners

making technology investments count

Mainstay Partners LLC
www.mainstaypartners.net

901 Mariners Island Blvd, Ste. 105
San Mateo, California 94404-1592
(p) 650.638.0575 (f) 650.638.0578

Research and analysis for this study was conducted by Mainstay Partners LLC, an independent consulting firm that has performed over 300 studies for leading information technology providers including Cisco, Oracle, SAP, Microsoft, Dell, Lexmark, HP, EMC and NetApp.

This case study was based on interviews with security executives currently using SSA solutions. Information contained in the publication has been obtained from sources considered reliable, but is not warranted by Mainstay Partners LLC.