mainstay partners

making technology investments count

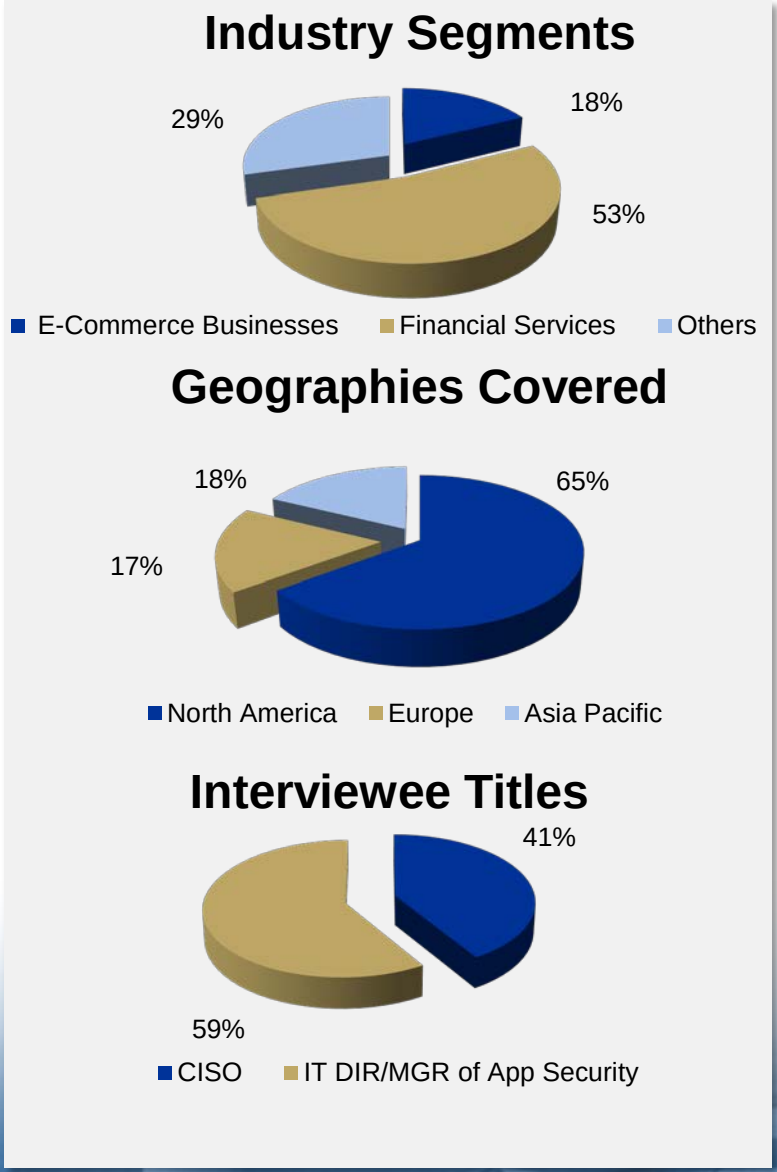
SSA Return on Investment Research Results

November 2010

Agenda

- Research Background
- ROI Benefit Framework & Findings
- The ROI Journey
- Use Cases

Project Background



- Objective: provide an independent analysis of Software Security Assurance's (SSA's) business impact
- Research gathered results from 17 Fortify customers globally
  - Global Financial Services, Government Agencies, and Fortune 500 Enterprises
- Interviewed senior IT leadership including Chief Information Security Officers (CISOs) and IT Security Directors
- All customer data has been blinded to respect confidentiality

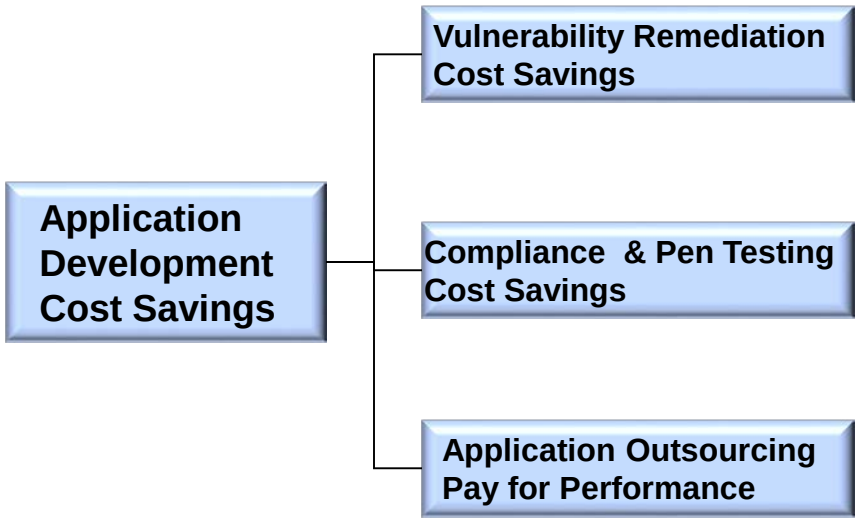
Research Methodology

- Interviewees were asked a series of qualitative and quantitative questions regarding:
  - Business/IT challenges pre-SSA
  - Pre-SSA software security business practices
  - Decision factors in making the SSA investment
  - Strategic/Operational/Financial benefits from deploying SSA
  - Operational/Financial Metrics used to track software security efficacy
  - Innovative uses/benefits of SSA
  - Key deployment lessons learned/best practices
- Most customers did not perform a detailed SSA business case or audit SSA benefits, limiting detailed financial data
  - Common benefit drivers, annual impact levels, and value tree frameworks are developed by consolidating customer proof points across interviews
  - External research was conducted to support customer benchmarks

Agenda

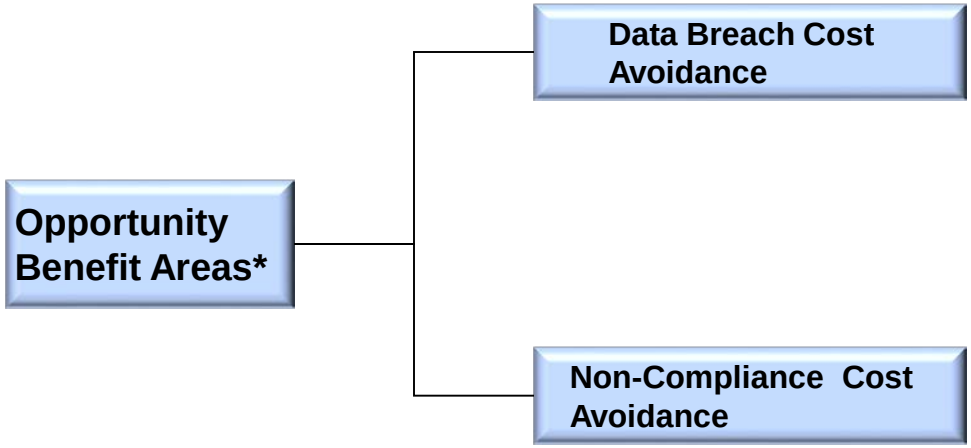
- Research Background
- ROI Benefit Framework & Findings
- The ROI Journey
- Use Cases

SSA contributed to significant annual development expense cost savings



- Streamline & minimize remediation costs for application development by identifying /fixing vulnerabilities at their origin
- Lower costs associated with compliance testing fees and penetration testing
- Decrease 3rd party development fees by incenting software security performance

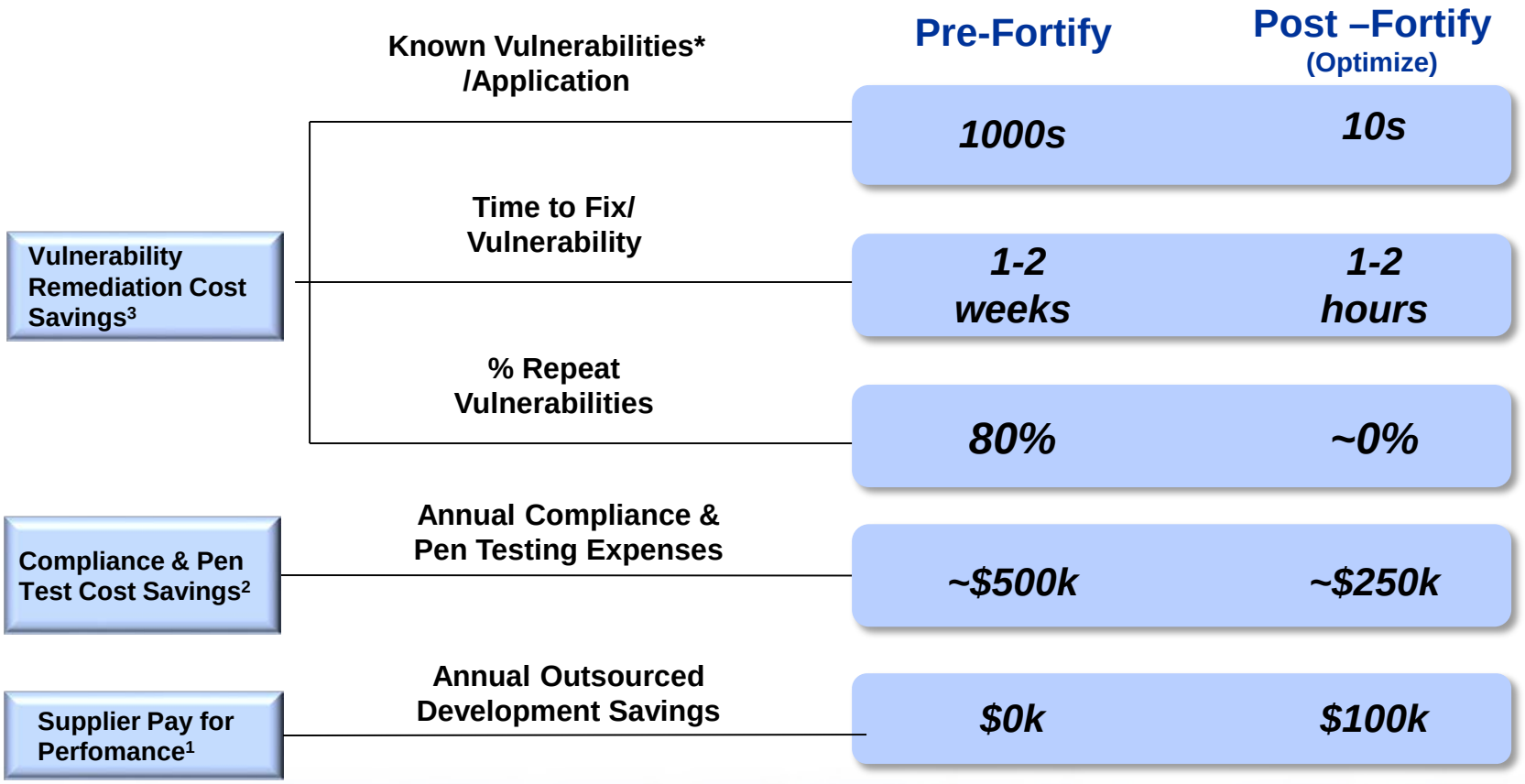
Opportunity cost savings areas included breach & compliance cost avoidance



- Minimize risks of reputational/brand impact & costs to remedy a breach (e.g., legal fees, customer churn, investigative costs, fix costs)
- Reduce the costs associated with non-compliance to mandated security standards (e.g., penalties, customer churn, forensic investigation costs, fix costs)

** Opportunity benefit areas may not apply to all companies*

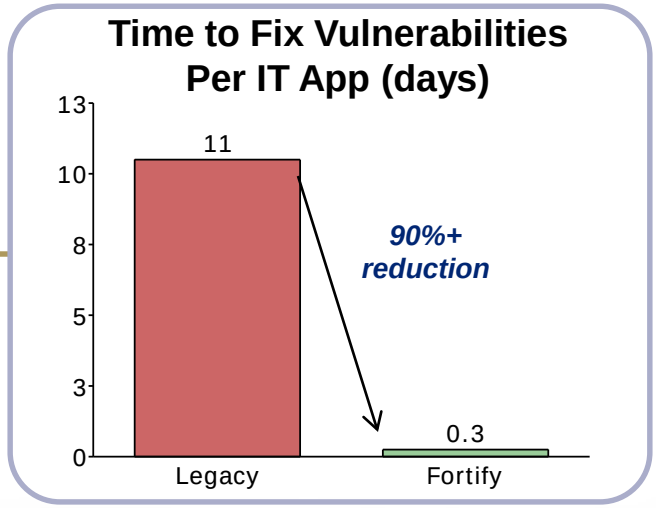
Benchmarks were captured from our interviews to help assess the full potential of SSA's impact



** Customers were only aware of 100s prior to SSA; majority of vulnerabilities were "unknown"*
1 – Benchmarks based on 1 customer proof point
2 – Benchmarks based on 4 customer proof points
3– Benchmarks based on 14 customer proof points

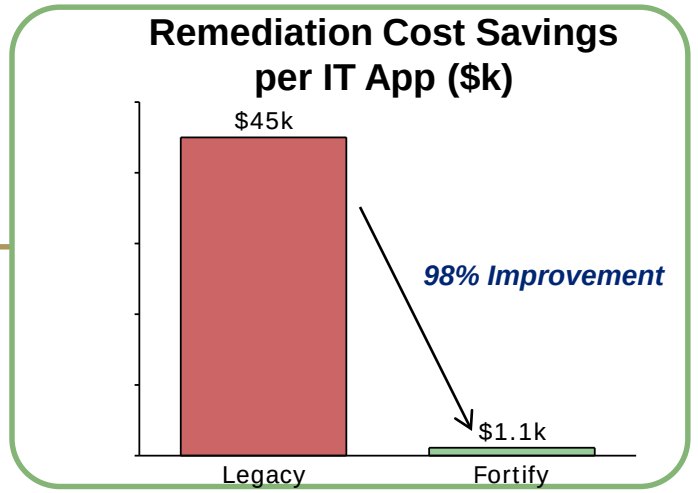
Application development cost savings included vulnerability remediation,

Vulnerability Remediation Application Development



By identifying the vulnerabilities earlier in the development cycle, the time to fix an error went from 1-2 weeks to 1-2 hours

Vulnerability Remediation Application Development

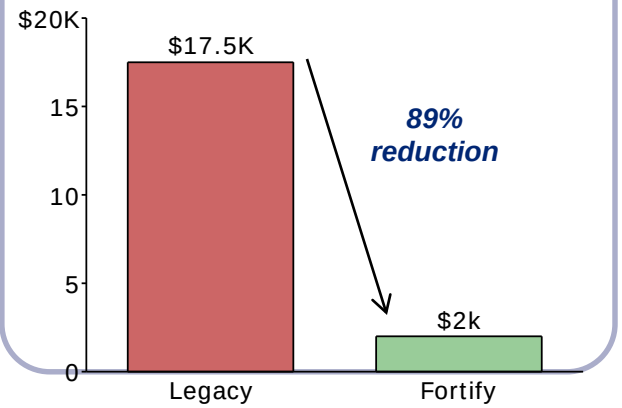


Applying these benefits, companies can save $44k annually, per application (based on a conservative assumption of 10 vulnerabilities/application)

…compliance & penetration testing,

Compliance Testing Fee Savings

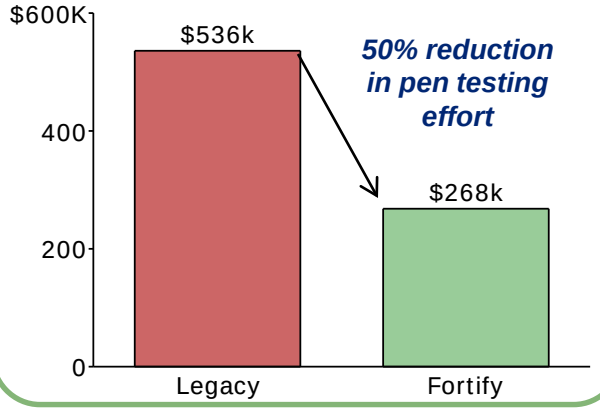
Auditor Compliance Fee Savings ($k)



The frequency of compliance testing and audit trail of results reduces the auditor compliance consulting fees by 89%

Penetration Testing Fee Savings

Penetration Testing Fee Savings ($k)



Penetration testing was reduced by 50% or more. Companies surveyed typically performed 5-25 penetration tests annually at a cost ranging from $25k-100k per test. Improved awareness, education, quality of code and automated testing reduced testing effort & in some cases reduced frequency of tests.

… and for an avant-garde organization, reduced third party development expenses

Supplier Pay for Performance

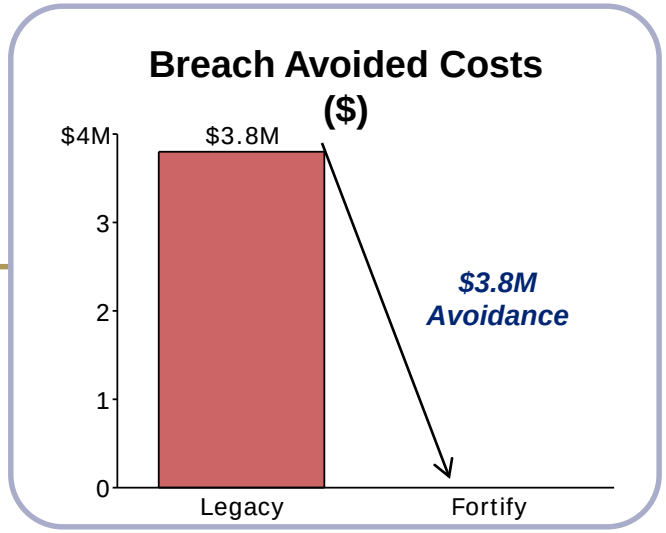
Supplier Pay for Performance ($k)

Application Development Annual Outsourcing Expenses	$10M
Average Fee Discount from SSA*	1%
Average Outsource Application Development Savings from SSA	$100k

*** Performance based fee arrangements for 3rd party development lowered overall costs**

Additionally, opportunity cost savings were discussed such as breach or non-compliance cost avoidance

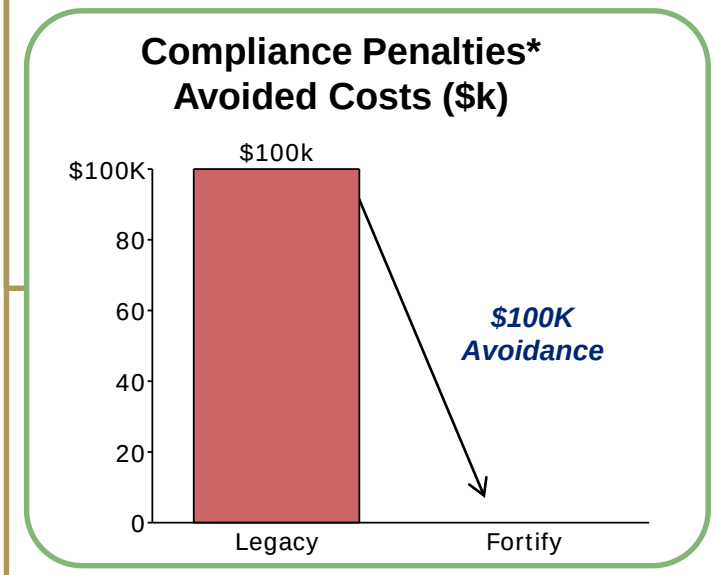
Breach Remediation Avoided Costs



Breach costs include legal fees, customer churn, remediation costs and disclosure expenses for public response. Research estimates the median breach cost at $3.8M* or $204 per compromised record

* Fourth Annual US Cost of Data Breach Study, Ponemon Institute, 2009

Non-Compliance Avoided Costs

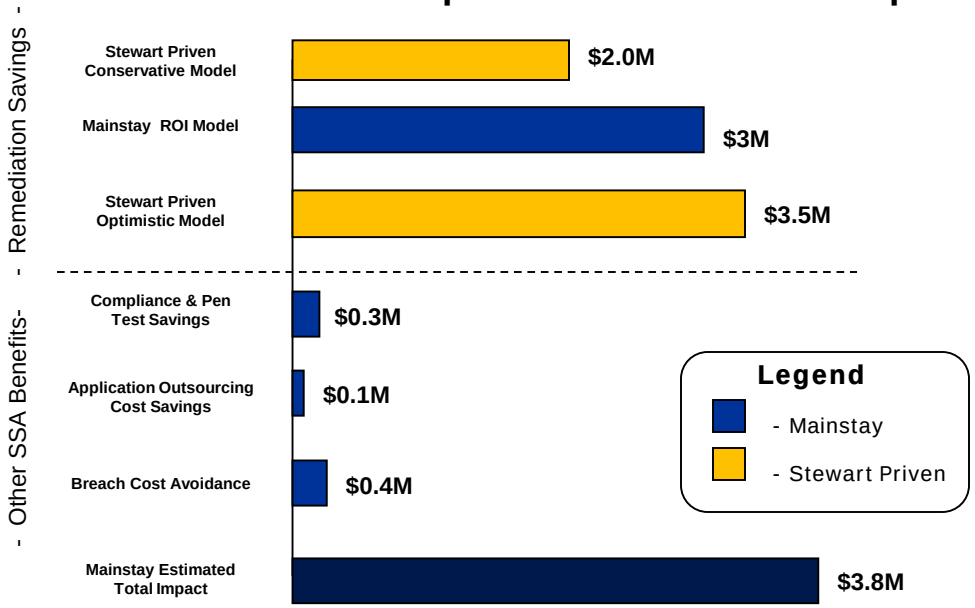


Non-compliance costs include penalties, fines, remediation costs. Conservative estimate based on PCI example which on average can last 3-24 months. At 6 months, penalties could reach $100k

* Source: "Industry View: Calculating the True Cost of PCI Non-Compliance", Ellen Lebenson, CSO Online

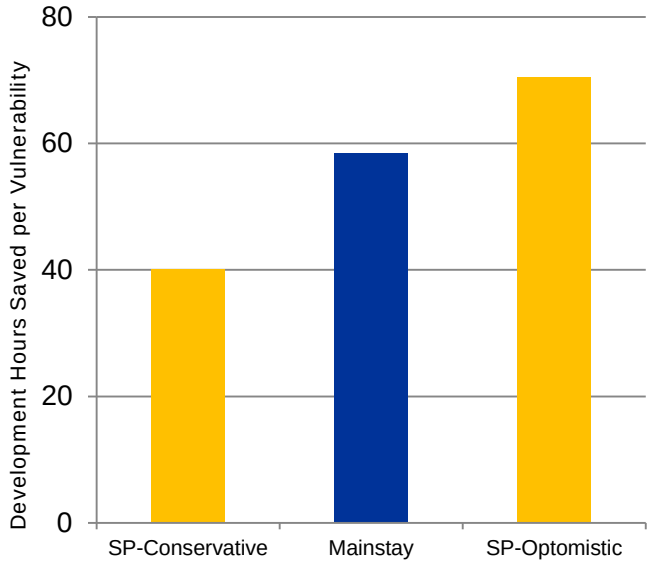
Annual SSA Total Economic Value Opportunity for Government – Comparative Analysis

Annual SSA Economic Impact – Government Example*



- Stewart Priven application development savings calculated using common assumptions (e.g., # of vulnerabilities, cost per hour)
- Mainstay application productivity estimates derived from 17 Fortify customer interviews
- Conservative assumptions taken for compliance, pen testing and pay for performance savings
  - For example, breach estimates only a 10% chance of an occurrence to reduce the $3.8M/event cost to only $0.4M per annum

Comparative Analysis Mainstay & Stewart Priven (SP) Models



- Stewart Priven conservative model estimates an average 40 hour savings from identifying the vulnerabilities primarily during code/unit testing and at government/acceptance testing
- Stewart Priven optimistic model estimates an average 70 hour savings from identifying the vulnerabilities primarily before or during code/unit testing
- Mainstay estimates found an average 58 hour savings by moving to primarily code/unit testing identification

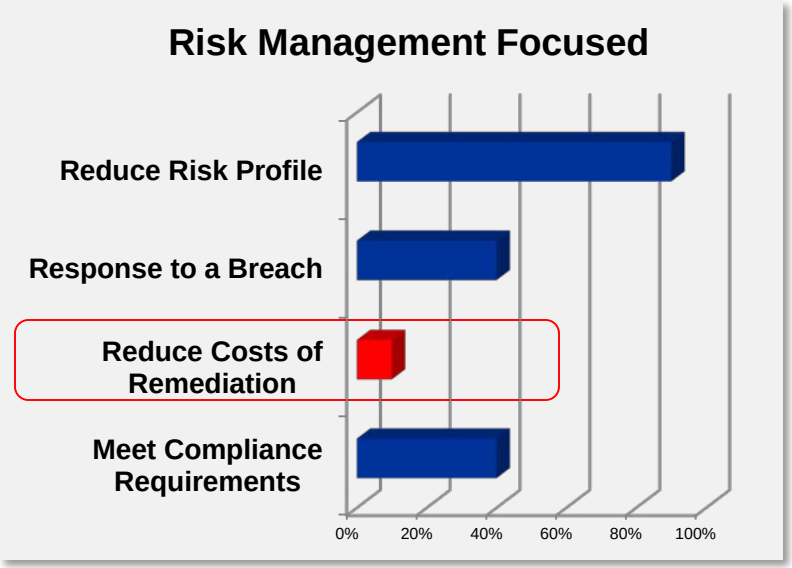
* Sample Agency- Assumptions; 500 critical/severe vulnerabilities; $3.8M cost per breach – 10% probability;

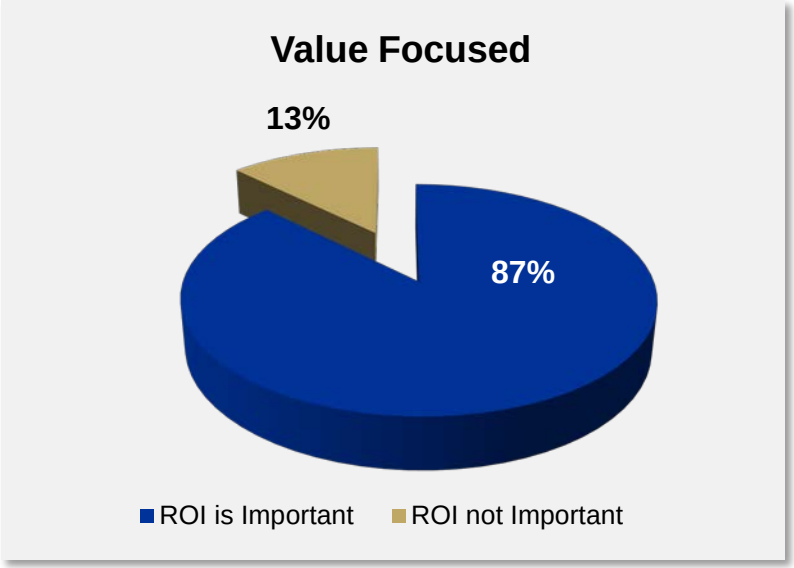
* Stewart-Priven Modeling: 2009 Presentation to PMI-MHS "Software Inspection Success"

Agenda

- Research Background
- ROI Benefit Framework & Findings
- The ROI Journey
- Use Cases

Initially selected for risk management, SSA proved to be a value creating investment

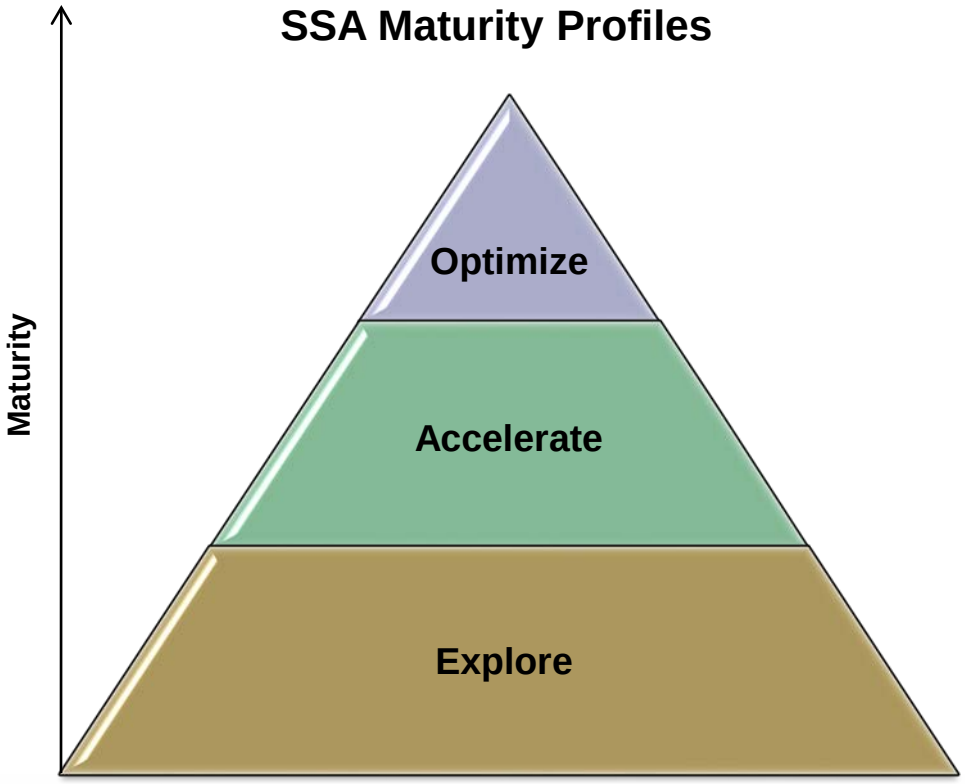




- SSA was viewed as a tool to identify and fix vulnerabilities
- No coherent security strategy, program or process prior to SSA
- No plans to build a comprehensive set of benefit metrics to define or quantify success at outset of the investment

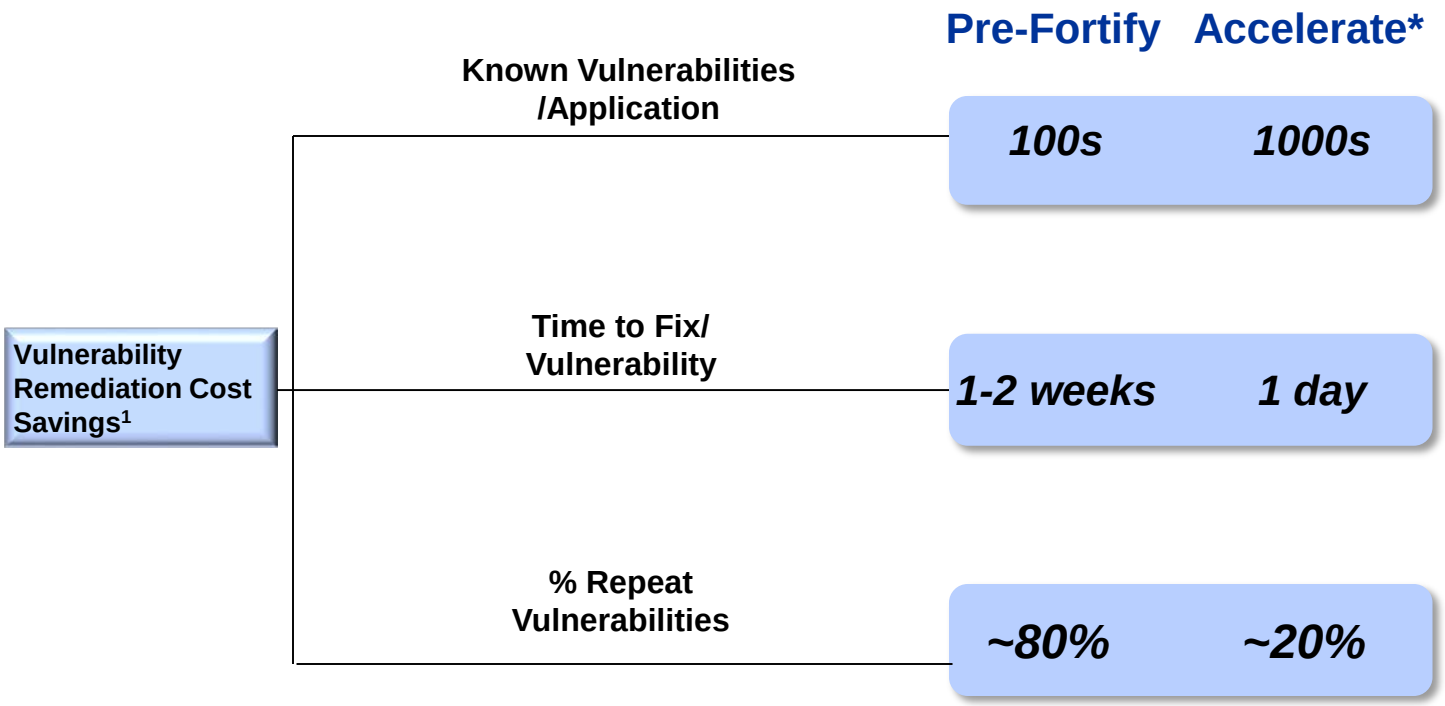
- Required acceptance from CIO & VP of Application development –outside of the security team's responsibilities
- Adoption required a 360 view of software security – people, process and technology transformation
- Nearly all security teams recognized the need for a business case/benefits analysis to gain adoption

Correspondingly, SSA's value to the organization matured over time



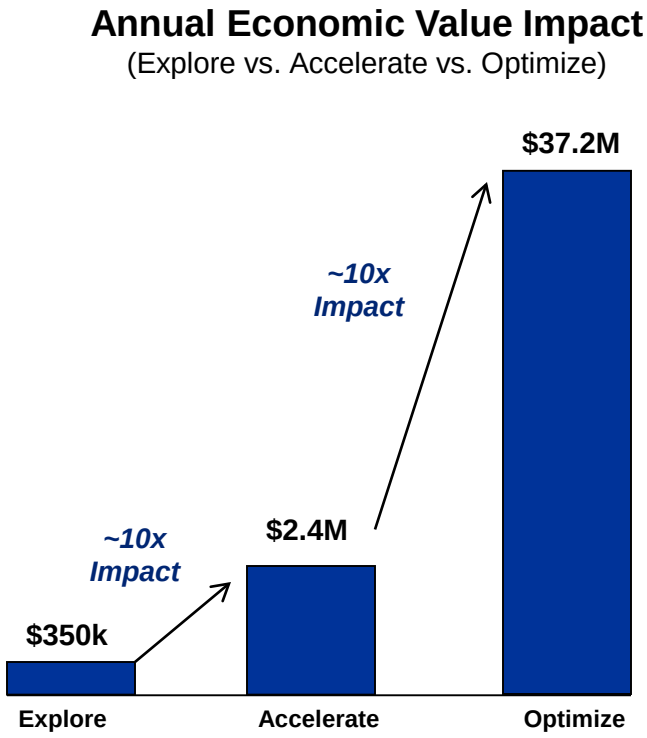
- **Explore**- Customers deployed SSA initially to uncover nearly 90% of the vulnerabilities hidden to the development teams. Started with a small set of applications for a pilot
- **Accelerate**- After the successful pilot, SSA was expanded to include the company's most critical applications
- **Optimize**– SSA was embedded into the software development lifecycle (SDLC) process to eliminate repeat issues and further streamline remediation efforts

Initial SSA benefits were focused on reducing vulnerability remediation costs



1 – 14 customer proof points
** Explore benchmarks were similar to Accelerate benchmarks but applied to a smaller set of applications*

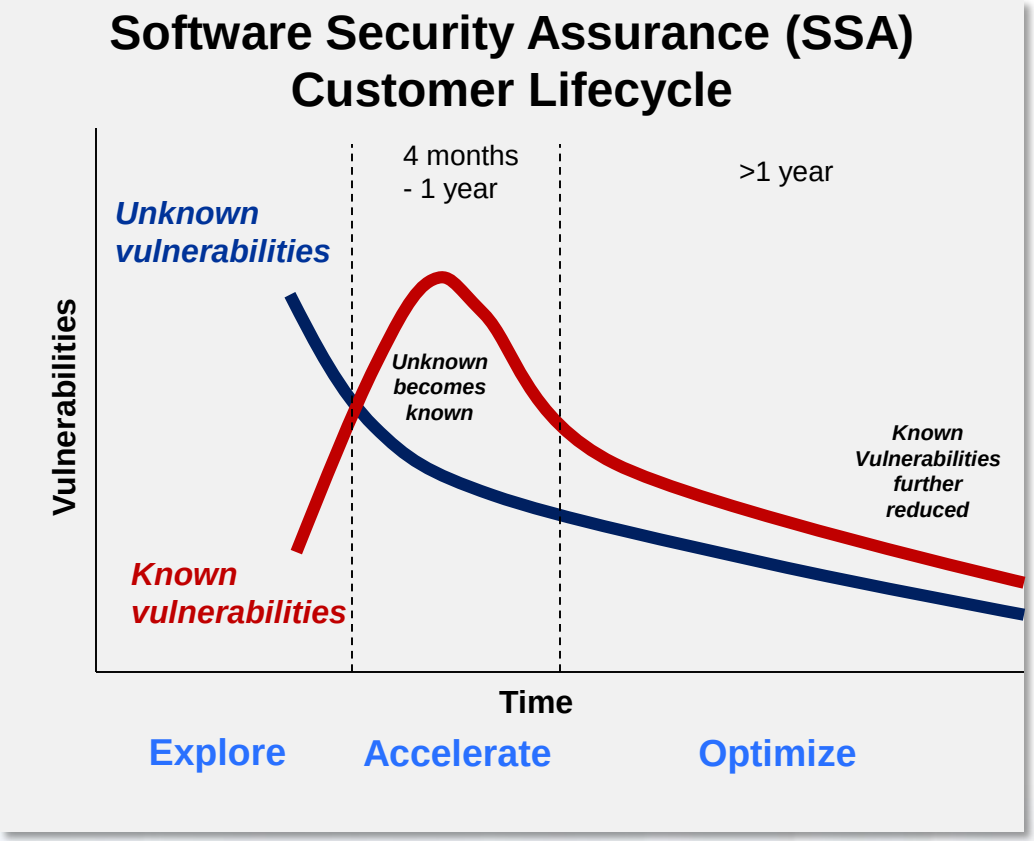
SSA customers were achieving exponential benefits as they matured



- "Explore" customers achieve out-of-the-box benefits by reducing vulnerability remediation costs in the piloted applications
- "Accelerate" customers scale these savings, leading to 10x value and payback in under 12 months
- Additional10x+ value realized when "Optimize" companies embed SSA into their SDLC

*** Sample Customer - Assumptions include: "Explore" deployment to 10 Applications; $20B customer; 500 critical/severe vulnerabilities;$100k Annual Pen/Compliance OPEX**

A common challenge to reaching "Optimize" is overcoming the **Vulnerability Speed Bump**



- The large number of unknown vulnerabilities discovered in "Explore" helped to accelerate adoption
- However, companies also became bogged down in fixing vulnerabilities – slowing their migration to "Accelerate"
- Best practice companies were able to pass over the "Vulnerability Speed Bump" developing the business case to **PREVENT** future vulnerabilities

Security teams successfully navigated to “Optimize” through a set of common best practices

PEOPLE

- **Secure top management commitment & invest in stakeholder education**
  - Provide board-level visibility to application security results
  - Set aggressive goals for applications and developer coverage in Year 1
  - Invest in application security education/ training for developers

+

PROCESS

- **Drive internal process and organizational change**
  - Mandatory requirements for acceptable risk in applications before deployment
  - Rapidly move from a centralized application security team to ‘local integration with developers’
  - Incorporate adherence to application security standards in developers’ appraisals

+

TECHNOLOGY

- **Integrate SSA into Application Lifecycle Management**
  - Embed SSA into SDLC automation tools
  - Link SSA into audit/compliance tools to automate and ensure audit trail
  - Integrate SSA into operational management tools (production)

Agenda

- Research Background
- ROI Benefit Framework & Findings
- The ROI Journey
- Use Cases

Govt. Agency - Showcases Benefits For Larger Rollout & Adoption

Government Agency

Objective	Adoption	Finding & Fixing	How it is leveraged
Overall security and risk strategy included SSA to bolster application security	*Initially positioned a small experiment in one department.* *Security-related application delays have reduced by 50% and the success has been leveraged to gain acceptance by other departments*	*From no scans to once a month for critical applications (50% of applications) and every 3 months for the remaining apps* *Found 100 times more vulnerabilities. Fixing effort went from a few days to a few hours. 20 hours of compliance savings*	*SSA leveraged as a proof of concept to make the case for institutionalizing within the organization*

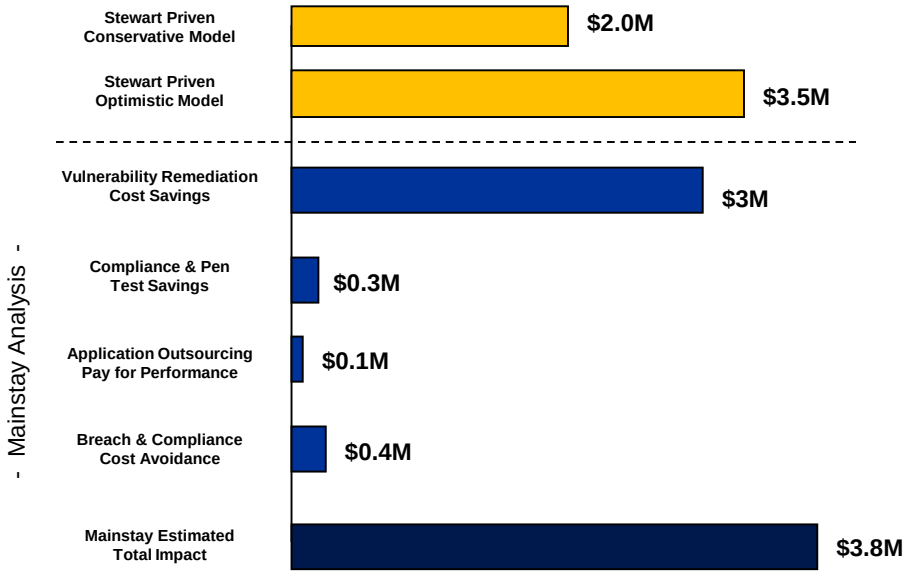
Maturity Level: Explore

Proof of concept was deployed to a few application teams identifying 100x vulnerabilities, greater visibility accelerating adoption

Appendix

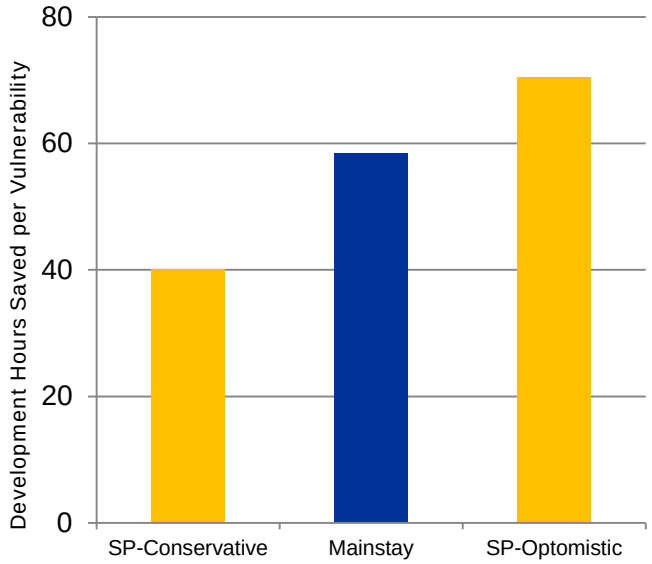
Annual SSA Total Economic Value Opportunity for Government – Comparative Analysis

Annual SSA Economic Impact – Government Example*



- Stewart Priven application development savings calculated using common assumptions (e.g., # of vulnerabilities, cost per hour)
- Mainstay application productivity estimates derived from 17 Fortify customer interviews
- Conservative assumptions taken for compliance, pen testing and pay for performance savings
  - For example, breach estimates only a 10% chance of an occurrence to reduce the $3.8M/event cost to only $0.4M per annum

Comparative Analysis Mainstay & Stewart Priven (SP) Models



- Stewart Priven conservative model estimates an average 40 hour savings from identifying the vulnerabilities primarily during code/unit testing and at government/acceptance testing
- Stewart Priven optimistic model estimates an average 70 hour savings from identifying the vulnerabilities primarily before or during code/unit testing
- Mainstay estimates found an average 58 hour savings by moving to primarily code/unit testing identification

* Sample Agency- Assumptions; 500 critical/severe vulnerabilities; $3.8M cost per breach – 10% probability;

* Stewart-Priven Modeling: 2009 Presentation to PMI-MHS "Software Inspection Success"