Application Security: Protecting Your Applications Against Exploit.

What can I do ASAP, this quarter, this year?

Paul Kitor
Security Solution Architect

HP Enterprise Security Products

Agenda

Protecting Your Applications Against Exploit

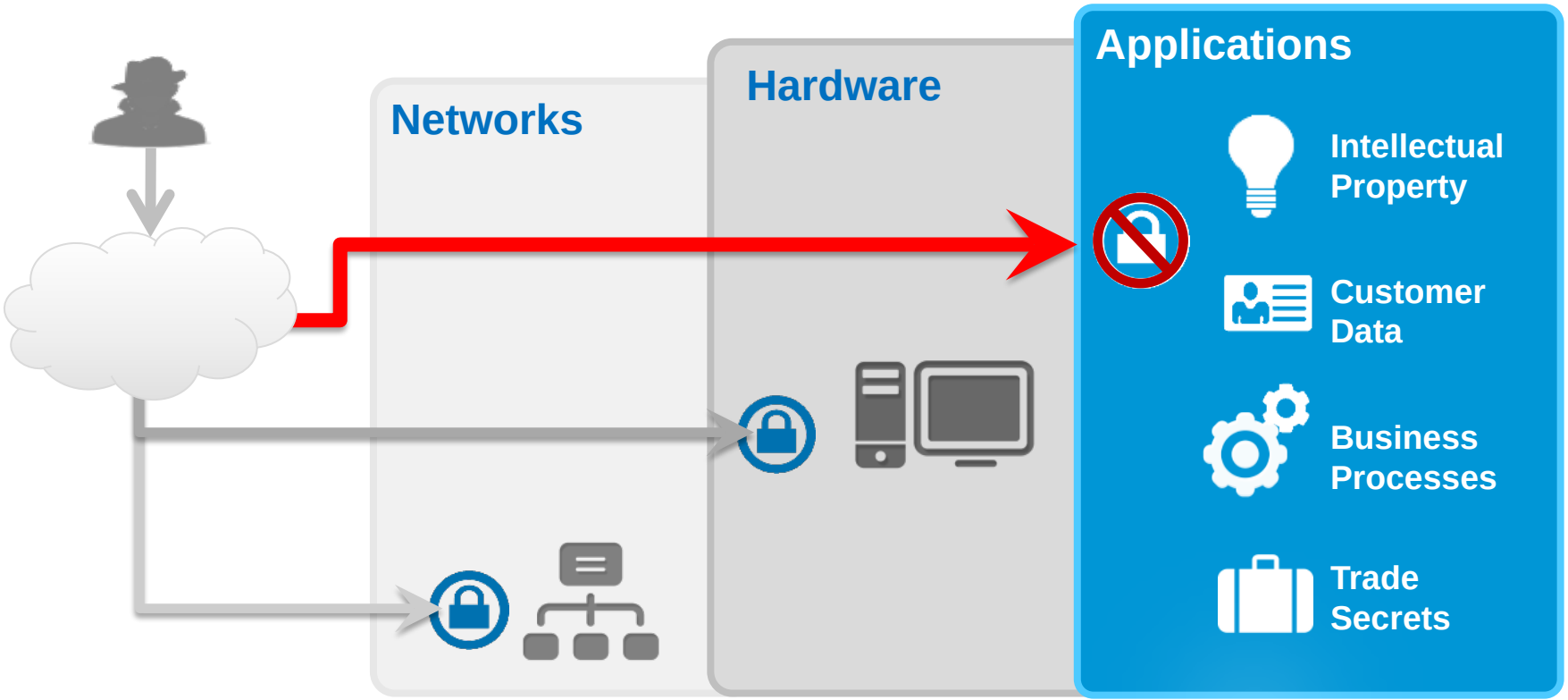
Why Application Security?

Protection / Assessment / Prevention

Software Security Assurance

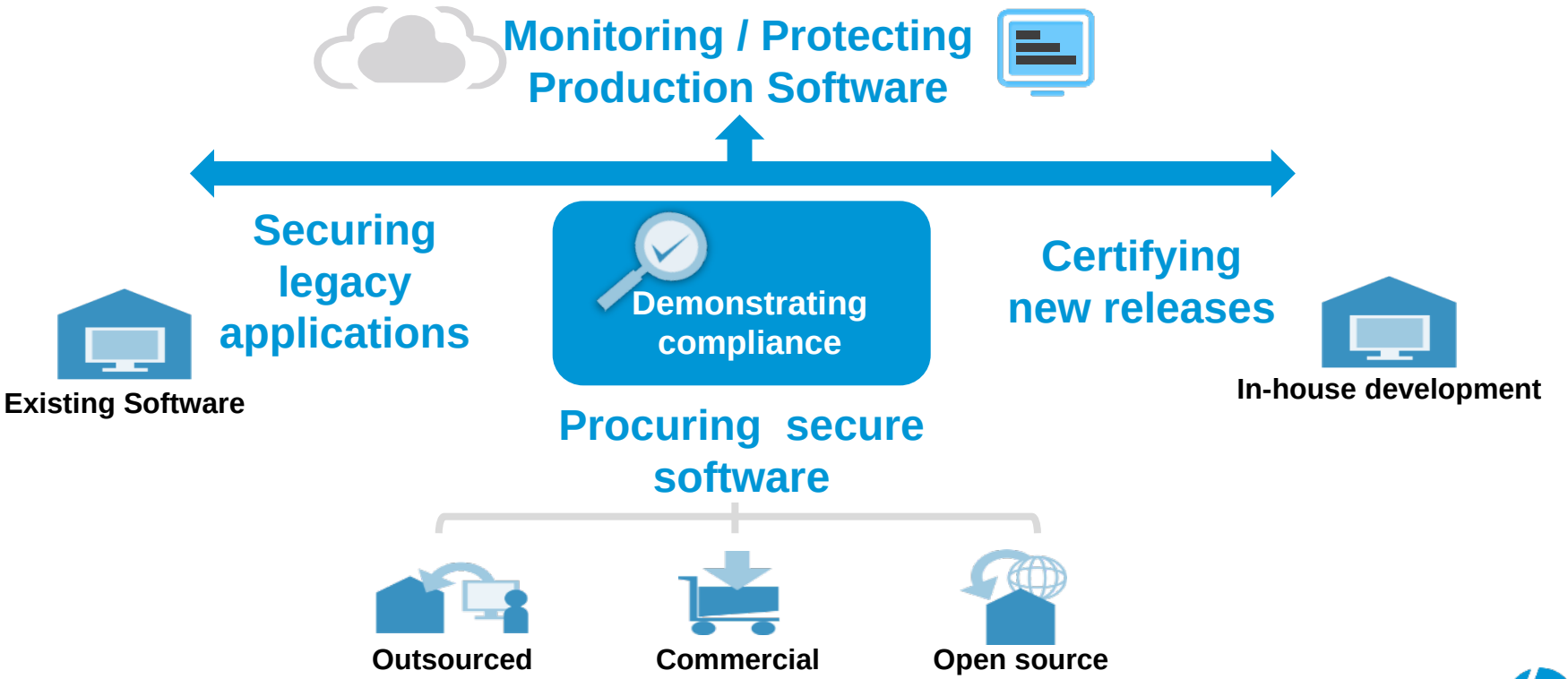
The Application Security Problem

Cyber attackers are targeting applications

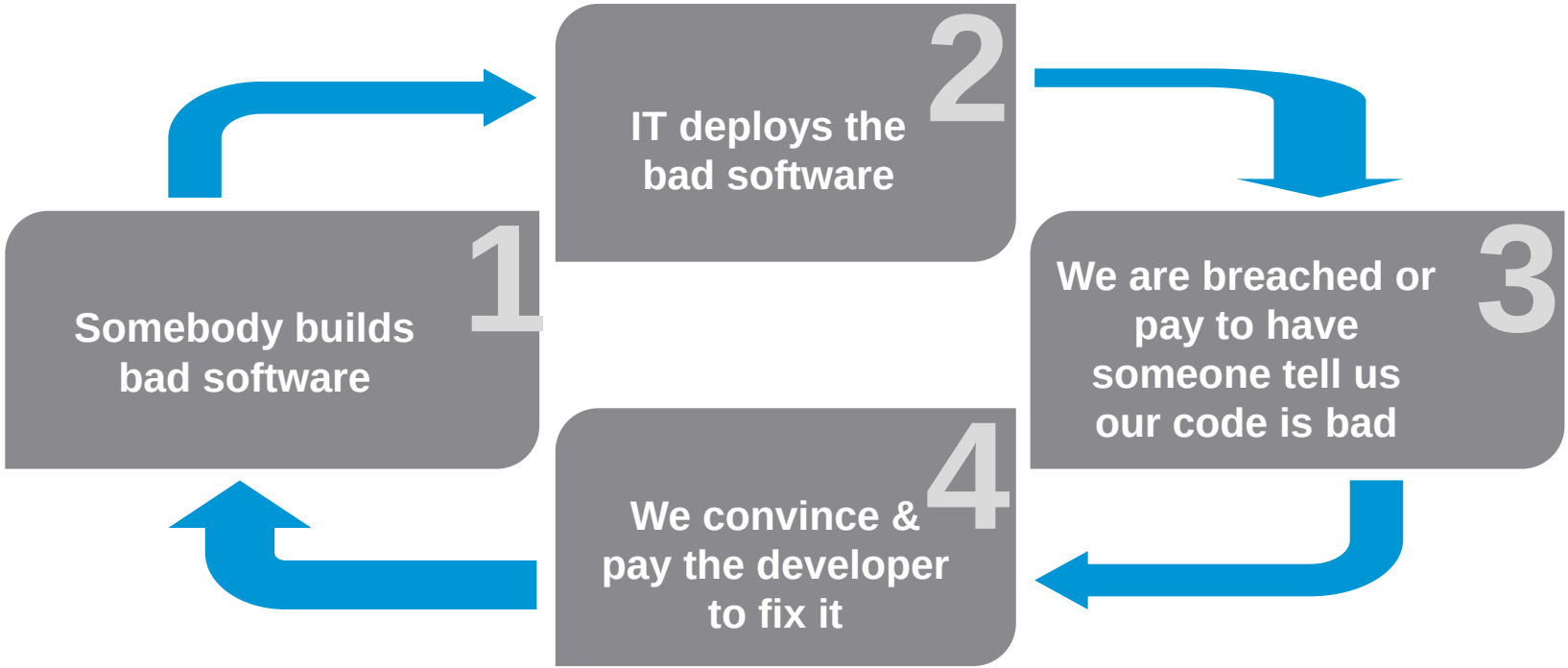


84% of breaches occur at the application layer

Application security challenges

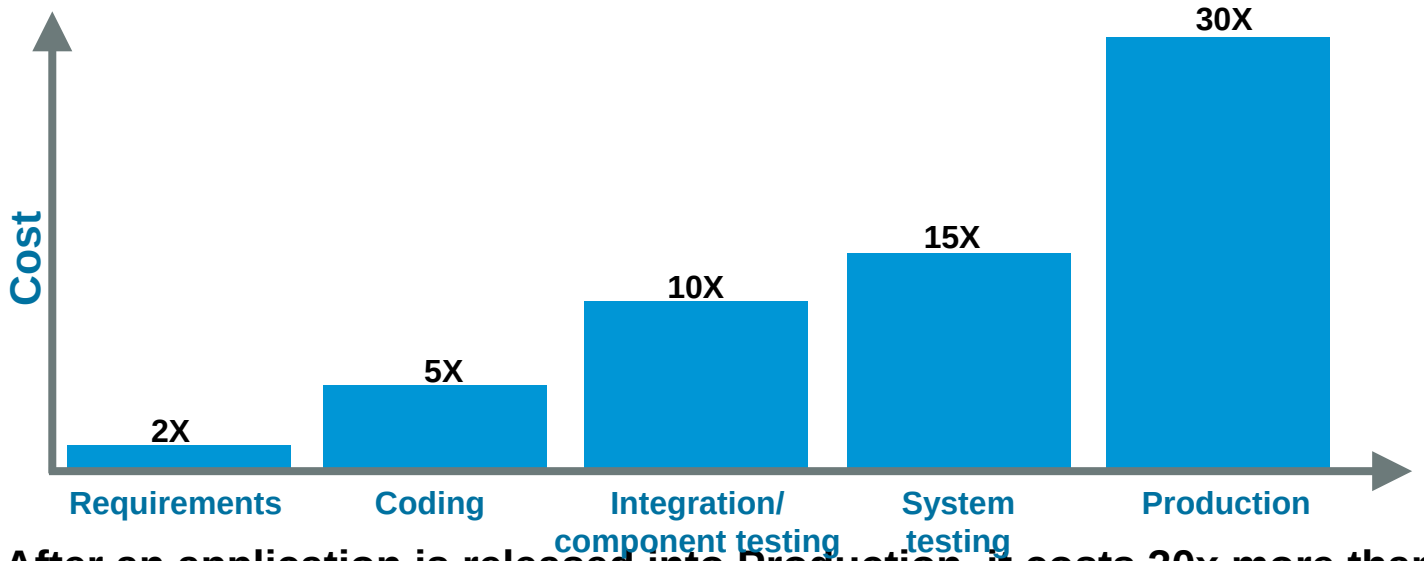


Today’s approach > expensive, reactive



Why it doesn’t work

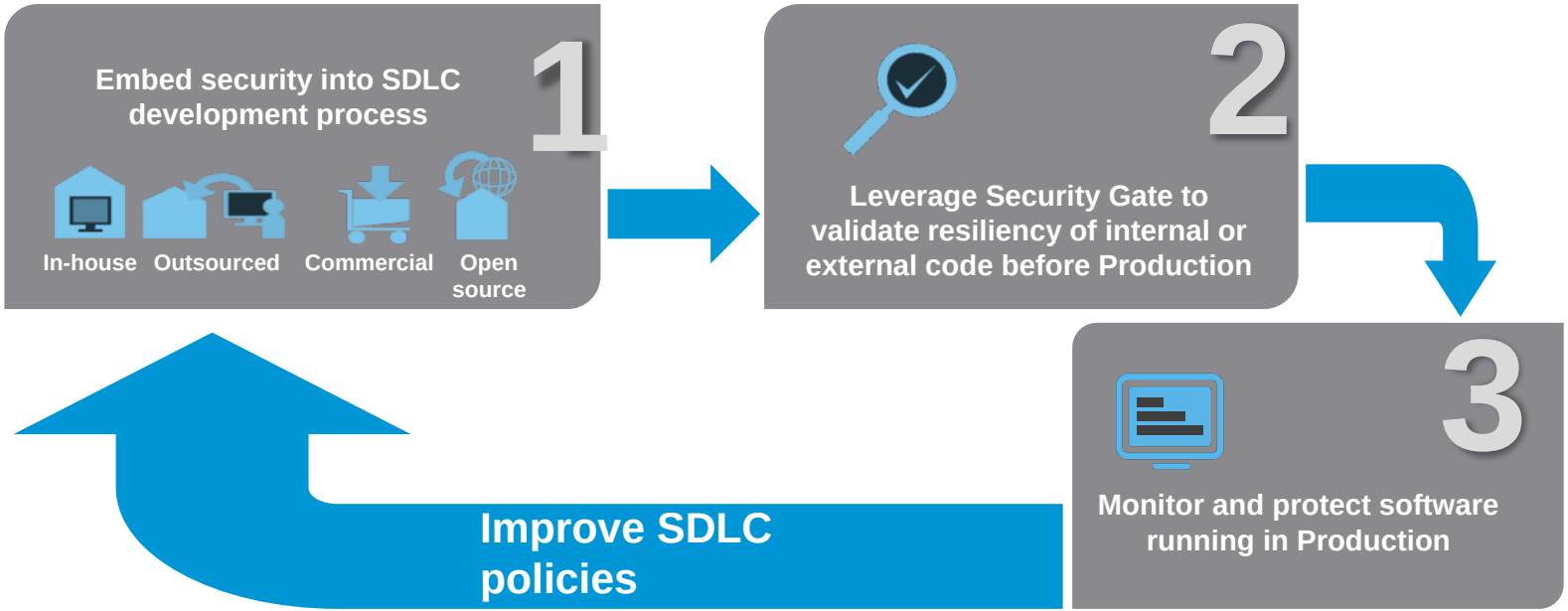
30x more costly to remediate in production



After an application is released into Production, it costs 30x more than during design.

Source: NIST

The right approach > systematic, proactive



This is application security

Agenda

Protecting Your Applications Against Exploit

Why Application Security?

Protection / Assessment / Prevention

Software Security Assurance

The HP Fortify Software Security Vision

Application Protection

Application Assessment

Software Security Assurance (SSA)

Protect

Fortify applications against attack in production

Logging, Threat Protection

Assess

Find security vulnerabilities in any type of software

Mobile, Web, Infrastructure

Assure

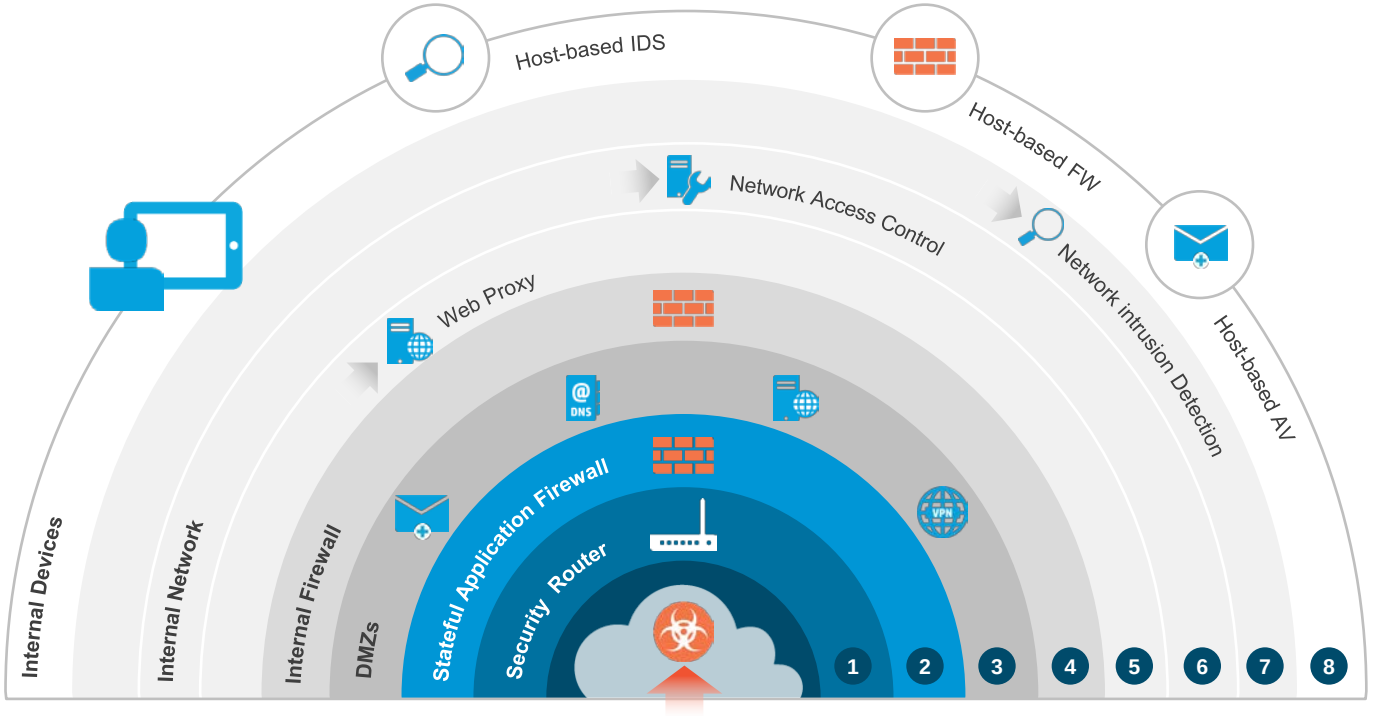
Fix security flaws in source code before it ships

Secure SDLC

What can I do ASAP?

The solution: Protection

Current solutions protect the perimeter



*Yet, **84%** of breaches occur in the application software*

Runtime Application Self-Protection

Runtime application self-protection (RASP) is a security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks.

Protect

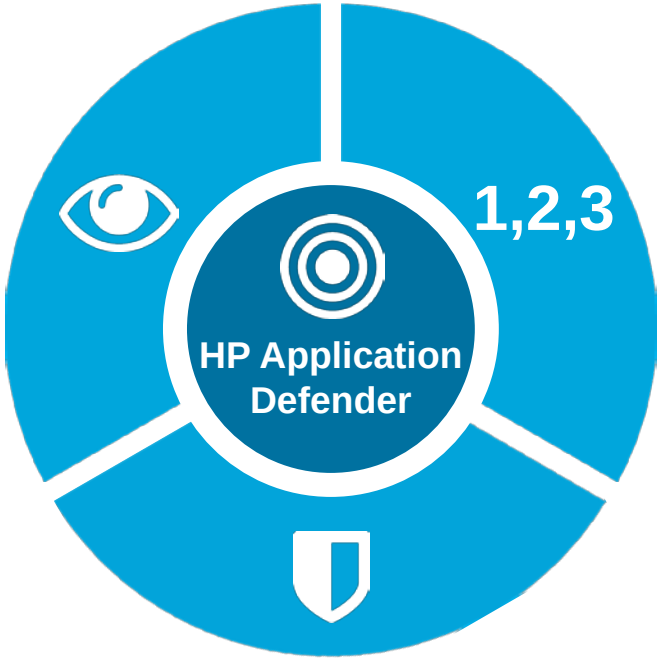
Fortify applications against attack in production

Logging, Threat Protection

HP Application Defender – Application Security Simplified

Visibility

Actionable information through interactive dashboards and alerts



Simplicity

Install quickly and easily with a three-step deployment, get protection up and running in minutes

Protection

Stop attacks from inside the application.

We stop what no one else can even see

HP Application Defender Solution

Simplicity

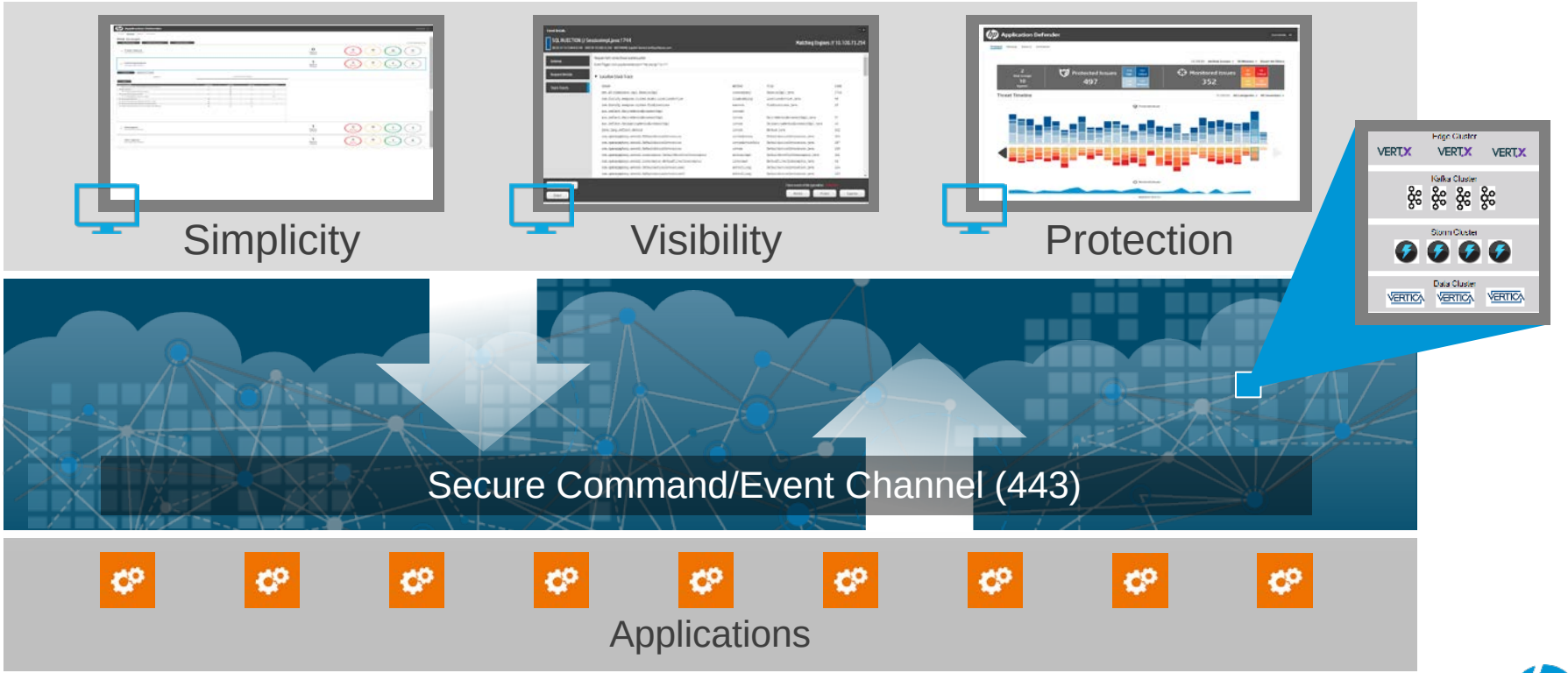
Visibility

Protection

Secure Command/Event Channel (443)

Applications

HP Application Defender Solution

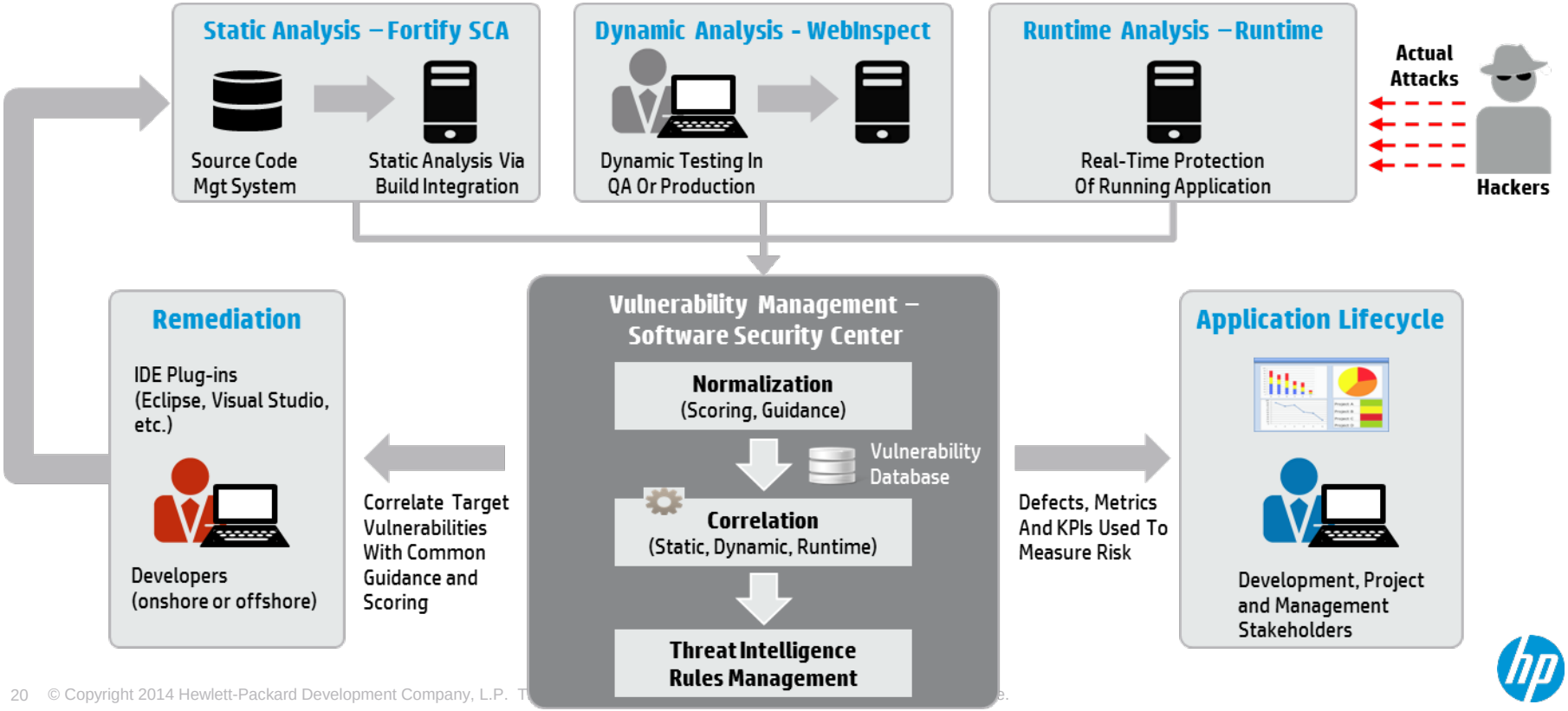


What can I do this Quarter?

Assessment

HP Fortify – Software Security Assurance

On-Premise and On-Demand

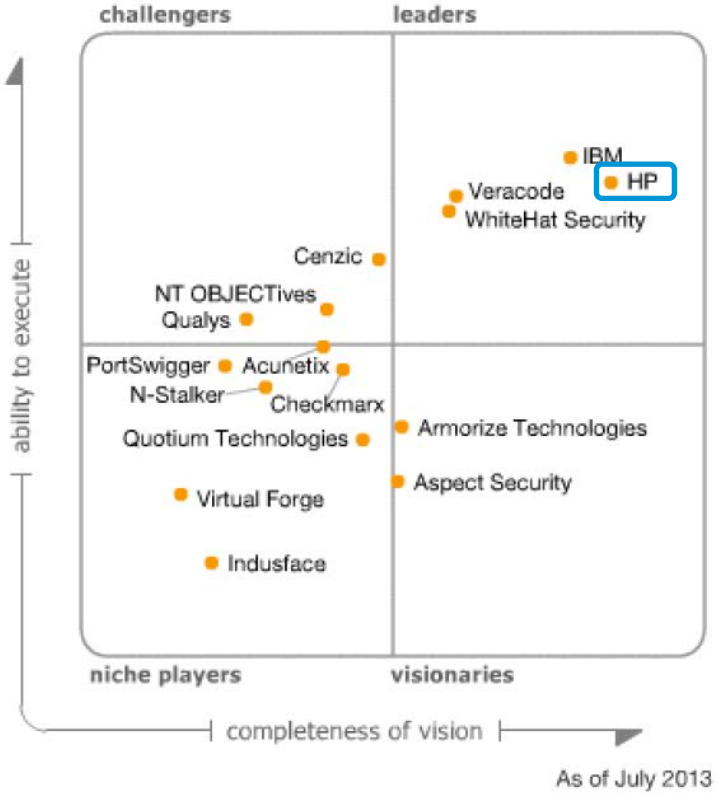


HP Fortify Named a Leader in Gartner Magic Quadrant

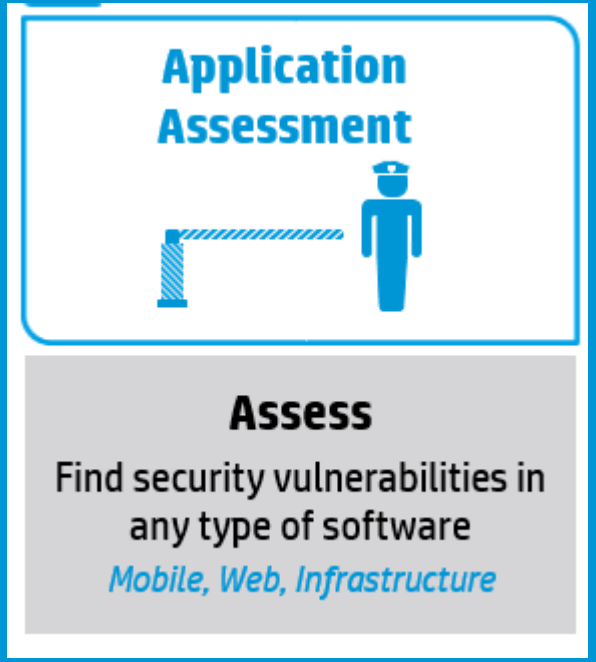
Gartner Application Security Testing

- *"HP offers comprehensive SAST capabilities with Fortify's strong brand name and breadth of languages tested.*
- *The company has innovative IAST capability with Fortify SecurityScope, which integrates with its WebInspect DAST.*
- *There is strong integration within HP's security portfolio, such as integration of AST knowledge into ArcSight and DAST knowledge into TippingPoint's IPS for WAF-like protection.*
- *HP uniquely offers runtime application self-protection (RASP) technology"*

– *Gartner*



Security Testing

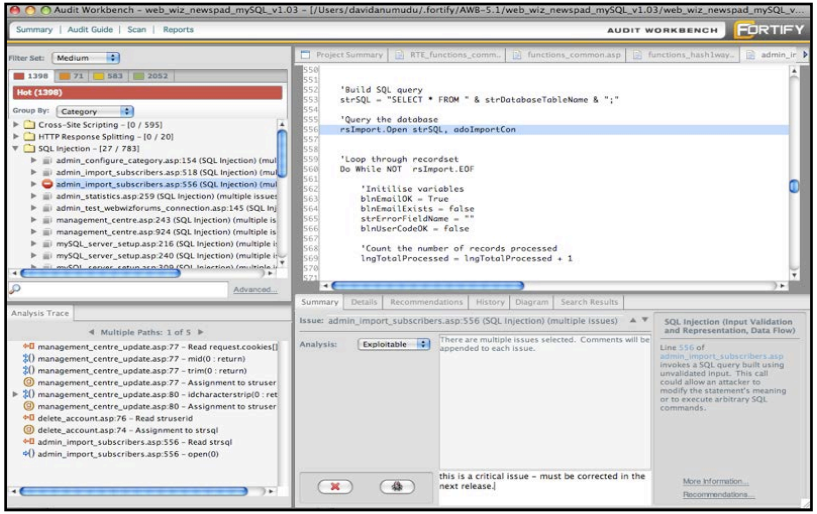


HP Fortify Static Code Analyzer (SCA)

Static analysis – find and fix security issues in your code during development

Features:

- Automate static application security testing to identify security vulnerabilities in application source code during development
- Pinpoint the root cause of vulnerabilities with line of code details and remediation guidance
- Prioritize all application vulnerabilities by severity and importance
- Supports 21 languages, 500+ vulnerability categories

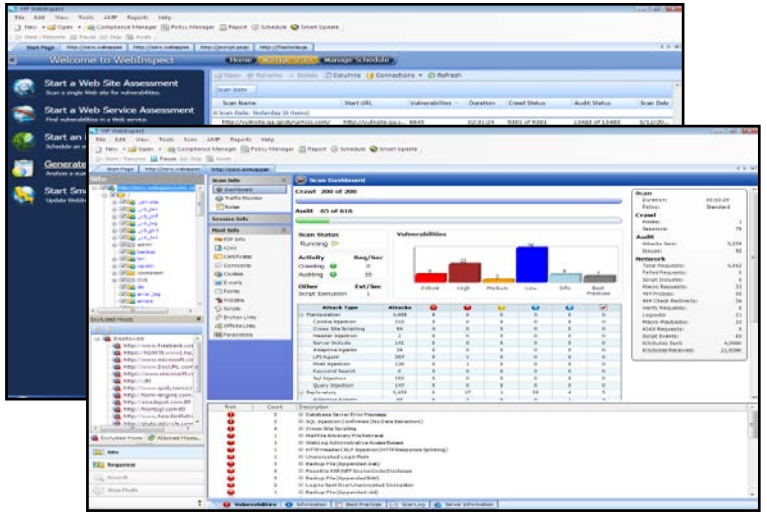


HP WebInspect

Dynamics analysis – find critical security issues in running applications

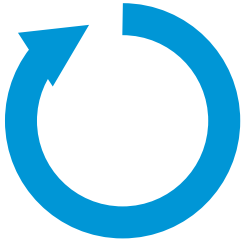
Features:

- Quickly identify risk in existing applications
- Automate dynamic application security testing of any technology, from development through production
- Validate vulnerabilities in running applications, prioritizing the most critical issues for root-cause analysis
- Streamline the process of remediating vulnerabilities



HP Fortify on Demand

Get results fast with security testing software-as-a-service



Simple

Launch your application security initiative in <1 day

- No hardware or software investments
- No security experts to hire, train and retain

Fast

Scale to test all applications in your organization

- 1 day turn-around on application security results
- Support 1000s of applications for the desktop, mobile or cloud

Flexible

Test any application from anywhere

- Secure commercial, open source and 3rd party applications
- Test applications on-premise or on demand, or both

HP Fortify on Demand at a glance

Comprehensive and accurate

Static Testing	Dynamic Testing	Audit & Analysis
HP Fortify SCA	HP WebInspect	Manual

Powerful remediation

Analysis & Reports

Online Collaboration

Broad support

- ABAP
- C/C++
- Cold Fusion
- Java
- Objective C
- Python
- ASP.NET
- Classic ASP
- Flex
- JavaScript/AJAX
- PHP
- T-SQL
- C#
- COBOL
- HTML
- JSP
- PL/SQL
- VB.NET
- VB6
- VBScript
- XML
- Ruby

Fast, secure & scalable

1 Day Static Turnaround

Virtual Scan Farm

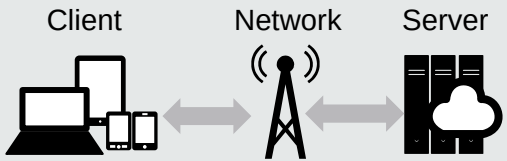
Encryption

Third Party Reviews

Mobile Security Testing

All platforms
- Apple iOS
- Android
- Windows, Blackberry

Multiple analysis types
- Source Code
- Running Application
- Protocol Analysis



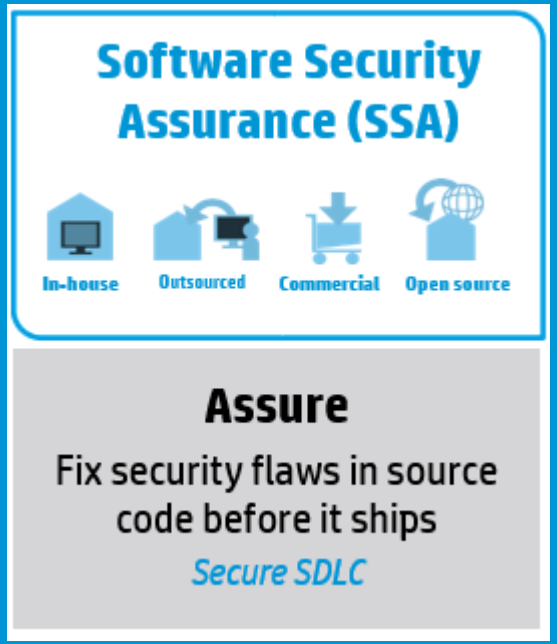
Breadth of testing

- 10,000+ applications
- 18 different industries represented
- 5 Continents
- Civilian and Defense Agencies across US Government
- Vendor Management and Internal Management
- Development teams from 1 to 10,000s

What can I do this Year?

Prevention

Secure Development



Open Software Assurance Maturity Model

www.opensamm.org

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

- ◊ *Evaluating an organization's existing software security practices*
- ◊ *Building a balanced software security program in well-defined iterations*
- ◊ *Demonstrating concrete improvements to a security assurance program*
- ◊ *Defining and measuring security-related activities within an organization*

Open Software Assurance Maturity Model

www.opensamm.org

OpenSAMM defines four business functions: **governance**, **construction**, **verification**, and **deployment**. Each of these has three associated security practices. And for each security practice, SAMM defines three maturity levels. It provides the following visualization.

Building Security In Maturity Model

http://bsimm.com

The Building Security In Maturity Model is the result of a study of 67 software security initiatives. It describes activities companies are currently doing around software security so you can compare them with what your organization is doing. With your organizational goals and objectives in mind, you can use BSIMM to determine which additional activities might make sense. It gives you an overview of how software security teams tend to be organized, and how large those teams typically are.

Building Security In Maturity Model

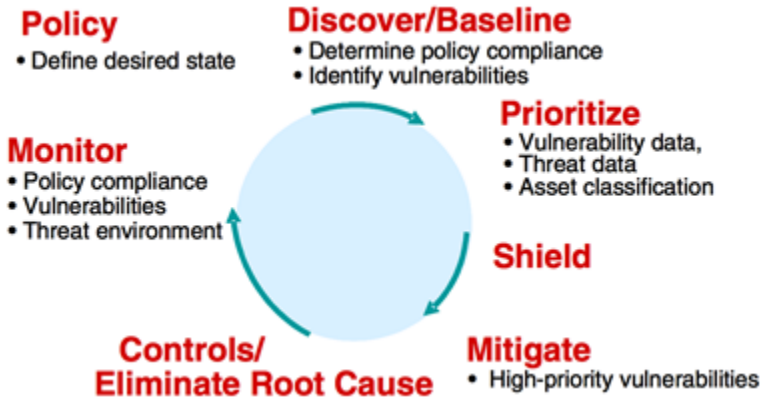
http://bsimm.com

The BSIMM is organized similarly to OpenSAMM into what it calls the Software Security Framework (SSF). It has four domains: governance, intelligence, secure software development lifecycle (SSDL) touchpoints, and deployment.

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Vulnerability Management

Vulnerability management is the “cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.” Gartner defines it as an ongoing multi-step process.

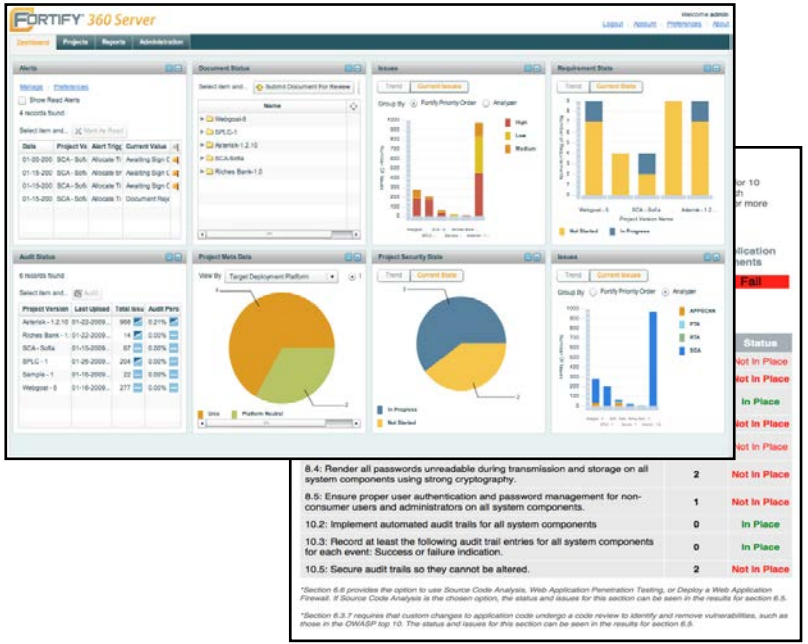


Software Application Security

Management, tracking and remediation of enterprise software risk

Features:

- Specify, communicate and track security activities on software projects
- Role-based, process-driven management of software security program
- Integrations into key development environments
  - Build integration, defect tracking, source control, 3rd party analysis engines
- Flexible repository and reporting platform for security status, trending and compliance
  - Normalized, correlated vulnerability repository
  - Aggregated risk metrics

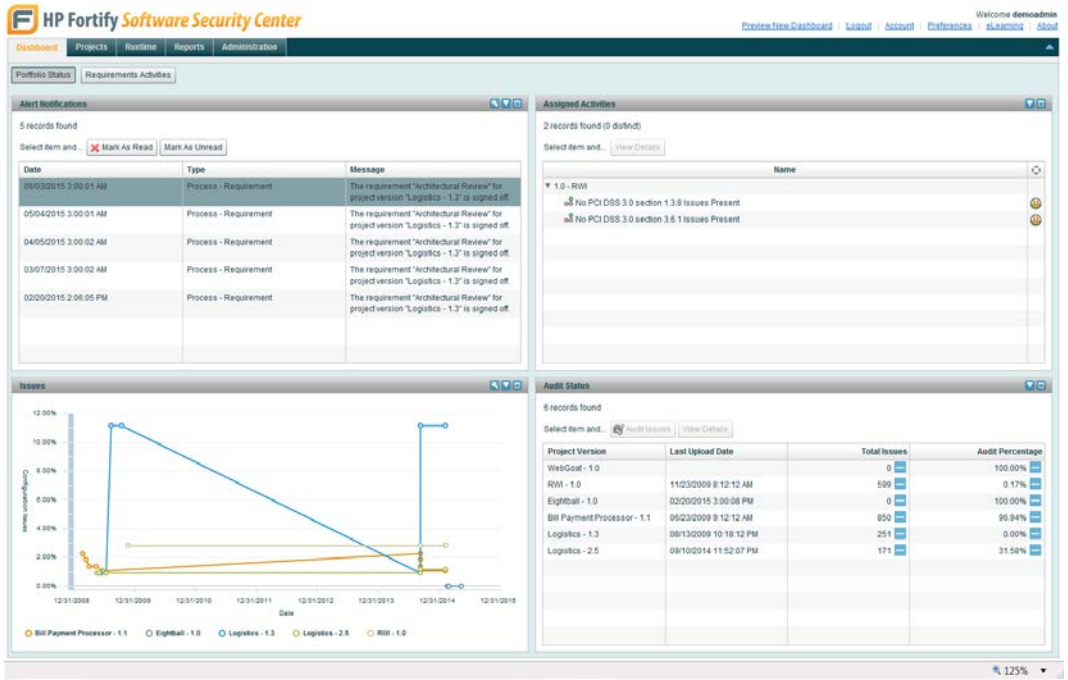


HP Fortify Software Security Center

Configurable Dashboards

Reveal the requirements and assigned activities required to manage application risk across your portfolio.

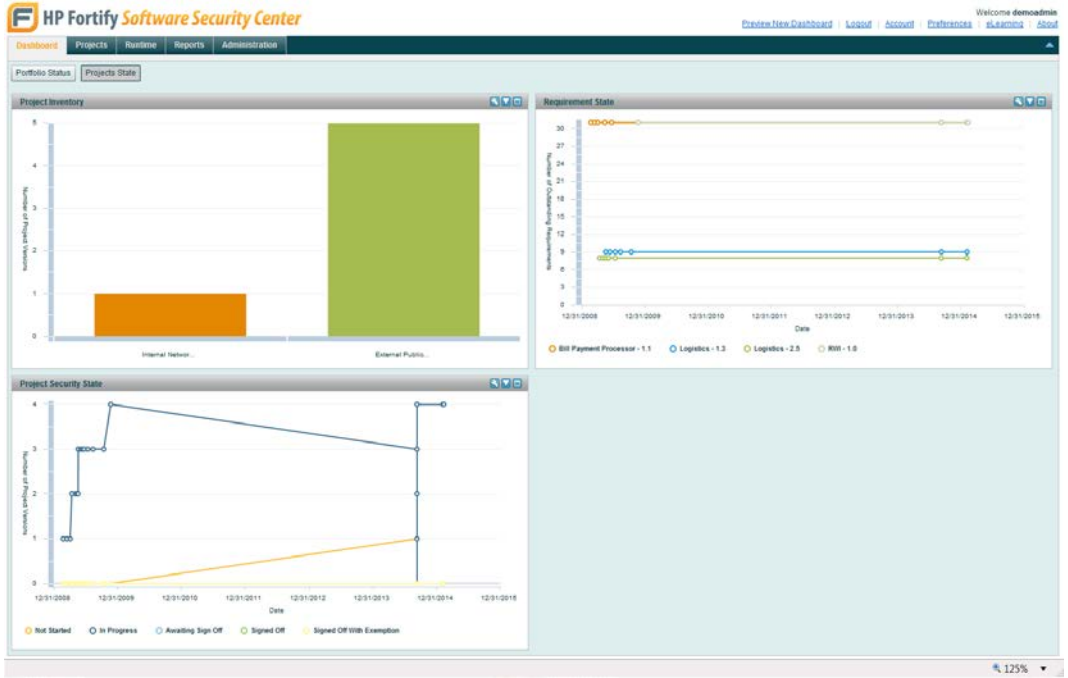
Present the portfolio metrics that track the sucess of your Software Security Assurance process.



HP Fortify Software Security Center

Configurable Dashboards

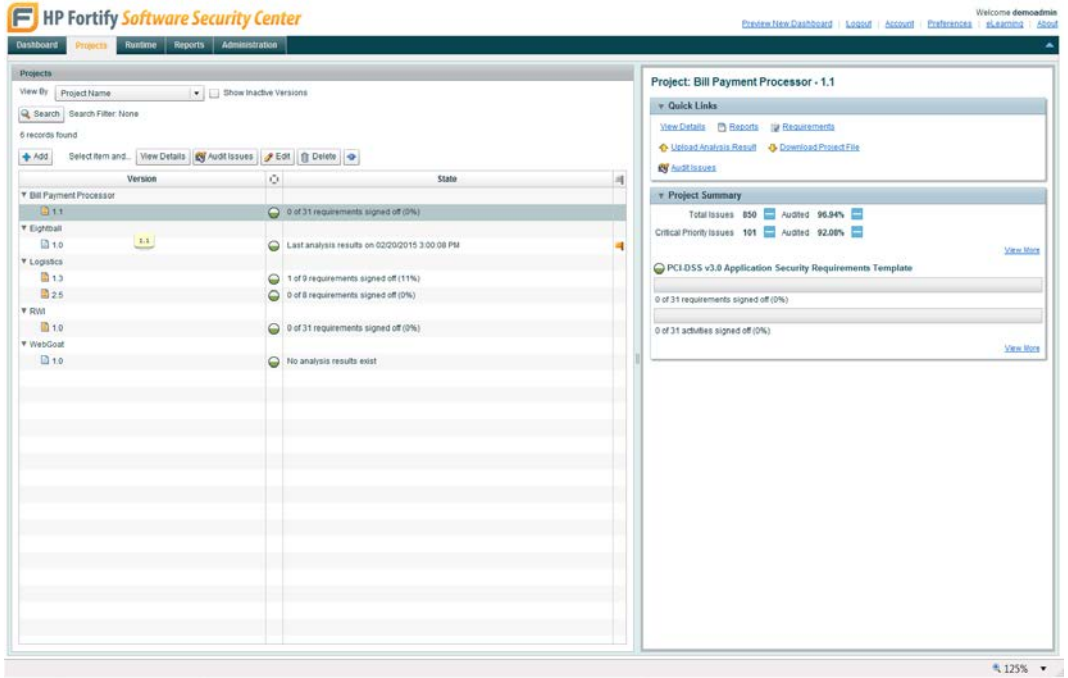
Reveal the state of each project in a selection of dashboard views.



HP Fortify Software Security Center

Project Summary

Select any project from your portfolio to get a quick Project Summary.

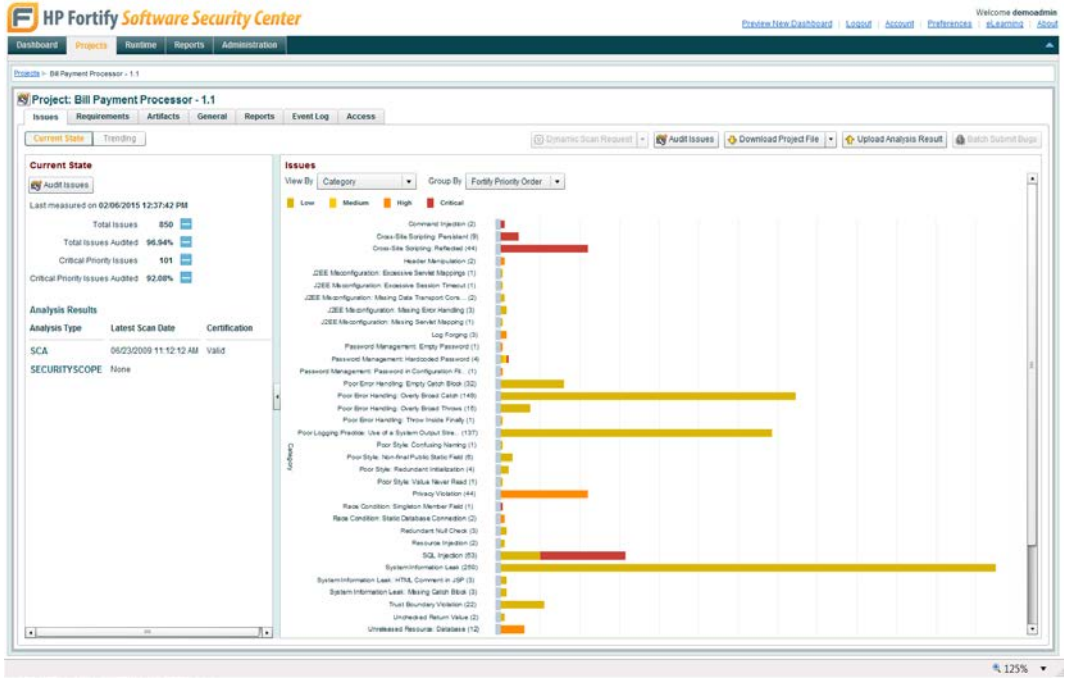


HP Fortify Software Security Center

Project Details

Click View Details to drill down into a project's security state.

Key Performance Indicators expose a project's risk level.

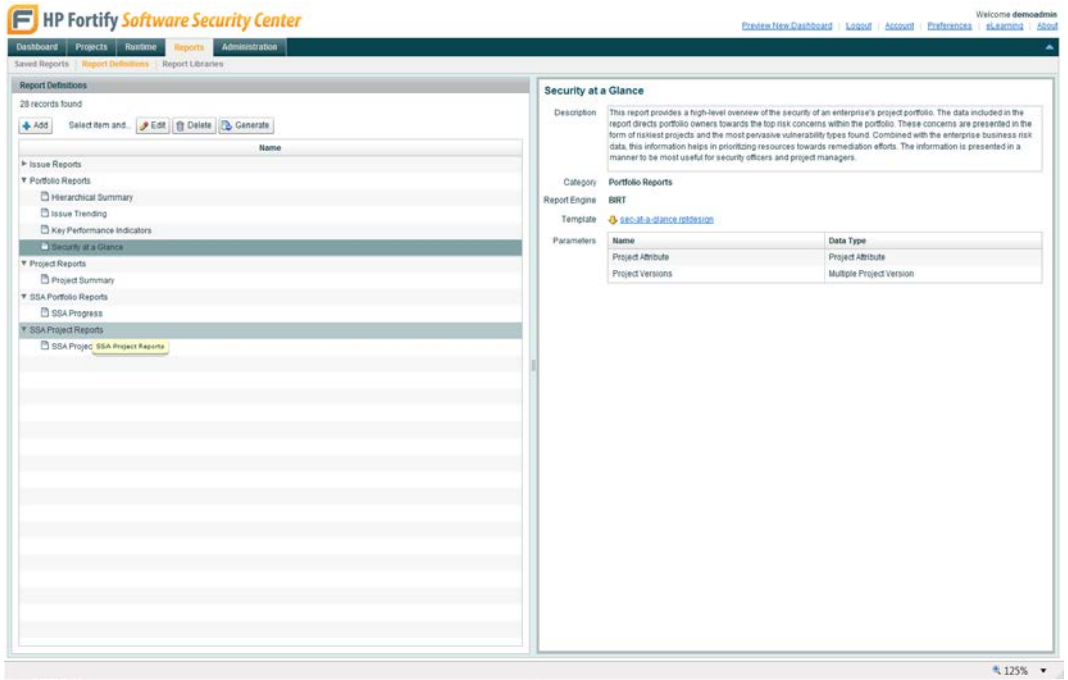


HP Fortify Software Security Center

Portfolio Report Definitions

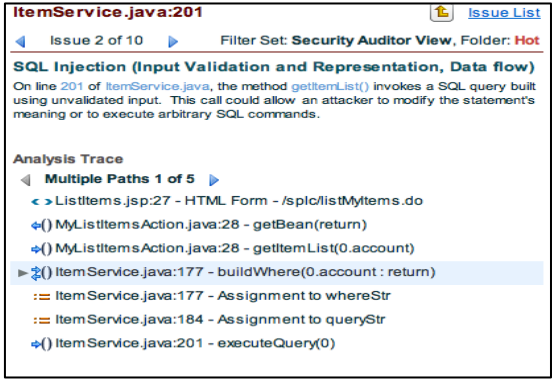
Report on the security status of your application portfolio.
Report on the status of your Software Security Assurance process.
Report types include:

- Hierarchical Summary
- Issue Trending
- Key Performance Indicators
- Security at a Glance
- SSA Progress



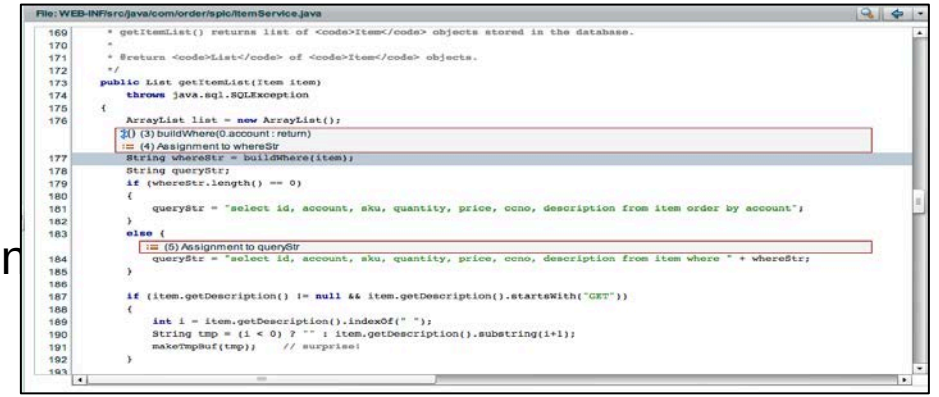
Secure Development Tools

Manage remediation and audit workflows



Online collaboration

- Reduce overhead of engaging development
  - Easy web-based, IDE-like navigation
  - Consistent Presentation & Auditing
- Defect-Tracking Integration
  - One-click integration
  - Deep link back for details



Developer IDE plug-ins

- View results and manage remediation

Audit Workbench

- Security auditor view of the process

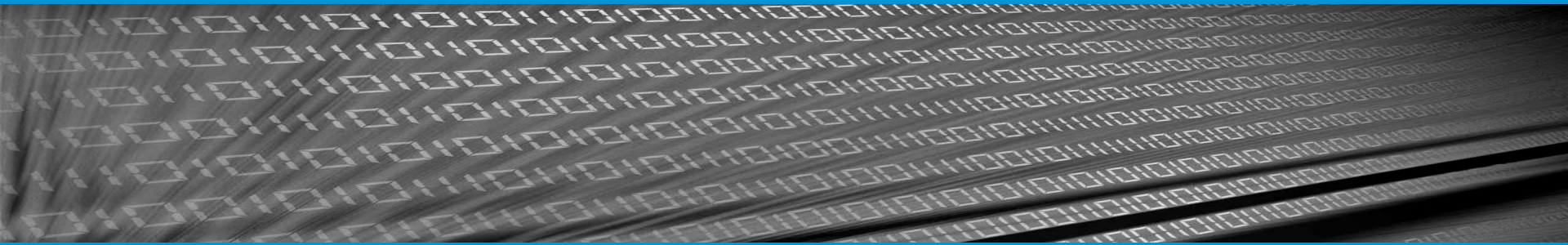
Summary

Summary: Find, Fix and Fortify

HP Fortify Software Security Center

1. **Find & Fix security issues** in development
2. **Fortify applications** against attack
3. **Save money** in development
4. **Reduce risk** from applications

Thank you

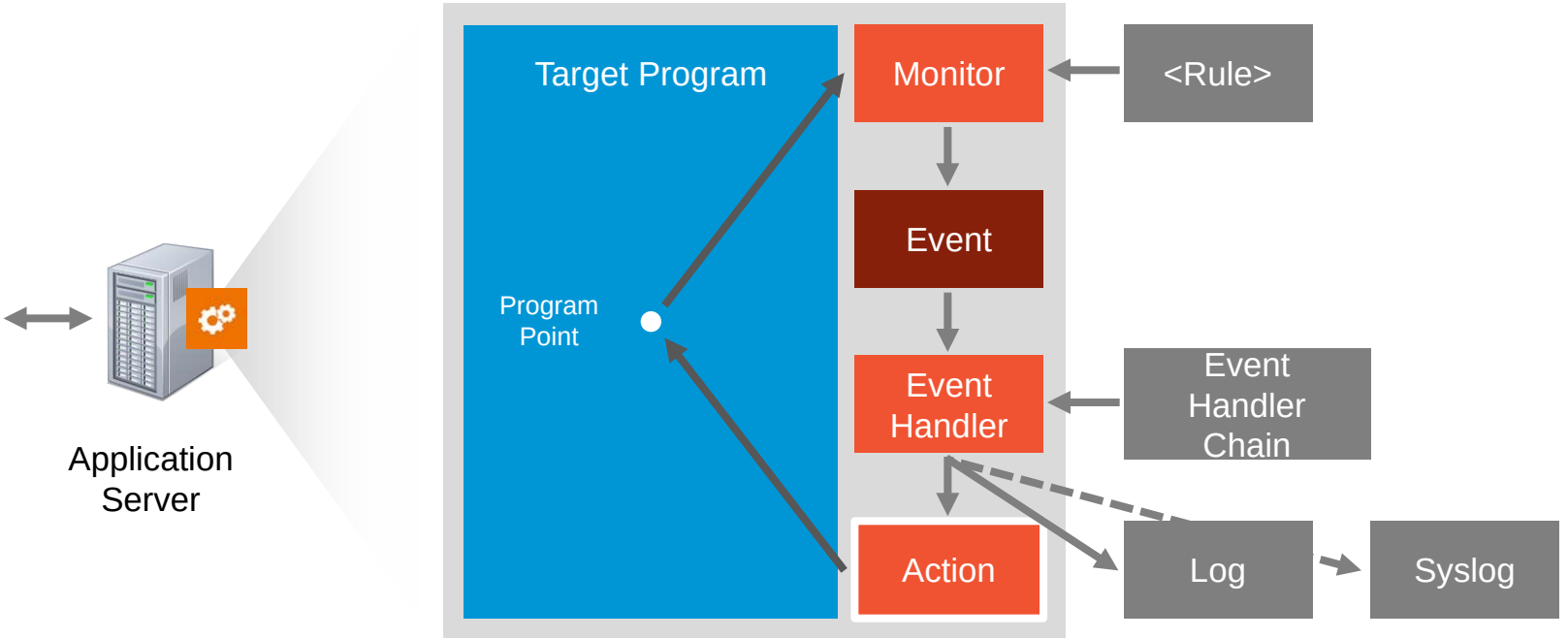


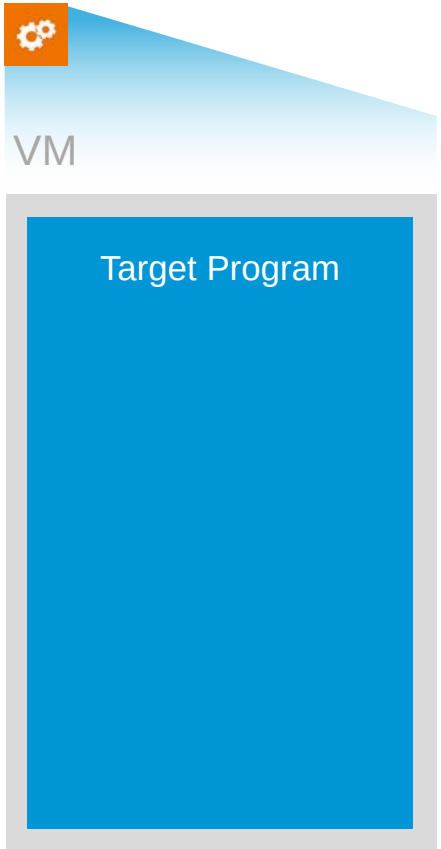
Appendix

Fortify Runtime Technology

Fortify Runtime Technology

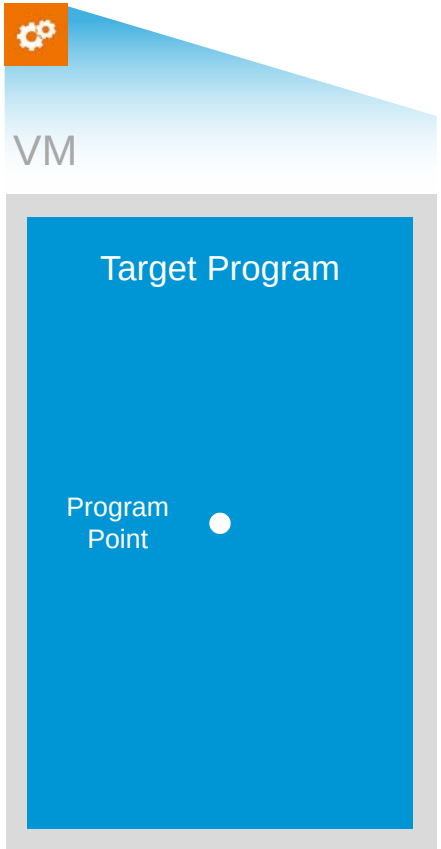
An **action** can change the state of the target program. It could throw an exception, show a message, or modify variable values.





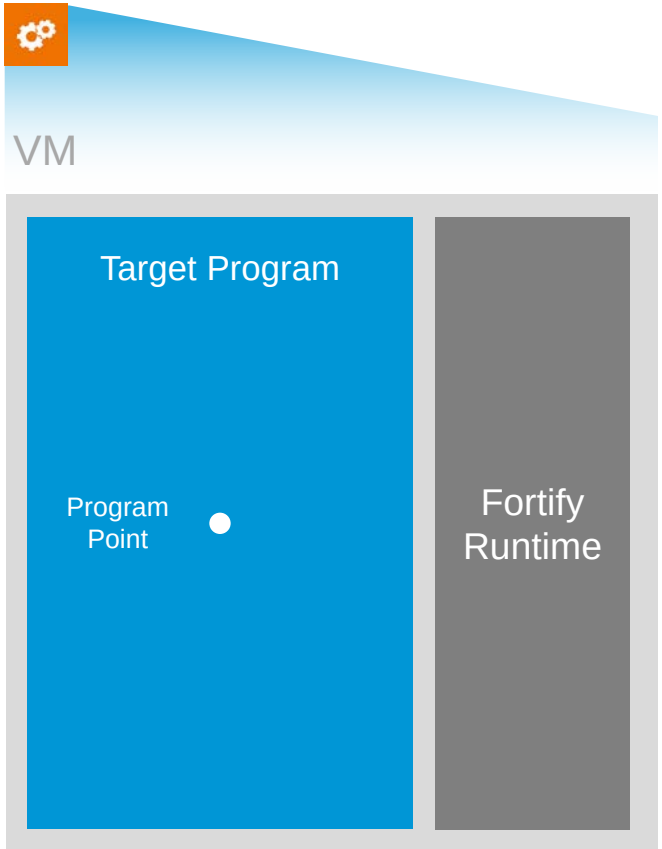
The Target Program is the user's code. It can be:

- An application server
- Any Java
- Any .NET program

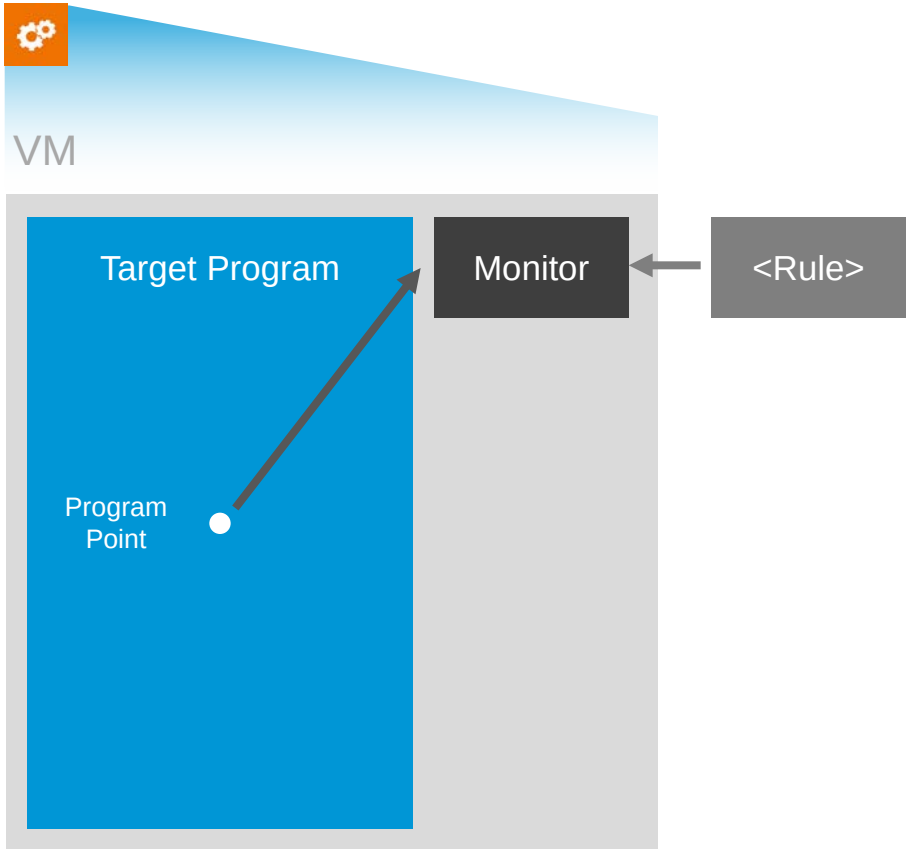


A Program Point is a location of interest in the target program.

- A program point can be:
- A sensitive method call
- Part of the attack surface
- Any method boundary

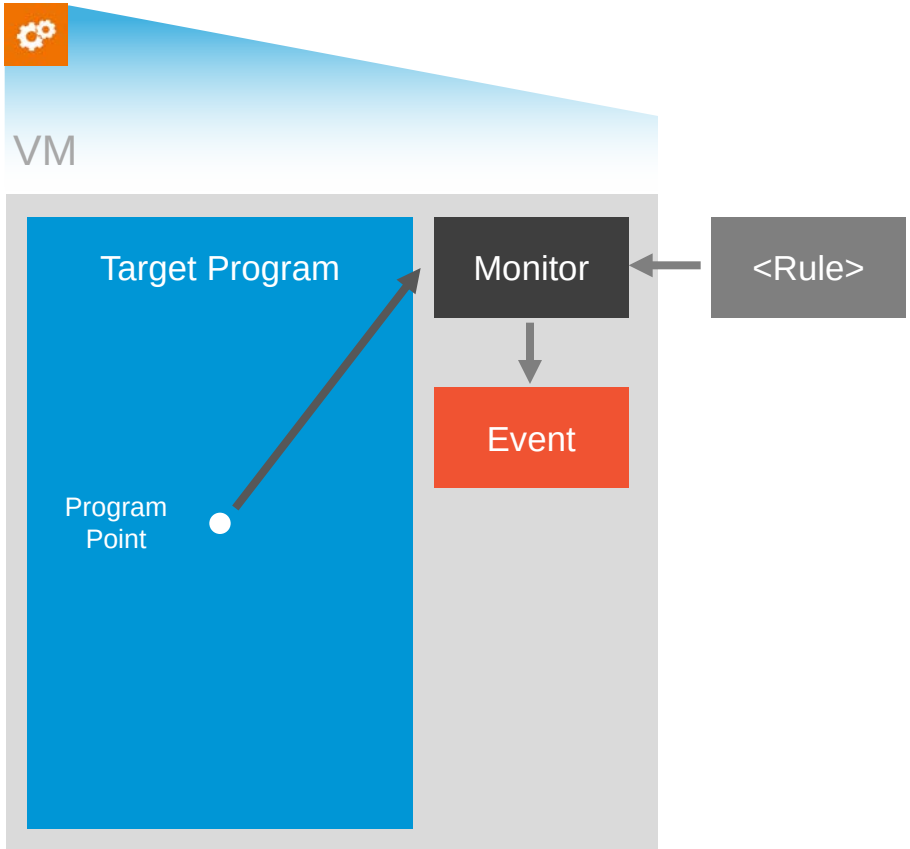


Fortify Runtime watches program points and takes action when required.

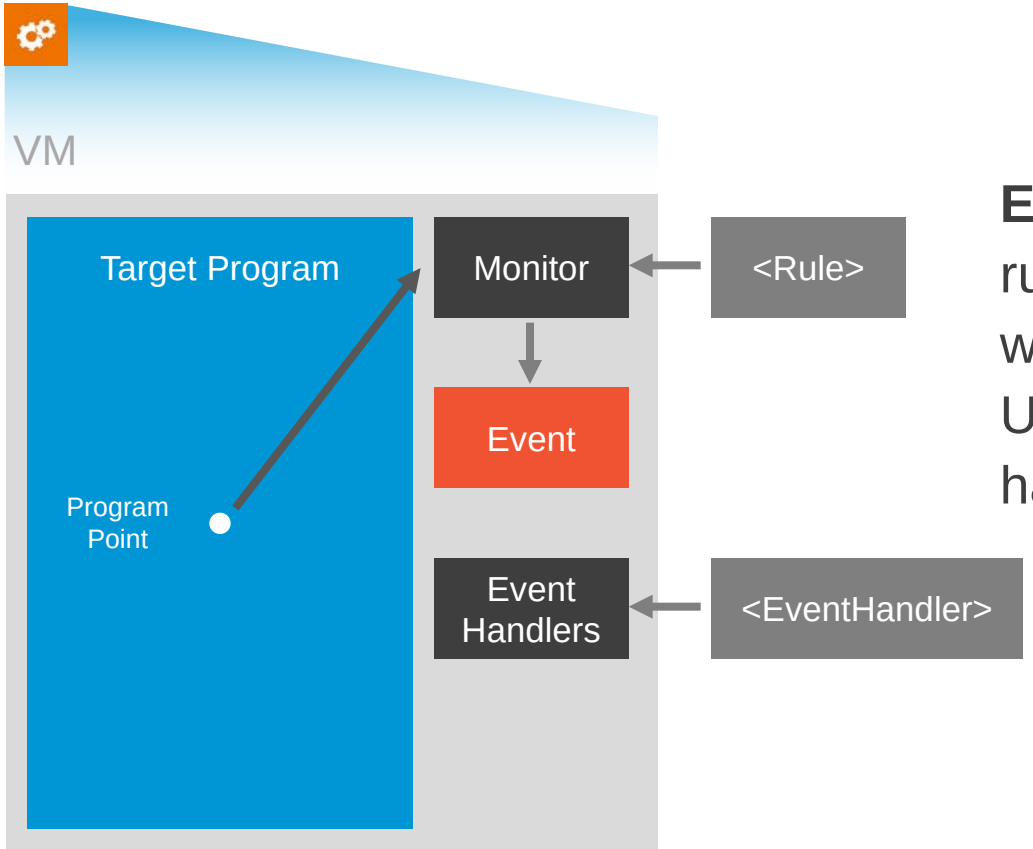


A rule specifies a program point and a **monitor**. Rules come in HP Application Defender rulepacks.

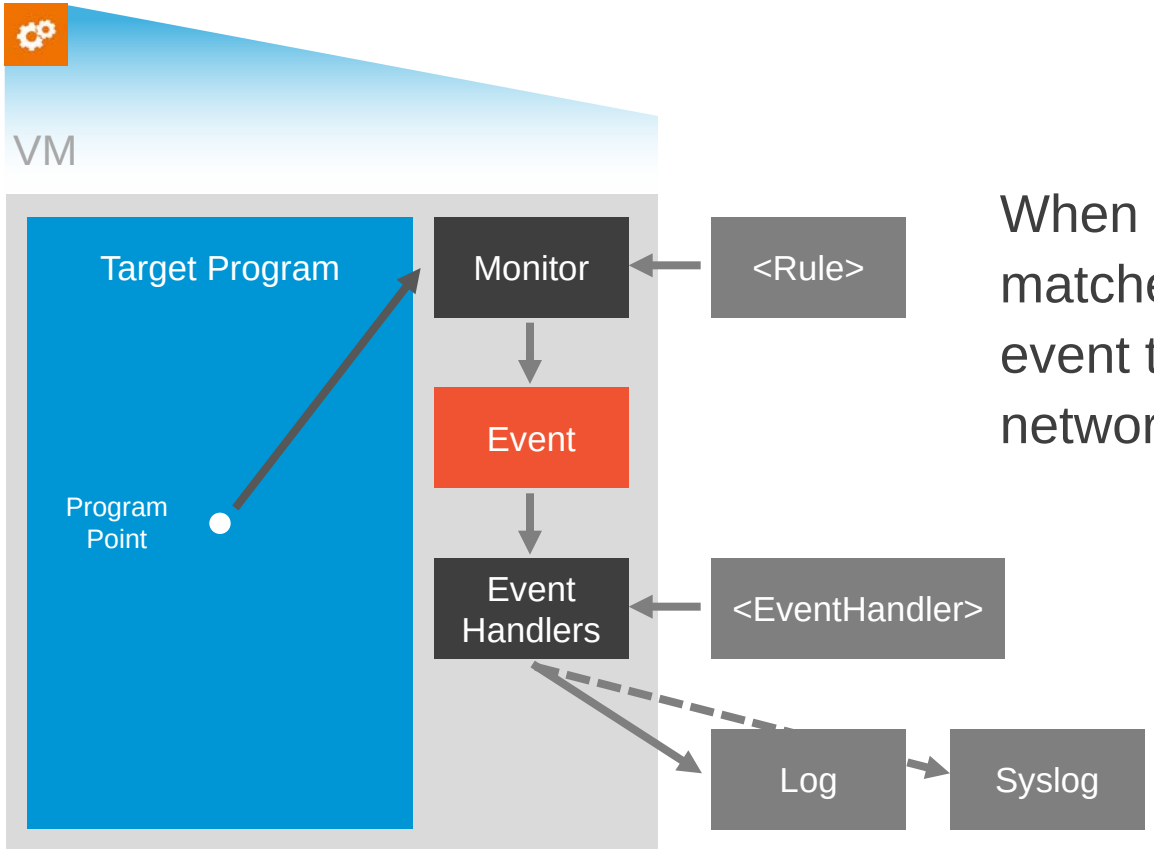
A **monitor** is an object that watches a program point.



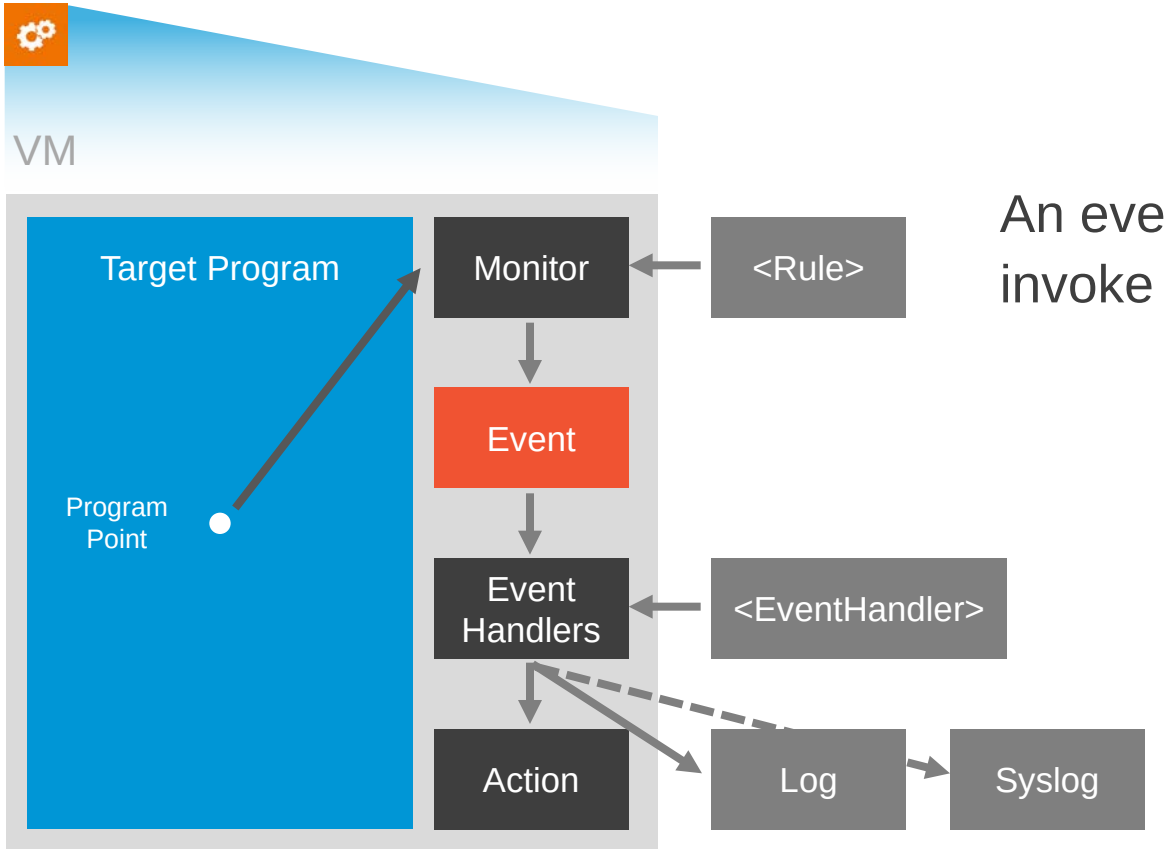
When a monitor finds what it's looking for, it creates an **event**.



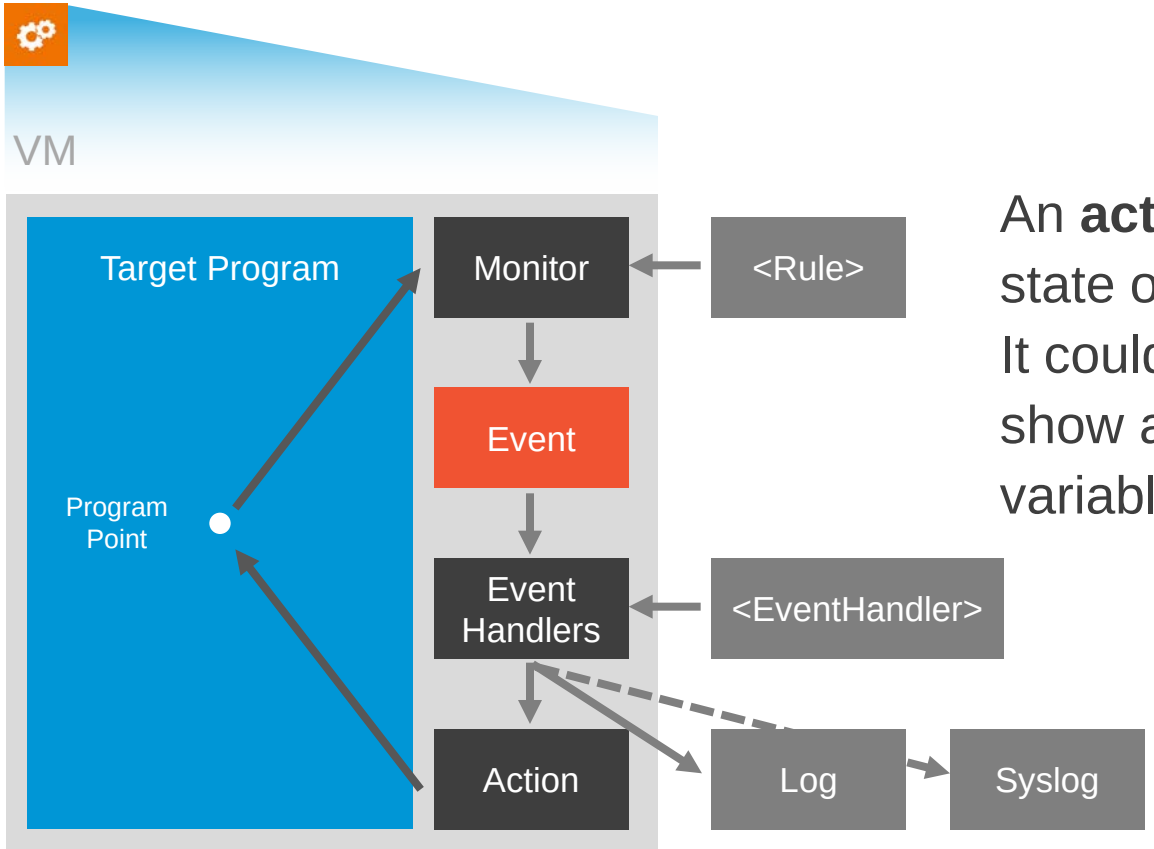
Event Handlers tell the runtime platform what to do with different kinds of events. Users can write their own event handlers.



When an event handler matches, it can **dispatch** the event to a log file or to a network service.



An event handler can also invoke an **action**.



An **action** can change the state of the target program. It could throw an exception, show a message, or modify variable values.