



HPE Fortify Users Group Aberdeen, MD

July 2017

Agenda

Time	Description
8:00 - 8:30am	Registration
8:30 - 8:45am	Welcome and introduction
8:45 - 10:00am	Fortify updates and roadmap
10:00 - 10:30am	Networking Break
10:30 - 12:00pm	Best practices learned from Securing DevOps: Scan automation and integration that can be applied anywhere
12:00 - 1:00pm	Lunch Break
1:00 - 2:00pm	Capabilities to help expand and mature your SwA program: Security Assistant, Audit Assistant, Parallel Processing, and .Net Scanning
2:00 - 2:30pm	How Fortify and HPE can help with RMF
2:30 - 3:00pm	Break
3:30 - 3:45pm	Open technical Q&A session

Introduction

- | | |
|---------------------|----------------------------------|
| – Scott Snowden | Fortify Federal SE Manager |
| – Haleh Nematollahy | Sr. Security Solutions Architect |
| – Tim Angelos | Fortify DOD Account Executive |
| – Bruce Oehler | Army Core Account Executive |
| – Liam Redden | Partner- Carahsoft |
| – Steven Klien | Partner - Carahsoft |



Hewlett Packard
Enterprise

HPE Security Fortify

Vision & Roadmap

2Q17 Scott Snowden, Fortify Federal Sales Engineering Manager

Forward Looking Statements

- This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard Enterprise's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard Enterprise may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.

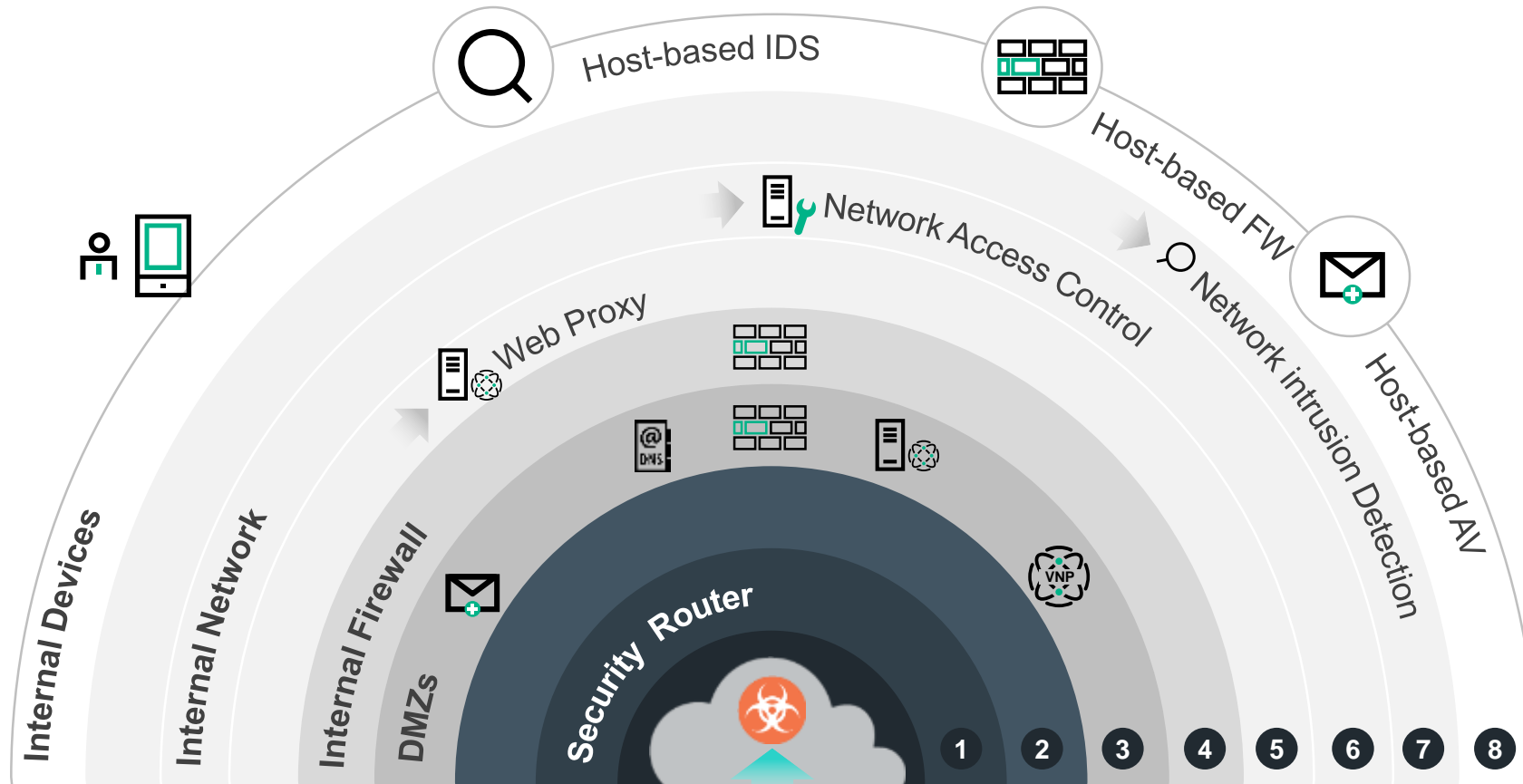
HPE Confidential Information

- This document contains HPE confidential information.
- If you have a valid Confidential Disclosure Agreement with HPE, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HPE and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HPE's prior written approval.



Our Vision & Strategy

Existing network and perimeter based security is insufficient



84% of breaches exploit vulnerabilities in the application layer

Yet the ratio of spending between perimeter security and application security is **23-to-1**

- Gartner Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves (2014)

Vision

Enable DevOps and the next-gen SDLC by accelerating integration, automation and agility for both on-demand & on-prem solutions to enable customers to release the most secure applications at Enterprise speed

Go Faster, more securely, with less manual intervention



HPE Security Fortify Leadership

Over a decade of successful deployments backed by the largest security research team

- 10 out of 10 of the largest information technology companies
- 3 out of 3 of the largest independent software vendors
- 5 out of 5 of the largest telecommunication companies
- **3 out of 3 US Military Branches**

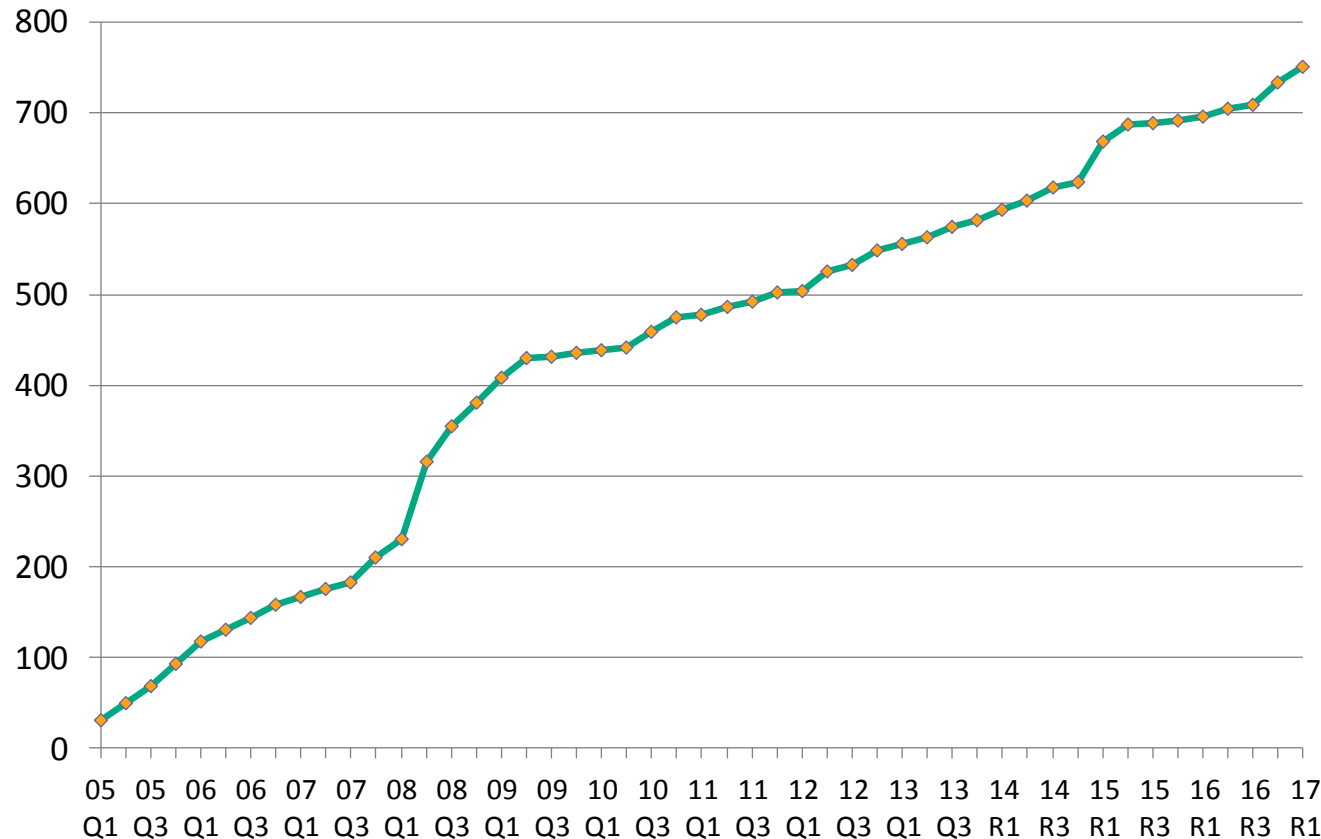
Figure 1. Magic Quadrant for Application Security Testing



Fortify Software Security Research

24 languages - 751 Vulnerability Categories

Quarterly updates to the Secure Coding Rulepacks identify the latest categories of software vulnerabilities



Growth in Vulnerability Categories (2005 – 2017)

Example Categories:

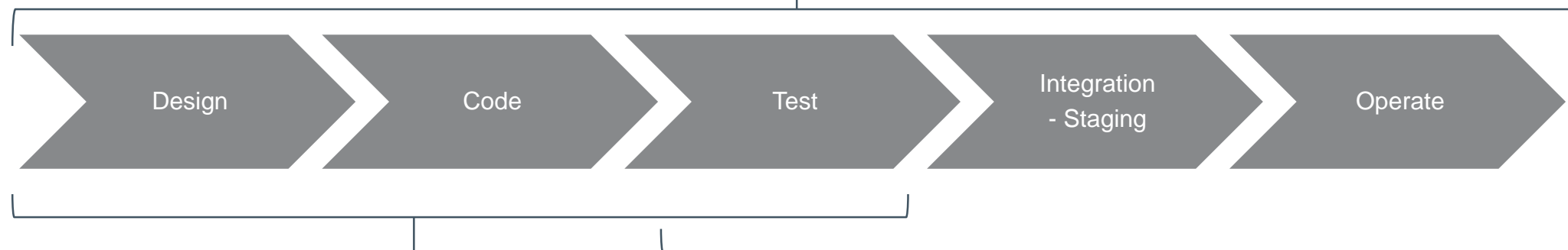
- Command Injection
- Cross-Build Injection
- Cross-Site Request Forgery
- Cross-Site Scripting
- Header Manipulation
- JavaScript Hijacking
- LDAP Injection
- Privacy Violation
- Session Fixation
- SQL Injection
- System Information Leak
- Unhandled Exception
- Weak Cryptographic Hash
- Weak Encryption

For more, go to:

<https://vulncat.hpefod.com>

Software Security Assurance (SSA & SDLC)

Security



Development

Fortify Static Suite

Static Code Analyzer (SCA)

Audit Workbench (AWB)

IDE Plugin

Software Security Center (SSC)

Hybrid

Fortify Dynamic Suite

WebInspect (WI)

WebInspect Enterprise (WIE)

Continuous Web Monitoring (CM)

On-demand Web Scans

Software Security Center (SSC)

Testing / Operations

Visibility & Defense

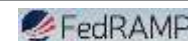
Fortify Runtime

Protection

Logging

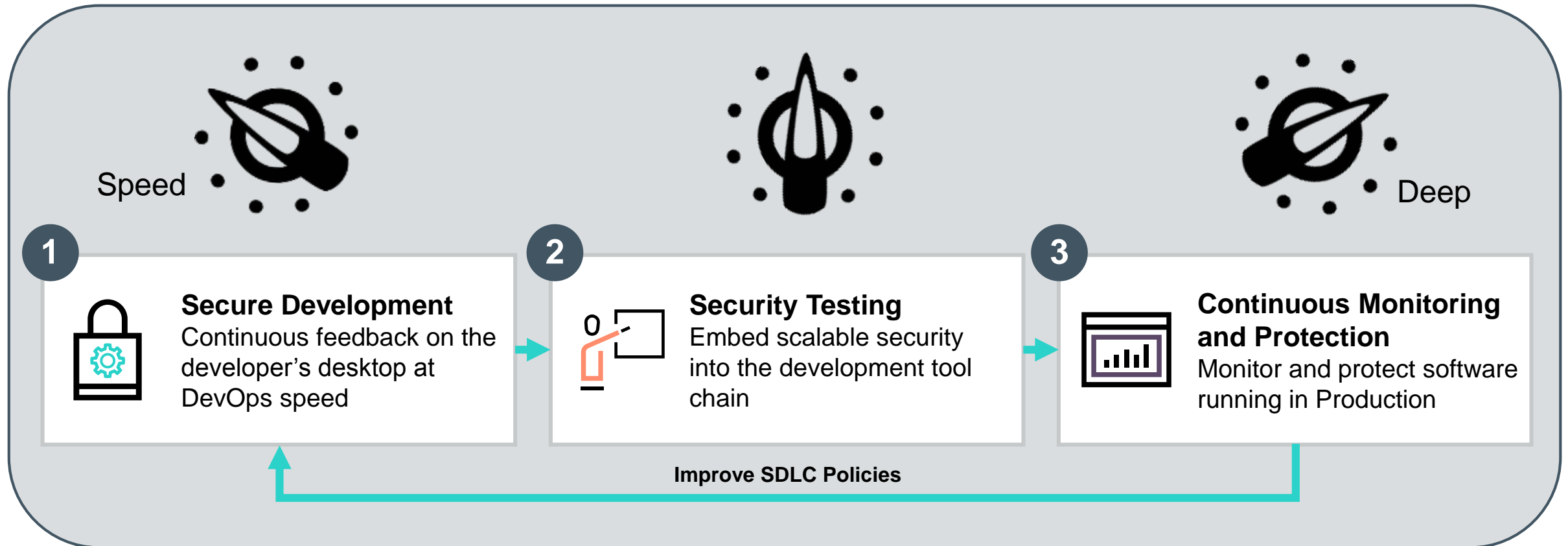
AppDefender

Fortify On Demand (FOD) / Vendor Management

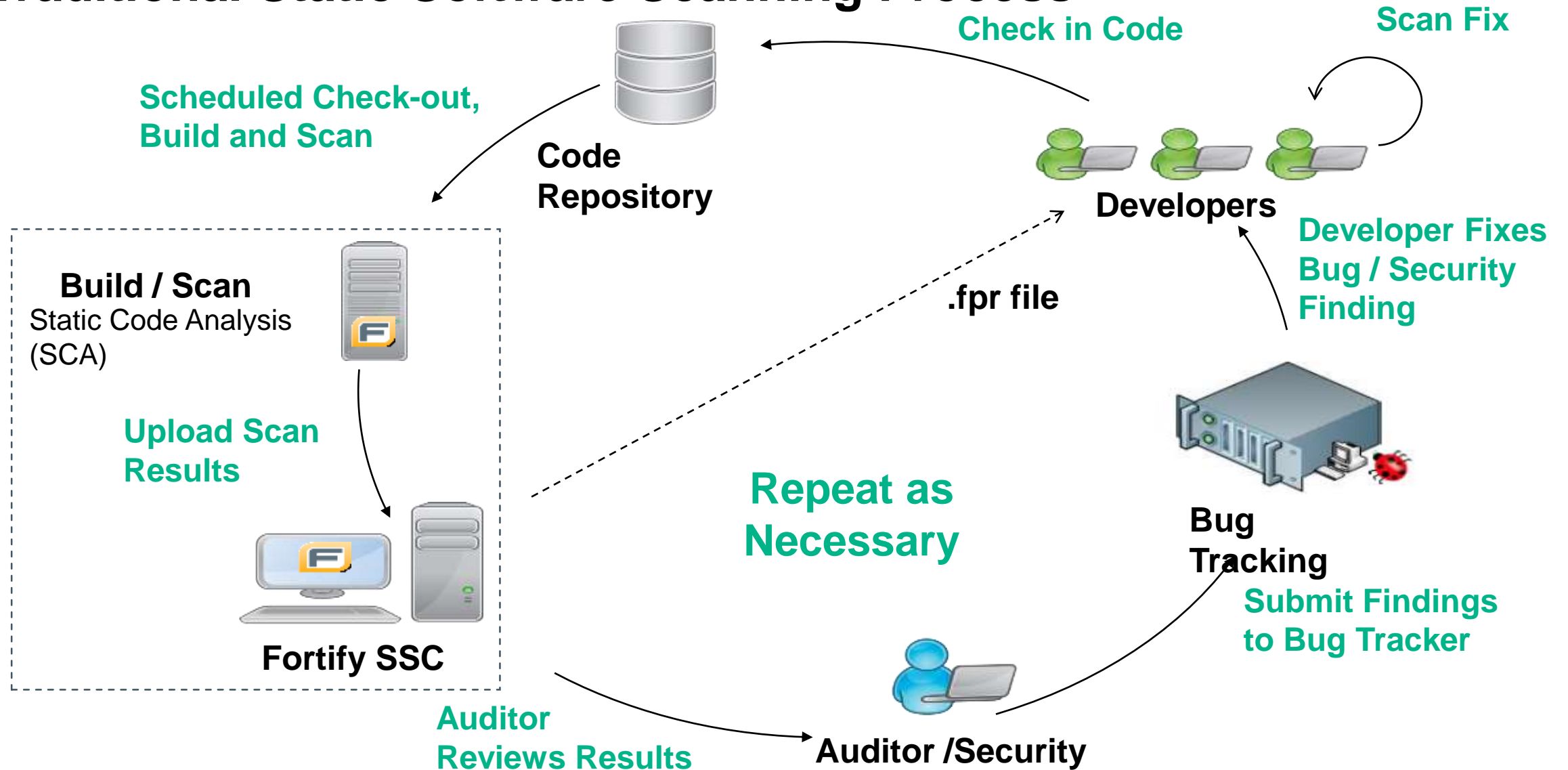


Application Defender

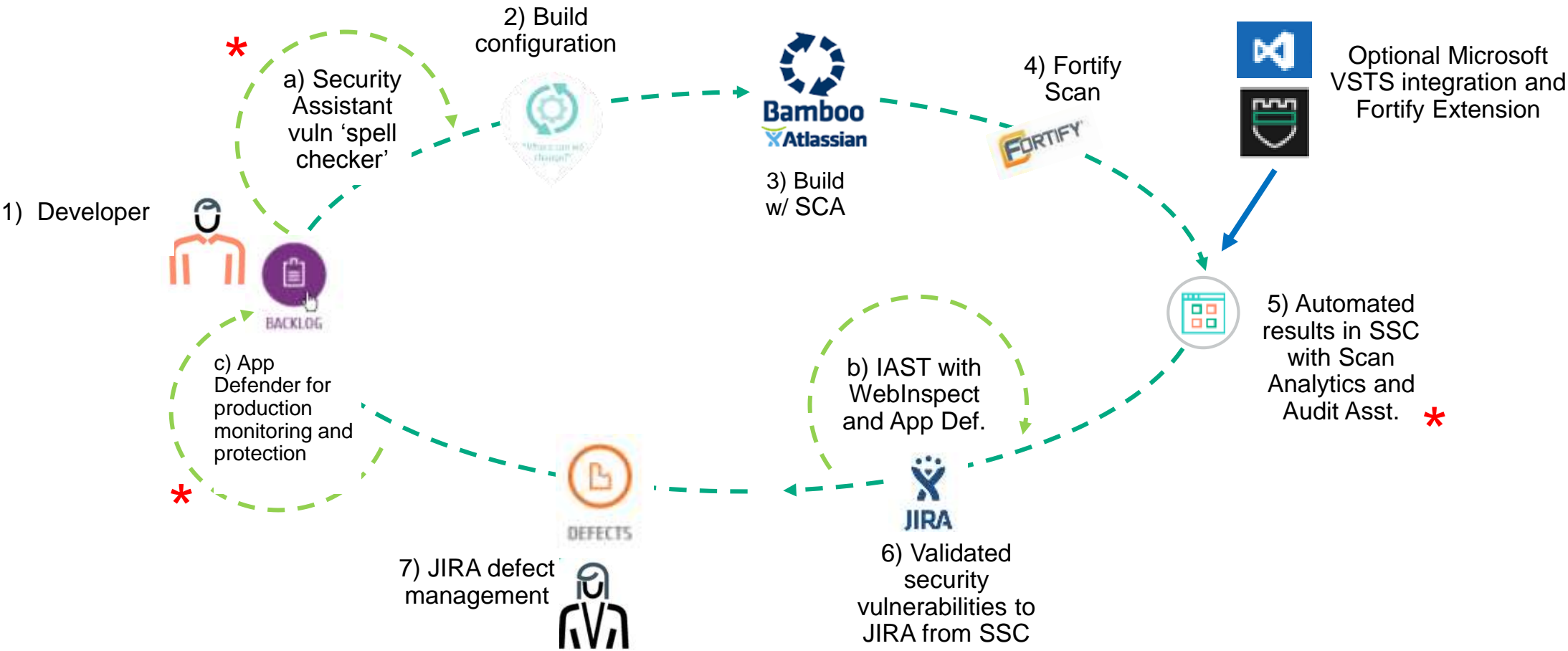
Securing DevOps– Build it in



Traditional Static Software Scanning Process



Securing DevOps with Fortify





Fortify Recent Changes

Fortify Support and Versioning

Use portal if possible – faster routing and response

If you have issues with the support team send SE the ticket number

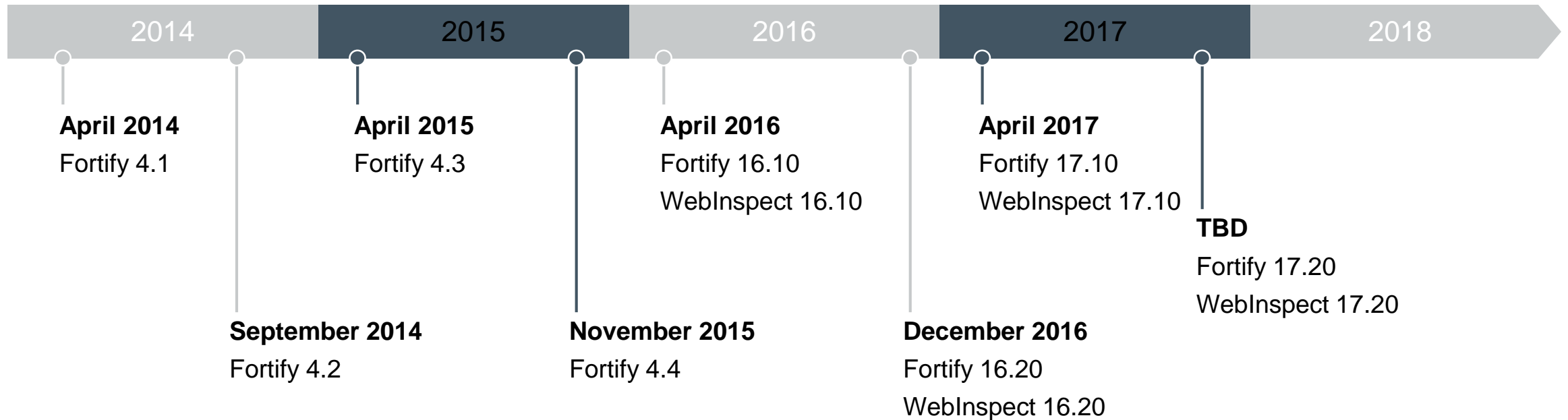
- <https://support.fortify.com>
- fortifytechsupport@hpe.com
- <https://www.protect724.hpe.com/welcome>

(Go to Fortify place, Content and then choose videos. Excellent WebInpsect Intro and Full detail videos)



Fortify Timeline

Versioning has changed to major version matching calendar year



Ver. 16.1 Summary

April 2016

- **SCA Improved framework and language support**
 - Objective C++
 - Initial Swift support
 - Improved Ruby (1.9.3) and Django (1.7) support
 - Java ByteCode
 - Higher Order functions and Type Inference
- **AWB** – group by source file type
- **CloudScan** improved management capabilities
- **SSC** – Full CAC support
 - Improved RESTFul API and documentation (http://<SSC_HOST>/ssc/html/docs/api-reference/index.jsp/)
 - TFS bug tracking integration support
- **Plug-ins** –
 - New Maven plug-in
 - VS plug-in now support BIRT reporting and improved TFS bug tracking integration



Fortify Ver. 16.2 Summary

December 2016

- **Audit Assistant / Scan Analytics**
- **SCA Improved framework and language support**
 - Swift support 2.x
 - Improved .Net scanning – no need for pre-compile and support for Azure applications
 - Gradle integration
 - Incremental scanning support
- **CloudScan** fully integrated into SSC and improved management capabilities
- **SSC**
 - Jira 7 support
 - Improved RESTFul API and documentation (http://<SSC_HOST>/ssc/html/docs/api-reference/index.jsp/)
 - Support for DISA App STIG 4.1
- **Plug-ins** –
 - X.509 PKI support to SSC
 - VS 2015
 - Eclipse plug-in now supports languages other than Java



Fortify Ver. 17.1 Summary

April 2017

– SCA

- Apple
 - Swift 2.2 and 3.0.2 support with support for Swift MVC Model Class
 - Support for Xcode 8.2
- .Net
 - Support for C# ver. 6 and VB.NET ver. 14
 - .Net Async/Await support
- Angular
 - Technical Preview for AngularJS Support
- Salesforce
 - Support for Apex and VisualForce
- Python
 - Performance improvements for Python
- Multi-threaded scanning

– SSC

- Improved interactions with Dynamic Scan results
- Issue Attachment support for Dynamic Scans
- Ability to view issues assigned to you
- Advanced Audit and Conflict strategy settings
- Scheduled alerts

– Other

- Kerberos Visual Studio plugin support
- X.509 Visual Studio plugin support
- New custom tags

WebInspect

Version 16.20

- Privilege Escalation Testing – Test if a lower-privilege user can gain access to critical web pages
- Traffic Viewer Tool – Visualize scan progress or vulnerabilities while simultaneously parsing the traffic data
- Native Selenium Support – Selenium IDE script support for use as both automated login & workflow macros
- Link Source Settings – allows users to select Pattern-based or DOM-based link parsing
- New Audit Engines – Directory Extension and File Prefix audit engine

Version 17.10

- Single Page Application (SPA) Support – Improved support for SPA scanning (Technology Preview)
- Visual Studio Team Services – VSTS integration for automation of scan during build
- Site Explorer Improvements – More ways to export results
- WISwag tool improvements – REST API invocation of WISwag and improved scanning of Swagger services
- REST API improvements – Additional REST API for added automation of functionality
- Incremental scanning capabilities
- Windows Server 2016 support

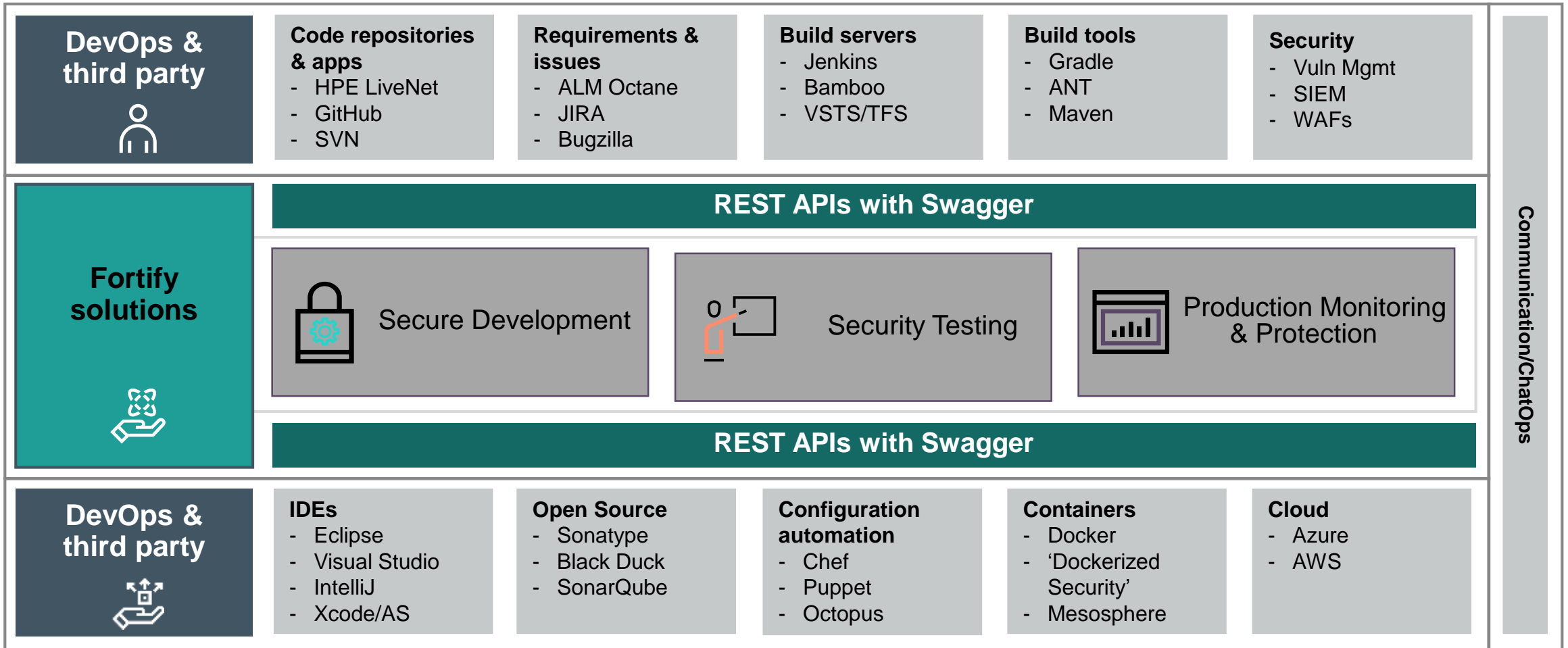




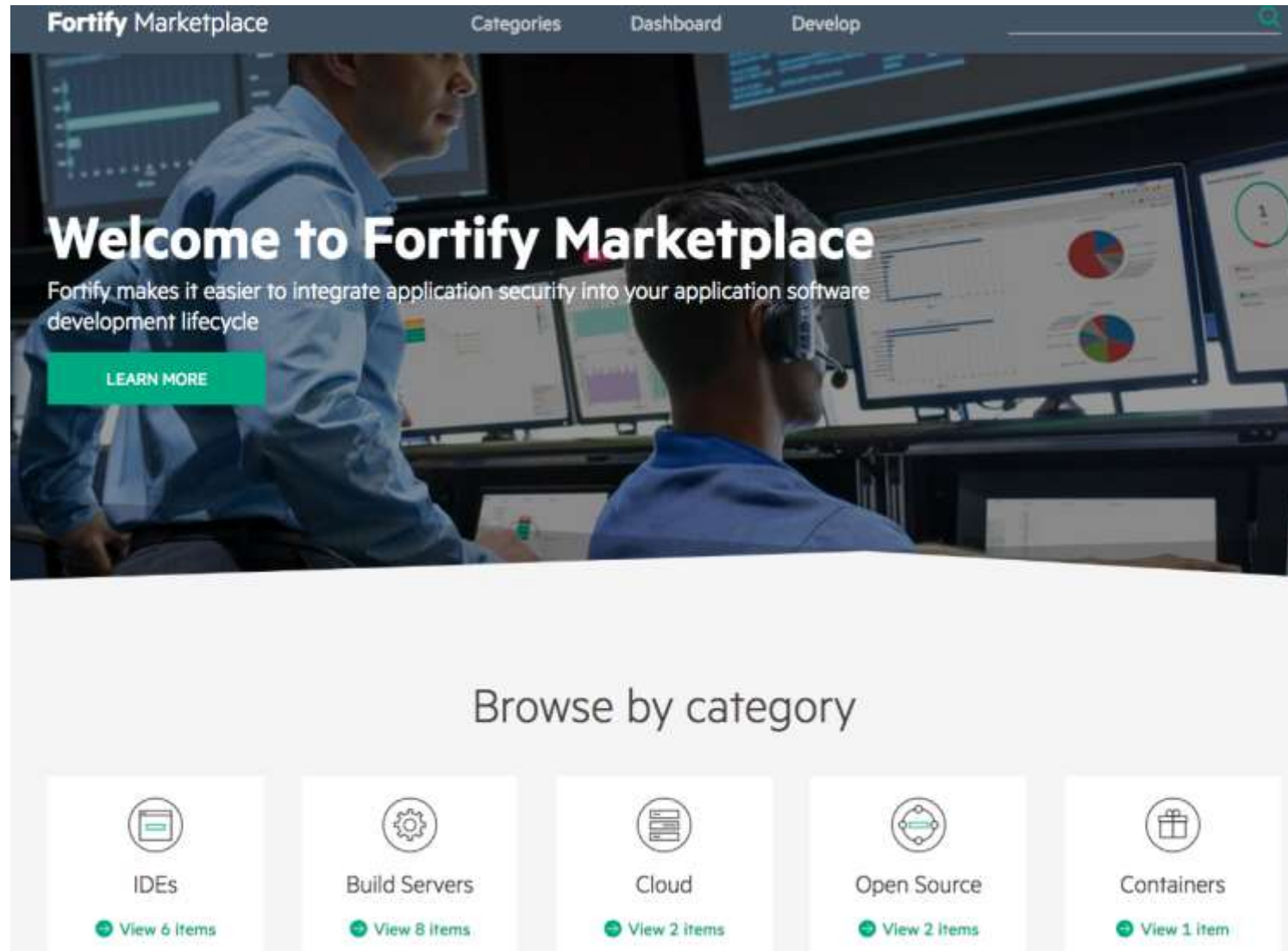
Integrating Security → Fortify Ecosystem

Fortify Ecosystem

<https://marketplace.saas.hpe.com/fortify/category/all?product=Fortify>



Fortify Ecosystem Marketplace



Fortify Ecosystem- FoD 'Swaggerized' REST API

Fortify on Demand Web API Explorer		
Applications Show/Hide List Operations Expand Operations		
DELETE	/api/v3/applications/{applicationId}	Deletes an application
GET	/api/v3/applications/{applicationId}	Retrieves an individual application by id
PUT	/api/v3/applications/{applicationId}	Update an application
GET	/api/v3/applications	Retrieve a collection of applications
POST	/api/v3/applications	Create a new application and release
GET	/api/v3/applications/{applicationId}/auto-report	Returns the associated auto-run report type for the application.
POST	/api/v3/applications/{applicationId}/auto-report	Set-up the associated auto-run report for the application
GET	/api/v3/applications/{applicationId}/users	Returns a list of users that have access to the application
GET	/api/v3/applications/{applicationId}/user-permissions	Returns the permissions the current user has for the application
GET	/api/v3/applications/{applicationId}/releases	Returns a list of releases for the given application
GET	/api/v3/applications/{applicationId}/scans	Returns a list of scans for the given application
Attributes Show/Hide List Operations Expand Operations		
GET	/api/v3/attributes	Retrieve a list of attributes
DynamicScans Show/Hide List Operations Expand Operations		

API Reference in SSC

Hewlett Packard Enterprise

HPE Security Fortify Software Security Center

Overview

- Authentication
- Embed
- Request
- Response
- Search
- Full-Text Search
- Custom Action
- Bulk Request
- File Upload/Download

Key Concepts

The Server API is a typical RESTful API that supports the following key things:

1. Use the following basic URL format:
`http://[SSC Server Name]:[SSC Server Port]/[SSC API Path]`
2. Use the following headers:
 - All GET, POST, PUT and DELETE requests:
`Accept: application/json`
 - All POST and PUT requests require:
`Content-Type: application/json`
3. To authenticate using an SSC user account use *Basic Auth*. An application should only use *Basic Auth* for the initial login.
4. For a list of index resources, see [Index Resources](#).
5. For a list of query parameters, see [Query Parameters](#).

SSC REST API DOCUMENTATION **Explore**

activity-feed-events : Retrieve list of activity feed entries	Show/Hide	List Operations	Expand Operations
GET /api/v1/activityFeedEvents	Get resources		
alertable-event-types : Retrieve the list of event types for which alerts can be created	Show/Hide	List Operations	Expand Operations
alert-definitions : Alert definitions management	Show/Hide	List Operations	Expand Operations
alerts : Retrieve list of fired alerts	Show/Hide	List Operations	Expand Operations
api-auth-controller : Api Auth Controller	Show/Hide	List Operations	Expand Operations
api-bulk-request-controller : Api Bulk Request Controller	Show/Hide	List Operations	Expand Operations
artifacts : Project version artifacts management	Show/Hide	List Operations	Expand Operations
artifact-scan-errors : Retrieve the list of scan errors of all the scans associated with artifact	Show/Hide	List Operations	Expand Operations
artifact-scans : Retrieve list of the scans associated with the artifact	Show/Hide	List Operations	Expand Operations
attribute-definitions : Attribute definitions management	Show/Hide	List Operations	Expand Operations

Hewlett Packard Enterprise

Fortify Ecosystem- SCA with VSTS



Visual Studio | Marketplace

Visual Studio Team Services > Build and release > HPE Security Fortify VSTS extension

HPE Security Fortify VSTS extension
Eran Argaman | 7 installs | ★★★★★ (1)

Use the Fortify VSTS build tasks in your continuous integration builds to utilize the HPE Security Fortify tools.

[Install](#) [Download](#)

Build better code and secure your software. Use the HPE Security Fortify VSTS build tasks in your continuous integration builds to identify vulnerabilities in your source code.

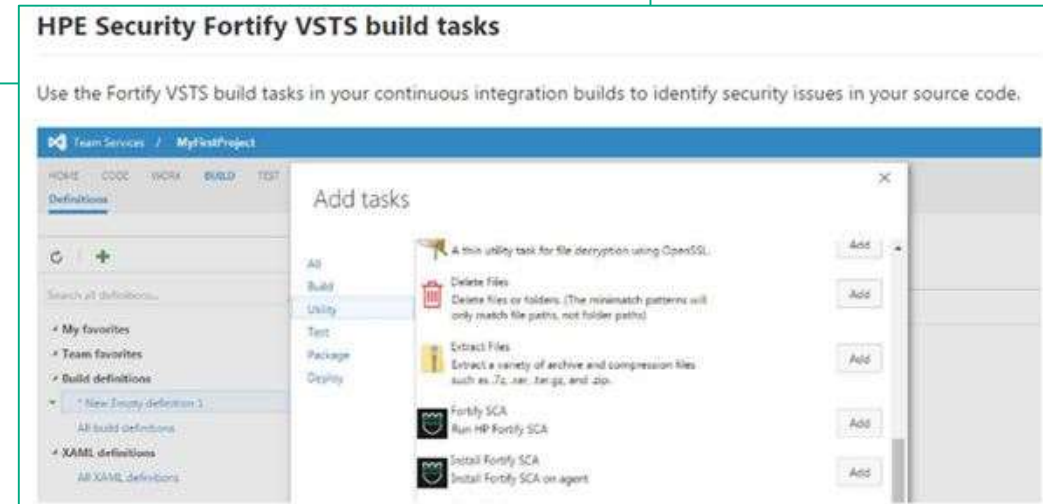
HPE Security Fortify Static Code Analyzer (SCA) is the most comprehensive set of software security analyzers that search for violations of security-specific coding rules and guidelines in a variety of languages. The SCA language technology provides rich data that enables the analyzers to pinpoint and prioritize violations so that fixes are fast and accurate. SCA produces analysis information that helps you deliver more secure software, as well as making security code reviews more efficient, consistent, and complete. Its design allows you to quickly incorporate new third-party and customer-specific security rules.

[Learn more](#)

Categories
Build and release

Tags
build ci continuous integration

Works with



HPE Security Fortify VSTS build tasks

Use the Fortify VSTS build tasks in your continuous integration builds to identify security issues in your source code.

Team Services / MyFirstProject

HOME CODE WORK BUILD TEST

Definitions

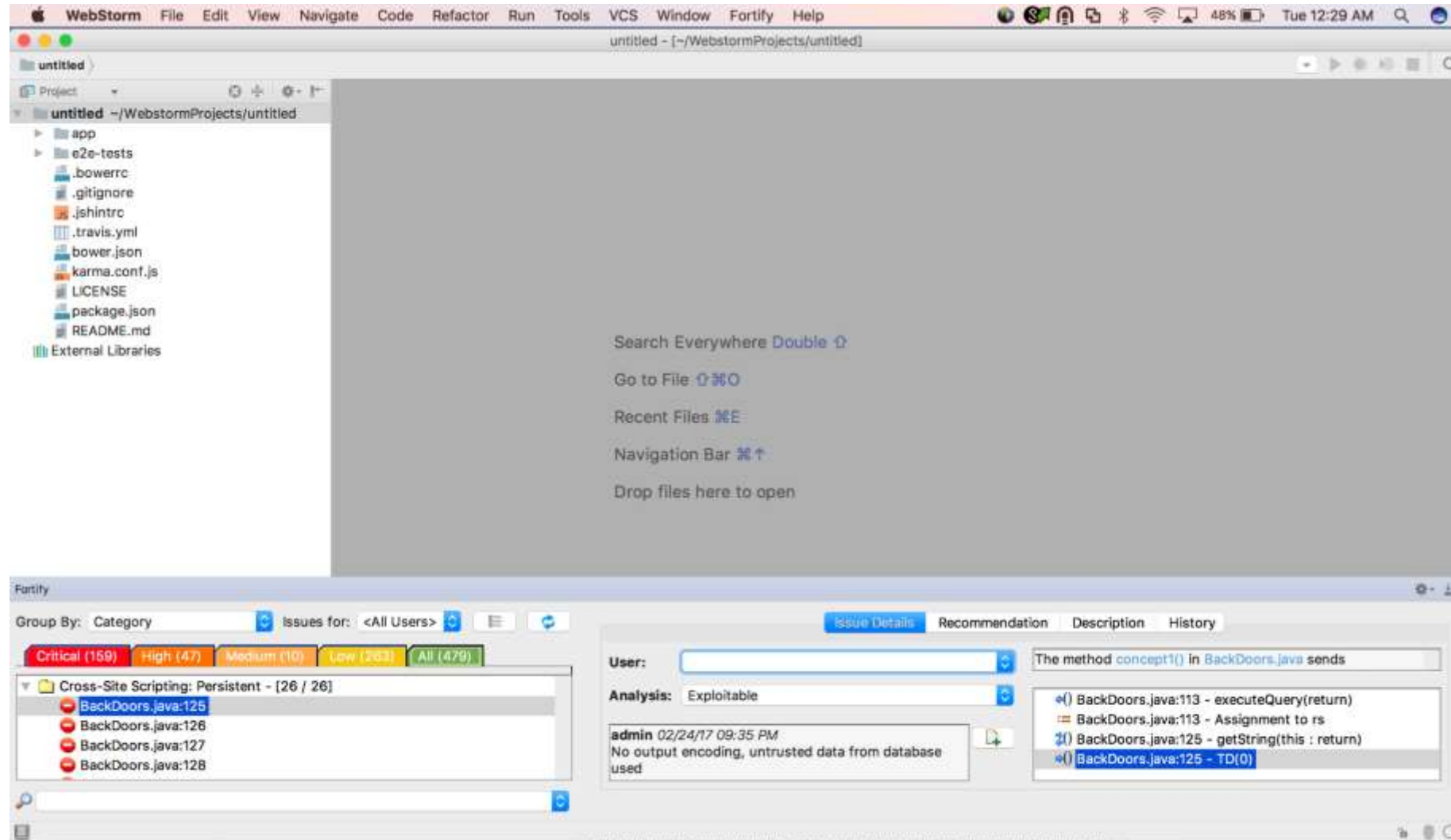
Search all definitions...

My favorites
Team favorites
Build definitions
New Empty definition 1
All build definitions
XAML definitions
All XAML definitions

Add tasks

- A thin utility task for file decryption using OpenSSL
- Delete Files
Delete files or folders. (The minimatch patterns will only match file paths, not folder paths)
- Extract Files
Extract a variety of archive and compression files such as .7z, .rar, .tar.gz, and .zip.
- Fortify SCA
Run HP Fortify SCA
- Install Fortify SCA
Install Fortify SCA on agent

WebStorm Remediation Plugin

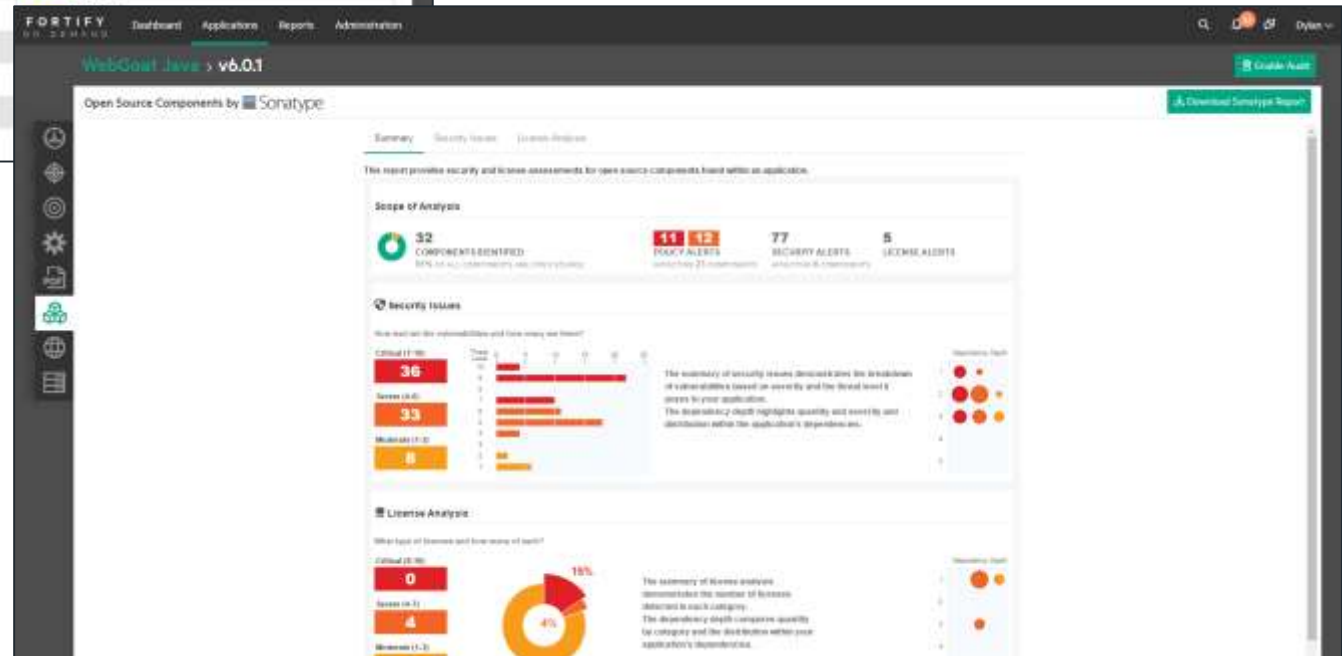
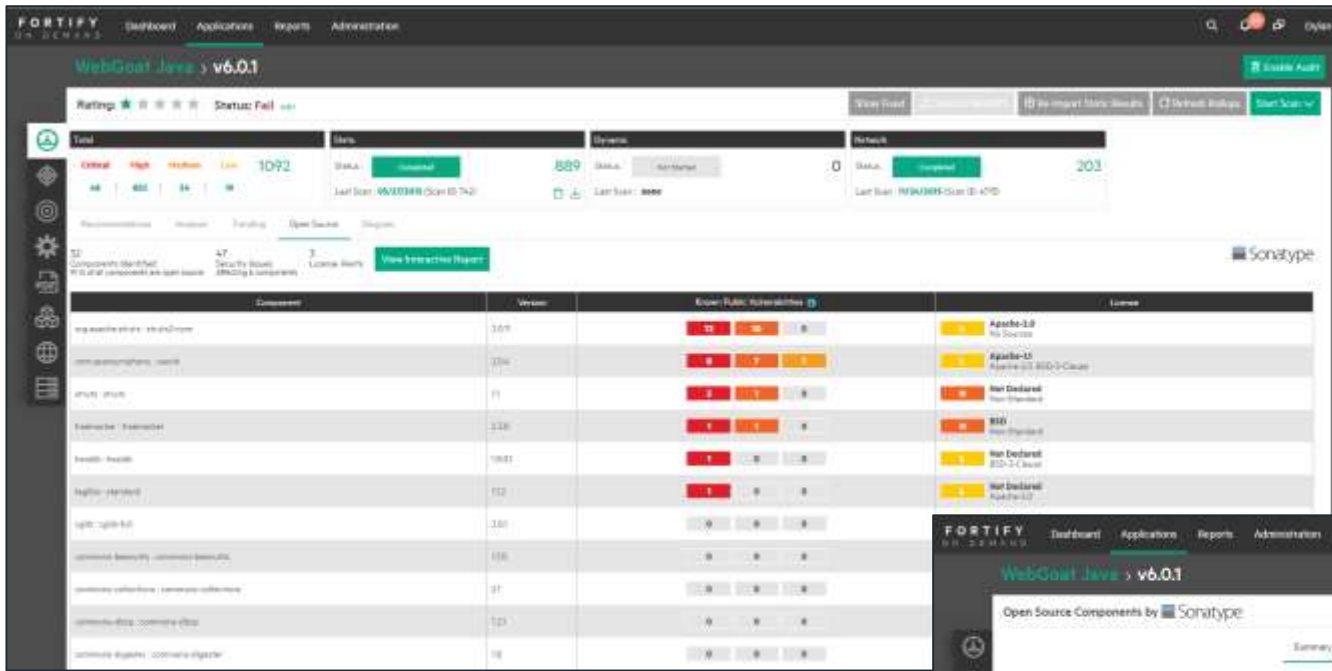


Fortify SSC Integration with Black Duck

Separated by Category & available in one unified view

The screenshot displays the HP Fortify Dashboard interface. At the top, the HP Fortify logo and 'Dashboard' label are on the left, a search bar is in the center, and an 'Application' menu is on the right. Below this, a dark header bar shows 'Bill Payment Processor | 1.1 | Audit' with a refresh icon. A navigation bar contains 'Version 1.1', 'Overview', 'Manage', 'Scan', and 'Audit' (highlighted in blue), along with a 'Filter' button. The main content area is titled 'PCI v3.0 Basic Project Template' and includes 'Group by Analysis...' and 'Filter by Select attributes' options, with an 'Advanced...' link. Action buttons 'Assign', 'Claim', and 'Refresh Table' are present, along with the text '0 of 880 issues selected'. Two blue expandable categories are shown: 'BLACK DUCK SOFTWARE' and 'SCA'.

Fortify Ecosystem- Open Source with Sonatype



Fortify Tools / Ecosystem Roadmap

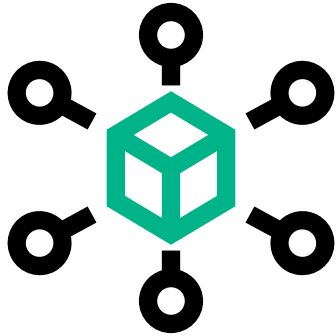
Current <i>Automate</i>	Planned <i>Accelerate</i>
<ul style="list-style-type: none">– Security Assistant for Eclipse– Jenkins SCA Plugin automation– WebStorm IDE plugin– VSTS/TFS extensions for SCA, WI, FoD– Remediation plugins and integration: Bugzilla/JIRA/ALM– Chef cookbooks for SSC/SCA– Audit Assistant and Scan Analytics– Swagger Supported REST APIs– FoD Chatbot– SCA multi-threading– Open source integration: Black Duck & Sonatype	<ul style="list-style-type: none">– Security Assistant for Visual Studio and IntelliJ– SCA Lightbend plugin for Scala– REST API samples/examples– Octane plugin with SSC with validated remediation– Bamboo plugin– Incremental analysis workflow within tools– Smartfix– IAST DevOps rulepack and remediation integration– Dynamic Audit Assistant– Dynamic for developers– SAP CVA SSC plugin update



Fortify SCA

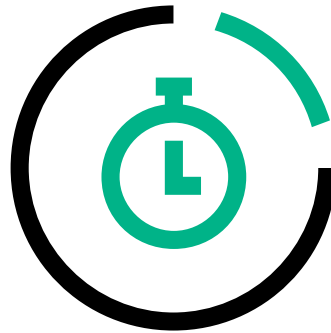
SCA Product Strategy

Roadmap focused on maintaining our leadership position while maximizing customer value



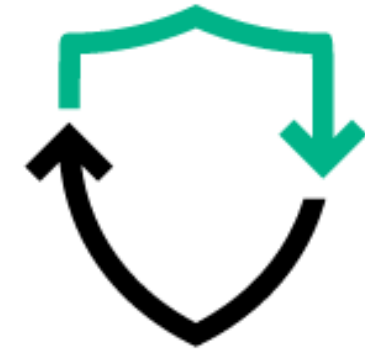
Expansion & Automation

Deliver the most through SAST capabilities across all modern development languages in the enterprise.



Time to value

Empower organizations to quickly assess their software and support modern development practices.



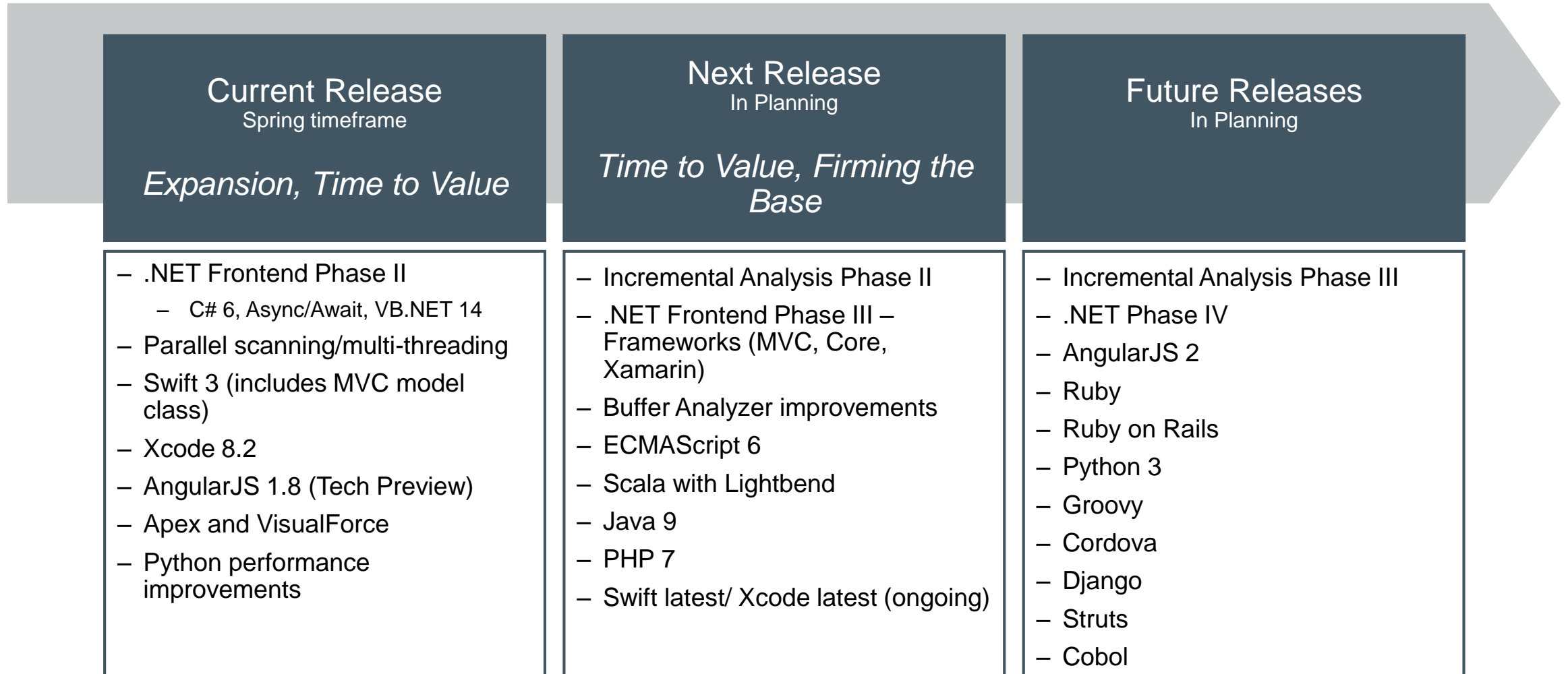
Firming the base

Keep our leadership edge by keeping up to date with core development languages.

Roadmap

	Spring 2017	Fall 2017	Spring 2018	Fall 2018
Firming the Base	.NET Phase II	Buffer Analyzer Improvements	.NET Improvements	
	Swift 3	ECMAScript 6	Ruby	Python 3
	Xcode 8.2	Java 9	AngularJS 2	Cobol
	Python performance improvements	Swift & Xcode latest	ECMAScript 8	
	Swift MVC	PHP 7	Swift & Xcode latest	
Expansion	AngularJS 1.x Tech Preview	.NET Phase III – Frameworks (Core, MVC, Xamarin)	.NET Frameworks	
	Apex and VisualForce	Scala	Cordova	Ruby on Rails
		AngularJS 1.x		Groovy
Time to value	High Performance Parallel Scan	Incremental Analysis Phase II	Incremental Analysis Phase III	Incremental Analysis Improvements

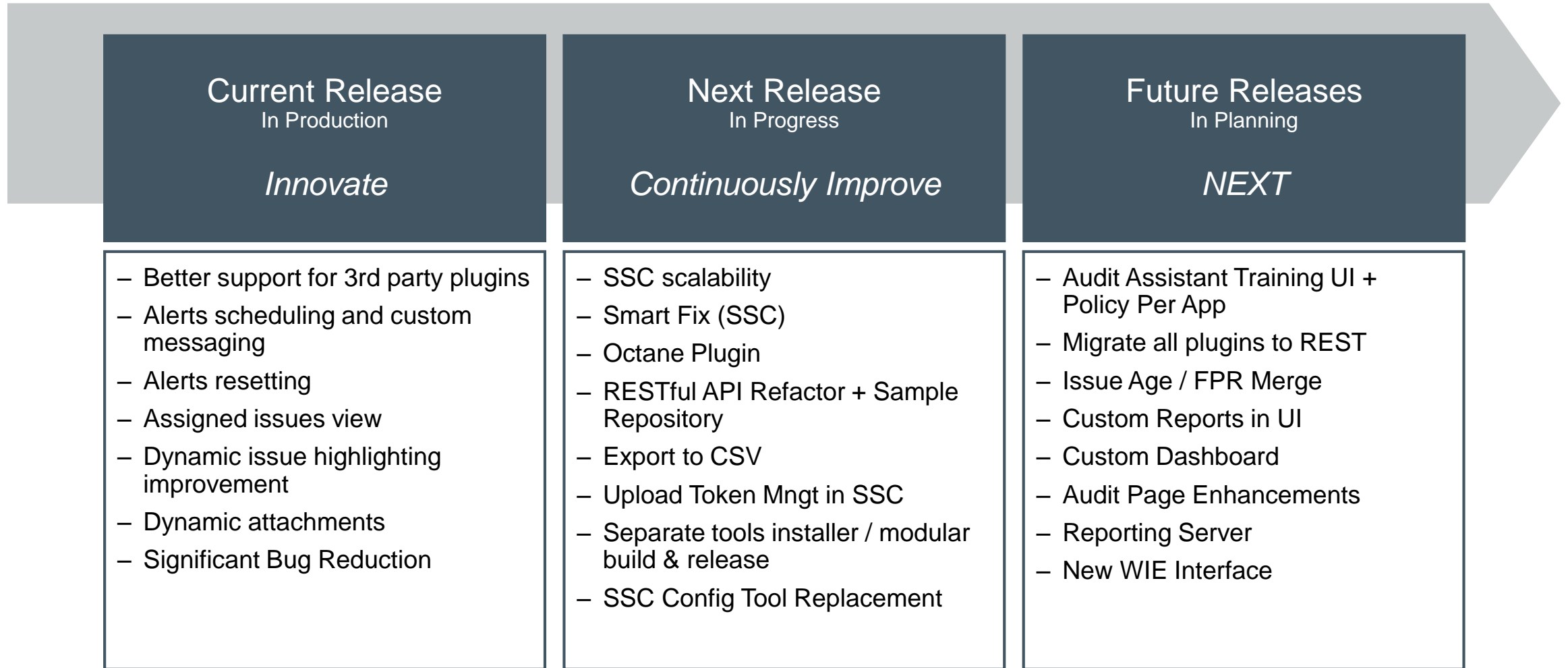
SCA Roadmap





Fortify SSC

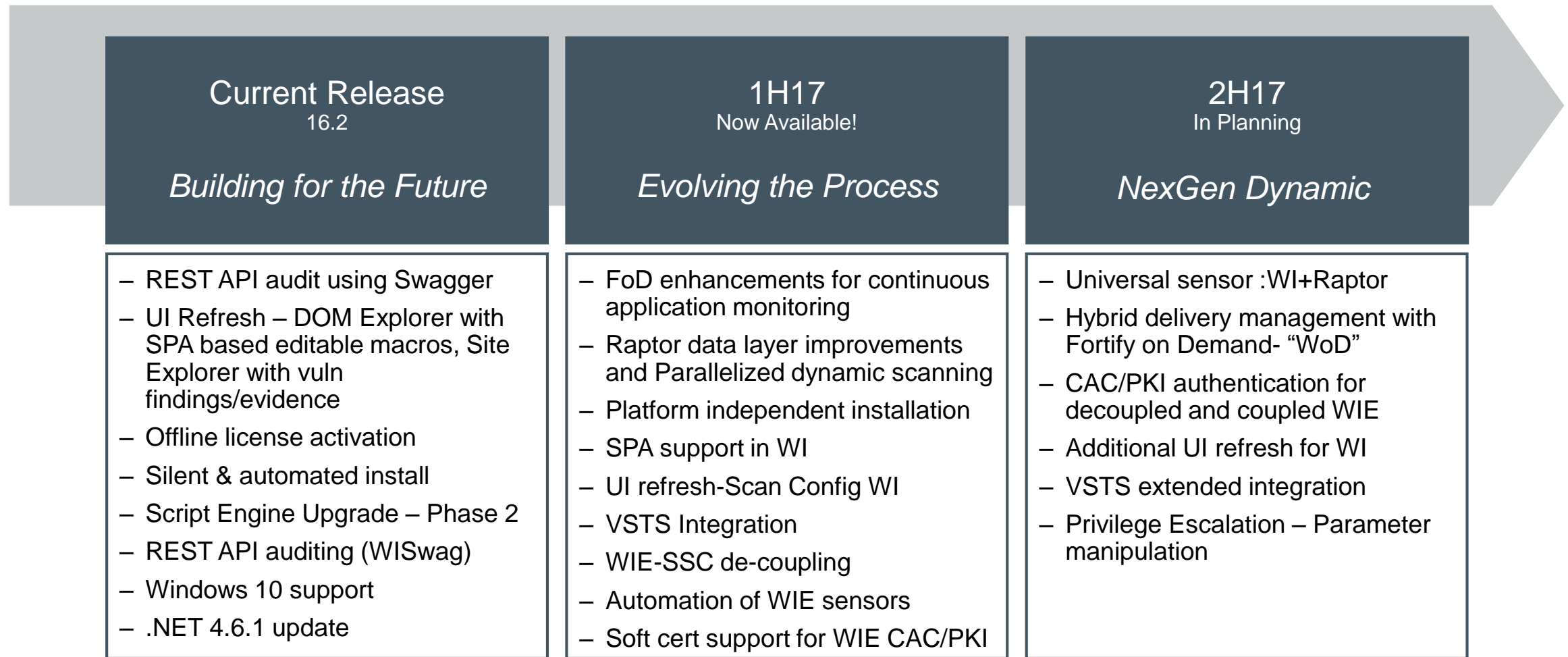
Fortify Software Security Center Roadmap





Fortify WebInspect/WebInspect Enterprise

Fortify WebInspect/WebInspect Enterprise Roadmap



REST API

API	Description
POST scanner	Create a new scan.
DELETE scanner/{scanId}	Delete a scan.
GET scanner/scans?Name={Name}&Status={Status}&StartsAfter={StartsAfter}&EndsBefore={EndsBefore}	Get a list of scans with optional filters applied.
GET scanner/{scanId}?action={action}	Get the status of a specific scan (Running, NotRunning, Complete, Interrupted).
GET scanner/{scanId}/log	Get the Scan Log of a specific scan.
GET scanner/{scanId}.{extension}	Export scan data to one of several formats.
GET scanner/{scanId}?detailType={detailType}	Export a scans data to xml. This is the equivalent of using File>Export>Scan Details in the Webinspect UI.
PUT scanner/{scanId}	Add sessions to a scan.
PUT scanner/{scanId}?action={action}	Update the scan status.
GET scanner/macro	Get a list of available macros.

- Integration with 3rd party ecosystem.
- Service based architecture

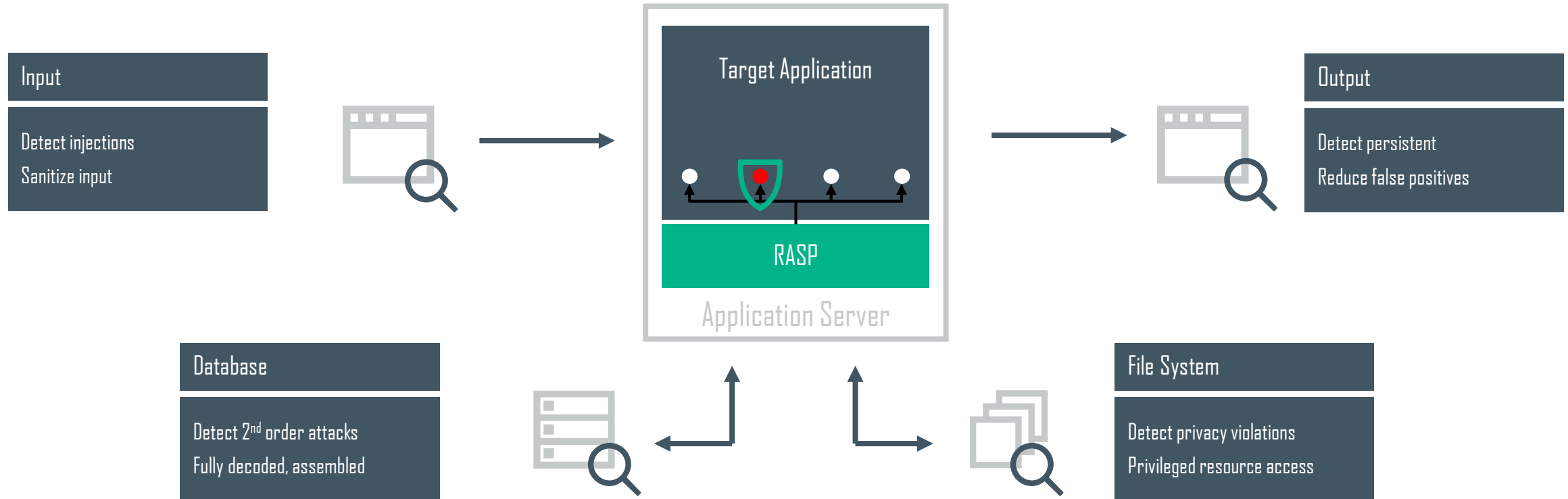
```
C:\Users\aravindv>curl http://localhost:8083/webinspect/scanner/scans
[{"ID":"627ed0d8-ab15-4d11-902c-d743d00239f5","Name":"","StartTime":"2016-08-25T18:39:15","Status":"Complete"}, {"ID":"72b1d291-6fe0-4804-8844-b76a32e965e4","Name":"Site: http://zero.webappsecurity.com/","StartTime":"2016-08-26T11:46:25","Status":"Interrupted"}]
C:\Users\aravindv>
```



Application Defender

HPE Security Fortify Application Defender

Context-Sensitive rules for increased coverage and accuracy



HPE Security Application Defender Overview



Protection for zero-day Struts2

Requires no code changes

- Struts2 S2-045, CVE-2017-5638 is a critical vulnerability which can lead to remote code execution. A new protection rule, Malformed Request: Bad Content-Type, was promptly added to the protection rulepack which can accurately detect and block this attack.
- Fortify SRG shines again
 - S2-045 was released in March as CVE-2017-5638.
 - SRG quickly acted to provide a protection rule in Application Defender.
 - However, further research by our SSR team uncovered an additional attack vector. Our SSR team published this additional vector in S2-046, and created an additional rule to protect against this vector



Fortify Application Defender - Protection

30 Vulnerability Categories – Oct 2016

Discovery: Known Vulnerability Scanner Activity	Forceful Browsing	Poor Error Handling: Unhandled Exception
ClassLoader Manipulation: Struts	Java Deserialization	Privacy Violation: Internal
Command Injection	Header Manipulation	Slow Method Call: Slow Database Query (Batch Processing)
Command Injection: Shellshock	LDAP Injection	Slow Method Call: Slow Database Query (Web Request)
Cookie Security: HTTPOnly not Set on Session Cookie	Malformed Request: Missing Accept Header	SQL Injection
Cross-Site Scripting	Malformed Request: Missing Content-Type	System Information Leak
Dangerous File Inclusion: Local	Malformed Request: Use of Unsupported Method	XML Entity Expansion Injection
Dangerous File Inclusion: Remote	Method Call Failure: Database Query	XML External Entity Injection
Denial of Service: Parse Double	Open Redirect	XPath Injection
Directory Listing	OGNL Injection	

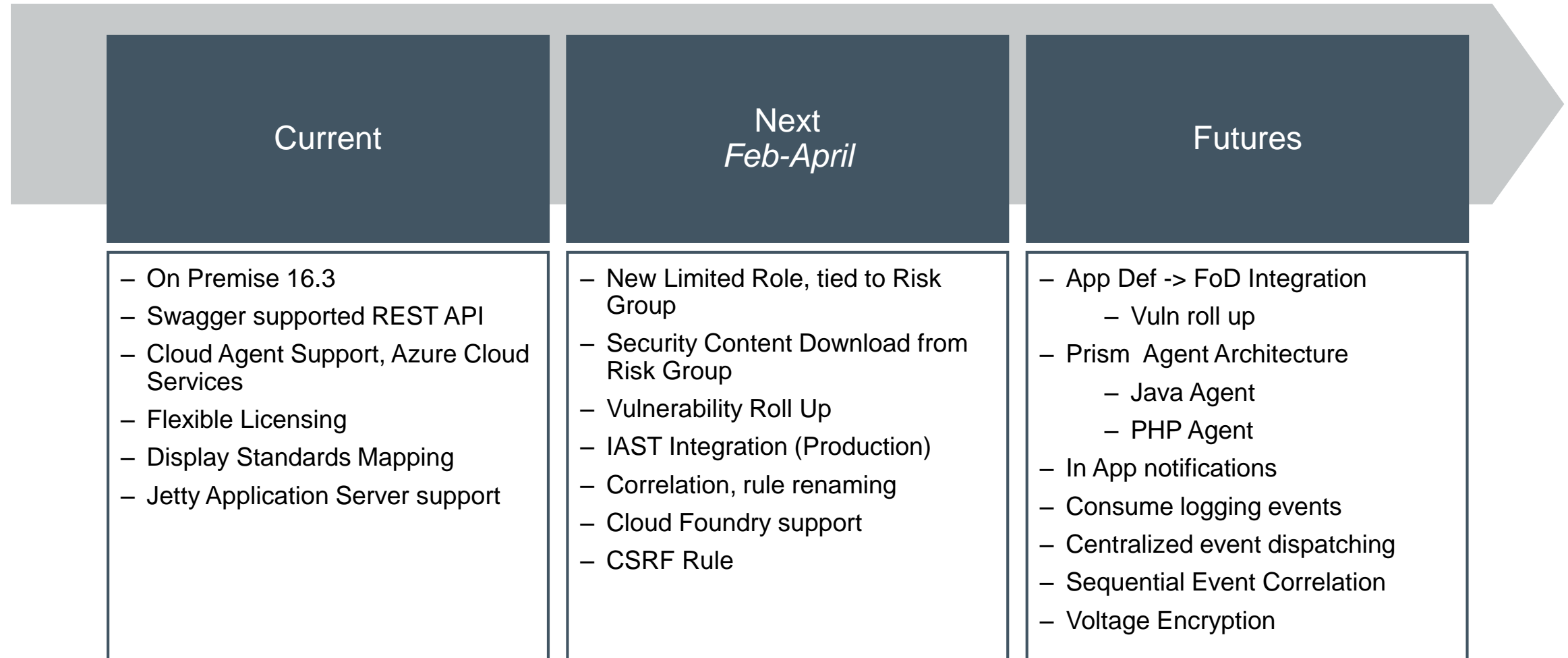


Fortify Application Defender – Application Logging

60 Application Logging Categories – Oct 2016

Command Execution	HTTP Session Start	Security Exception Created: Illegal Access	Unified Logging:Slf4j
Crypto Exception Created: Bad Padding	HTTP Session Stop	Security Exception Created: Invalid Algorithm Parameter	User Logoff
Crypto Exception Created: Exemption Mechanism	Network Socket Bind	Security Exception Created: Invalid Key Specifications	User Logon: Failure
Crypto Exception Created: Illegal Block Size	Network Socket Close	Security Exception Created: Invalid Parameter Specification	User Logon: Success
Crypto Exception Created: No Such Cryptographic Algorithm	Network Socket Connect	Security Exception Created: Login Exception	User Management: Add User to Group
Crypto Exception Created: No Such Padding	Network Socket Shutdown	Security Exception Created: No Such Provider	User Management: Change Password
Crypto Exception Created: Short Buffer	Security Exception Created: Access Control	Security Exception Created: Privileged Action	User Management: Create Group
Database Query	Security Exception Created: Basic Key Exception	Security Exception Created: Signature	User Management: Create User
File Copy	Security Exception Created: CERT Certificate	Security Exception Created: Unrecoverable KeyStore Entry	User Management: Delete Group
File Create	Security Exception Created: CERT Certificate Revocation List	Security Exception Created: Unrecoverable KeyStore Key	User Management: Delete User
File Delete	Security Exception Created: CERT Path Builder	Spring Validation Failure	User Management: Remove User from Group
File Move	Security Exception Created: CERT Path Validator	Struts Validation Failure	Web AccessLog
File Read	Security Exception Created: CERT Store	Unified Logging: JCL	Web Application Running
File Write	Security Exception Created: Digest Security	Unified Logging: JUL	Web Application Start
General Exception Created	Security Exception Created: Generic KeyStore Exception	Unified Logging: Log4j	Web Application Stop

Application Defender Roadmap





Hewlett Packard
Enterprise

Thank you

Scott Snowden scott.b.snowden@hpe.com