Are you ahead or behind? Research findings on Application Security in DevOps

September 20, 2016

© Copyright 2016 Vivit Worldwide

Brought to you by

© Copyright 2016 Vivit Worldwide

Hosted By

Stevan Zivanovic
Principal Technical Account Director
Infuse Consulting
Agile SIG Leader

© Copyright 2016 Vivit Worldwide

Today's Speaker

Cindy Blake CISSP
Product Marketing Manager
Hewlett Packard Enterprise

© Copyright 2016 Vivit Worldwide

Housekeeping

- This “LIVE” session is being recorded
  Recordings are available to all Vivit members

- <u>Session Q&A:</u>
  Please type questions in the Questions Pane

© Copyright 2016 Vivit Worldwide

Webinar Control Panel

Toggle View Window between Full screen/window mode.

Questions

© Copyright 2016 Vivit Worldwide

Hewlett Packard Enterprise

Are you ahead or behind? Research findings on Application Security in DevOps

Cindy Blake, HPE Security Fortify
hpe.com/software/fortify

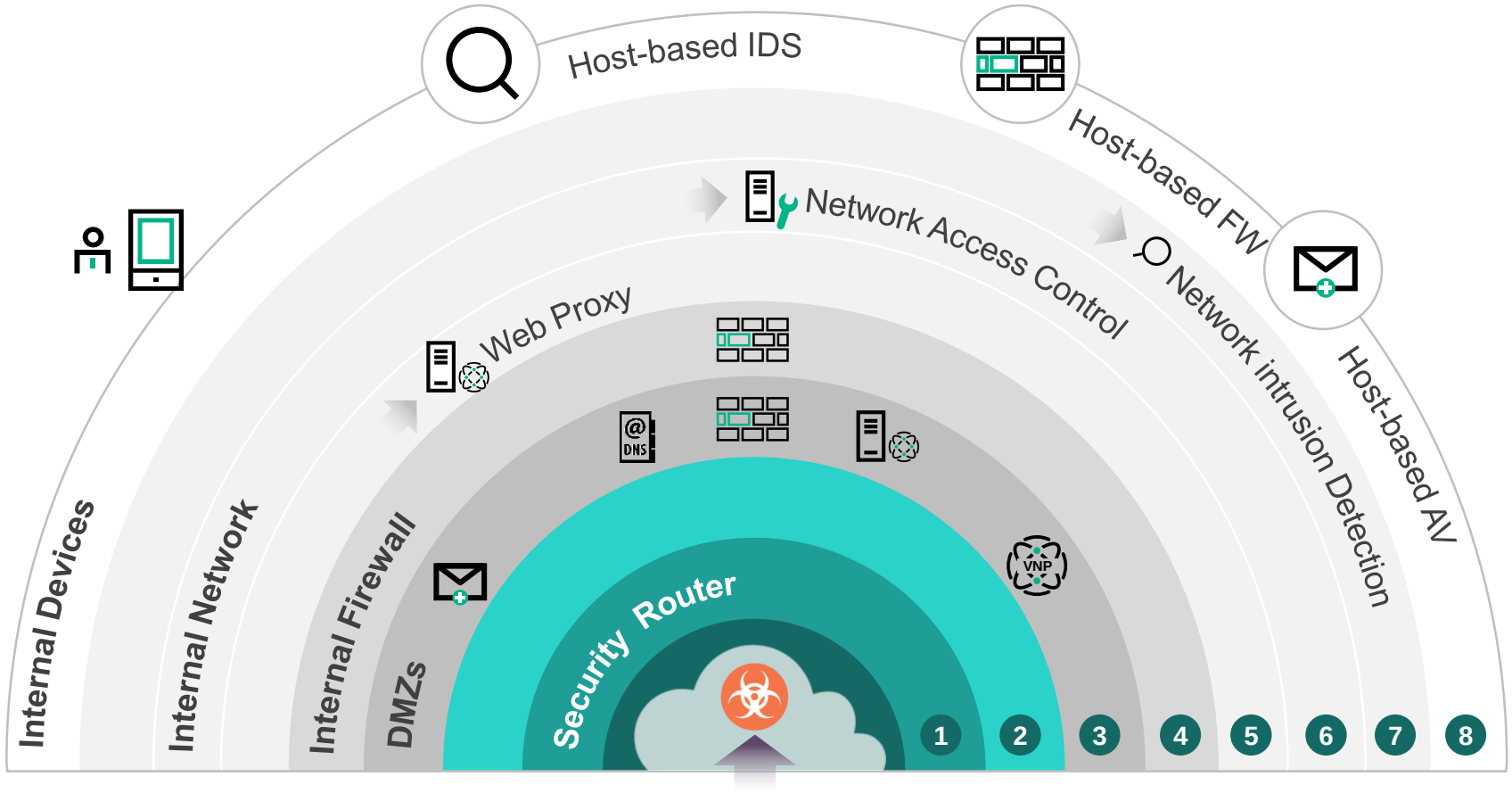
Sept 20, 2016

Agenda

- Why research Security in DevOps?
- Key Takeaways
- Translating research into action
- Use cases

Why research security in DevOps?

Existing network and perimeter based security is insufficient



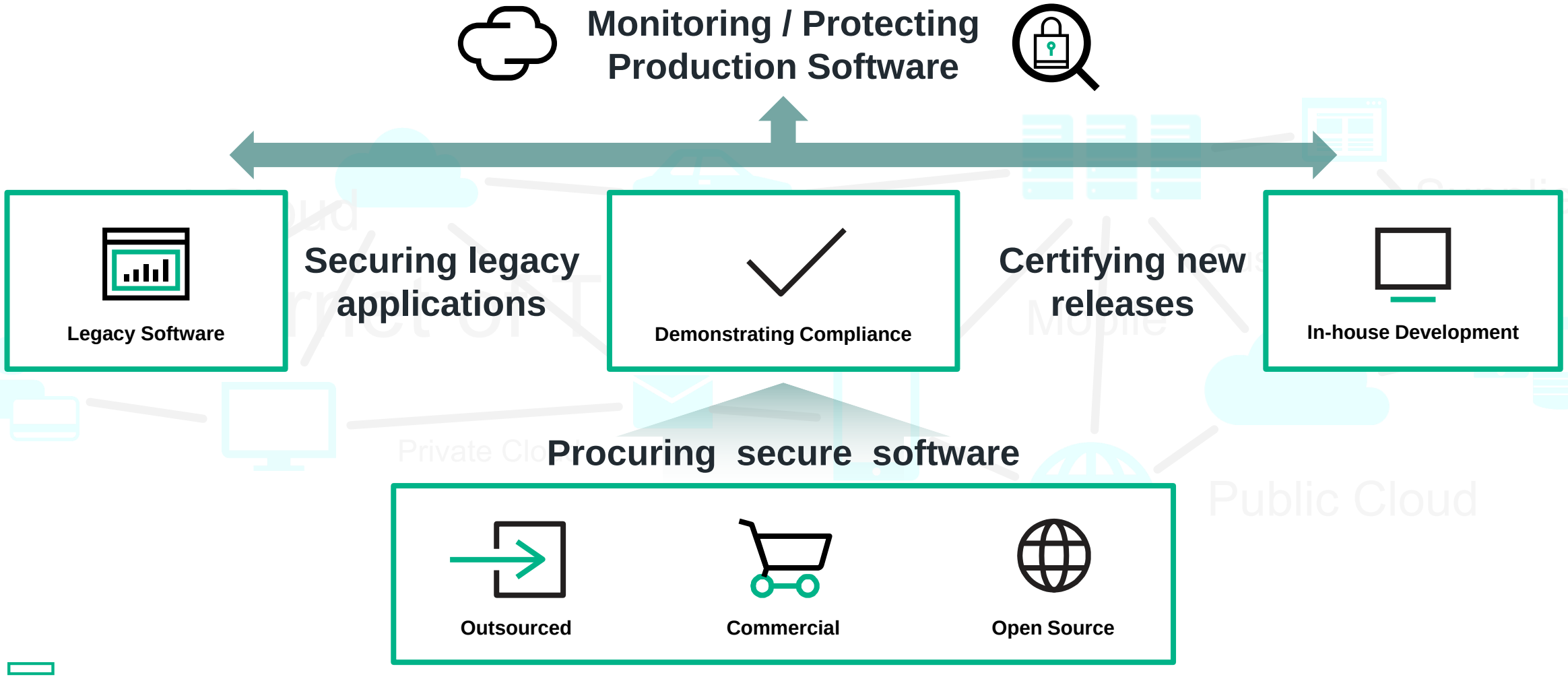
84% of breaches exploit vulnerabilities in the application layer

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

Hewlett Packard Enterprise

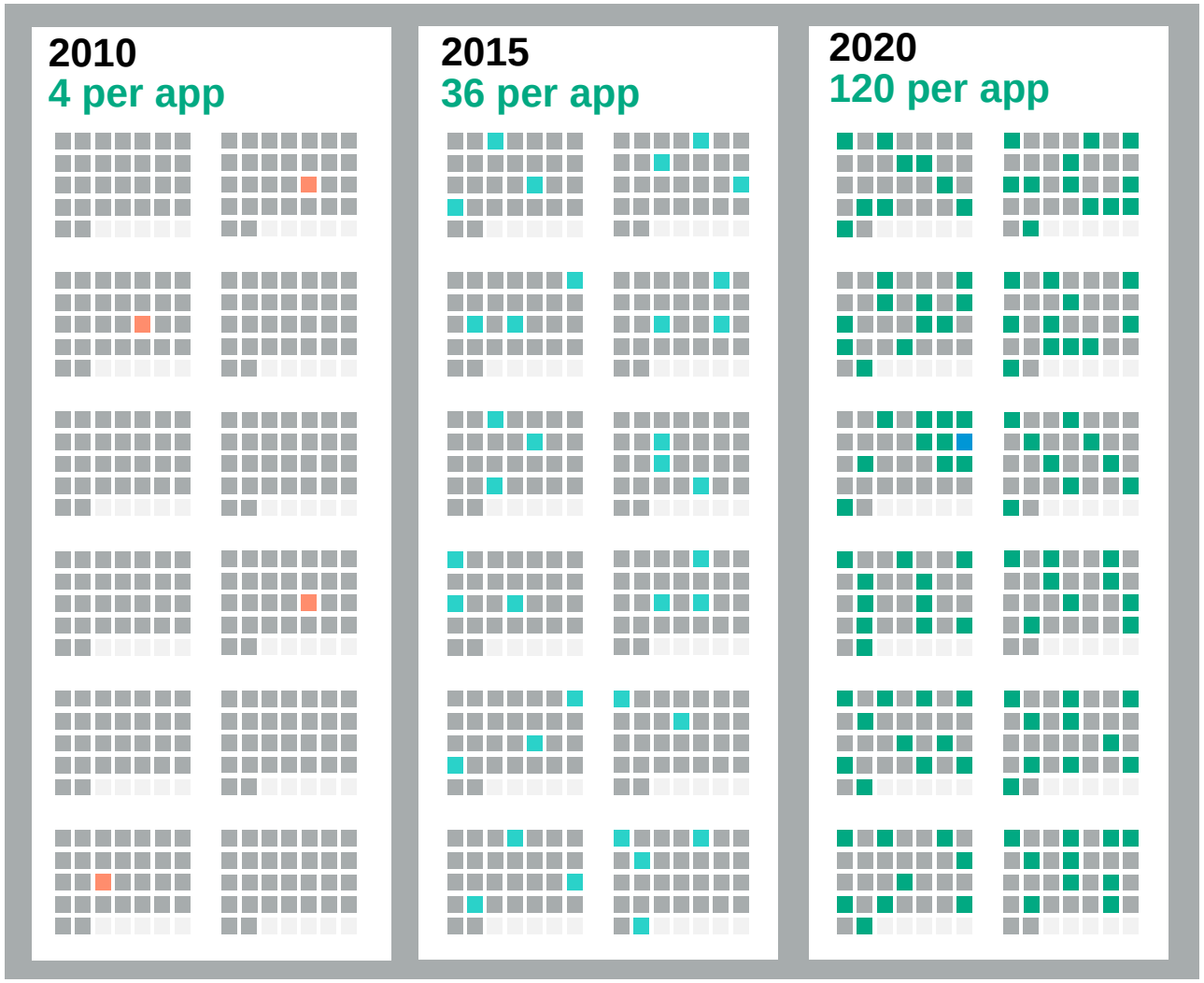
The number of apps is growing

Increasing platforms and complexity …many delivery models



Hewlett Packard Enterprise

Developers need to move at the speed of business innovation



Number of Releases per year

Thanks to consumerization, users now expect continuous improvements to apps rather than the traditional annual mega-updates

Hewlett Packard Enterprise

The study

DevOps AppSec Habits & Practices Research

Project Goal	Objectives
To assess the general habits, practices and tools used by those practicing DevOps, as well as their security point of view	- Evaluate the “dev” and “ops” sides of DevOps (Developers / IT Professionals that practice varying levels of DevOps) - Assess current practices, processes and tools used - Identify key pain points, challenges and barriers to DevOps - Determine the security point of view within DevOps

Key Takeaways

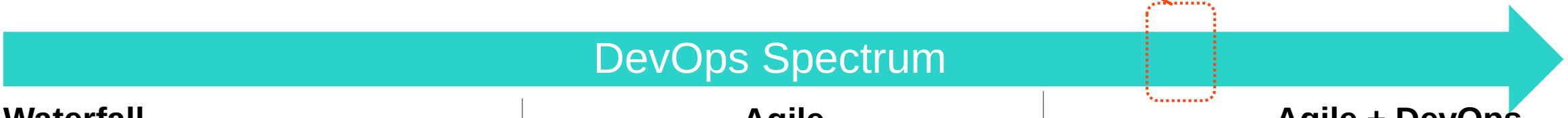
Key Takeaways - DevOps

1. It is a challenge for Enterprise organizations to go from Waterfall to Agile and then add DevOps on top of that
2. Most were still in the beginning stages of DevOps: Putting in place teams, deploying new tools, learning how to work together
3. Developers embrace DevOps; IT Ops see the benefits, but do not like to lose control over their infrastructure
4. Certain tools have been instrumental in supporting DevOps

Advanced, DevOps-forward organizations few and far between

Those practicing more advanced DevOps appeared to be organizations that were “born” into it (i.e., Facebook, Google, AirBnB) and did not face the barriers most Enterprise organizations have to overcome (i.e., Compliance mandates that do not allow for *automated deployment*.

Most seemed to be about here – working to advance both DevOps and Agile practices.



Waterfall

Most Enterprise organizations appear to have moved away from a Waterfall methodology

Agile

Many organizations still working to become more agile and have not even begun to consider DevOps

Agile + DevOps

Very difficult to find those at the very end of the spectrum – most will not and are not trying to be the most advanced..

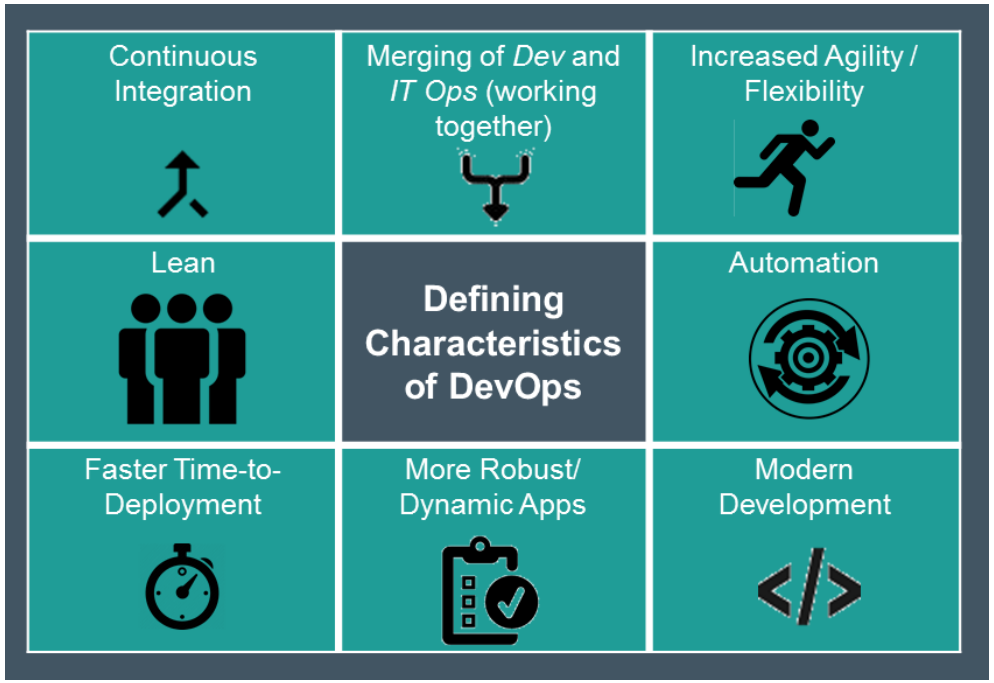
It was evident that most of the participants *wanted* to be practicing DevOps, but did not have the more sophisticated practices and processes in place. To get there, they need a combination of tools and change in processes and practices.

Hewlett Packard Enterprise

Defining characteristics of DevOps
Agility, *Automation*, *Continuous*

Similar to “the cloud” a few years ago, DevOps is somewhat of a buzzword that is seen as the next big thing, but most do not know exactly what it means to their organization.

There were key characteristics that rose to the top:



“I look at DevOps as automating processes that five years ago people would do manually. So things like automatically building everyone’s branch when they check in any new code. Or automatically running a code analysis tool at night on what people have committed. Automatically deploying stuff to production.”
(IT Ops)

For most, it is an *Evolution* and not a *Revolution*

Among those interviewed, there did not appear to be an urgency in terms of fully implementing DevOps. For these companies, processes like *continuous delivery* are an ideal state, but not essential right now. Those that have to have them to do business, often already do (i.e., SaaS Providers, ISVs).

Continuous Integration

Difficult to accomplish; can break system

Automated Regression Tests

Very few doing, but can recognize value

Infrastructure as code

Many do not really know what this means.

Automated Browser Testing

Some confusion as to what this is; may be unique for some apps

Continuous Delivery

The "end goal" of DevOps; most are still on scheduled release.

Clustered Deployments

A start towards automated deployments.

Real-time Reports

Many would like a real-time dashboard, but still do not have.

Automated Deploy to Production

Most still deploy first pre-prod environments; not comfortable yet.

It was difficult to tell how long it would take for these Enterprise organizations to implement the more advanced processes and how far along they would actually get. So far, they have been very happy with some of the more immediate benefits (i.e., faster app delivery)

Advanced, cloud-like environments most supportive of DevOps

In order to fully implement DevOps, an on-demand infrastructure is needed (Continuous Deployment). Most IT Ops are working to get their on-premise infrastructure in shape (Private Cloud), while others are finding it easier to go straight to the cloud.

On-premise DevOps infrastructure:

- Highly virtualized
- Increase use of Containers
- More “Software Defined”
- IT becoming a service center

Why Cloud?

- Infinite scalability
- On-demand infrastructure
- Pay-per-use (never over-provision)
- Developer friendly (i.e., PaaS)

“Even our production software runs in virtual environments. We’re moving away from physical hardware.” (App Manager)

“We’re finding it with moving towards the Linux platform, we’re trying to get more out of our servers using the containers because they are much more efficient.” (IT Ops)

It is a challenge for Developers and IT Ops to work together

- Breaking down silos
- Cultural barriers
- Resistance to change
- Complexity of tools
- Defining security
- Too many tools!
- Job Security (IT)

It's the classic conflict between infrastructure team and application development teams. There are politics and there's also territorial type dynamics. (App Manager)

Top Challenges Highlighted in Teal

Key Takeaways - Tools

- Most were satisfied with their tools, but were only using a fraction of their capabilities
- Git is de facto standard for version control. Almost all interviewed are using
- A number of Microsoft tools were used for practicing Devops (e.g. TFS/VS)
- Many were still in process of fully implementing/utilizing tools for continuous deployment (e.g. Chef, Puppet)
- Jenkins was most frequently mentioned for continuous integration; TeamCity also frequently mentioned
- HPE tools mentioned most for testing, monitoring and security

Key Takeaways - Security

5 There is a lot of confusion surrounding App Security – Developers often think of protecting the source code first, not the app's security vulnerabilities

6 Developers and IT Ops care about security, but feel it is under control or someone else's issue (i.e., Security, InfoSec, Compliance Departments)

7 Security has yet to be fully integrated into the DevOps process (i.e., SecDevOps)

8 Usage and awareness of application security tools appeared to be low - Most rely heavily on perimeter/firewall security and 3rd party security consultants

22

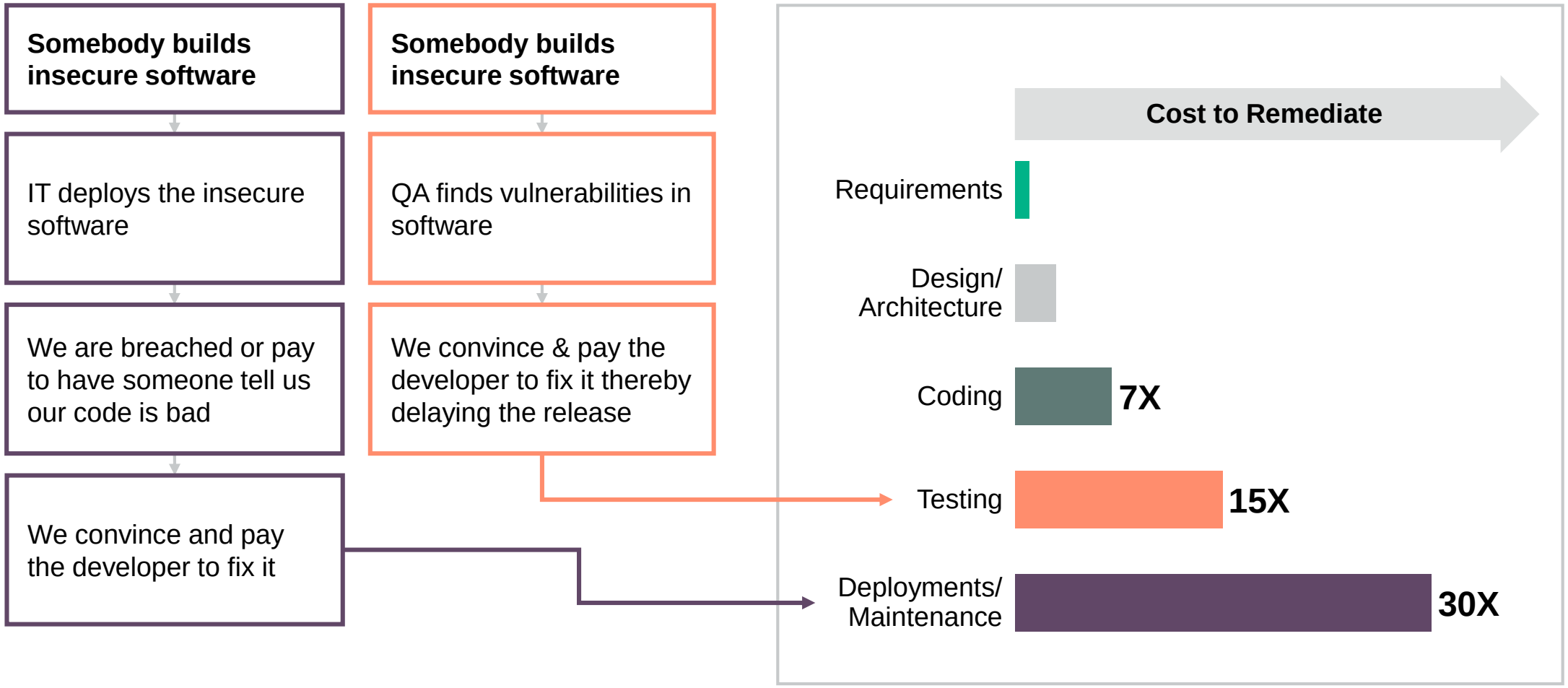
Contribute your thoughts.
Take the survey:
surveymonkey.com/r/VivitSecDevOps

Watch for a comprehensive report this Fall:
State of Secure DevOps

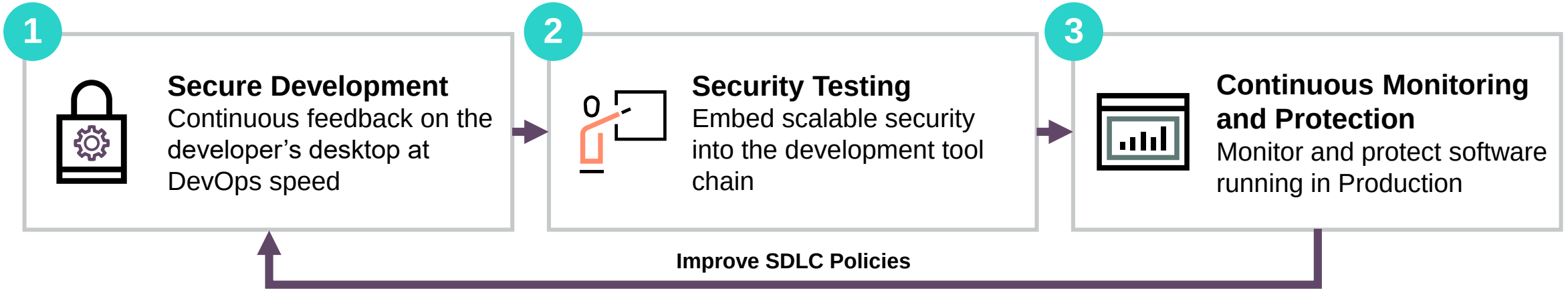
Hewlett Packard Enterprise

Translating research into action

A reactive approach to AppSec is inefficient and expensive



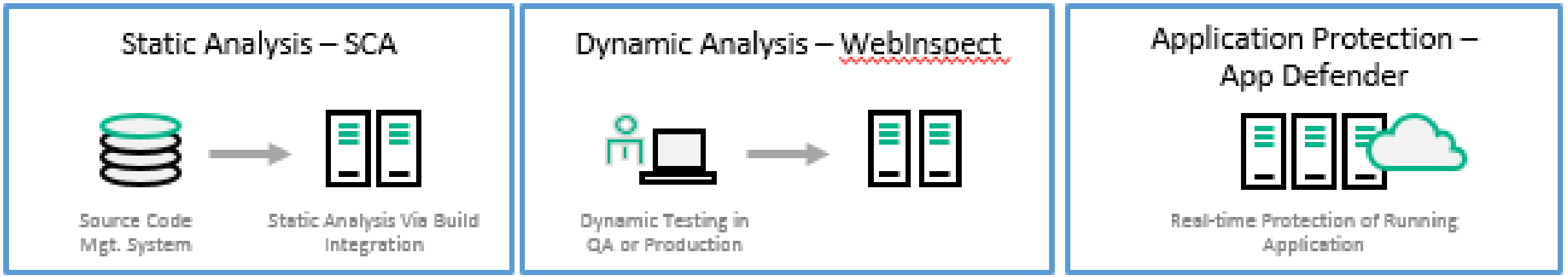
The right approach for the new SDLC – Build it in



This is application security for the new SDLC

HPE Security Fortify Application Security Solutions

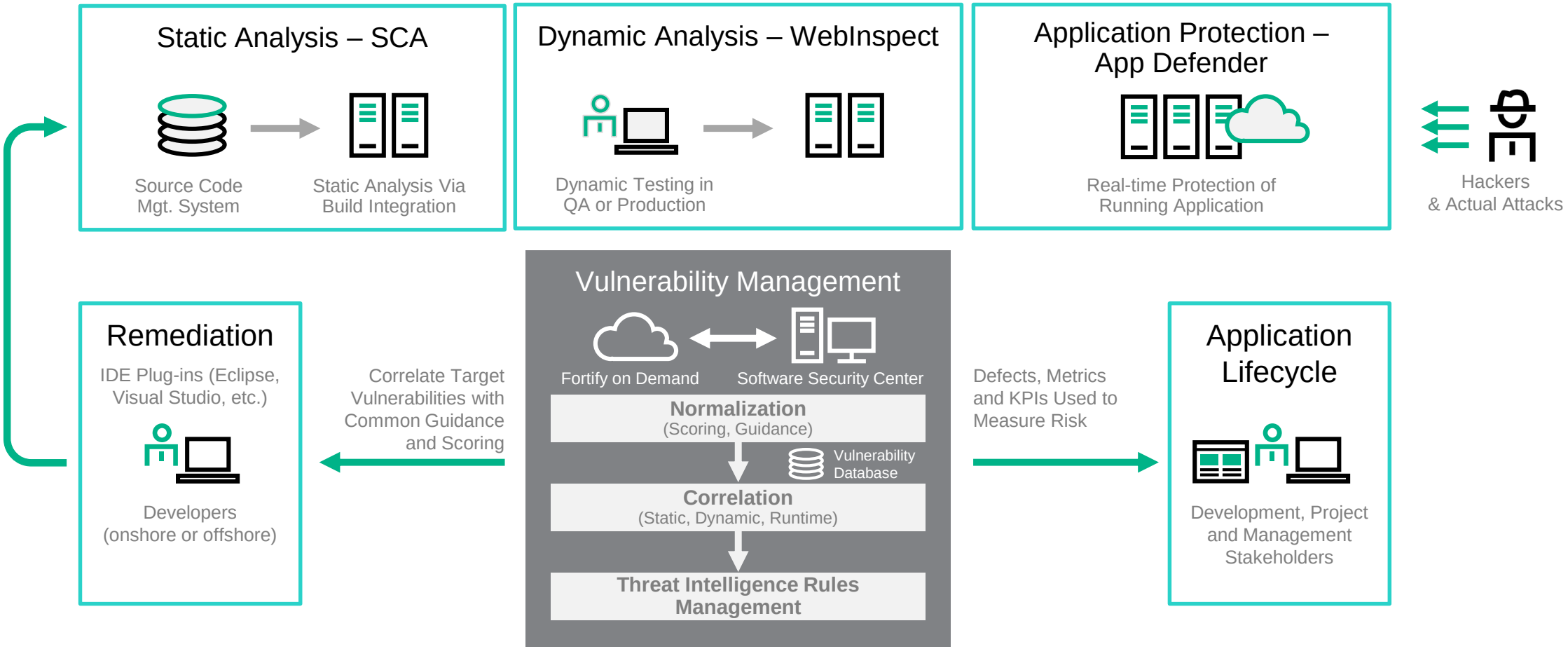
On premise and on demand



Hewlett Packard Enterprise

HPE Security Fortify Application Security Solutions

On premise and on demand



Hewlett Packard Enterprise

Use cases: Where is your focus?

Use case 1: Eliminate defects early

Bring application security closer to the Developer

What you need:

Appsec solution for developers to identify and remediate security vulnerabilities in source code **within the native developers environment**

Real-time, instant security results as the developer is writing code.

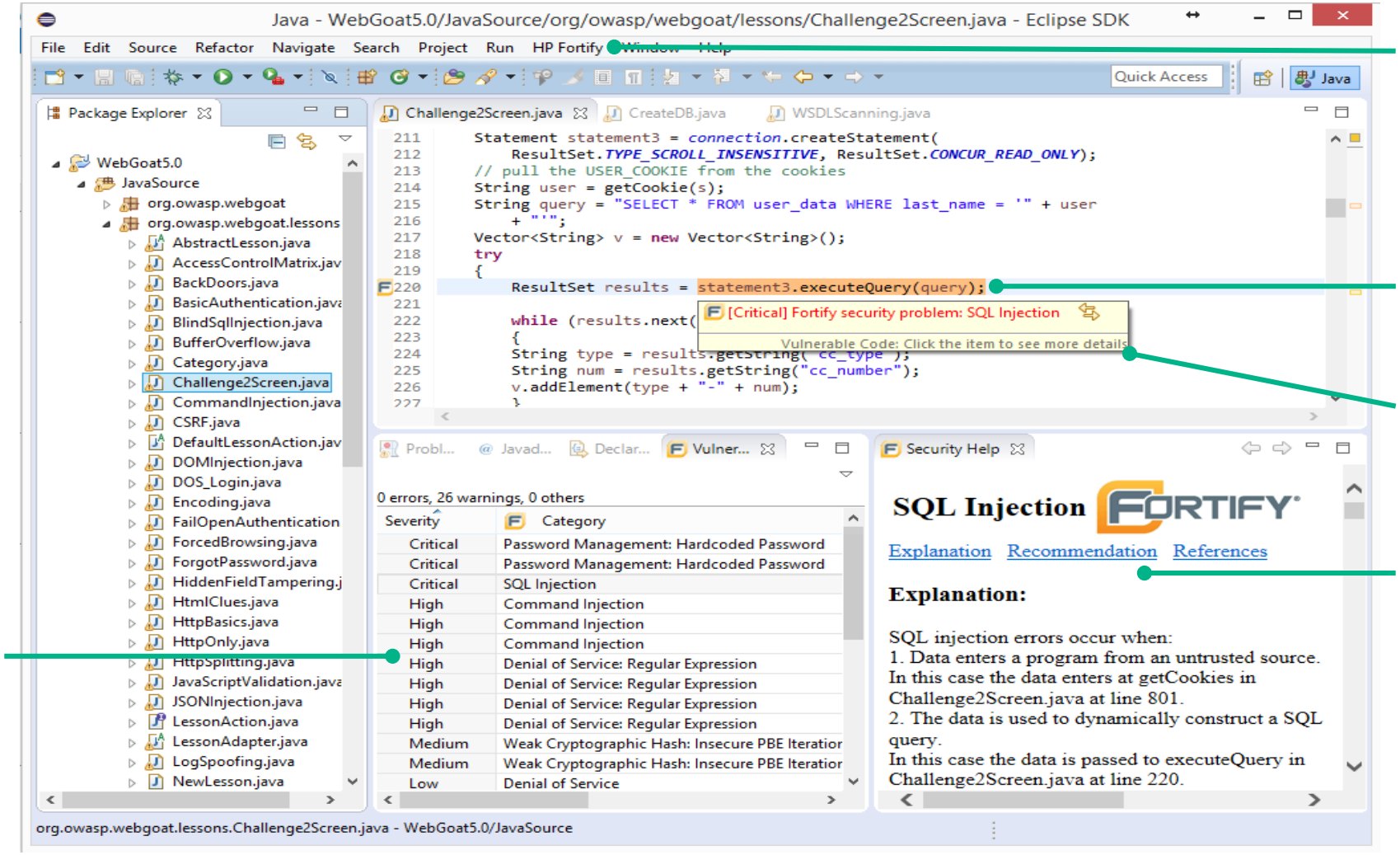
Enable immediate remediation ensuring secure code as your “shift left” in your dev process.

Enable developers to assess for security weaknesses.

Shift left to resolve security defects during development

HPE Security Fortify DevInspect and SCA

Security Assistant feature: Real-time lightweight analysis of the source code



Fortify menu for additional options

Vulnerable line of code is highlighted as developer code & provides tips for additional information

Level of criticality

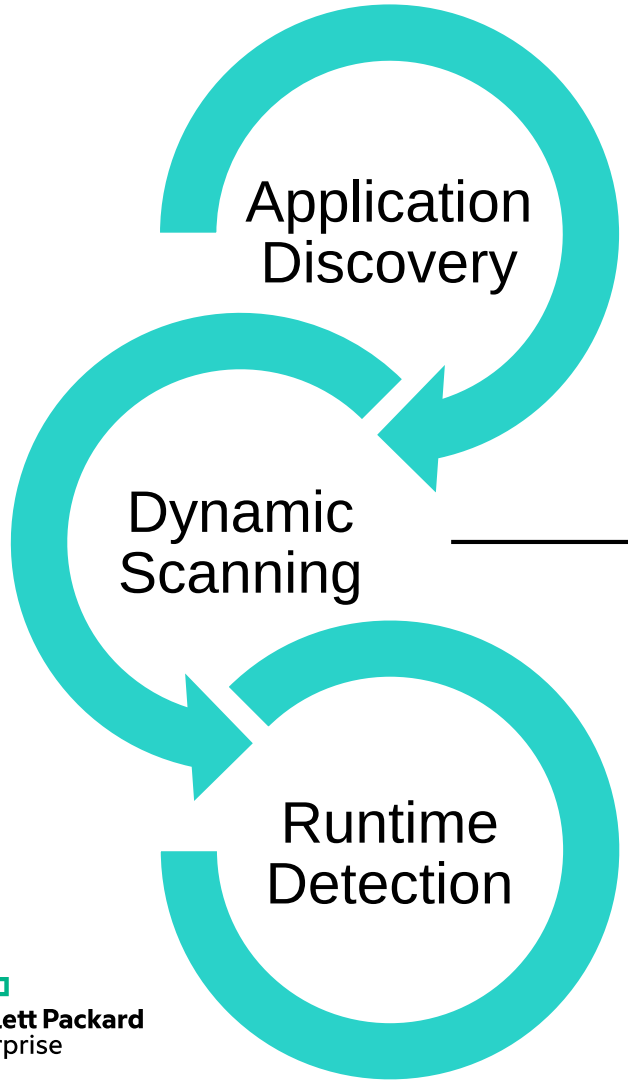
Type of vulnerability, explanation and detailed remediation guidance

All issues detected in the project

Hewlett Packard Enterprise

Use case 2: Rapid deployments

Continuously discover, profile and assess your entire application portfolio



Regional websites
Marketing campaigns
Mergers & acquisitions

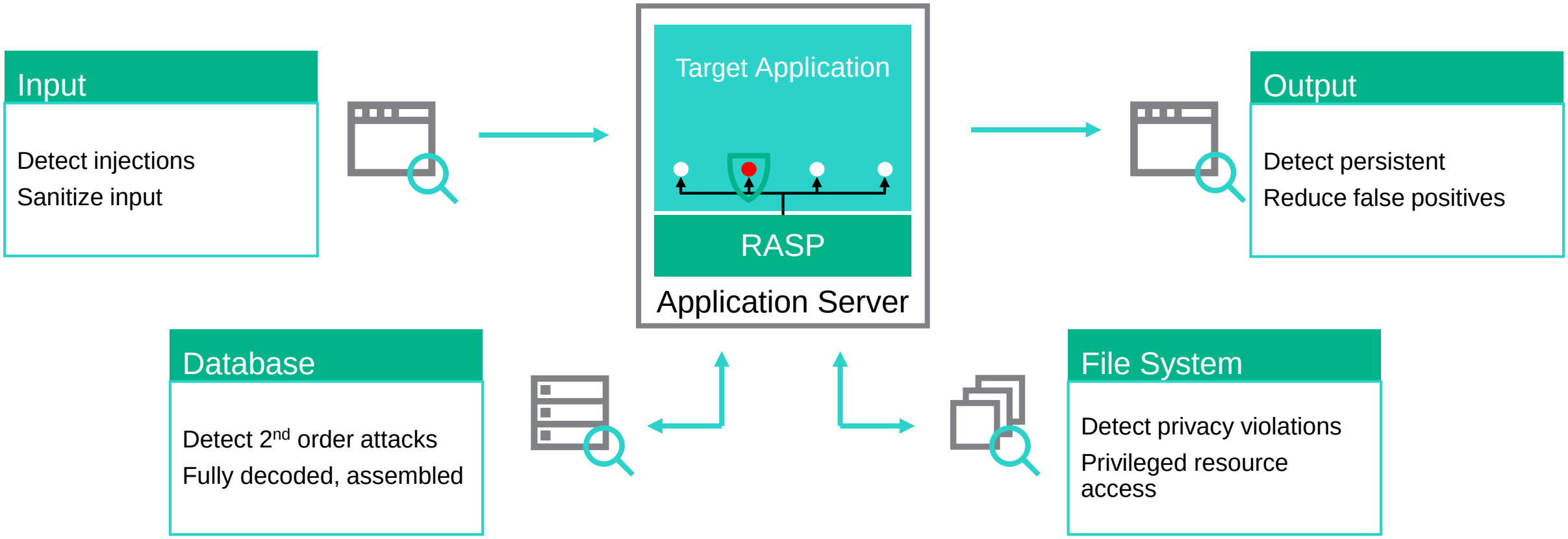
New vulnerabilities
Risk profile changes
Insecure deployments

Exploit attempts
Suspicious user behavior
Data extraction

Hewlett Packard Enterprise

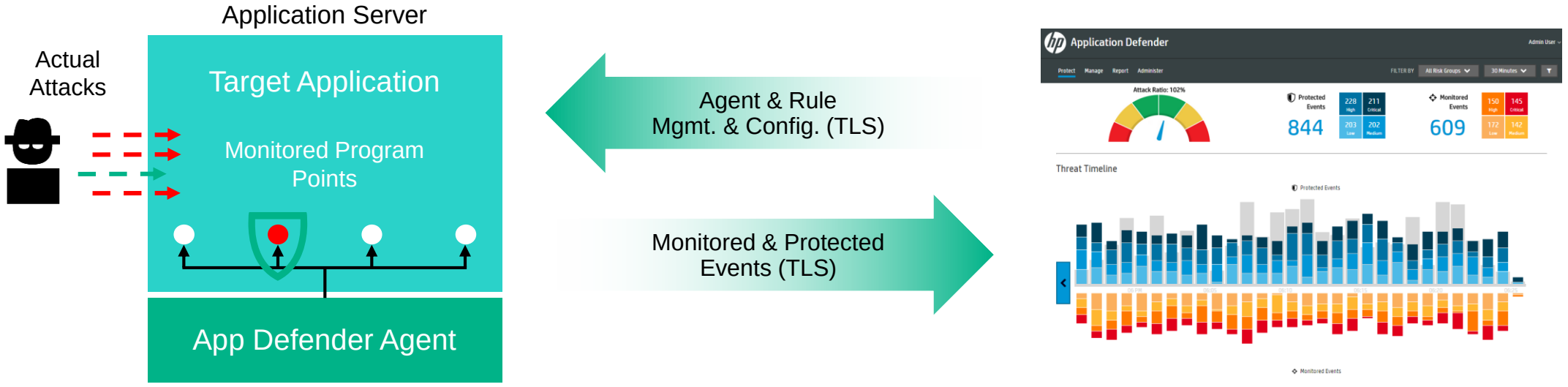
Runtime detection

How it works



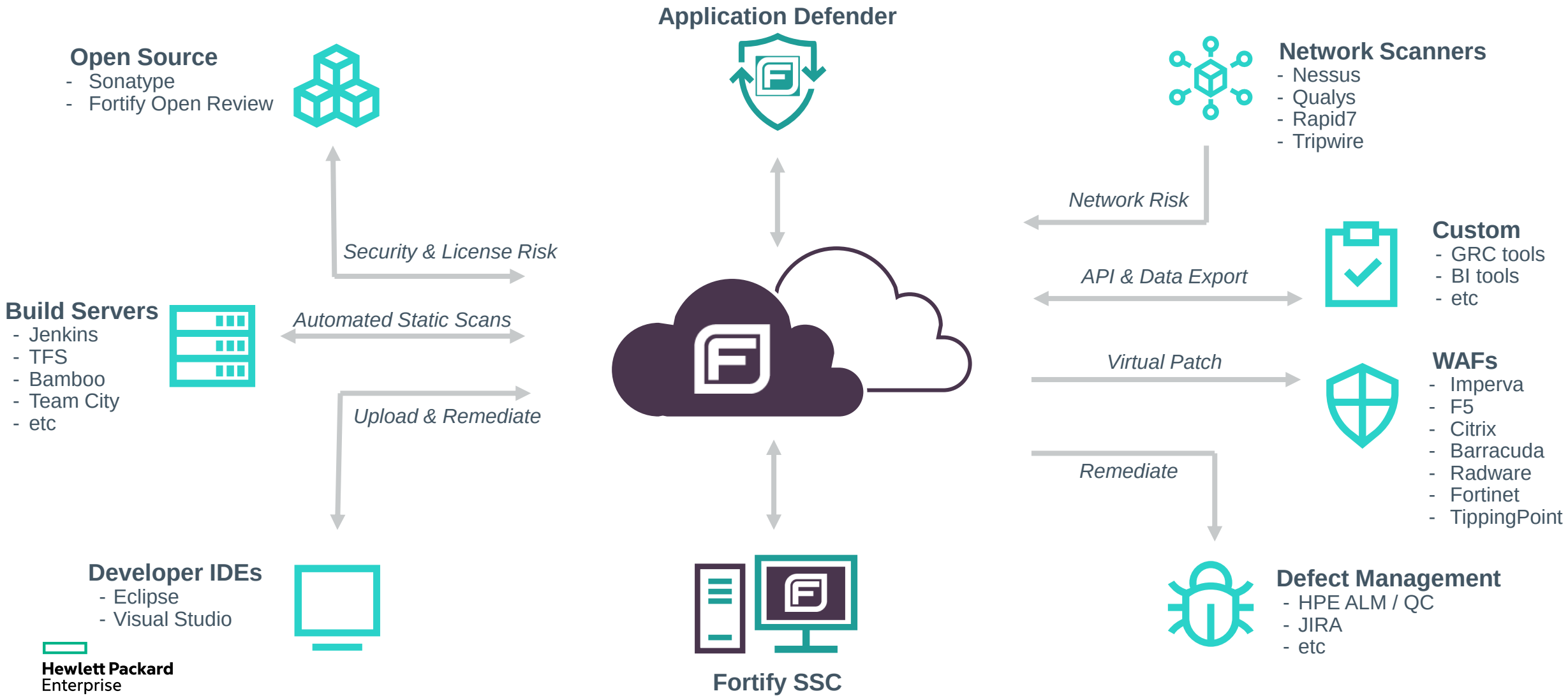
HPE Security Fortify Application Defender

Runtime Application Self Protection



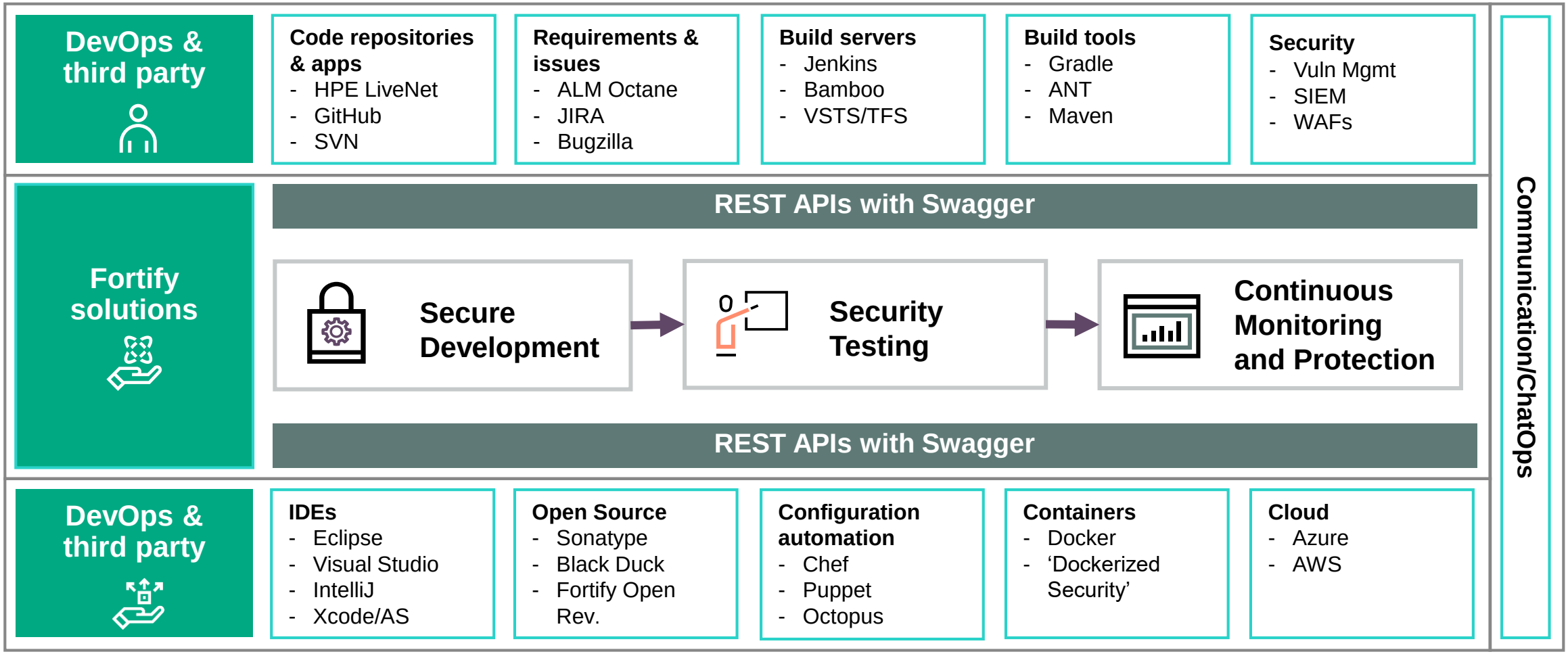
Use case 3: Continuous Integration and Deployment

Automate and integrate security testing



Hewlett Packard Enterprise

Fortify Ecosystem



Application Defender & Containers

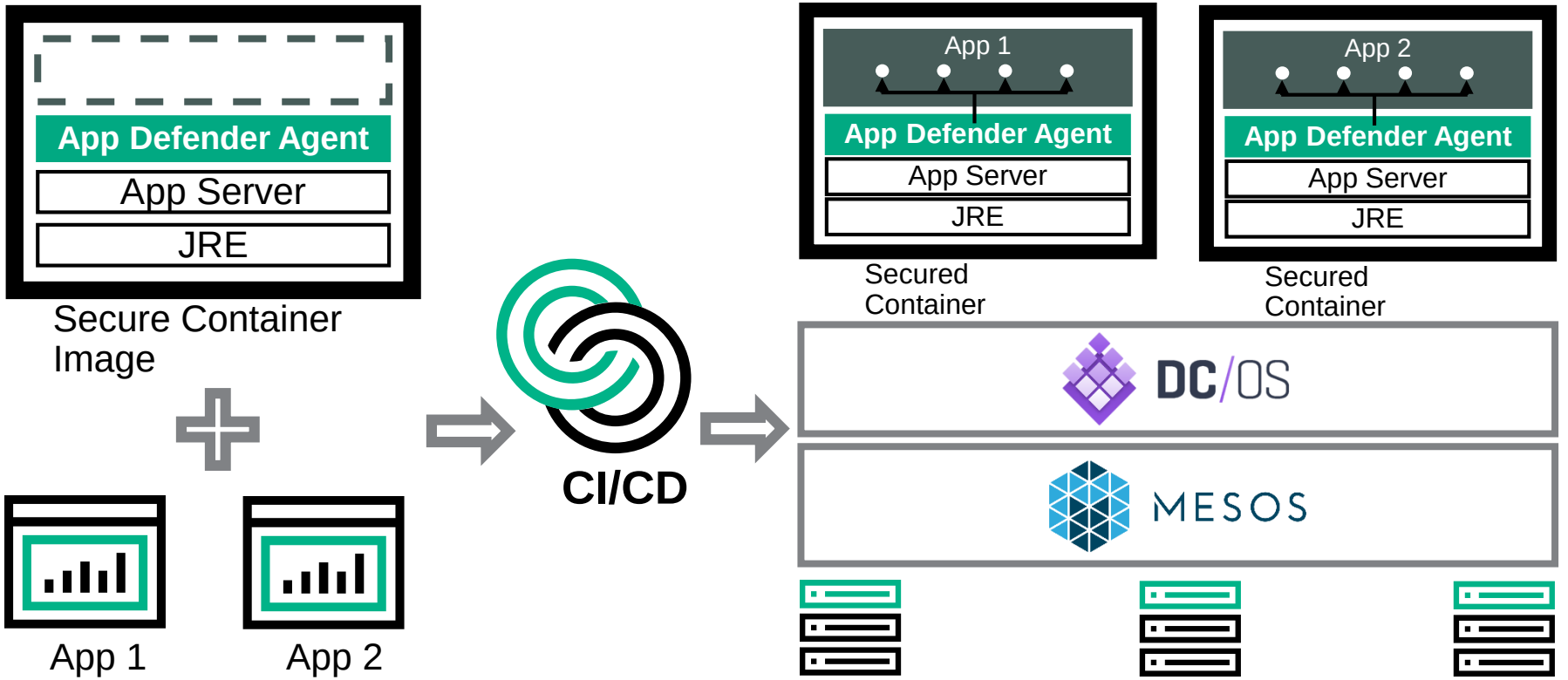
Automatically Deploy Secured Applications

MESOSPHERE

Built in security

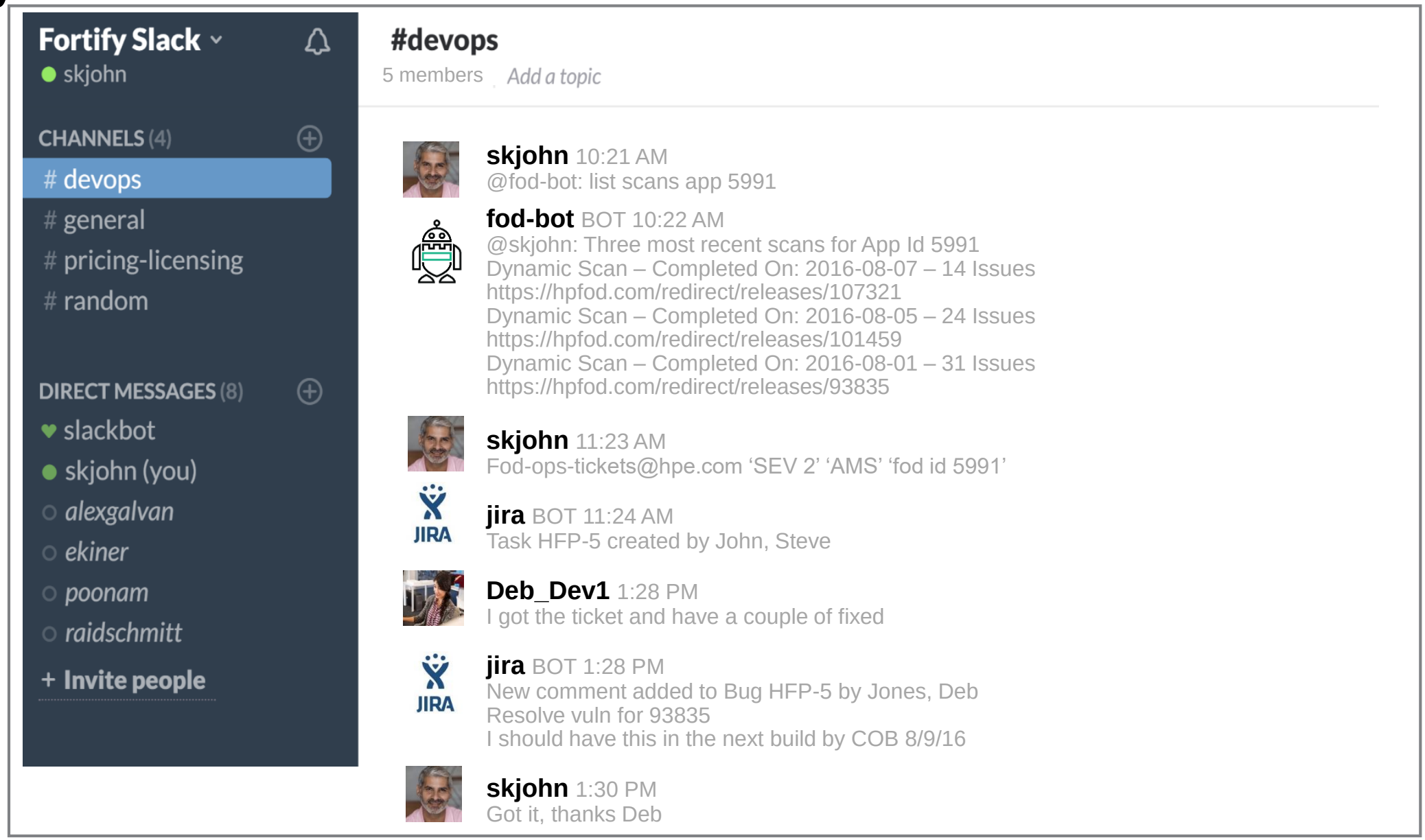
Enterprise Friendly

Scalable



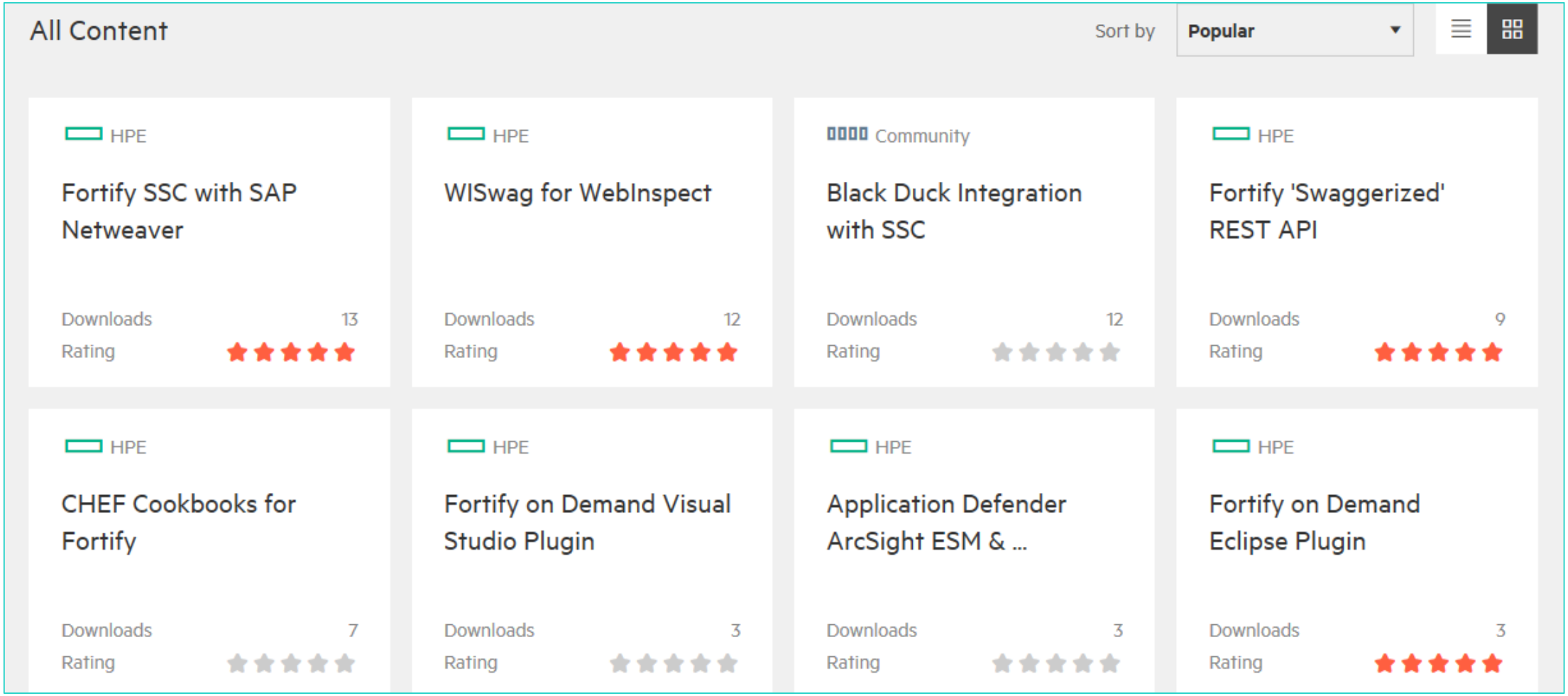
Hewlett Packard Enterprise

Fortify on Demand ‘fod-bot’ with Slack

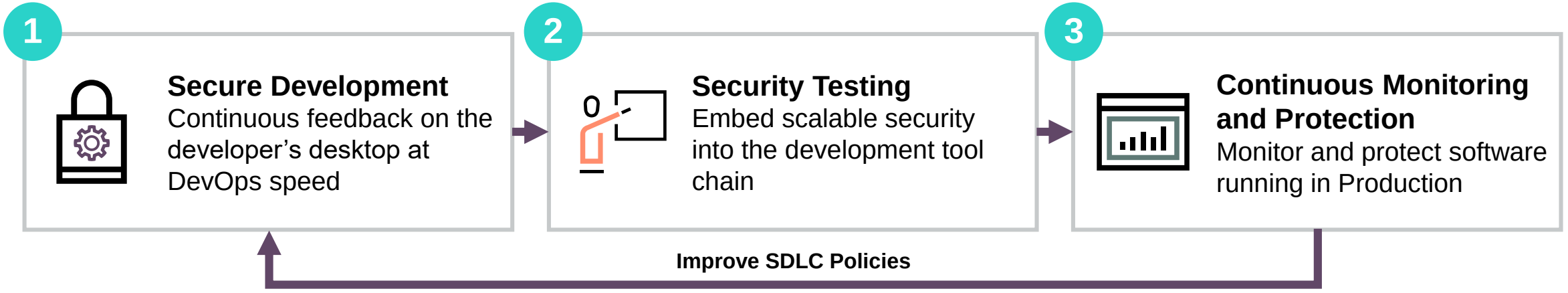


Fortify Ecosystem

hpe.com/software/fortifyEcosystem



The right approach for the new SDLC – Build it in



This is application security for the new SDLC

For more information:

www.hpe.com/software/fortify

Thank you

- Complete the short survey and opt-in for more information from Hewlett Packard Enterprise.

www.hpe.com

www.vivit-worldwide.org

© Copyright 2016 Vivit Worldwide