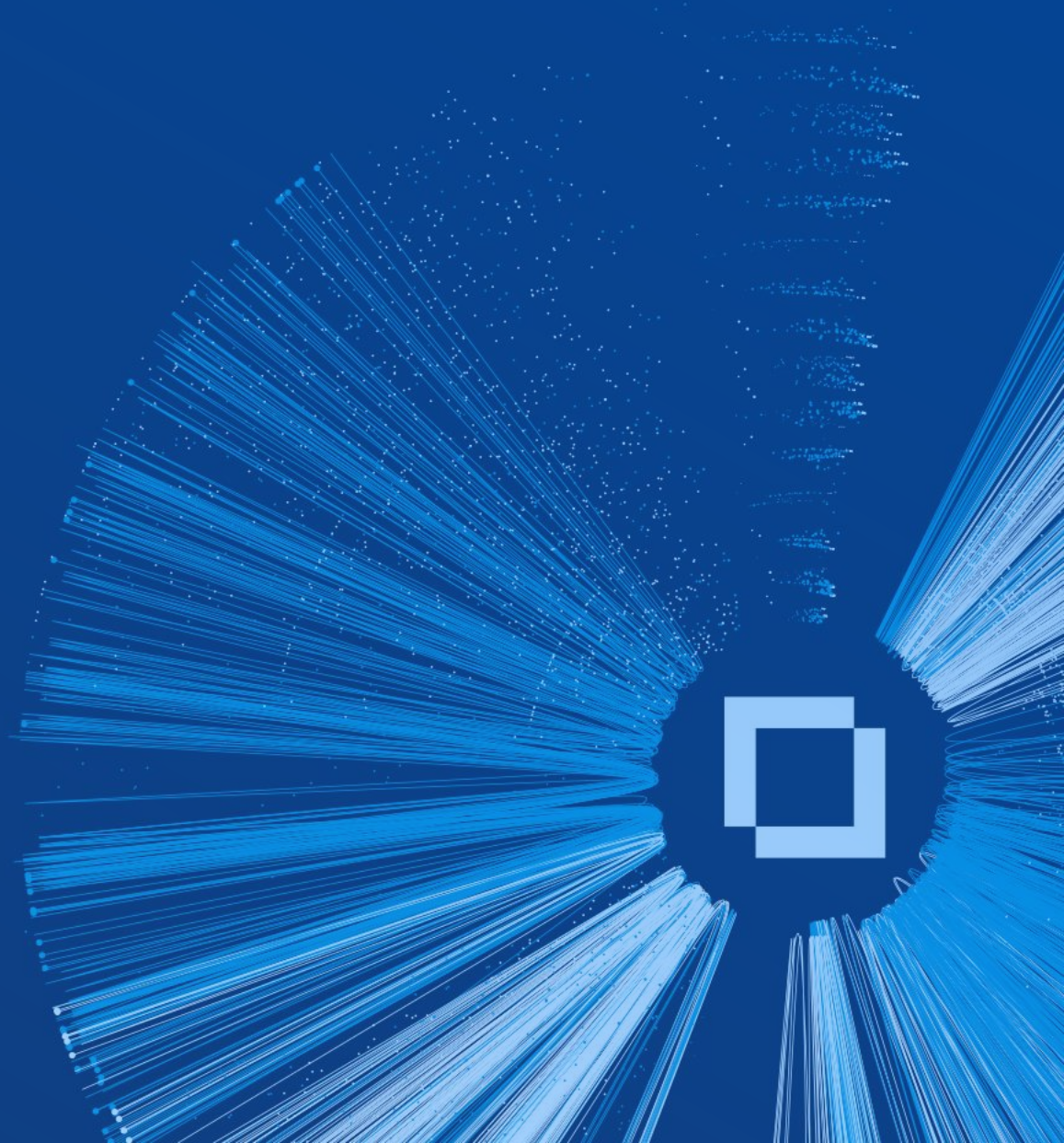
MICRO FOCUS



Summit 2019

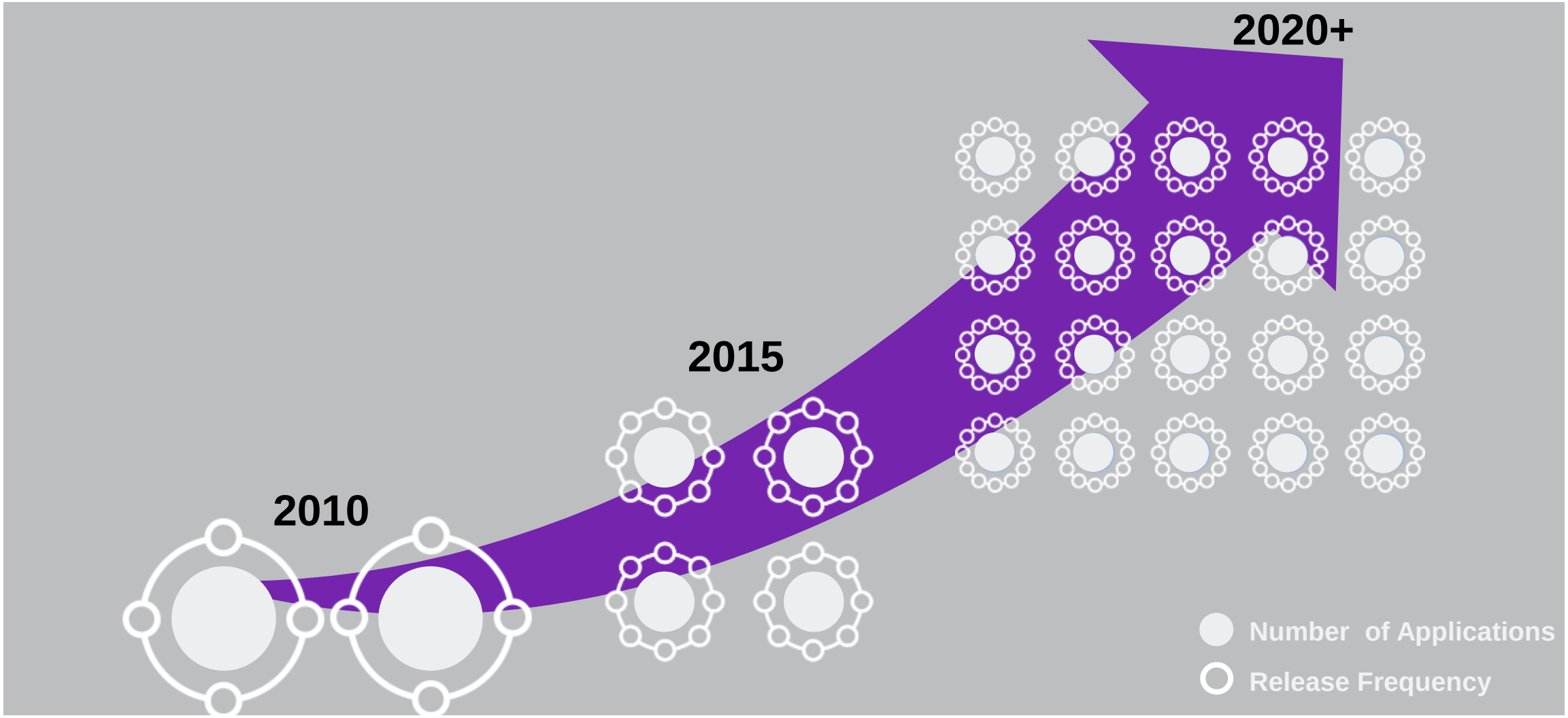
#MFSummit2019

MICRO FOCUS

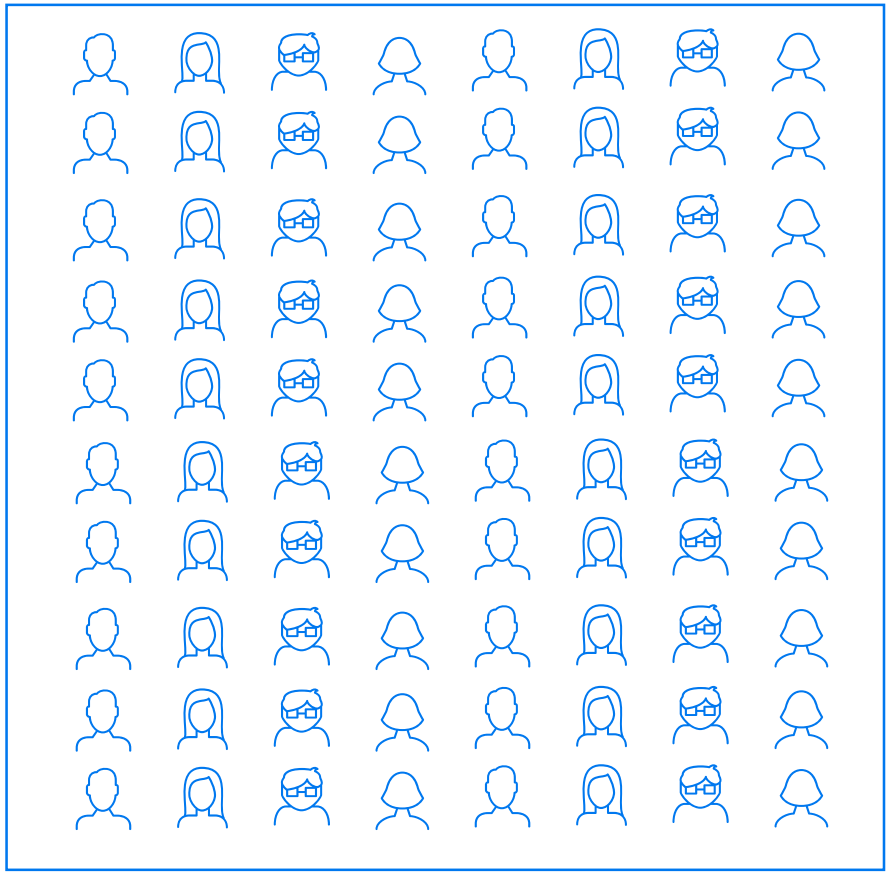
Seguridad en entorno DevOps

Jacinto Grijalba González
Cybersecurity Sales Manager
+34 664352913

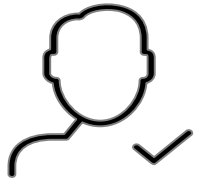
Today's business needs are dramatically increasing the number of applications and the frequency of releases



Development teams are growing at an 80:1 ratio to security teams



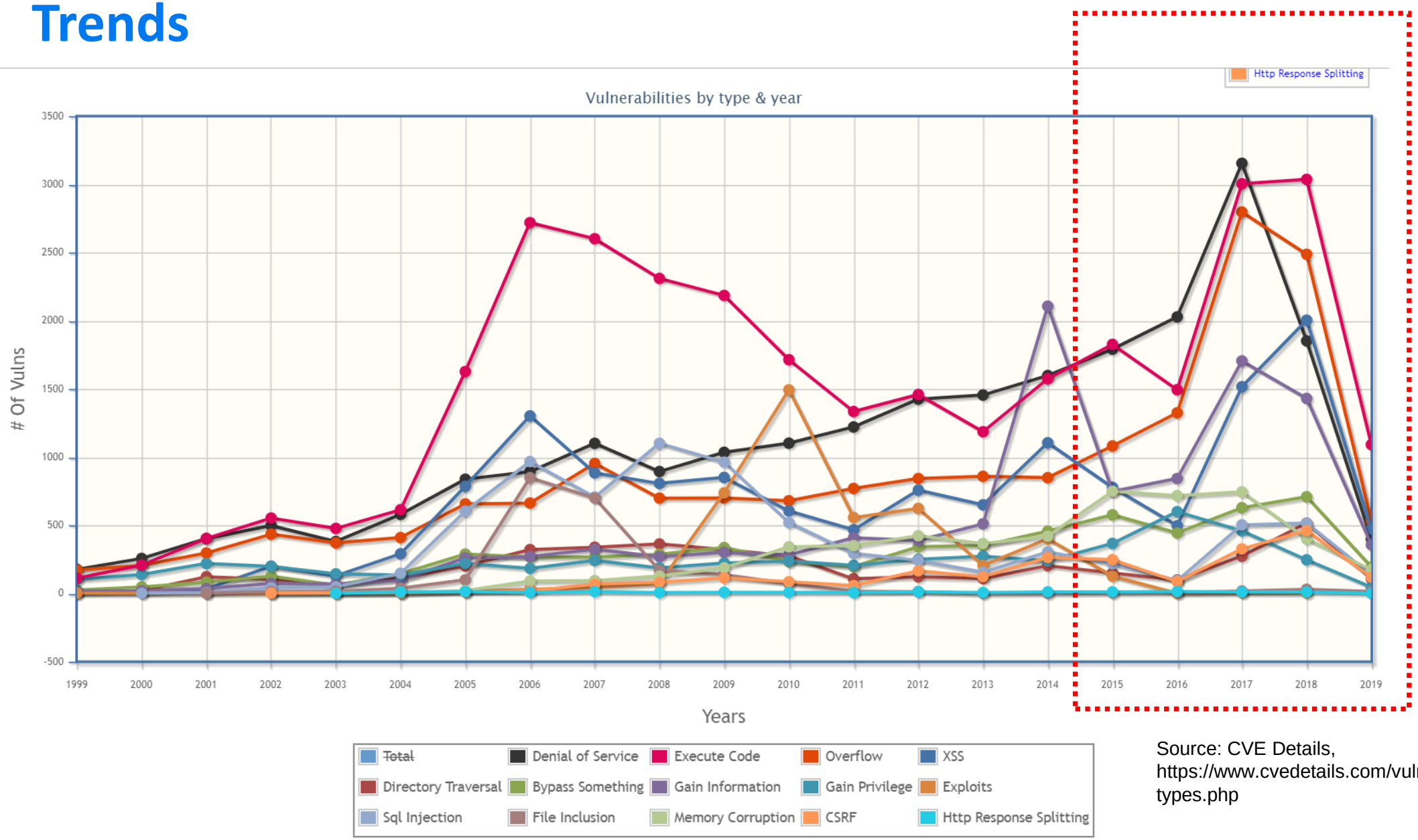
VS



Reference: Micro Focus Application Security Research Update

Data for selected years and top vulnerability categories

Trends



Source: CVE Details, https://www.cvedetails.com/vulnerabilities-by-types.php

Based on Micro Focus Application Security Risk Report

- Key Takeaways Include:

1

Fortify on Demand analysis shows broad vulnerability in apps

The majority of web or mobile applications analyzed had at least one critical or high severity issue

2

OWASP Top 10 is a starting point

1 out of 2 apps had critical or high vulnerabilities not covered by the OWASP Top 10 2017 (Report of 2018)

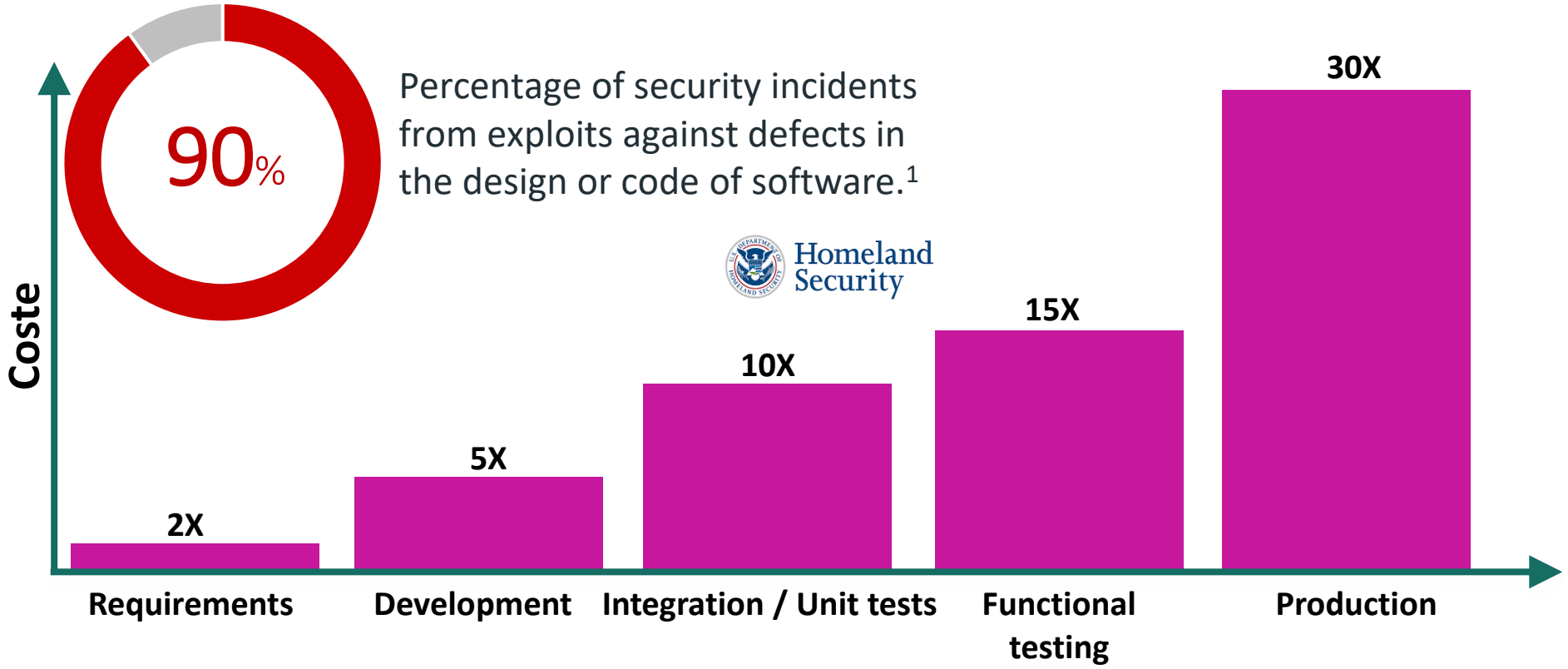
3

GDPR is forcing strong protection of customer data

GDPR strongly hints at the use of encryption and pseudonymization as acceptable approaches to protect personal data; applications are a potential weak link.

What is the cost of doing nothing?

Approximately 30 times more expensive to remedy in production

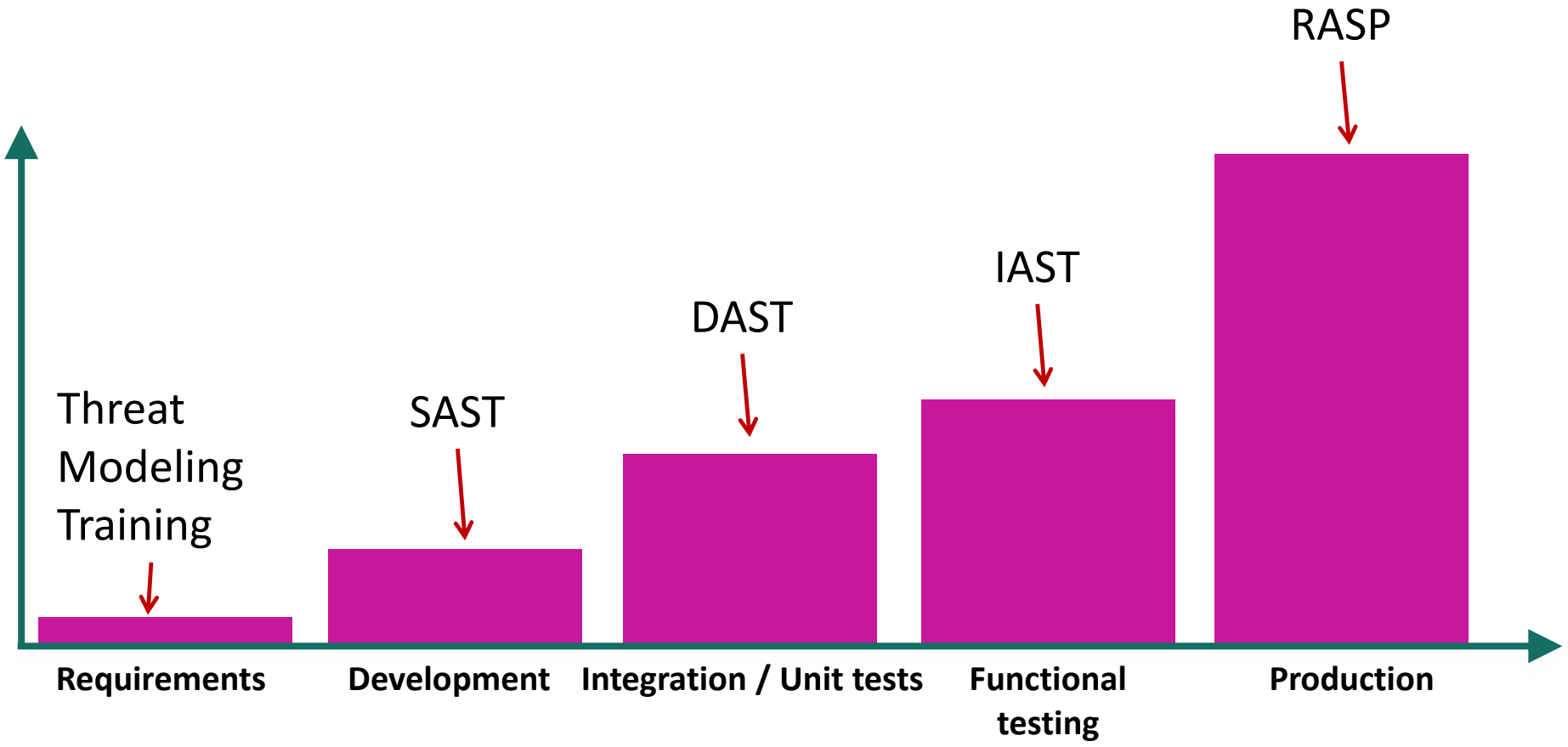


- After deploying an application in production it is 30 times more expensive to fix a vulnerability than during the design phase.

Source: [1]U.S. Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT)
[2]2017 Application Security Research Update" by the HPE Software Security Research team, 2017

Source: NIST

Application Security Testing Techniques



SAST: Static Application Security Testing

DAST: Dynamic Application Security Testing

IAST: Interactive Application Security Testing

RASP: Runtime Application Self-Protection

Application Security with Micro Focus Fortify

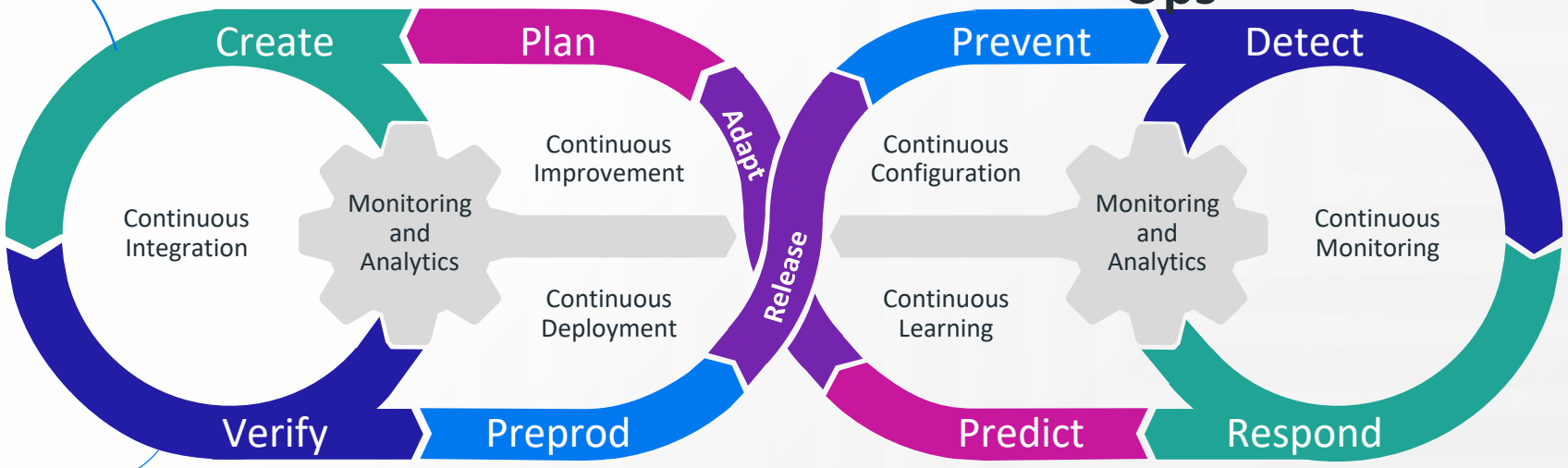
- Securing the SDLC (DevSecOps)

SAST

Fortify Static Code Analyzer (SCA)

RASP

Fortify Application Defender



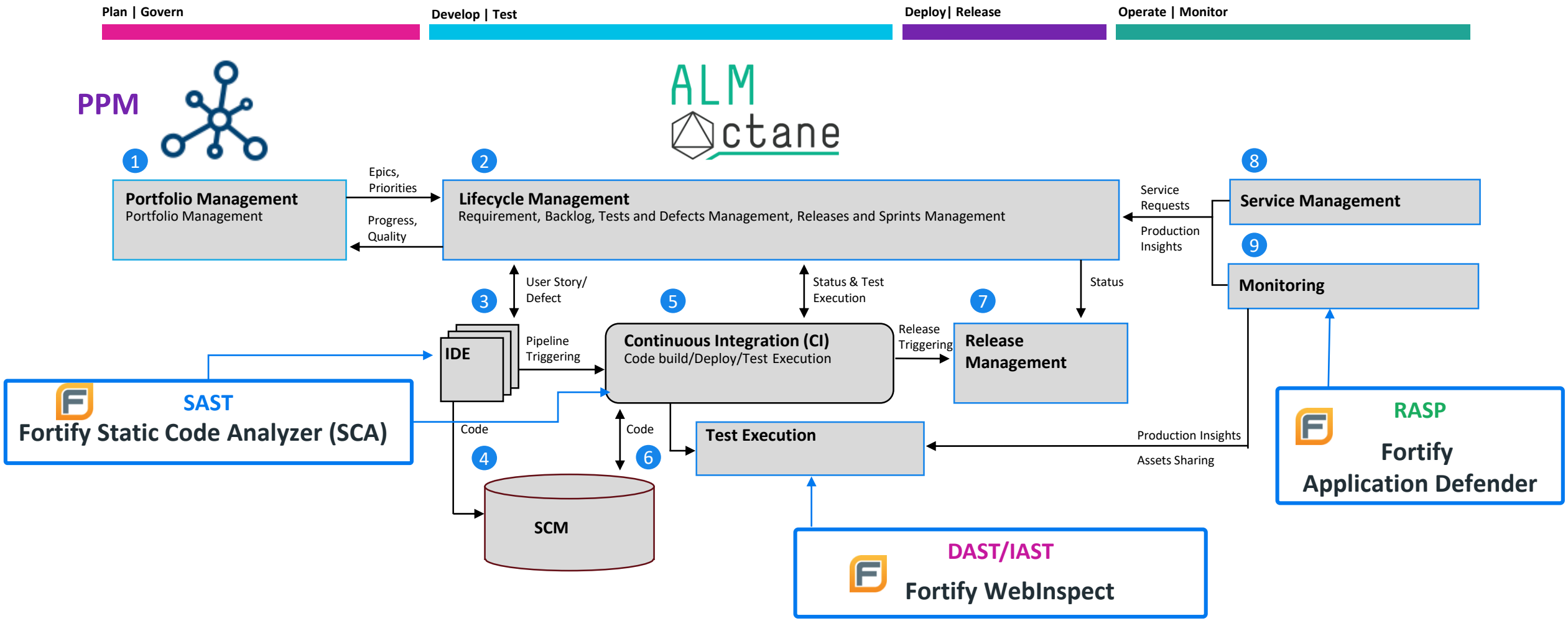
DAST/IAST

Fortify WebInspect

Continuous Delivery

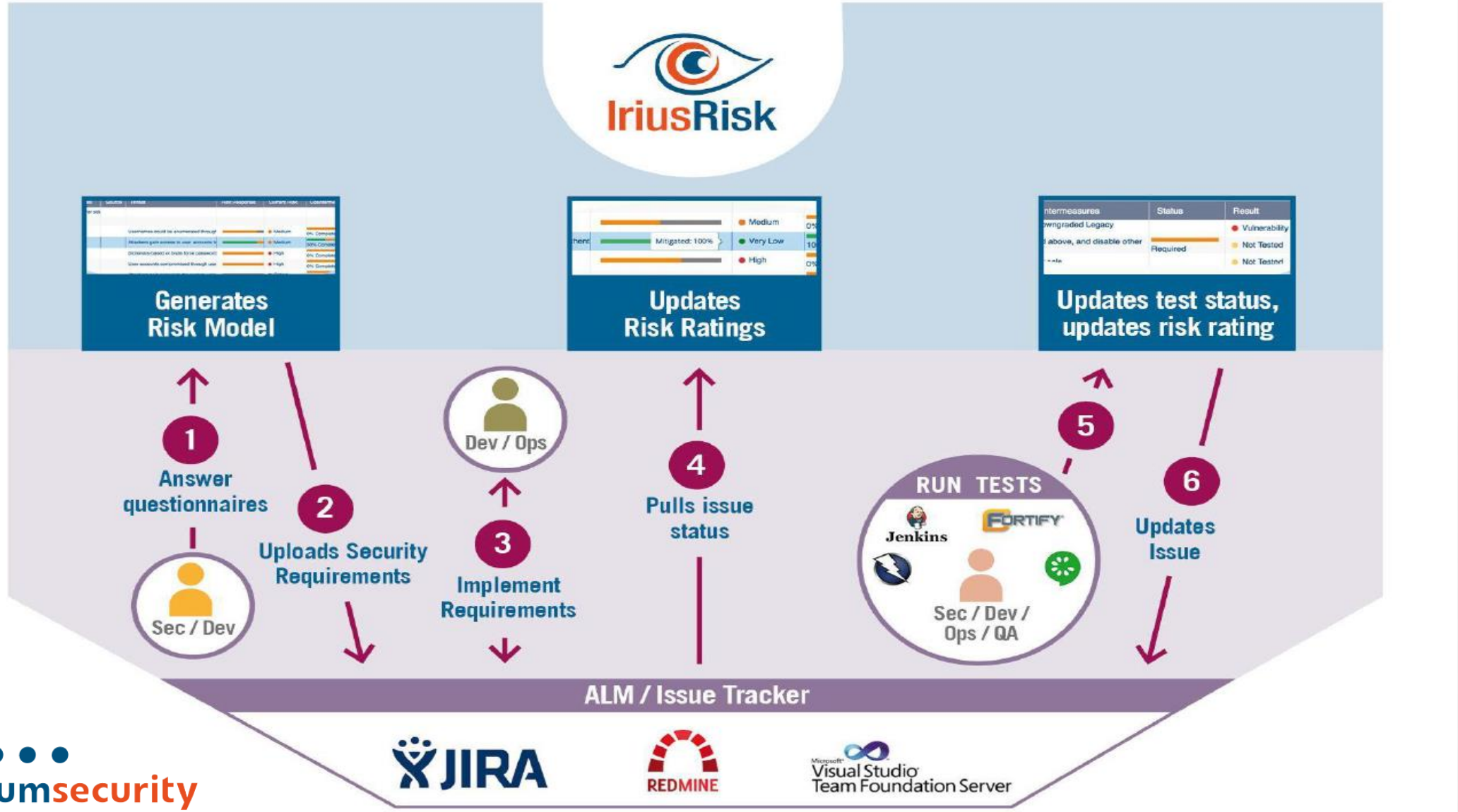
Source: "10 Things to Get Right for Successful DevSecOps," Gartner, Inc., 2017

Application Delivery with Micro Focus



- Open API to integrate any other customer tool in place
- MF Connect or Tasktop can be used to integrate seamlessly

Requirements Partner with ContinuumSecurity



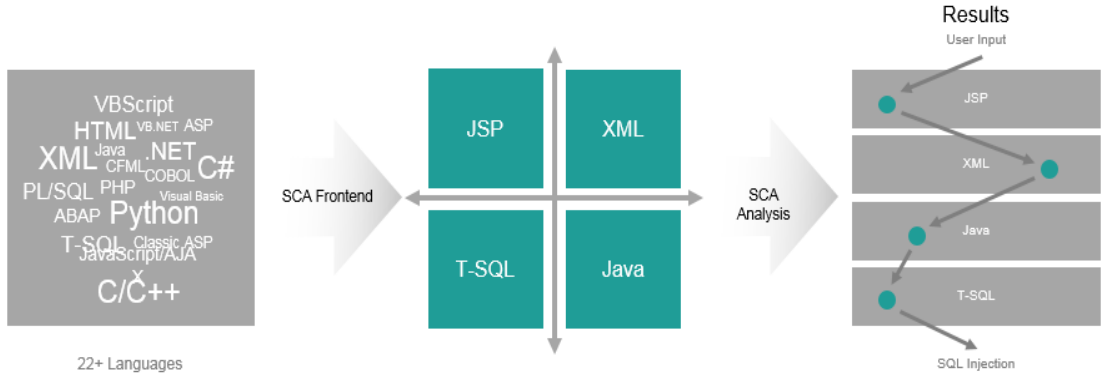
continuumsecurity

SAST - Static Application Security Testing

Fortify SCA

Static analisys (SAST)

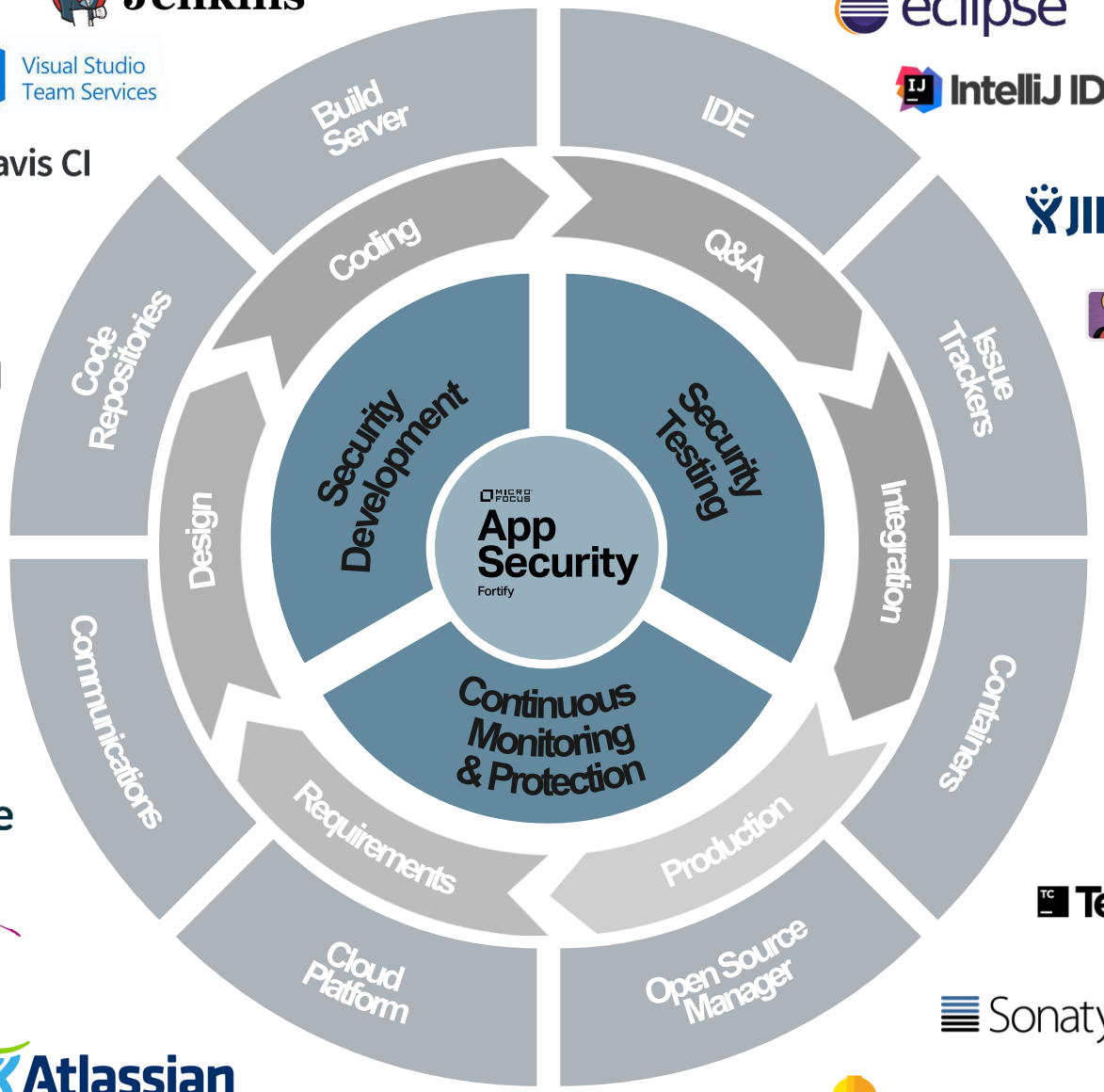
- **Save development time** and costs by identifying vulnerabilities during development
- **Developers can devote their time to development and innovation** instead of correcting errors of applications deployed in production
- **Identify the root cause** of vulnerabilities
- **Supports 792 unique vulnerability categories in 25 programming languages and more than 1,007,000 API** / framework / libraries (https://vulncat.fortify.com/es)



Features

- Pinpoint root cause of vulnerabilities – line of code detail
- Prioritize fixes sorted by risk severity
- Detailed “fix” instruction -- in the development language

Fortify integrates with what you use and protects your IT investments



Bamboo
Jenkins
Visual Studio
eclipse
IntelliJ IDEA
Visual Studio Team Services
Travis CI
JIRA
GitHub
Bugzilla
Subversion SVN
ALM Octane
Bitbucket
sonarqube
Maven
circleci
Gradle
TeamCity
Apache Ant
Sonatype
Atlassian
WhiteSource
Microsoft Azure
aws
BLACKDUCK

Fortify SCA has the broadest programming languages coverage in the industry

25+ programming languages and counting… SCA can scan source, byte and binary code.

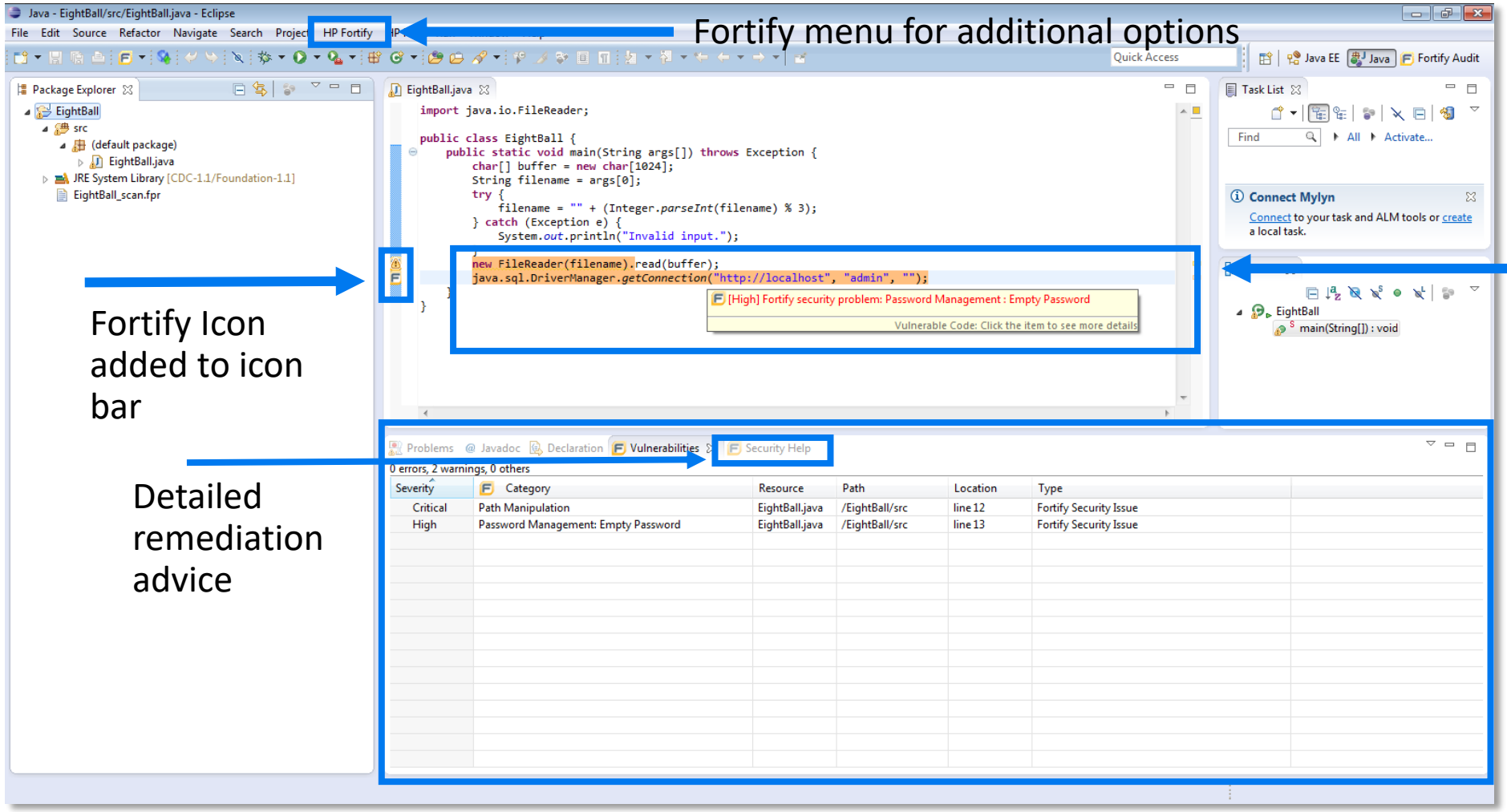
New with 18.20

Coming next

Security Assistant (Eclipse)

Real-time lightweight analysis of the source code

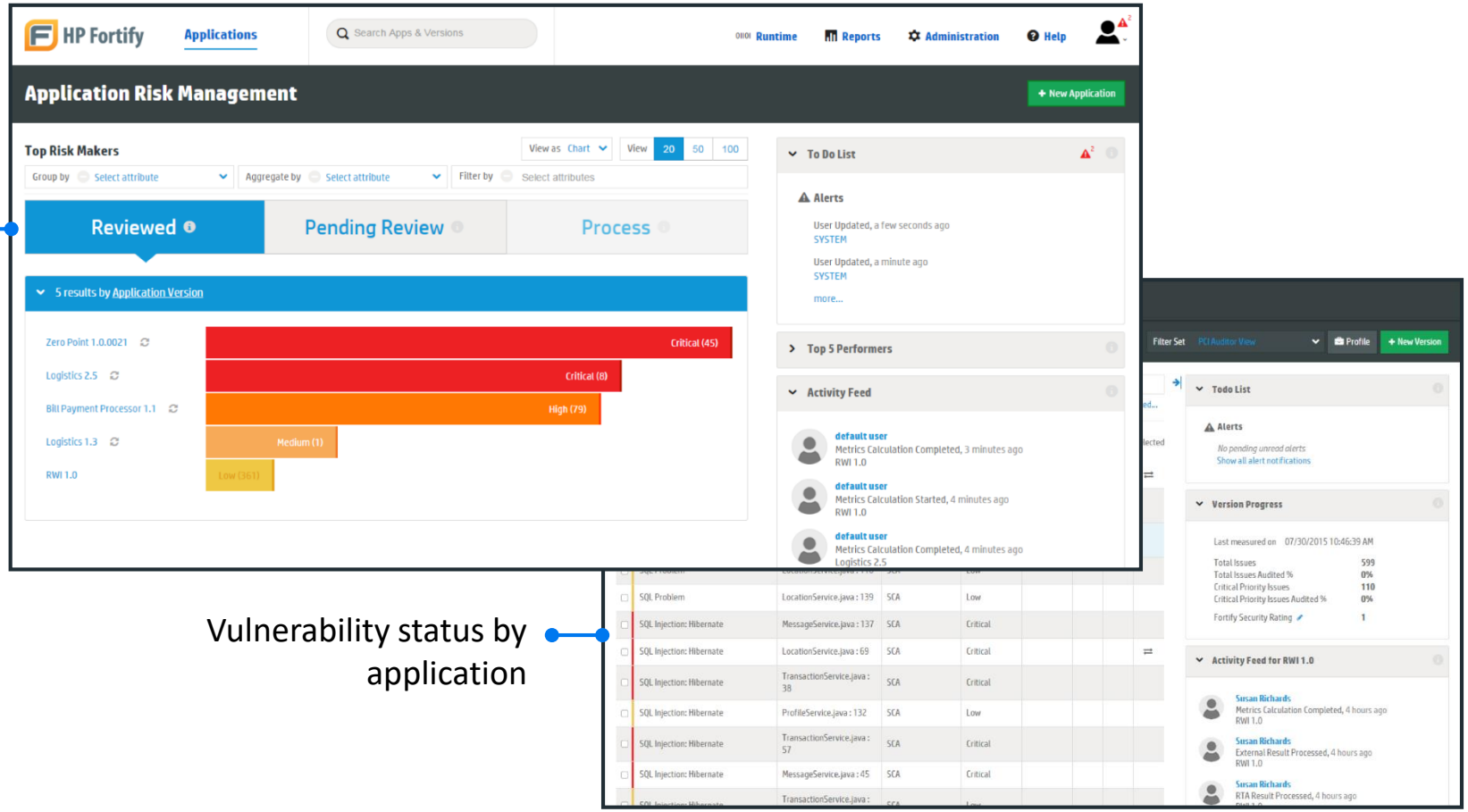
Code Review



Fortify Software Security Center

Reporting and Program Management

Global dashboard highlights risk across software portfolio



Vulnerability status by application

Runtime Application Self Protection

Fortify Application Defender

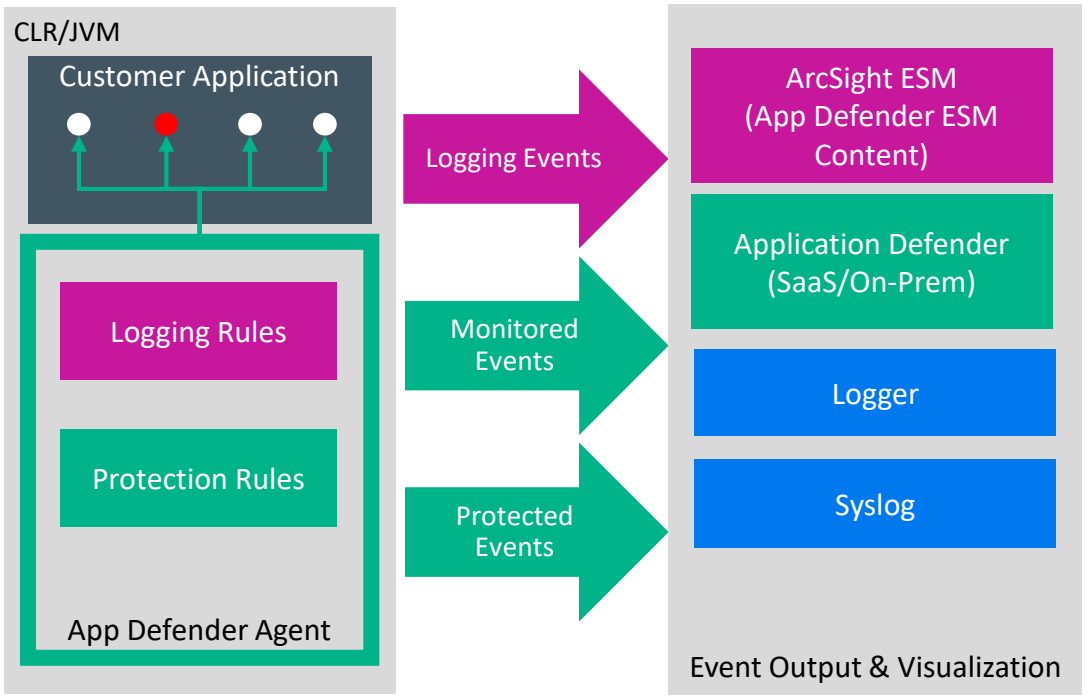
Application Logging and Protection

Application Logging

- Consistent out-of-the-box logging for any application
- 69 Logging categories
  - e.g. File Read/Write; HTTP Sessions Start/Stop; Login Succeed/Fail, DB sessions
- Send CEF events to ESM or Syslog

Application Protection

- Vulnerability exploit attempts and other security violations
- 33 Vulnerability categories
  - e.g. SQLi; XSS; Privacy Violation
- Monitor & Protect actions

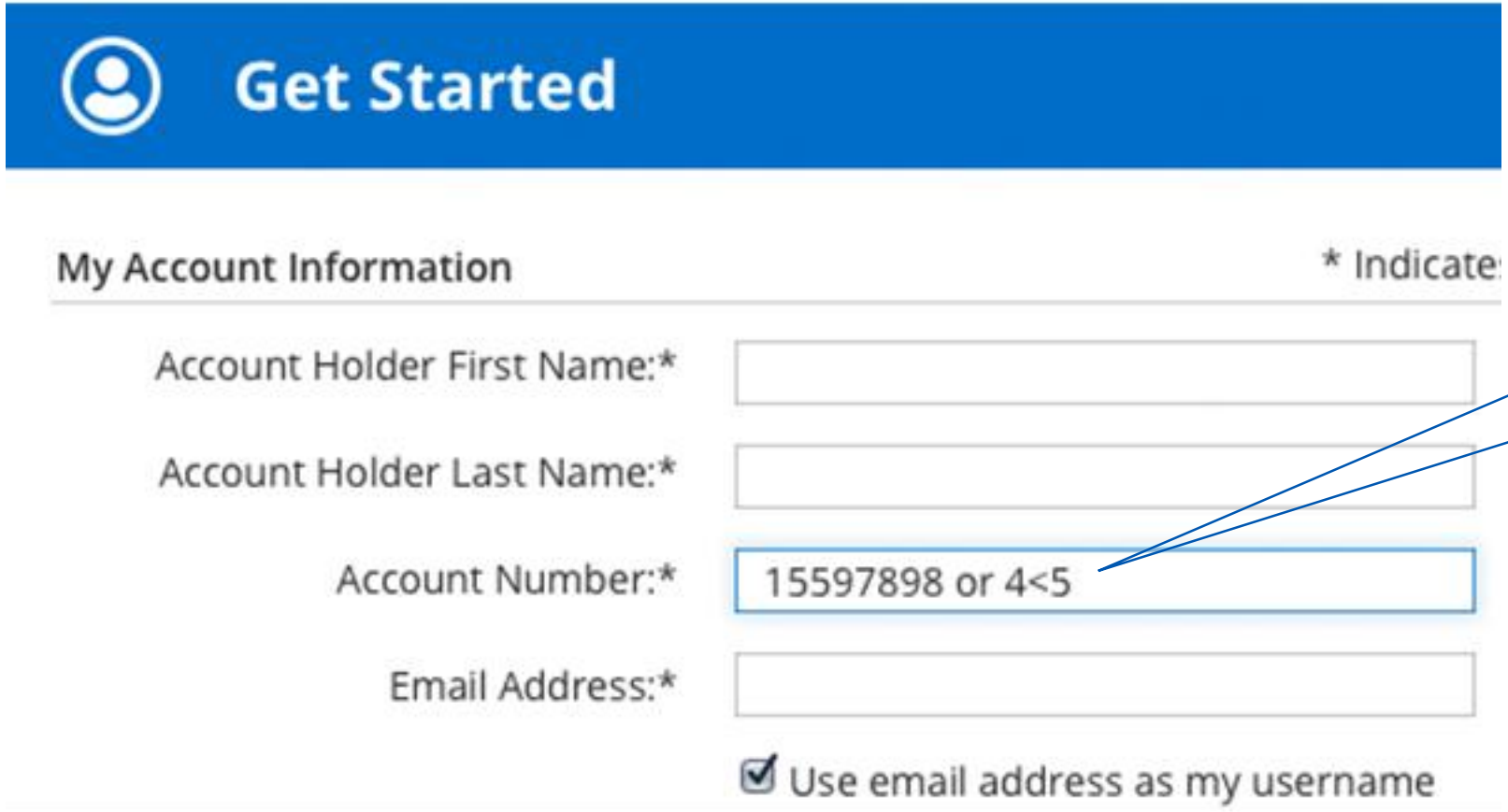


Runtime platform delivered to meet your needs

On-Premises or SaaS

Example: How it Works?

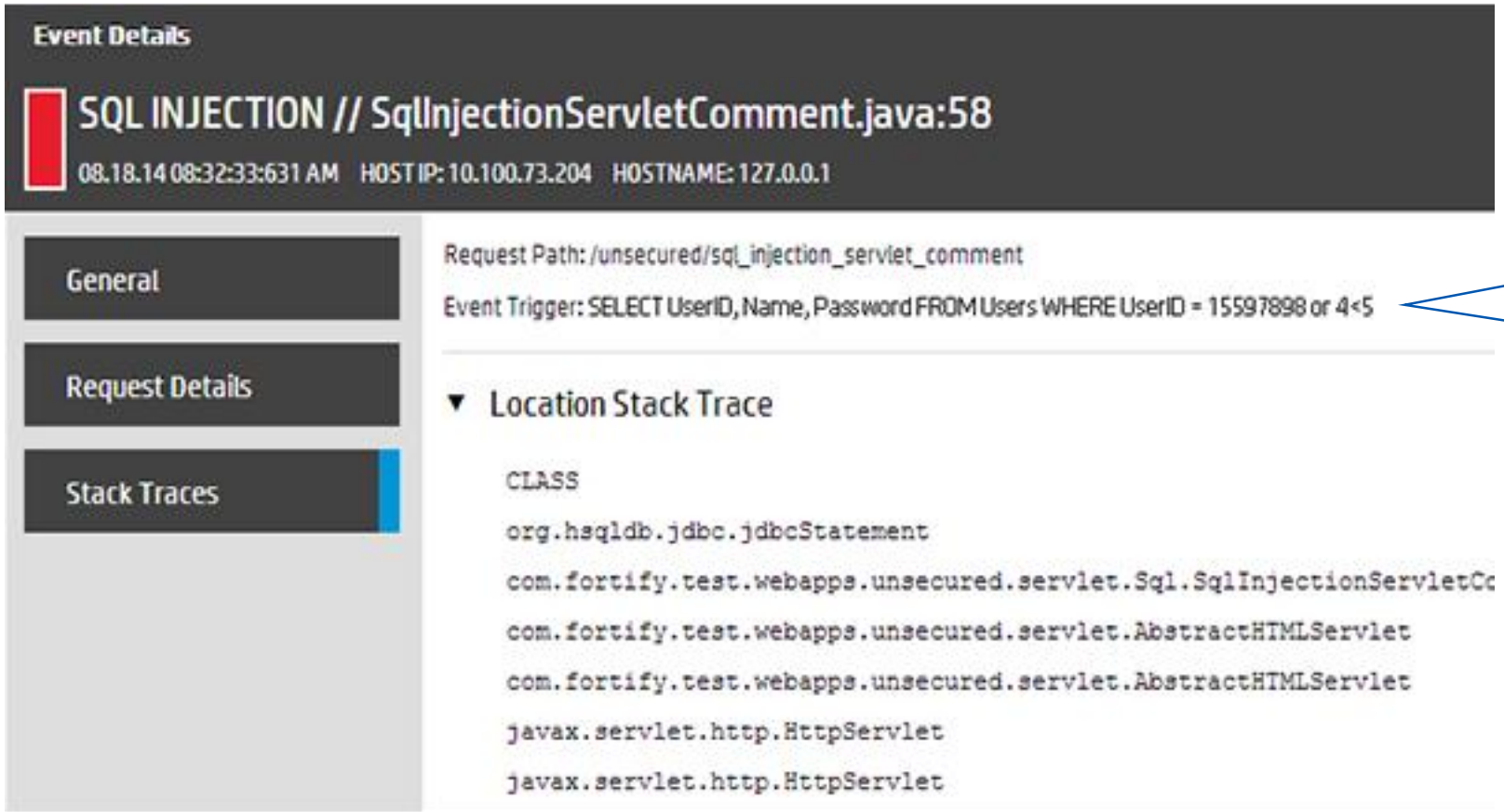
The Attack



A SQL injection attack is perform

Example: How it Works?

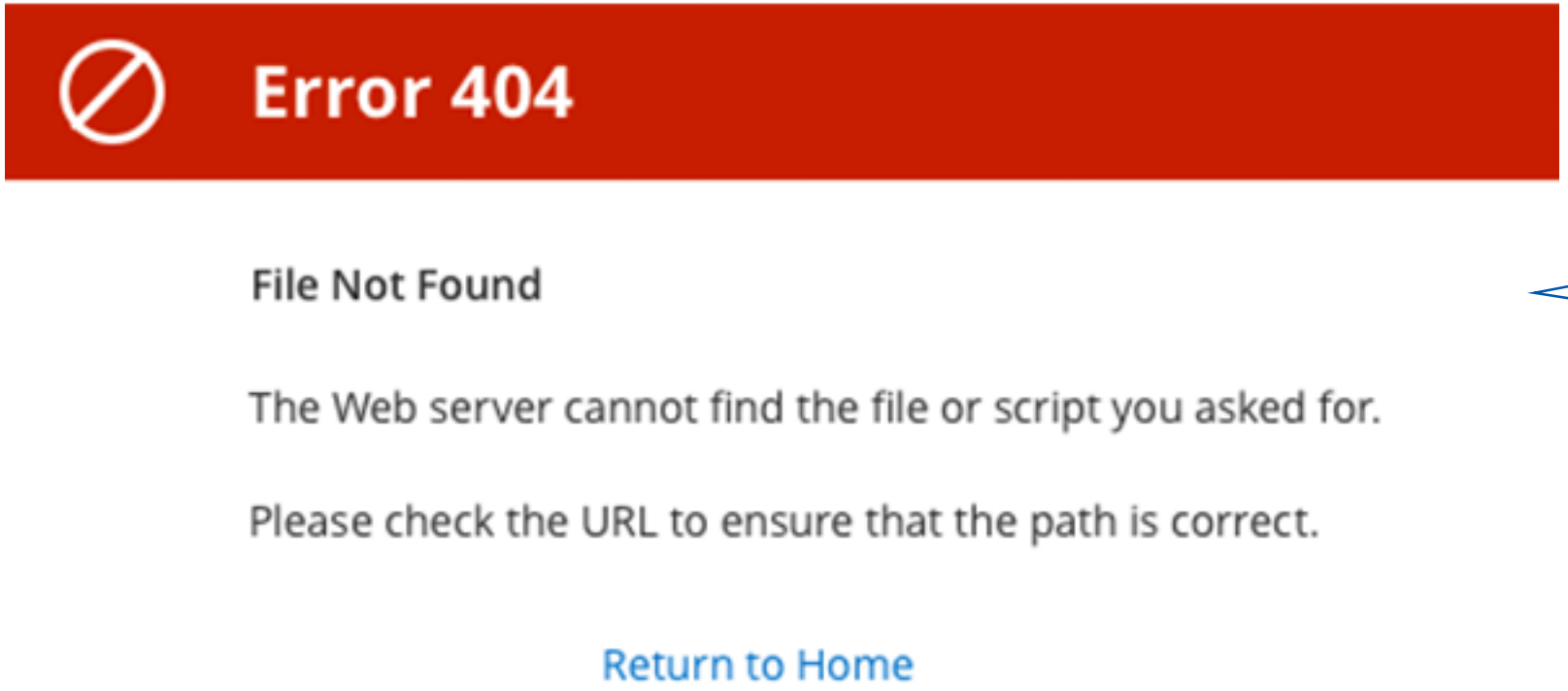
Detection



What Fortify Aplication Defender detects.

Example: How it Works?

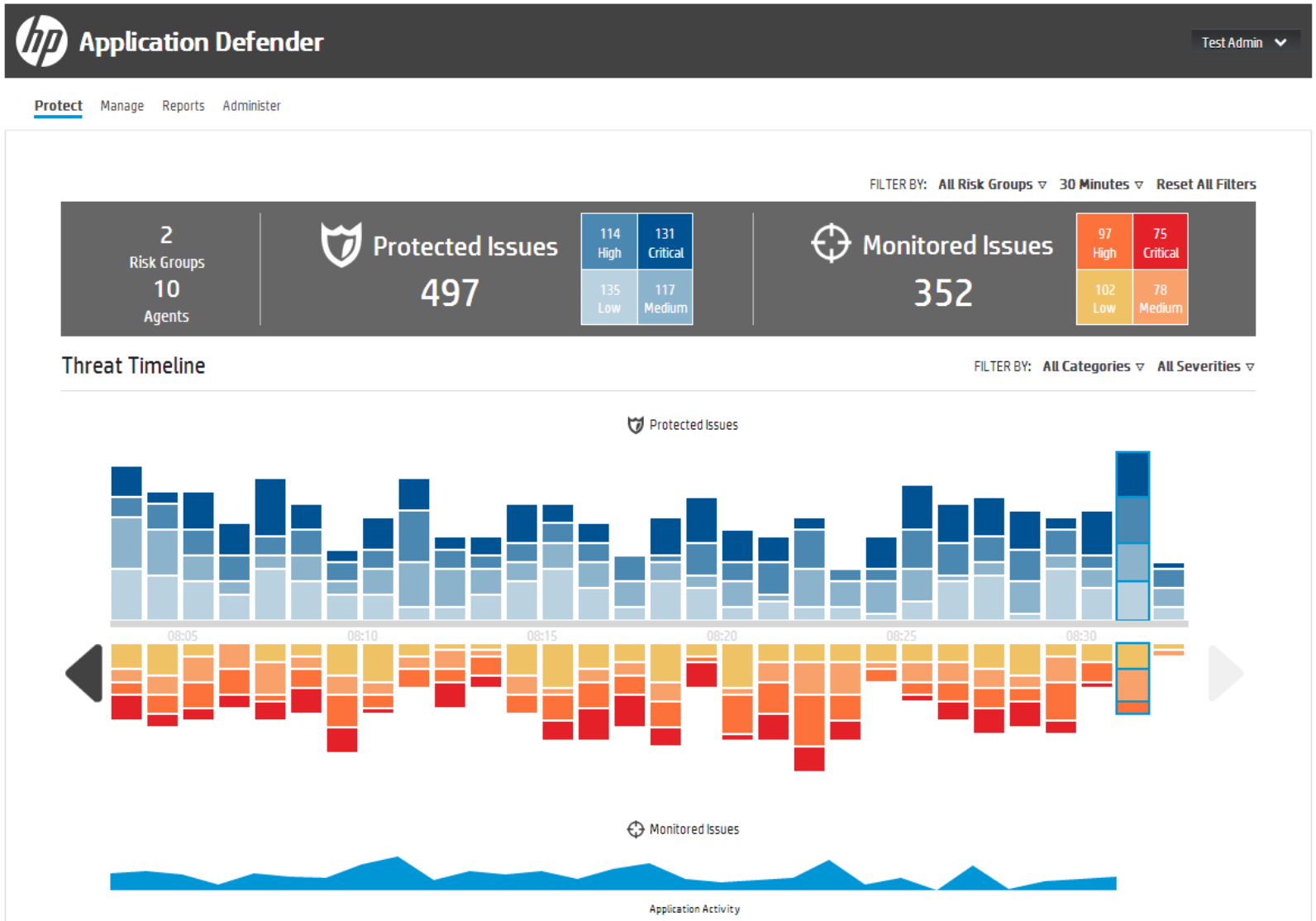
User Experience



What Fortify shows as result of the attack

Example: How it Works?

What the auditor check



Audit information to review

¿Por qué Fortify?

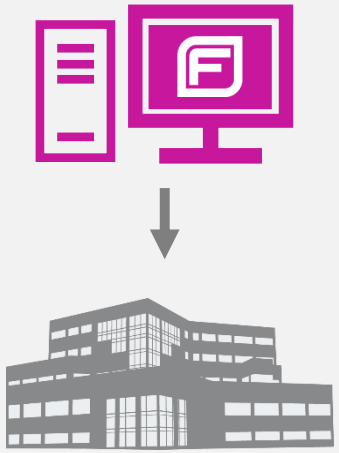
Application testing flexibility

on Demand

Fortify on Demand

on Premise

Fortify Software Security Center



Fortify Static Code Analyzer

- **Fortify Marketplace**

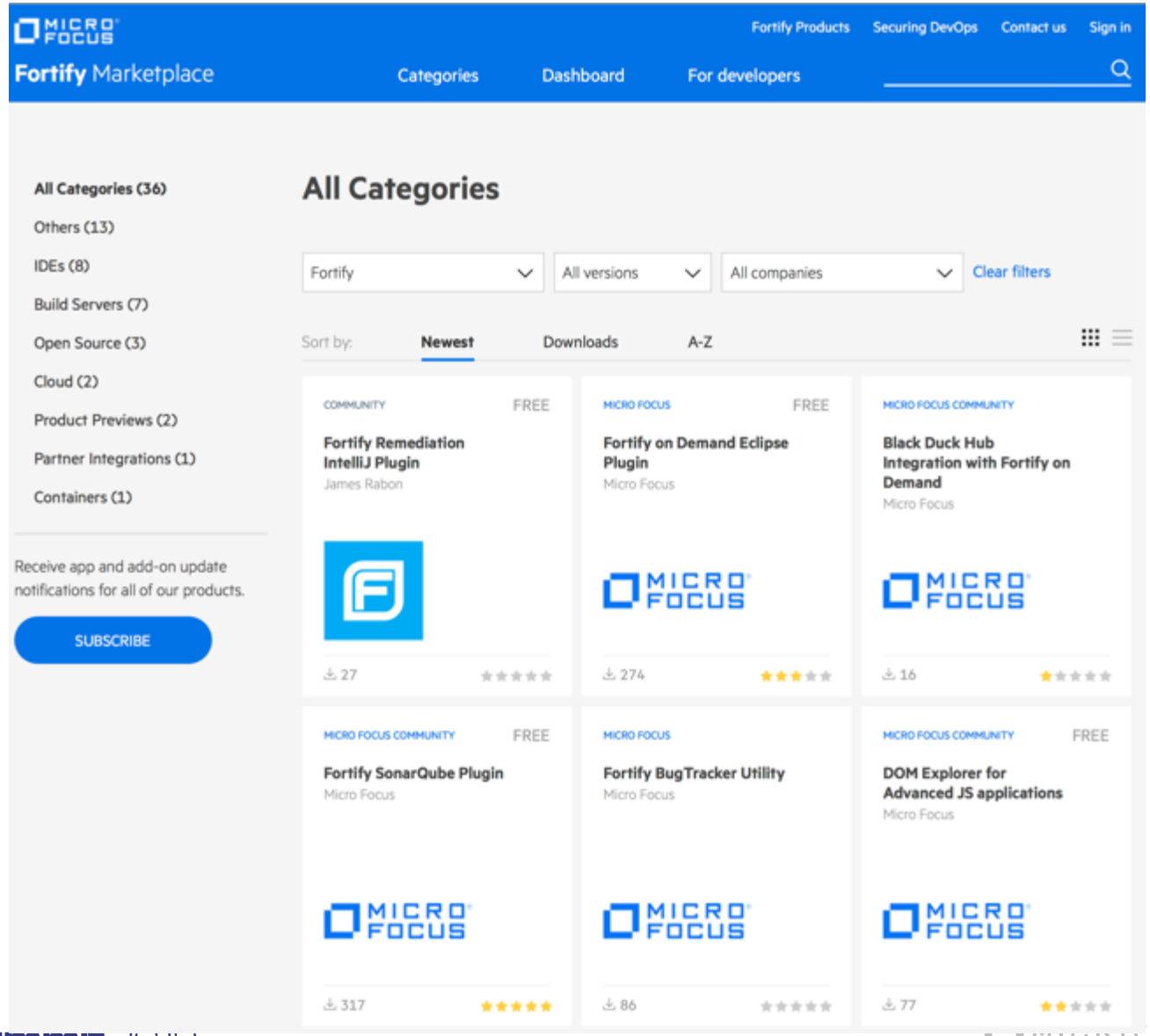
https://marketplace.microfocus.com/fortify/category/all?product

- **Github / fortify**

https://github.com/fortify
https://fortify.github.io

- **Fortify Security Kingdom**

https://vulncat.fortify.com



Fortify: once again been named a leader in Gartner MQ

Gartner Application Security Testing MQ 2019

Figure 1. Magic Quadrant for Application Security Testing

- **Fortify has once again (10 times) been named a leader in the 2019 Gartner Magic Quadrant for Application Security Testing.** Fortify has been a leader in every application security report Gartner has ever published since the first one in 2009 and has been the undisputed leader in both Completeness of Vision and Ability to Execute for the last four MQs. See below for the 2019 MQ graphic.
- Fortify is a well-known brand worldwide. It is a constant presence in customer shortlists for a wide range of AST use cases (either as a product or service, or both combined) particularly when multiple testing technologies are required. It has a historical reputation for delivering innovative products and services.
- Fortify has one of the most complete SDLC integrations — for example, by providing out-of-box integrations for popular IDEs and CI/CD tools.
- Fortify's SAST has the broadest language support and provides a range of deployment options making it a good fit for complex testing use cases. Its WebInspect IAST agent for Java and .NET is included at no cost for WebInspect DAST tool customers.
- Fortify has a comprehensive set of enterprise capabilities, as well as integration with major SCA vendors. Sonatype assessments are included for all FoD SAST customers at no additional charge.

2019

MICRO FOCUS

Summit 2019

#MFSummit2019

MICRO FOCUS