FORTIFY

Eszközök és módszerek a biztonságos alkalmazásokért

Hargitai Zsolt
üzletfejlesztési igazgató
zsolt.hargitai@microfocus.com

We aren’t saying Application Security is easy…

It’s a (long) process

Varies by organization (size, dev style, culture, AppSec maturity, etc)

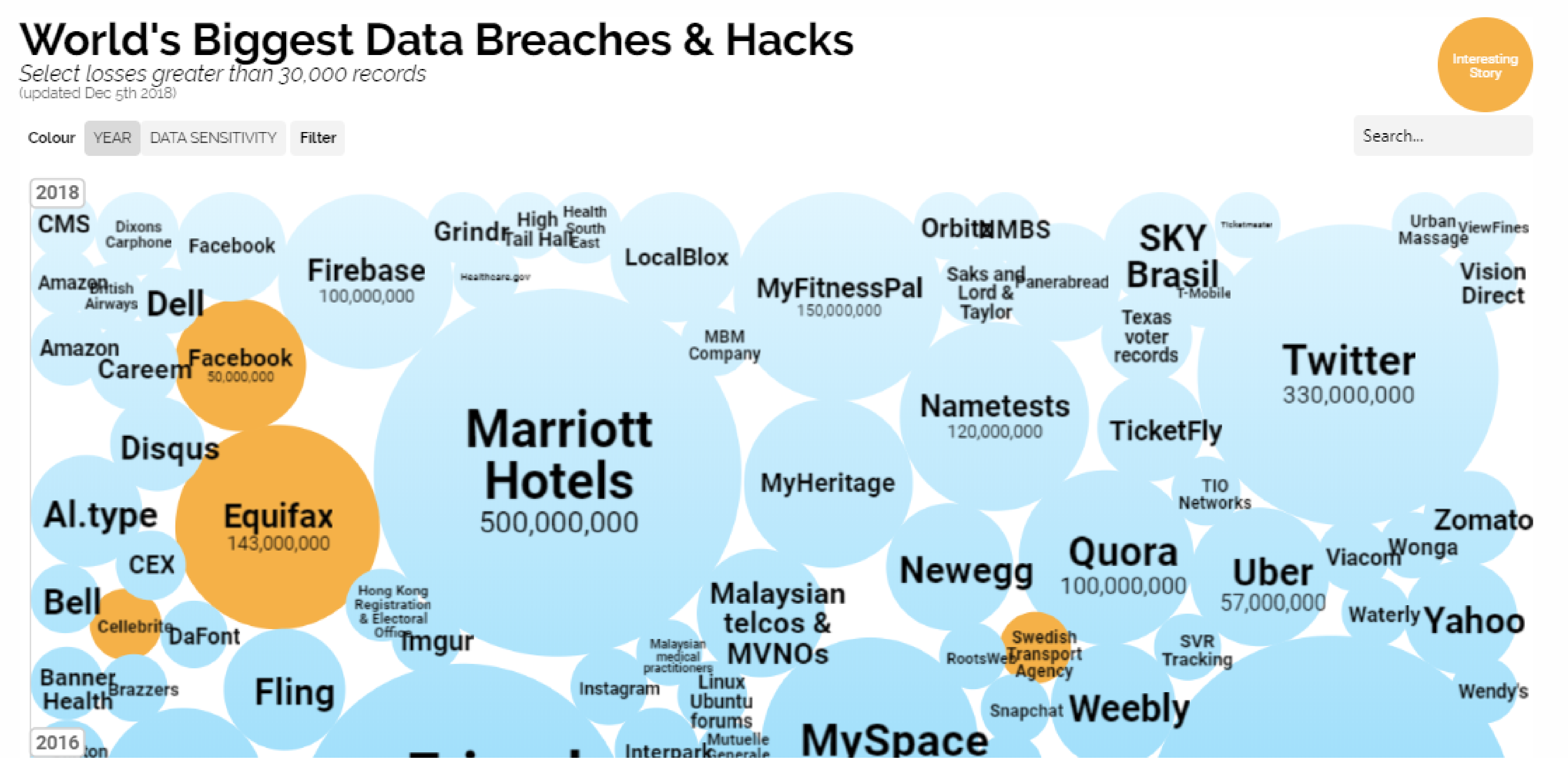
Get Started with Seamless AppSec in One Day

We simplified the story

NOT easy (no silver bullet)

…but you can start in a day and make significant progress

There is a major breach almost every week!



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

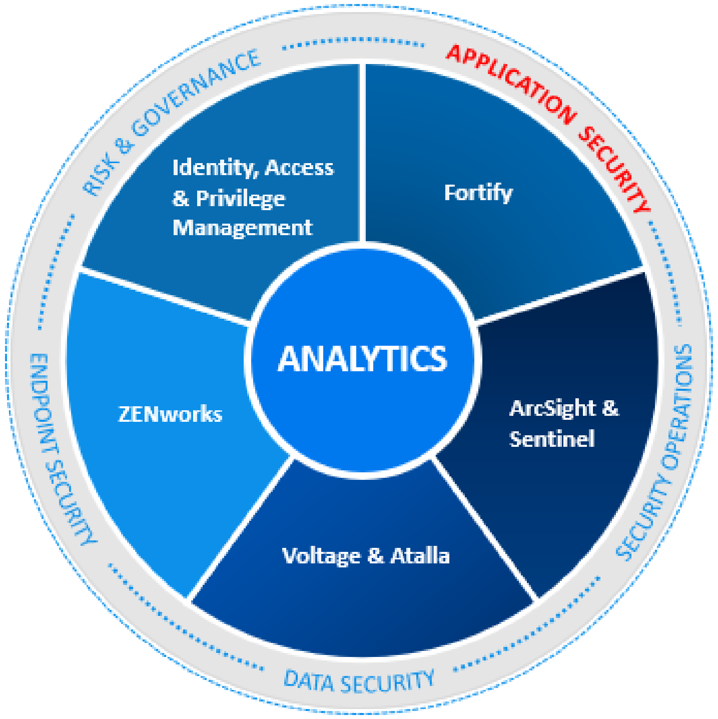
(updated Dec 5th 2018)

Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ Data for 2017-2018

Application security is more important than ever

The majority of security breaches today are from application vulnerabilities

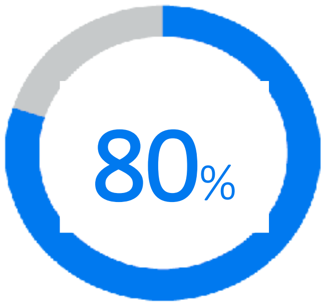
- Perimeter
- Network
- Endpoint
- Application
- Data



90%

Percentage of security incidents from exploits against defects in the design or code of software.[1]

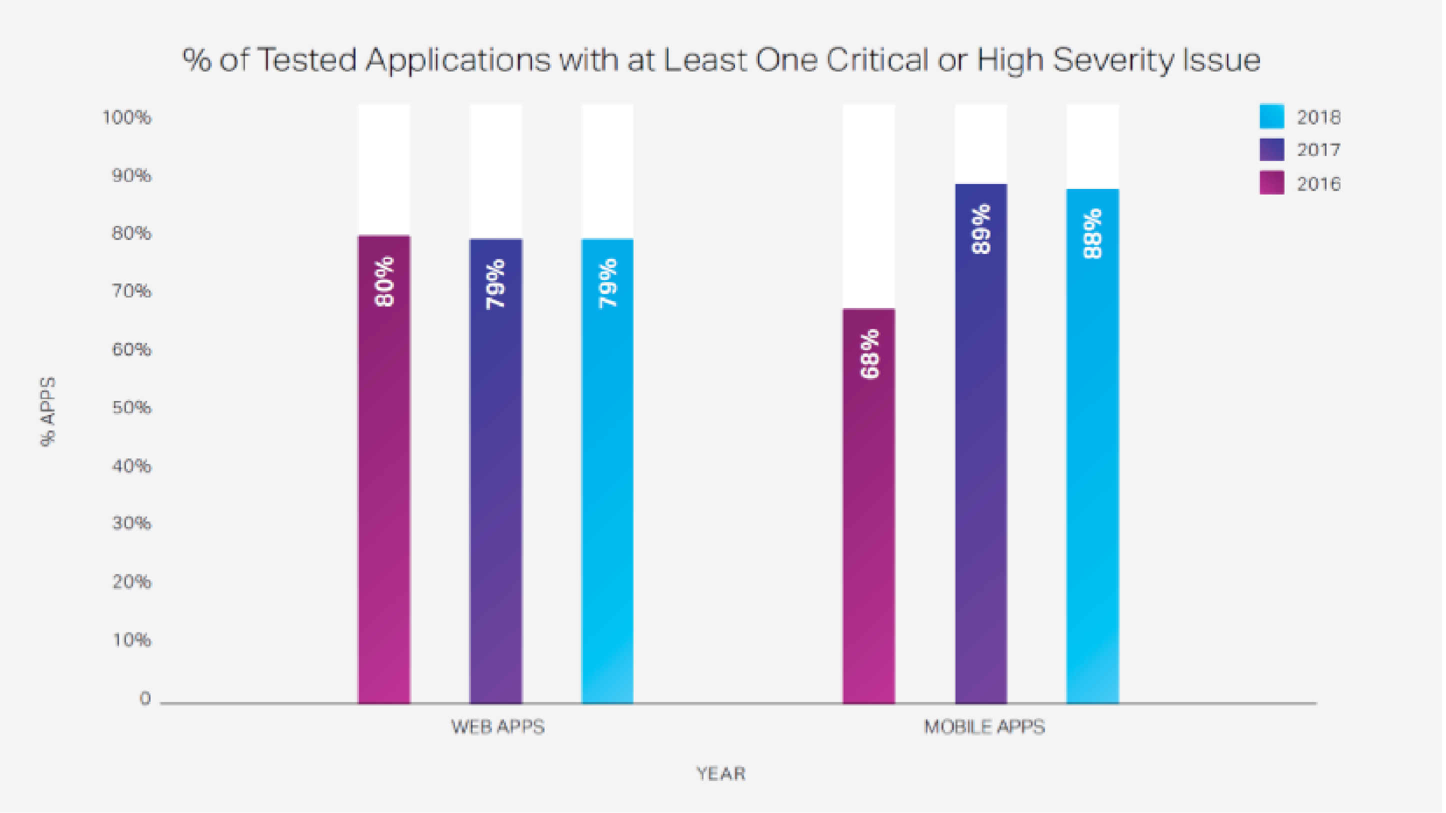
Homeland Security



Percentage of applications containing at least one critical or high vulnerability.[2]

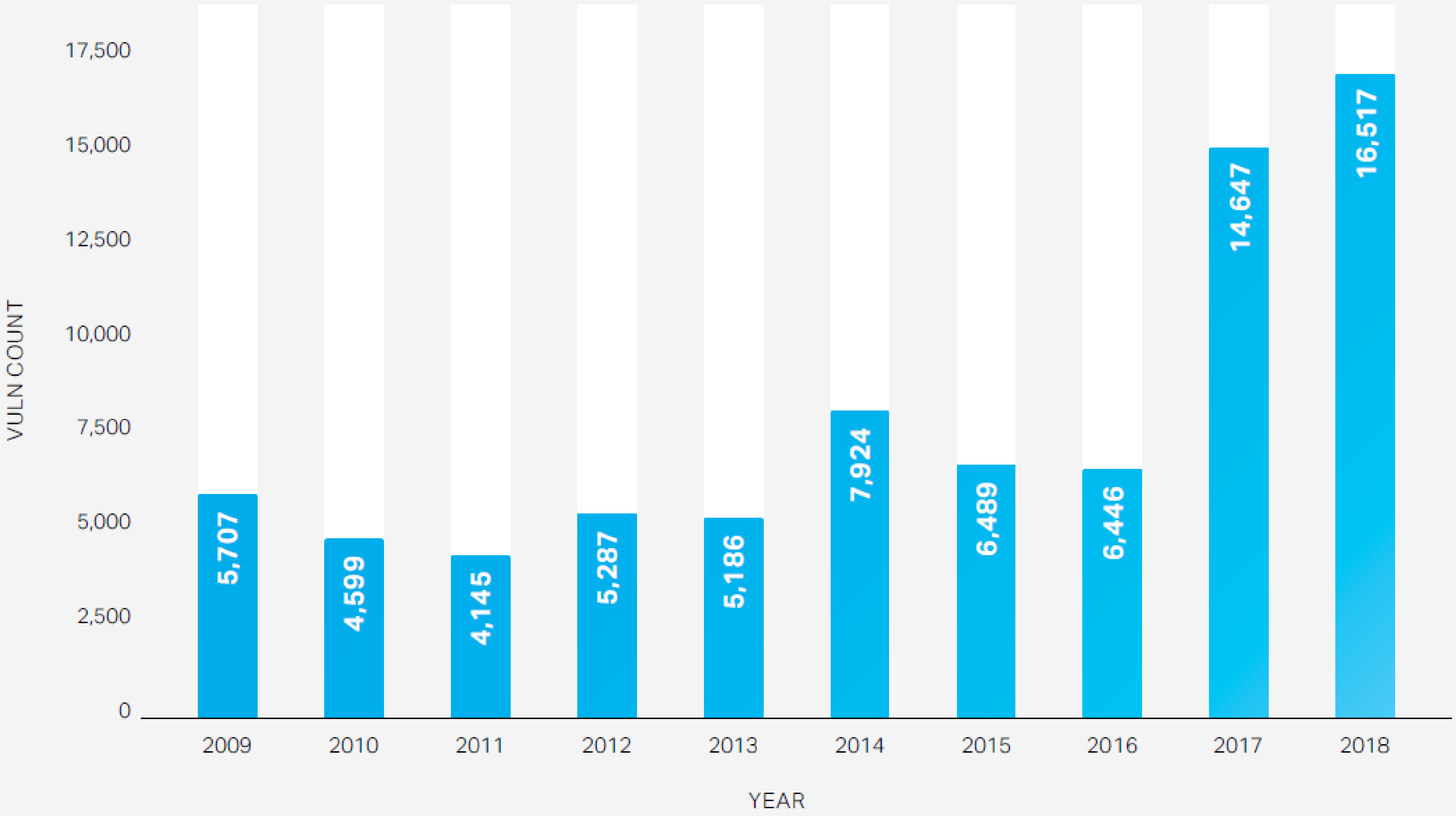
Source: [1] U.S. Department of Homeland Security’s U.S. Computer Emergency Response Team (US-CERT)
[2] 2017 Application Security Research Update” by the HPE Software Security Research team, 2017

Severe weaknesses prevalent in majority



Proactive approaches to application security consistently identify critical issues (known-unknowns).

Vulnerability Reports to NVD, 2009 to 2018



Next we compared the top 10 vulnerability categories with critical or high severity only.

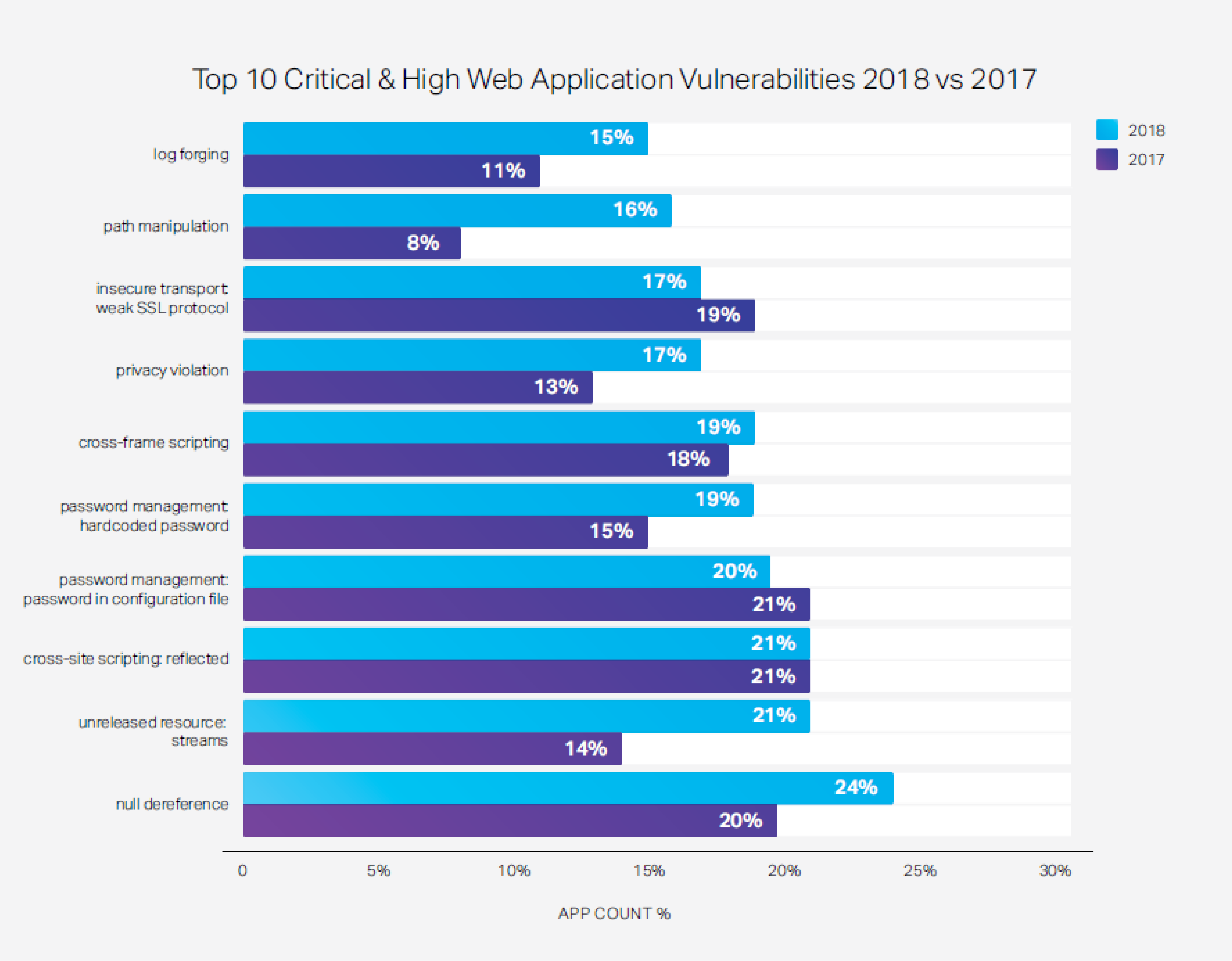
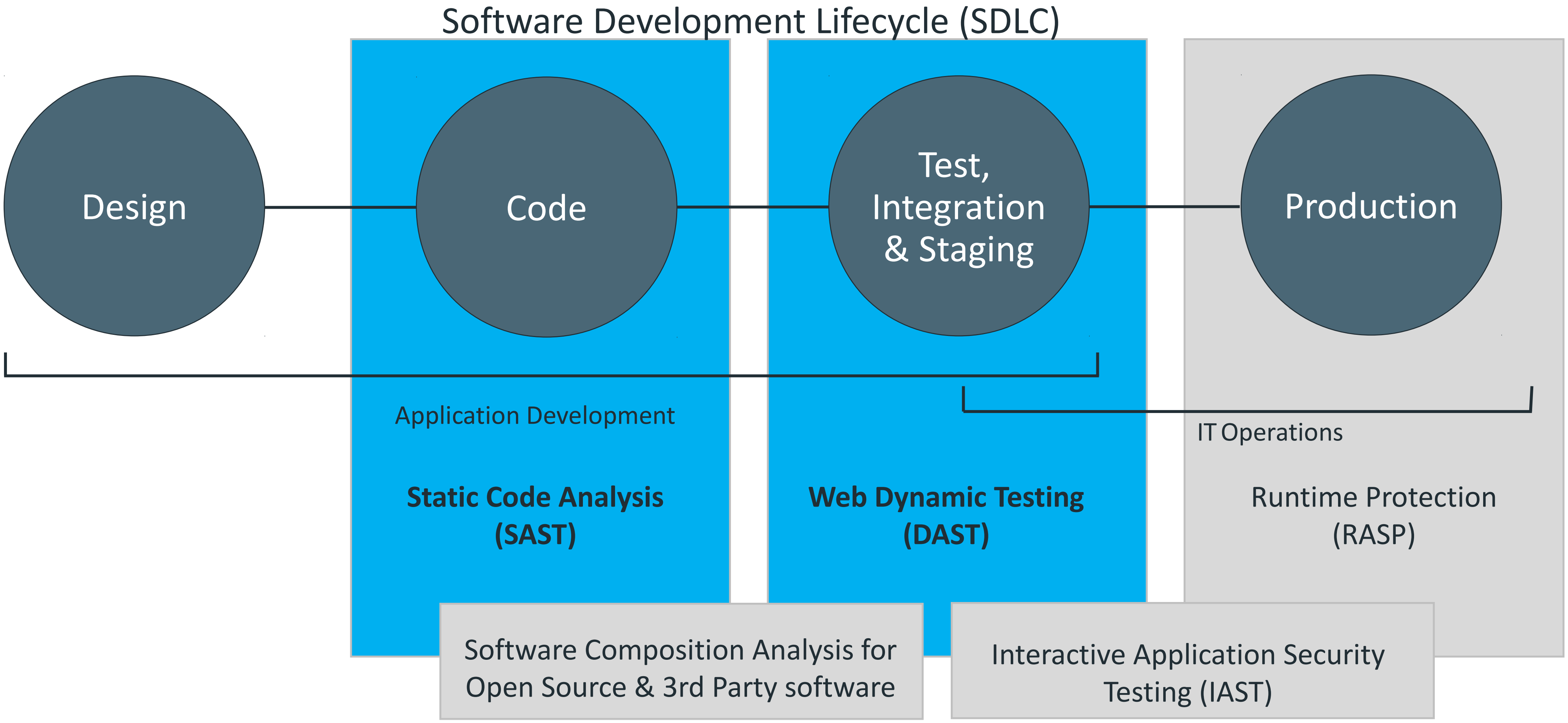


Figure 21. Critical and High issues in web applications 2018 vs 2017

Build Security INTO the software lifecycle



Software Development Lifecycle (SDLC)

Design

Code

Test, Integration & Staging

Production

Application Development

IT Operations

Static Code Analysis (SAST)

Web Dynamic Testing (DAST)

Runtime Protection (RASP)

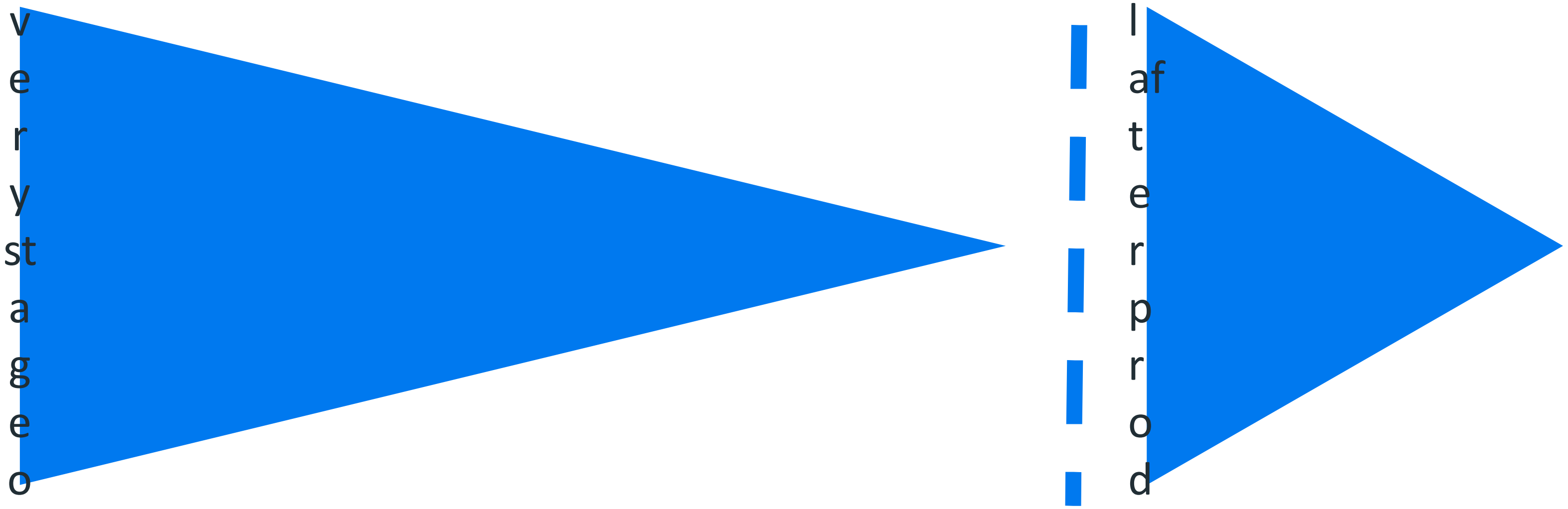
Software Composition Analysis for Open Source & 3rd Party software

Interactive Application Security Testing (IAST)

“Shift Left” earlier in development lifecycle means faster & cheaper

echange, every stage of dev cycle, e,

75%



Wait till after production

25%

*** But…35% test less than half of their apps**

Source: “2019 The State of Application Security in the Enterprise,” Micro Focus Fortify

FORTIFY

Getting Started in One Day

What can you do today?

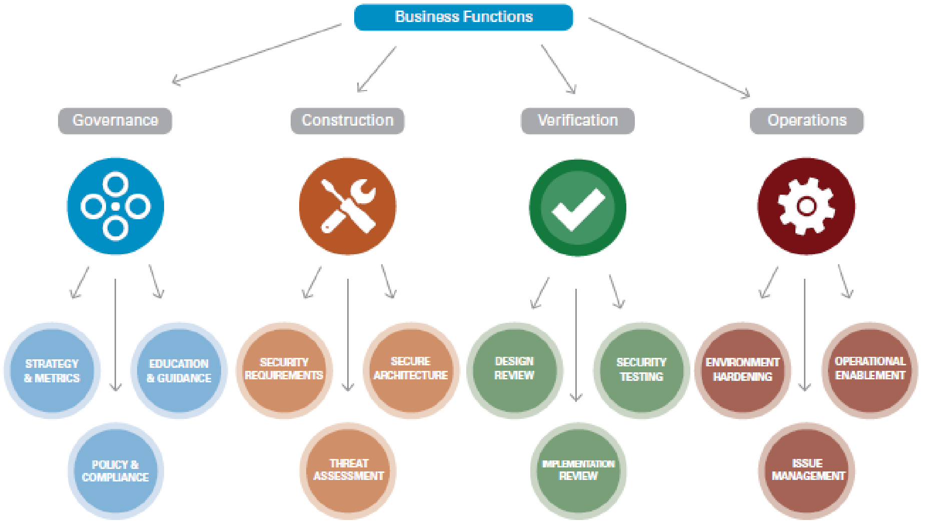
1. Follow an Established Maturity Model
2. Identifying Your Security Champions
3. Assessment Exercise
4. Define Your Initial Scope
5. Find the Right Tools to Fit These Requirements

1. Maturity Model

Start with a Security Maturity Model

OWASP SAMM (Software Assurance Maturity Model)

OWASP
Open Web Application Security Project

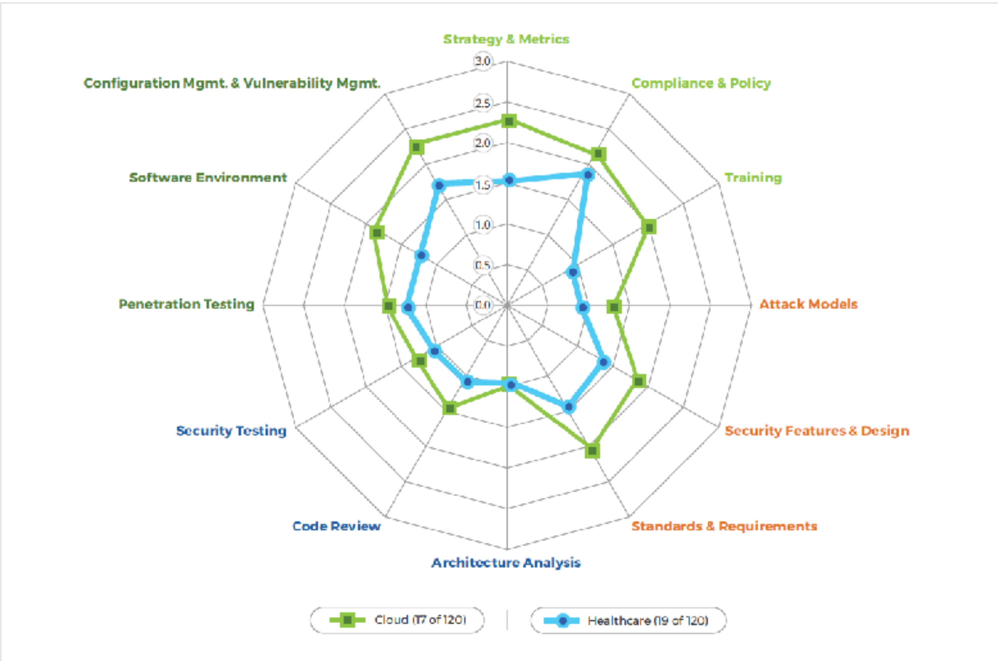


https://owaspsamm.org/

BSIMM: (Building Security in Maturity Model)

BSIMM

CLOUD VS. HEALTHCARE SPIDER CHART



https://www.bsimm.com/

2. Security Champions

What is a Security Champion?

According to OWASP

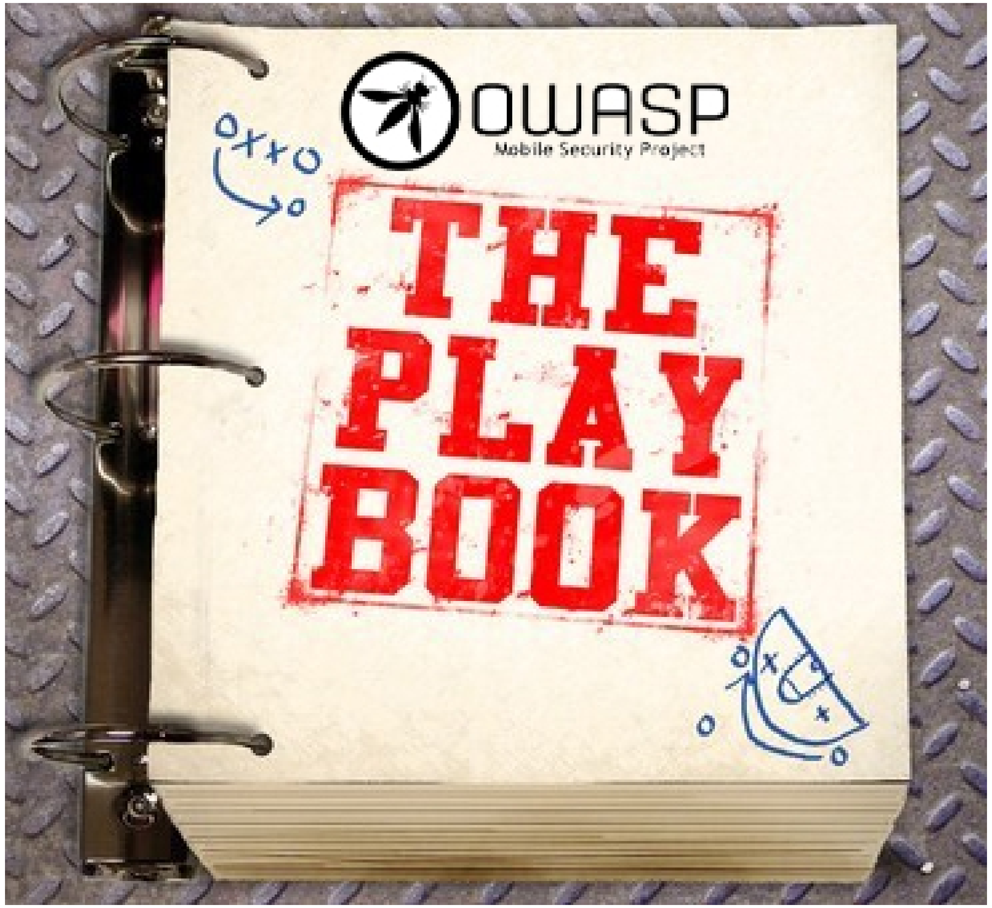
“Security Champions are active members of a team that may help to make decisions about when to engage the Security Team”

Why are Security Champions Important?

- Scaling Security Through Multiple Teams
- Engaging “Non-Security” Folks
- Establishing a Security Culture

OWASP Security Champion Playbook

The Security Champions Playbook describes the main steps for fast establishment of a Security Champions program regardless of the **company size** and **maturity** of the existing security processes.



3. Security Assessment

Types of Assessments

- Internal
- 3rd Party Vendor

Preparing for an Assessment

- Create a core assessment team
- Review existing security policies
- Create a database of IT assets
- Understand threats and vulnerabilities
- Estimate the Impact
- Determine the likelihood
- Plan the controls

4. Define Your Initial Scope

Define Your Initial Scope

What Applications and Development Teams to Start with

Whether to use SAST, DAST

What Integrations are Crucial for your organization

As a Service, On-Premise, or Hybrid

Enabling Your Developers

What does success look like for your organization?

5. Find the right tools

Fortify provides Seamless Application Security

Easy to Get Started

- Start in a day with Fortify on Demand with actionable results

Easy to Use

- Real-time security in the IDE for developers with Security Assistant
- Robust integration ecosystem

Fast

- Get scan results in minutes
- Adjust scans to achieve desired coverage for both SAST and DAST
- Apply machine learning to identify and prioritize the most relevant issues with Audit Assistant

Accurate

- OWASP Benchmark: Fortify SCA true positive rate is 100%

Scalable

- SaaS, on-premise, or hybrid
- Flexible to grow

Fortify is recognized for delivering value

- 10 out of 10 of the largest information technology companies
- 9 out of 10 of the largest banks
- 4 out of 5 of the largest pharmaceutical companies
- 3 out of 3 of the largest independent software vendors
- 5 out of 5 of the largest telecommunication companies

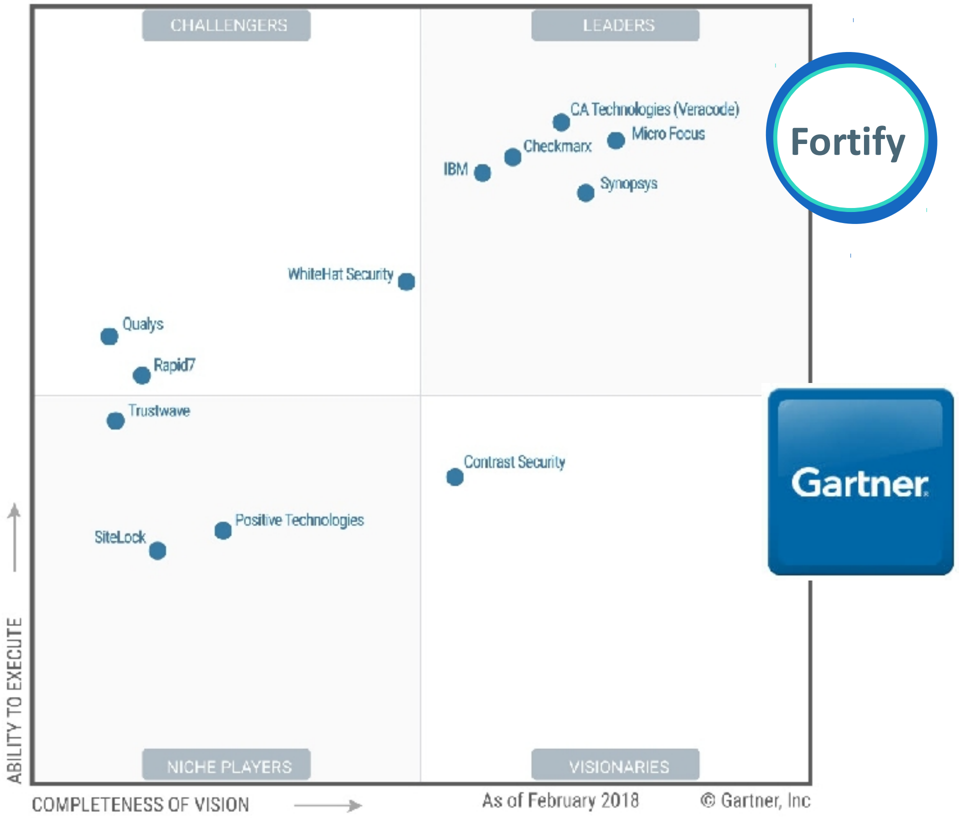
SAP acxiom ServiceMaster FICO

Aaron's novagalicia banco Affinity Credit Union nielsen

Cox Automotive DELTA Heartland Payment Systems centrica British Gas

2018 Gartner Magic Quadrant for AST

Figure 1. Magic Quadrant for Application Security Testing



Source: Gartner (March 2018)

Köszönöm a figyelmet

Hargitai Zsolt
zsolt.hargitai@microfocus.com