Do AppSec Shortcuts Exist?

Greg Wolford, CISSP
Veracode
gwolford@veracode.com
(817) 637-8349

Every company is a software company

On our current trajectory, GE is on track to be a top 10 software company.

— Jeff Immelt, CEO

Companies are producing more applications than ever before

A typical $500 million plus enterprise has developed

more than 3,079

applications

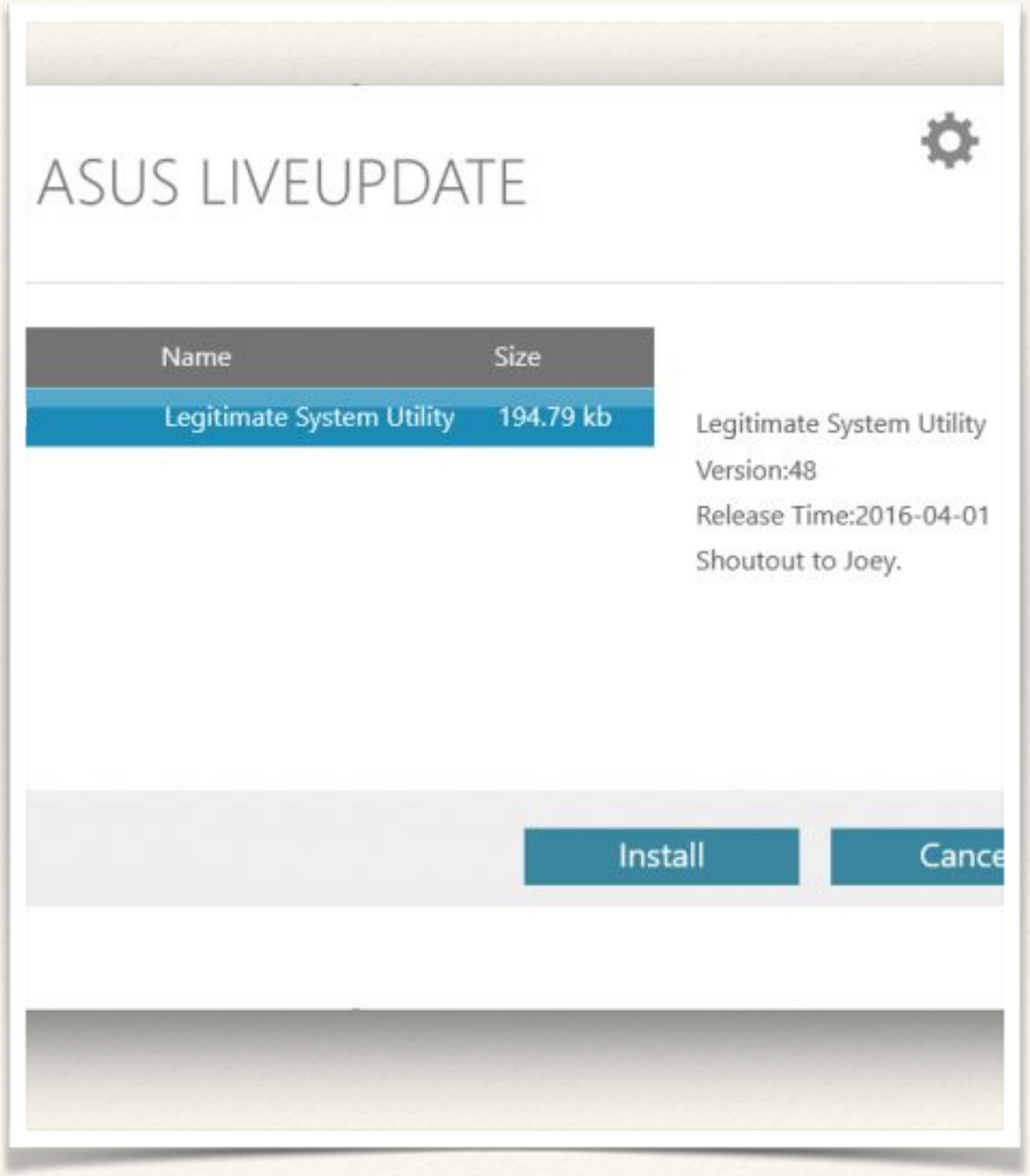
2014 State of the CIO, CIO Magazine

Despite their importance, applications are inherently insecure.

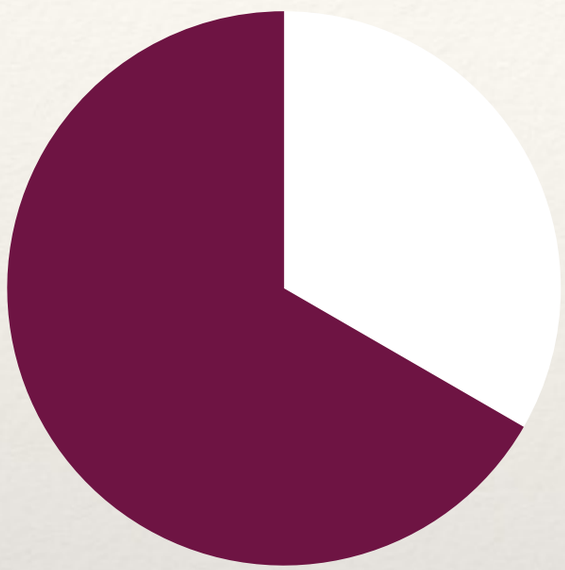
and increasingly the target for cybercriminals.

ASUS delivers updates over HTTP with no verification.

- "Content is delivered via ZIP archives over plain HTTP, extracted into a temporary directory and an executable run as a user in the "Administrators" NT group ("Highest Permissions" task scheduler).
- HTTP communications expose users to MitM attacks

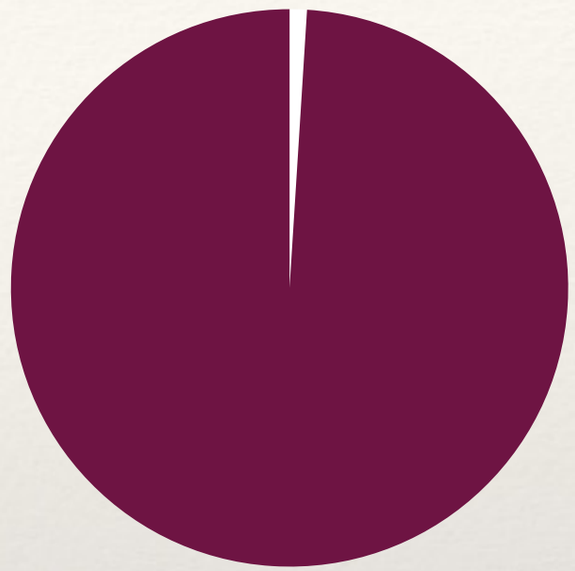


Yet security spending doesn't reflect reality



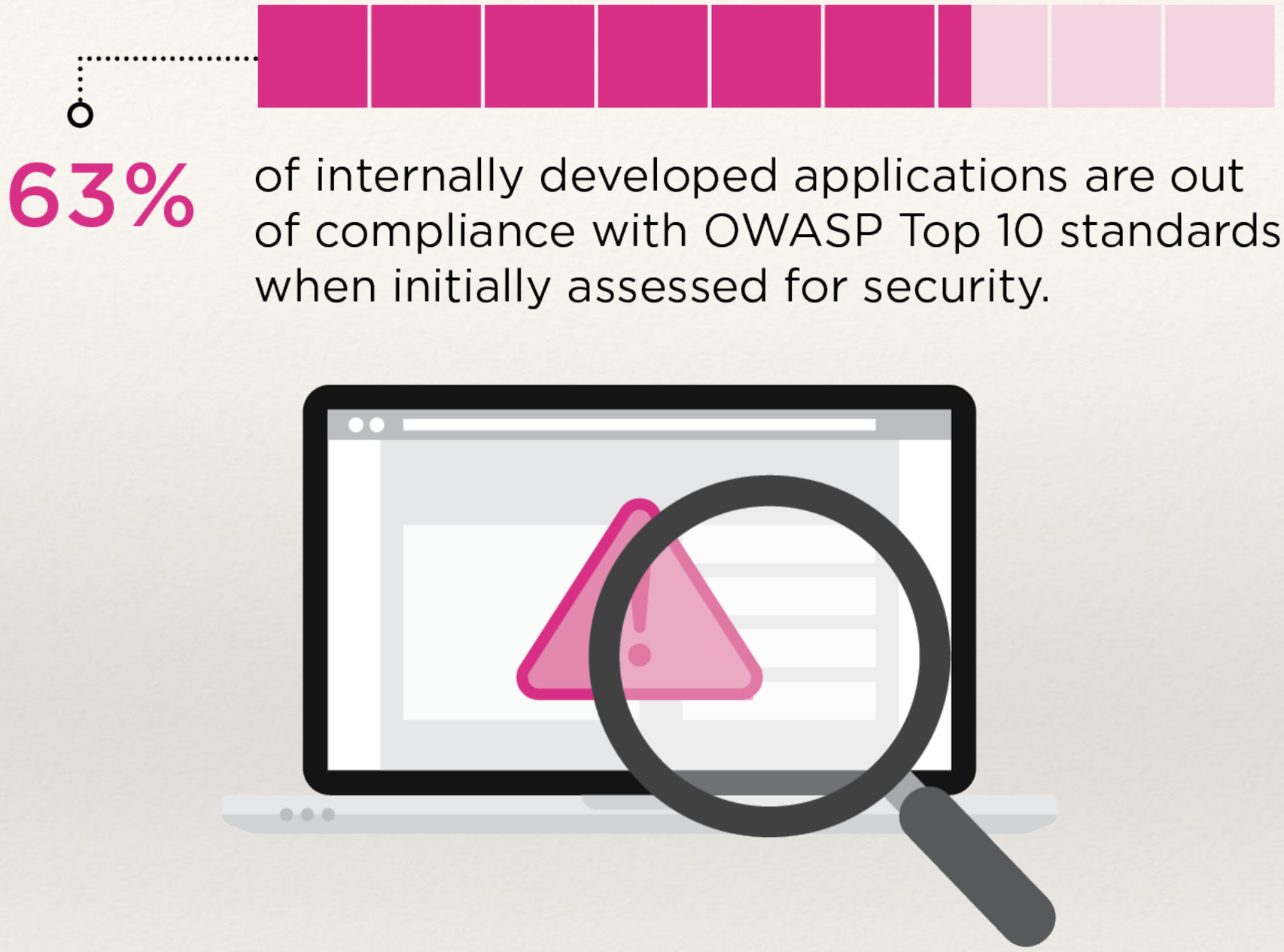
Applications are increasingly attacked

Application attacks are the most frequent pattern in confirmed breaches



Security spending misses the target

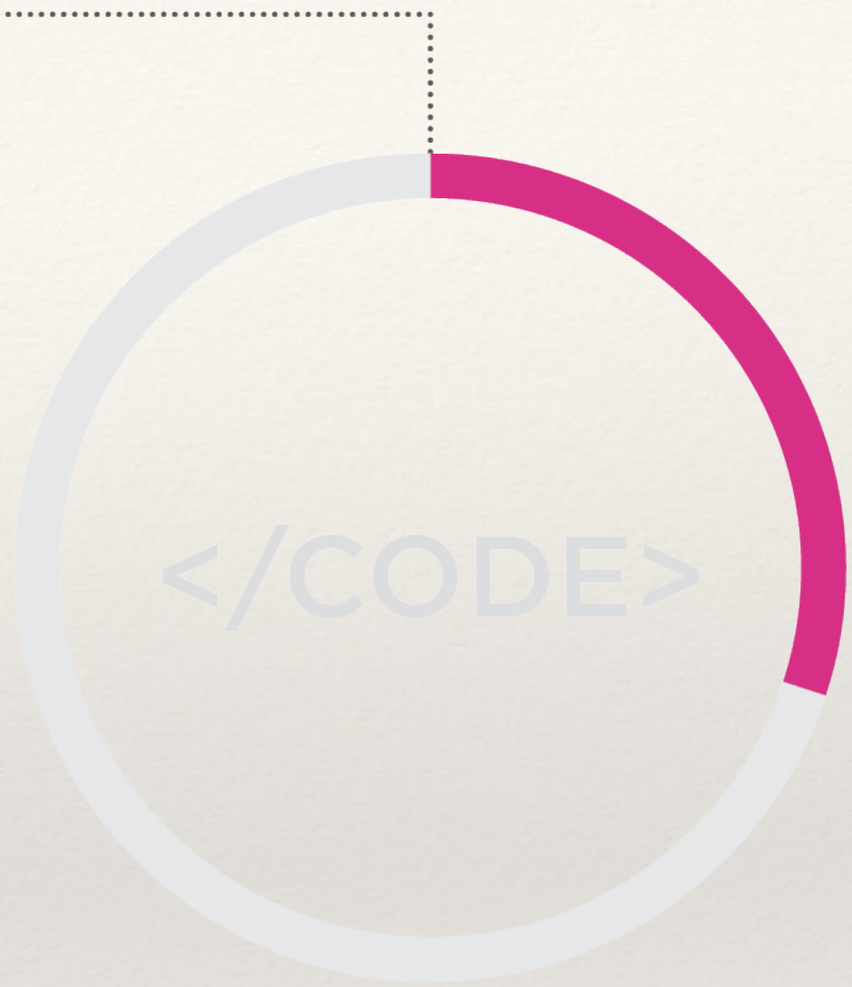
1% of security spending is focused on the application layer

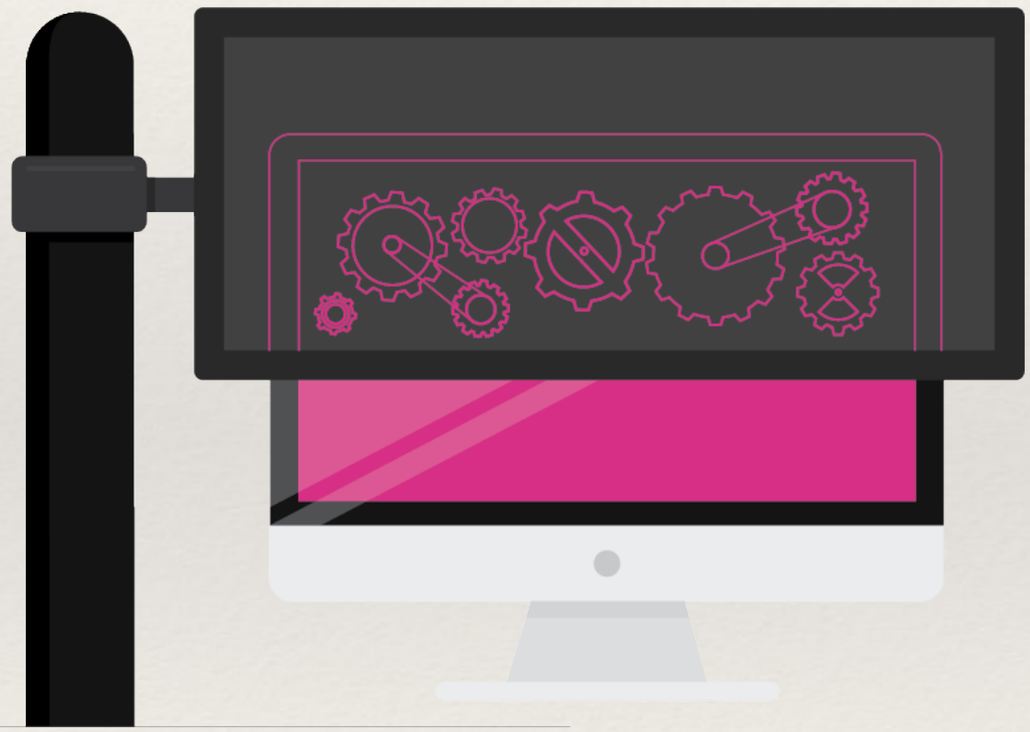


63% of internally developed applications are out of compliance with OWASP Top 10 standards when initially assessed for security.

State of Software Security Report: Focus on Industry Verticals, Volume 6, Veracode.

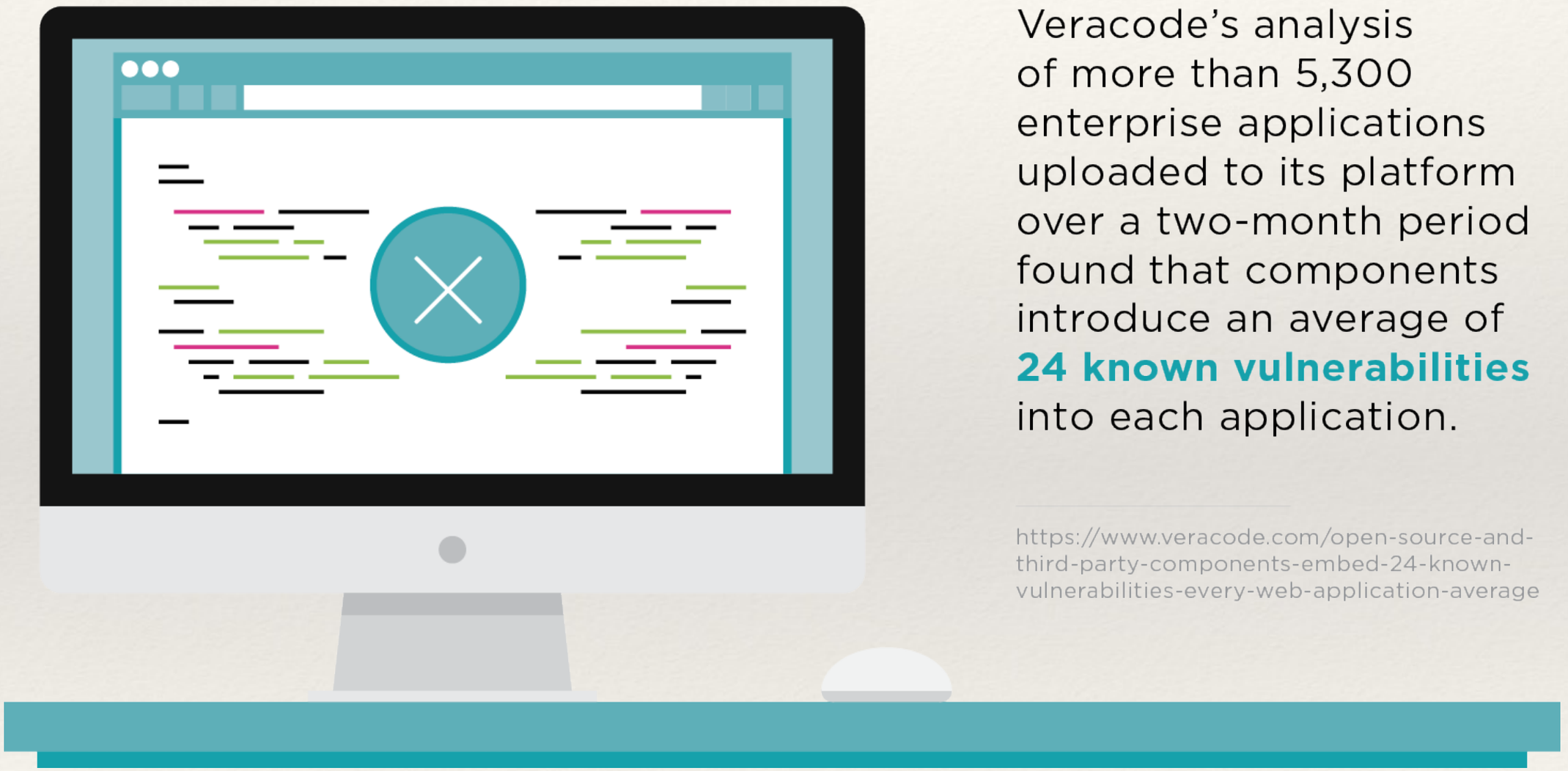
30 percent
of companies never scan for vulnerabilities during code development.





The biennial *Global Information Security Workforce Study* published by the International Information Systems Security Certification Consortium (ISC).

What a trillion lines of code tells you…



Veracode's analysis of more than 5,300 enterprise applications uploaded to its platform over a two-month period found that components introduce an average of **24 known vulnerabilities** into each application.

https://www.veracode.com/open-source-and-third-party-components-embed-24-known-vulnerabilities-every-web-application-average

U.S. Department of Homeland Security (DHS) research found that **90 percent** of security incidents result from exploits against defects in software.

CSOOnline.com, September 2, 2015

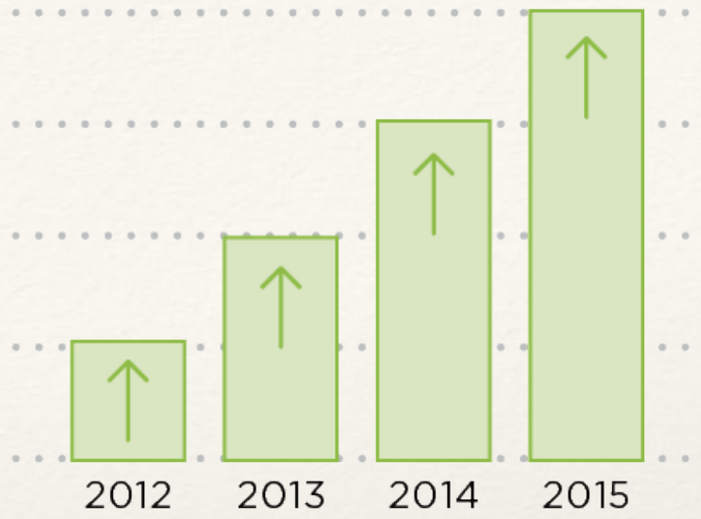
Lack of application security is damaging companies

Is poor software development the biggest threat?

Nearly **80 percent** of applications written in web scripting languages are vulnerable to at least one threat at an initial assessment.

Web and mobile applications account for **more than a third** of data breaches.

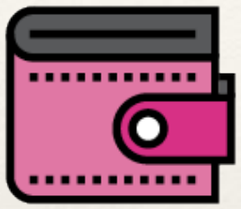
2014 Verizon Data Breach Investigations Report



Attacks at the application layer are growing by **more than 25%** annually.

Q3 2015 *State of the Internet Security Report*, Akamai, Dec. 8, 2015

High profile application layer breaches



TARGET

HOW: Sophisticated kill chain including exploitation of a vulnerable web application

RESULT: Hackers stole names, mailing addresses, phone numbers and email addresses from over 70 million shoppers

JPMORGAN CHASE

HOW: Vulnerability on website built and maintained by a third-party vendor in support of a charity

RESULT: Usernames and passwords for 76 million households and 7 million businesses accounts were stolen

COMMUNITY HEALTH

HOW: Targeted a flaw in OpenSSL, CVE-2014-0160, better known as Heartbleed

RESULT: The theft of Social Security numbers and other personal data belonging to 4.5 million patients

Why isn’t there a simple solution?

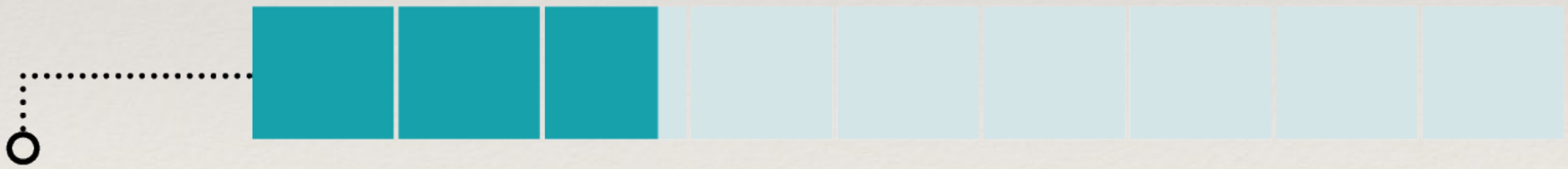
It begins at the beginning…

- Executive support / sponsorship
- Application inventory and classification
- Defined security policies
- Developer training

Few employ best practices…

79% of developers either have no process or an ineffective ad hoc process for building security into applications.

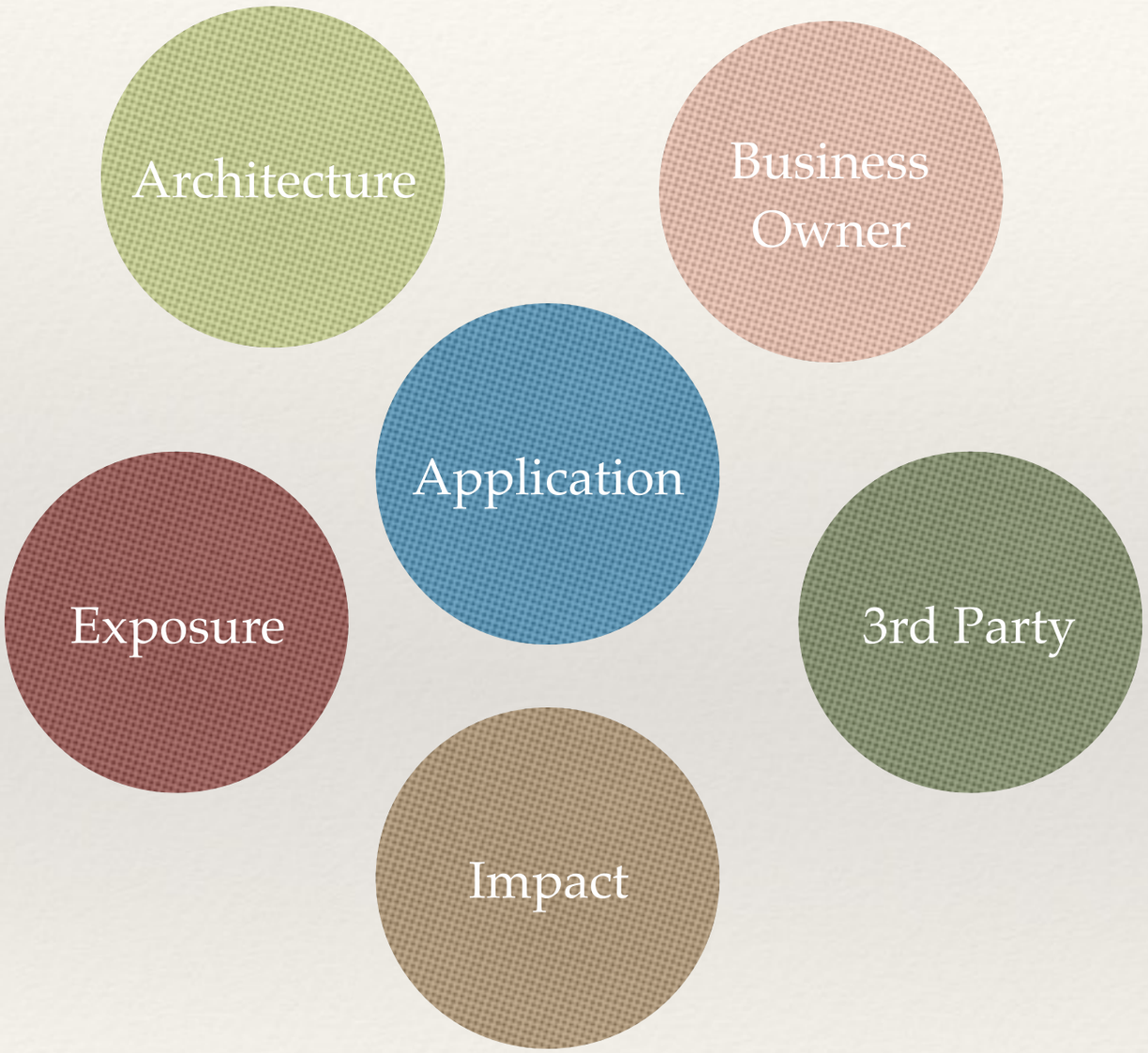
ACCORDING TO PONEMON



28% of organizations don't even know how many applications they have.

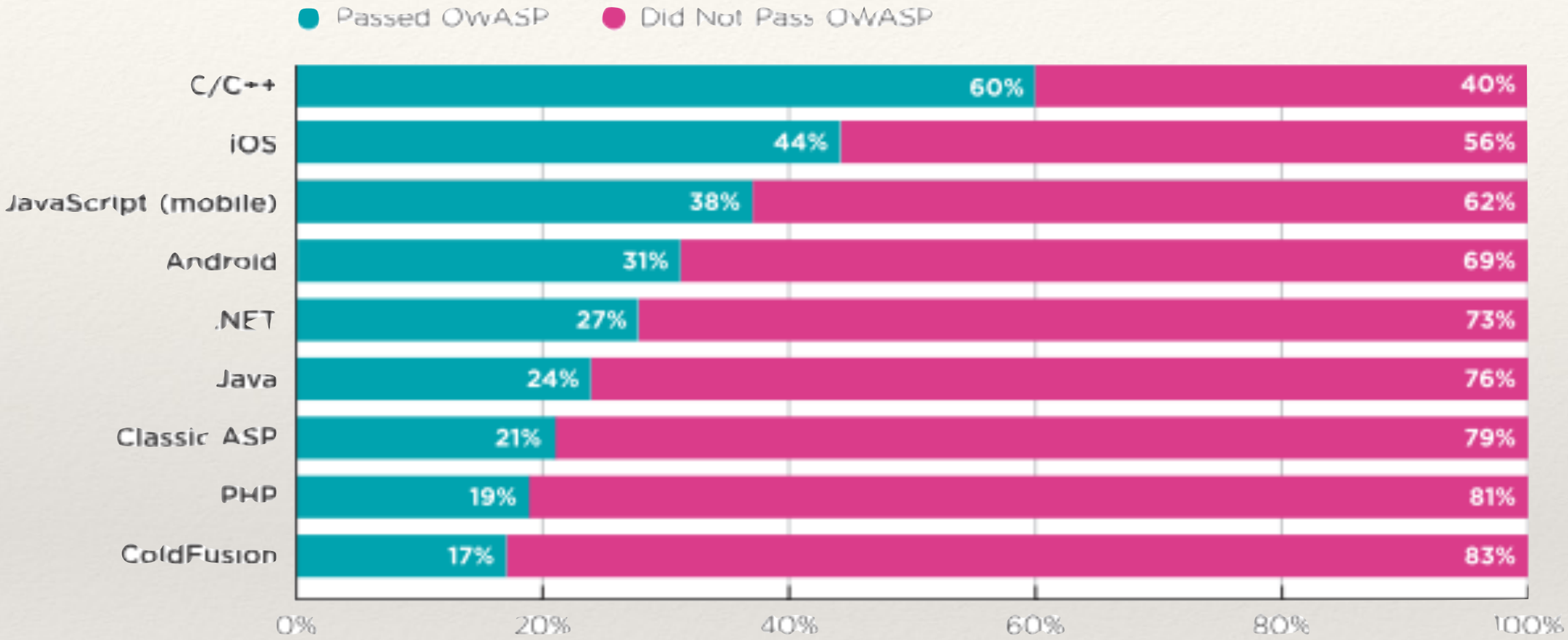
ACCORDING TO SANS

Understand where you're exposed



Application	Exposure	Architecture	Ownership	Busines
BizNet	External	WebApp	1st Party	
ClientBank	External	Mobile	3rd Party	
CustomerNet	Internal	WebApp	1st Party	
EZFileAdmin	Internal	WebApp	1st Party	
MySalesWorx	External	WebApp	3rd Party	

Understand inherent risk



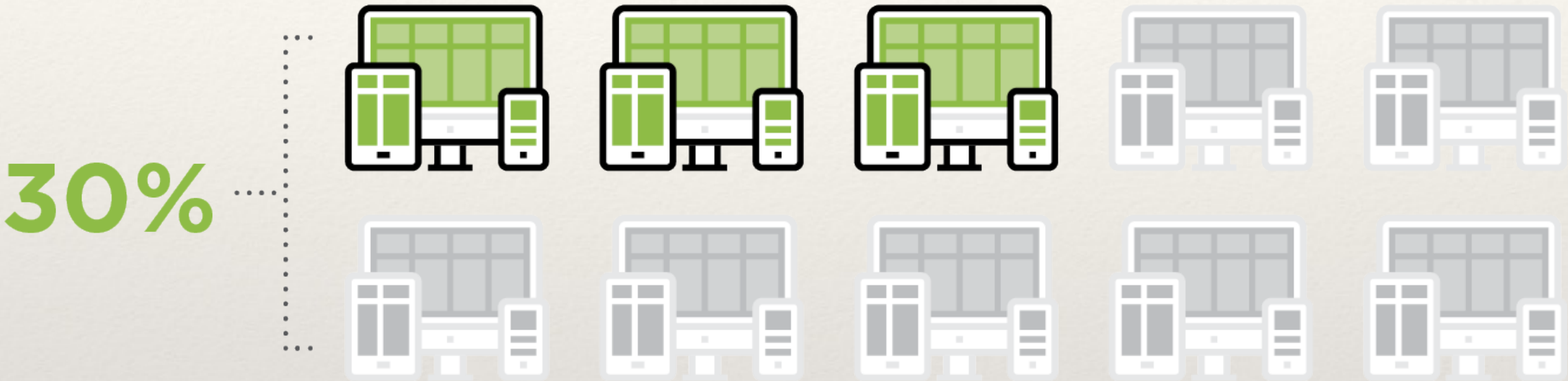
"When organizations are starting new development projects and selecting languages and methodologies, the security team has an opportunity to anticipate the types of vulnerabilities that are likely to arise and how to best test for them."

- Chris Wysopal, Co-Founder of Veracode

Know what you own and what's in the wild…

- Use a discovery solution to identify all public assets and exposed risks on your perimeter
- On average, user find 30% "unknown" sites
- Decommissioning legacy sites and servers reduces the attack surface and costs

Empower



Development organizations that leverage eLearning see a 30% improvement in fix rate.

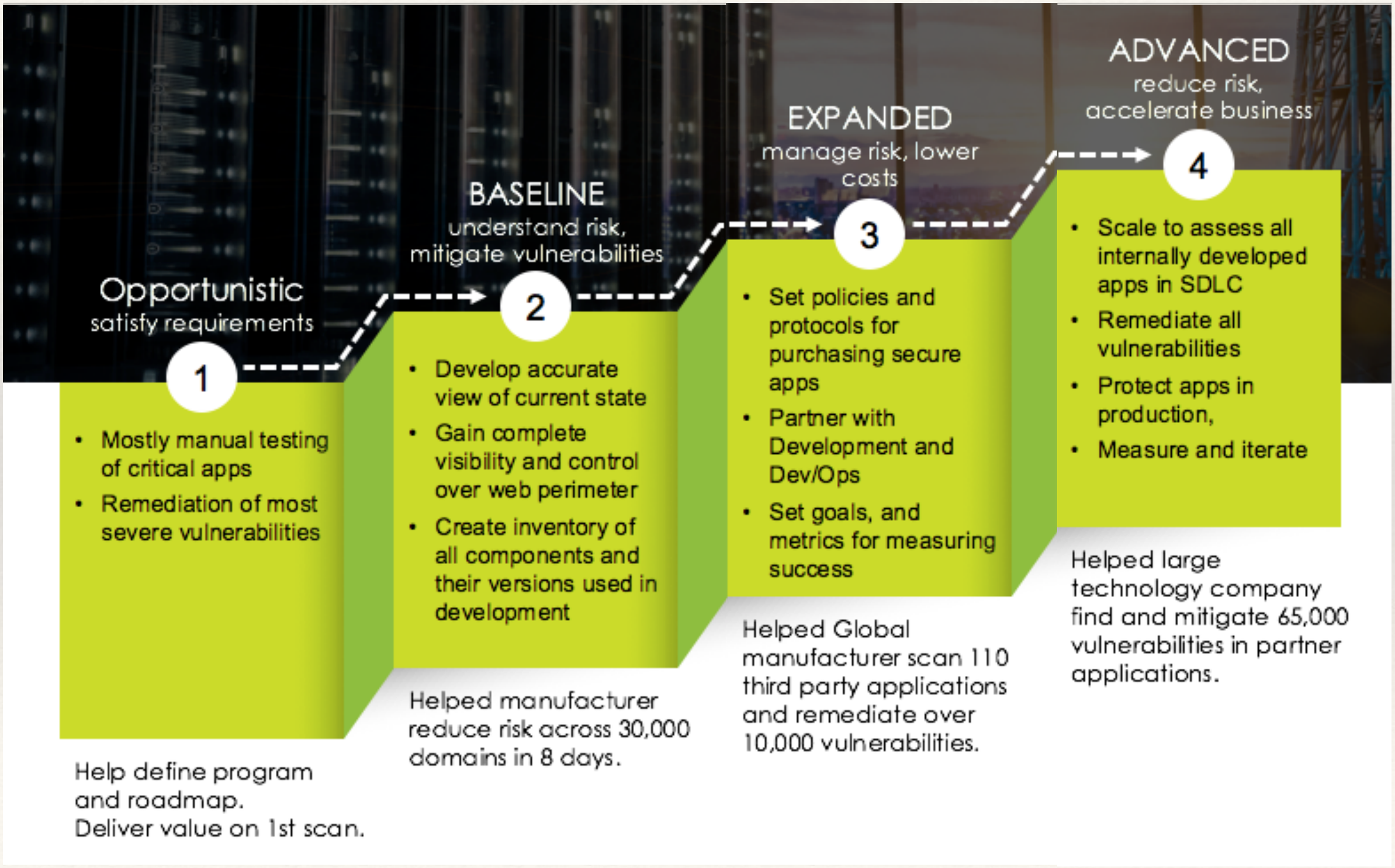
- *State of Software Security Report: Focus on Industry Verticals,* Volume 6, Veracode

Keeping the end in mind

The end goal for any organization should be a mature, robust security program that…

- Assesses every application, whether built in-house, purchased, or compiled
- Enables developers to find and fix vulnerabilities while they're coding
- Takes advantages of cloud based services and automation to improve scalability

Journey to an advanced AppSec program



Questions?