

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SPO2-T09

Making Security a Competitive Advantage

Sam King

CEO
Veracode
@samskritiking

Chris Wysopal

Founder and CTO
Veracode
@WeldPond

#RSAC

RSAConference2019

By 2050

3 billion more people on Earth

50% increase in food demand





●●●○○ AT&T LTE

12:38 AM

🔒 🔔 🔋

Today

All

Missed

⚠️

Emergency Alert

16m ago

Tornado Warning in this area til 12:45 AM CDT. Take shelter now. Check local media. -NWS



CHANGE THE WORLD

BOLDLY

RSA[®]Conference2019

The World's Software is Insecure

83%

Release software
without testing for
security

When first tested

78%

Fail to pass OWASP Top 10

85%

Have at least one vulnerability

87%

JAVA apps have at least one
vulnerable component

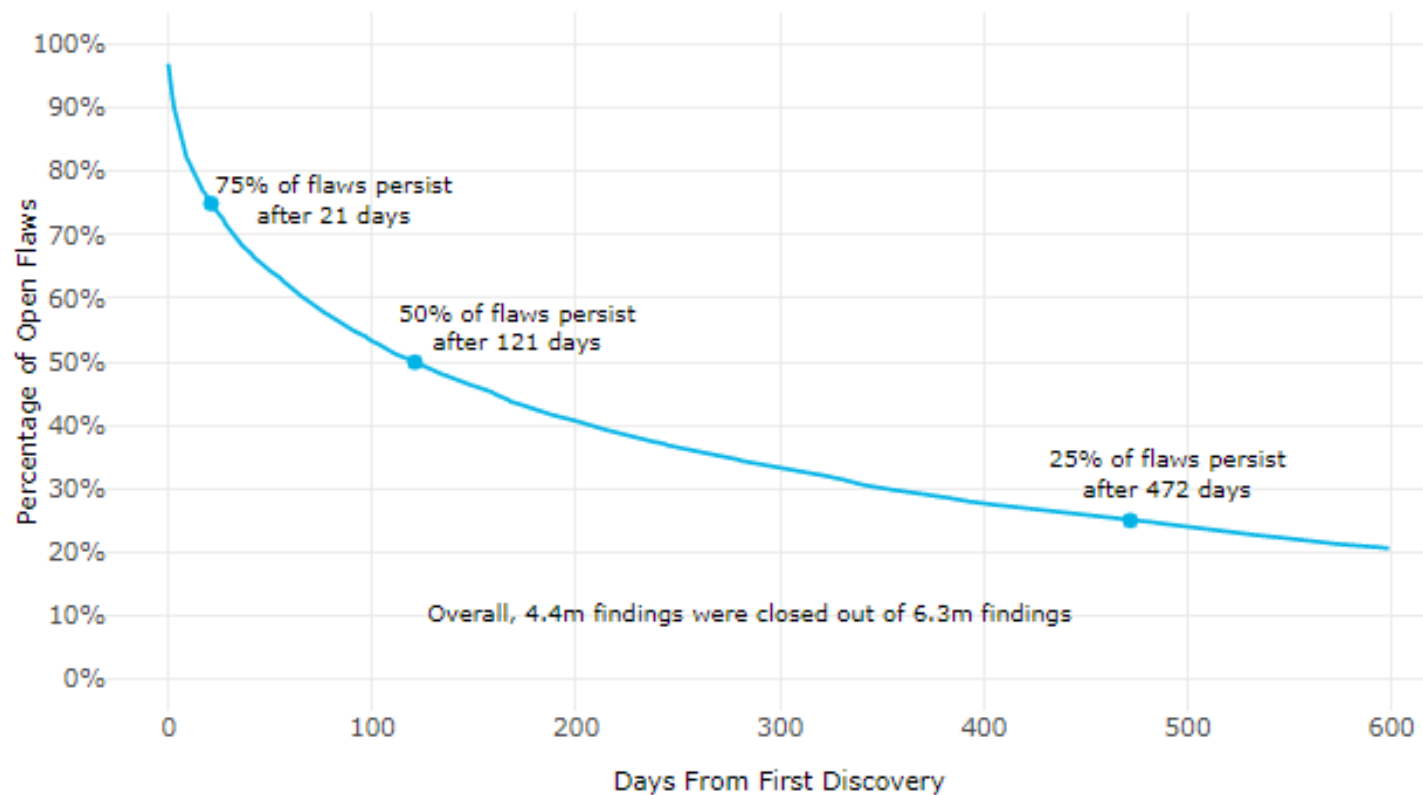
RSA®Conference2019

111 Billion

An abstract graphic in the bottom right corner consisting of numerous thin, curved blue lines and small blue dots, creating a sense of motion and connectivity, resembling a network or data flow.

Source: Cybersecurity Ventures Application Security Report

FLAW PERSISTENCE ANALYSIS



Cyberattacks occur across the entire global marketplace, and no industry is spared from its costs:

ANNUAL COST PER FIRM (IN MILLIONS)

Hospitality \$5.04

Retail \$9.30

Healthcare \$12.47

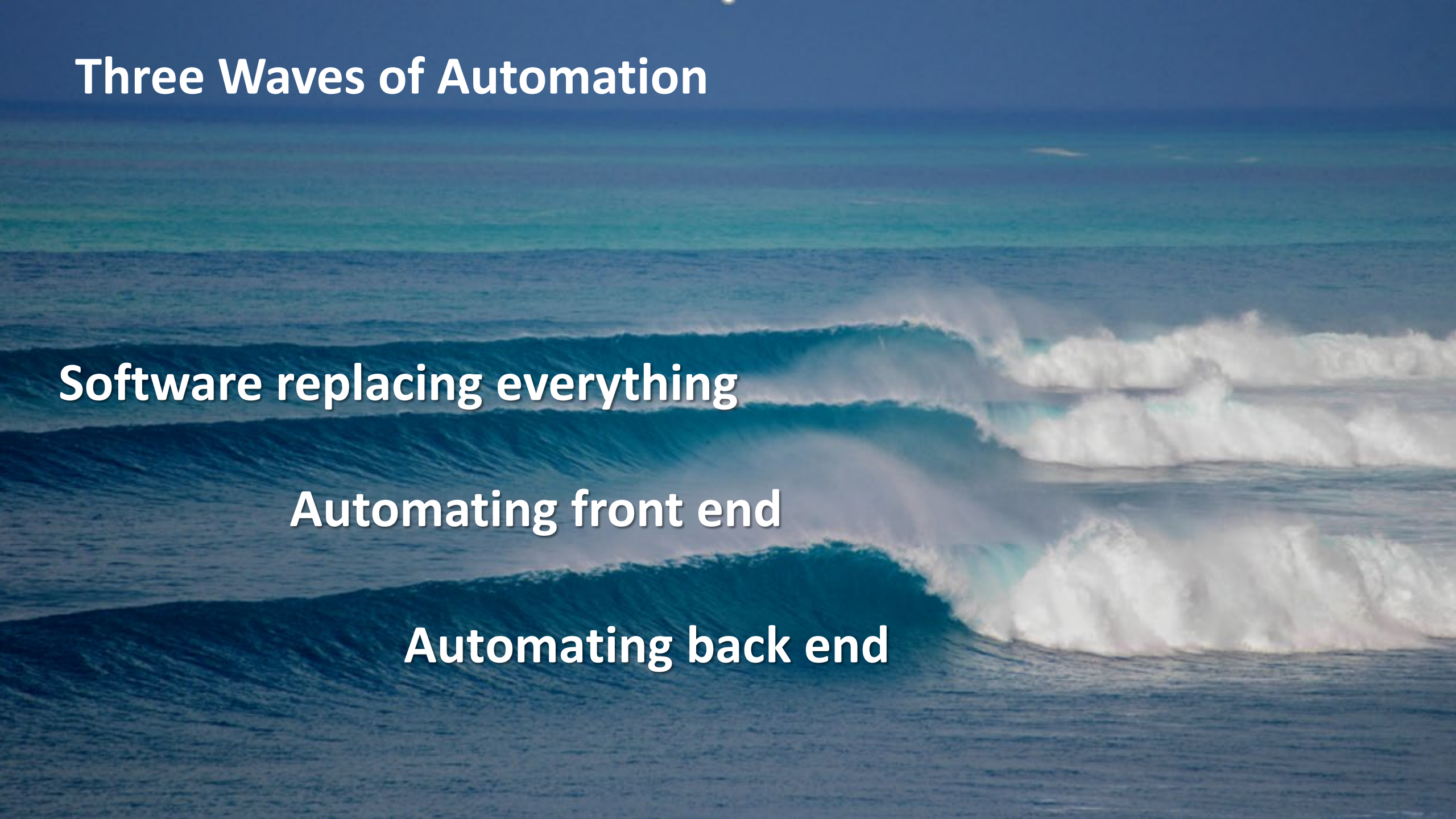
Aerospace & Defense \$14.46

Financial Services \$18.28

Source: Accenture Security's Cost of Cyber Crime Study



Three Waves of Automation

The background of the slide is a photograph of three ocean waves breaking from left to right. The waves are a deep blue color, and the water is turbulent. The sky is a clear, pale blue. The text is overlaid on the image in white, bold, sans-serif font.

Software replacing everything

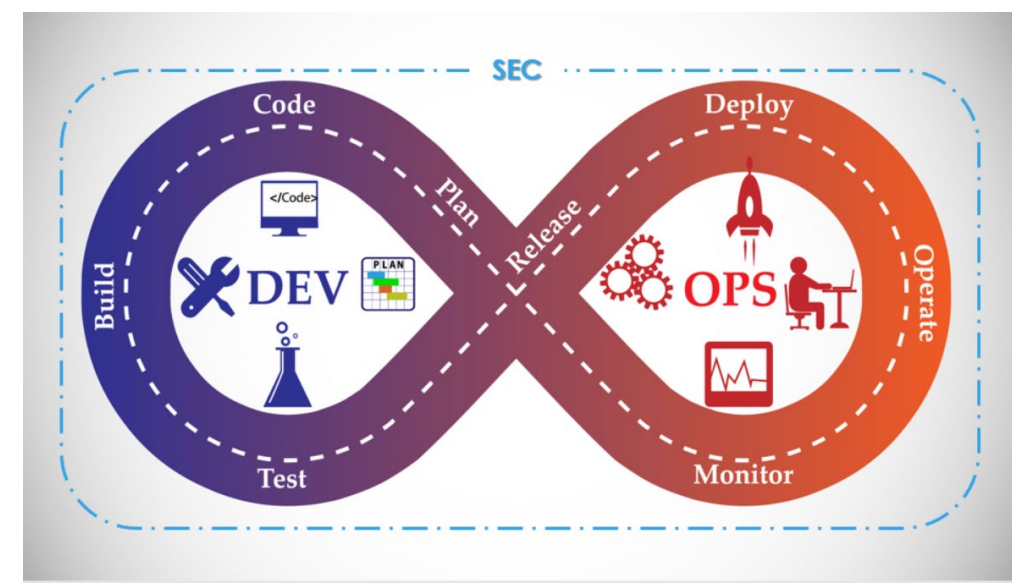
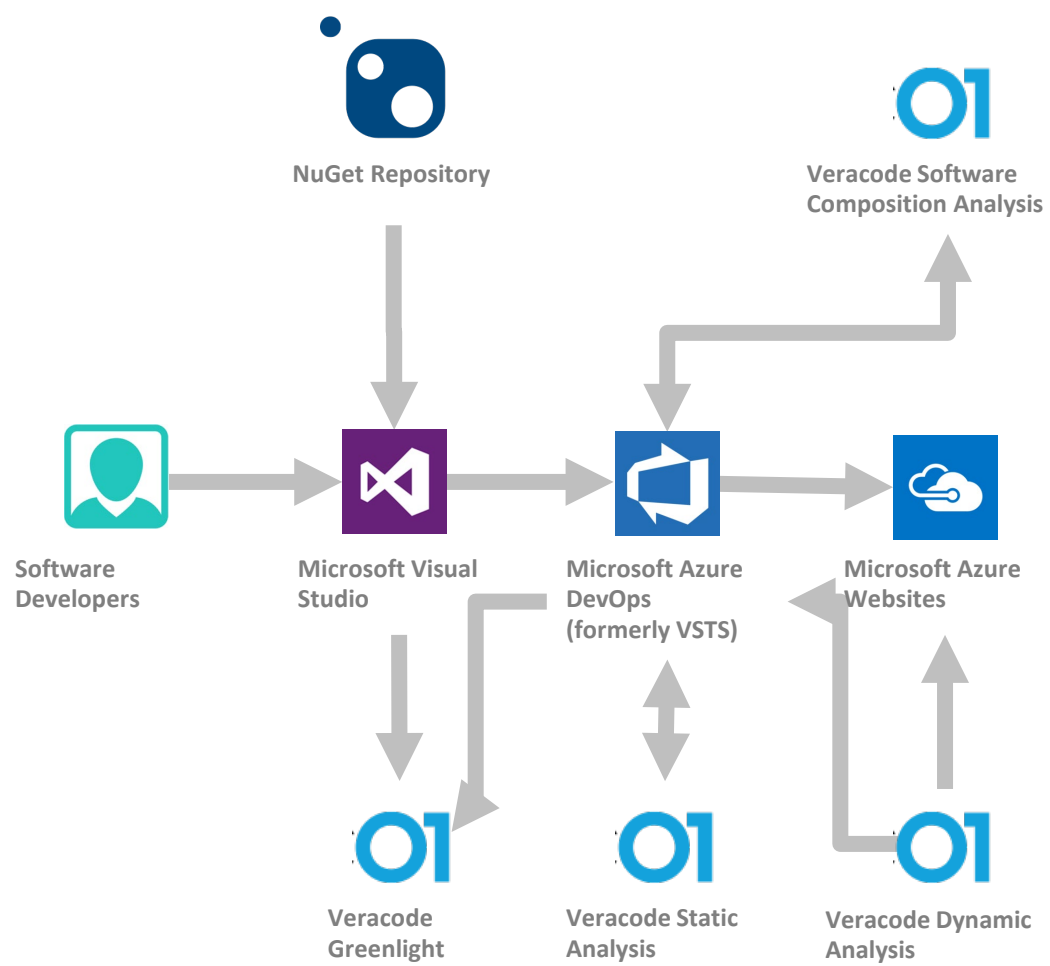
Automating front end

Automating back end



DEVSECOPS

BOLDLY



3 Keys to DevSecOps

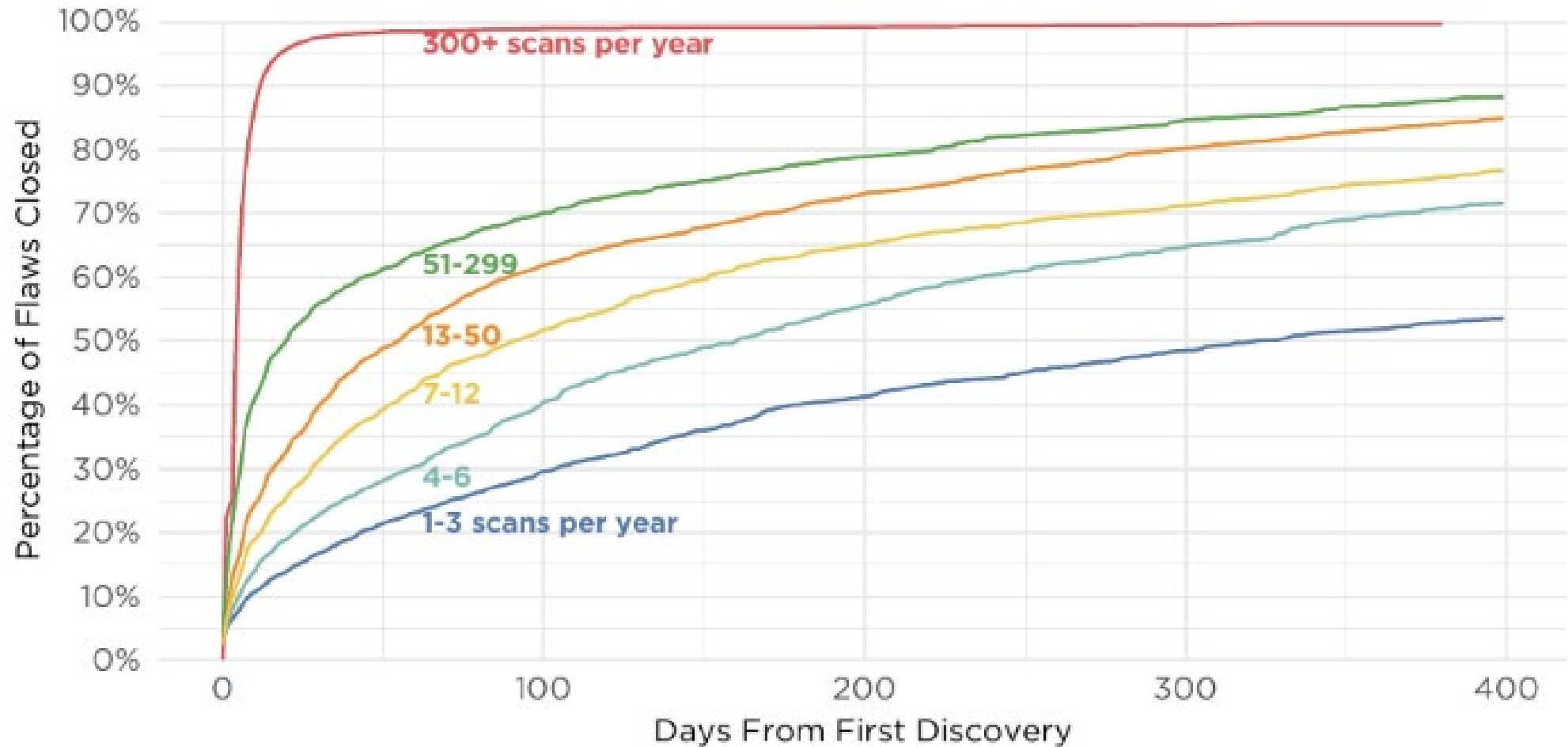
- Automate Security Testing
- Integrate into Developer Tools
- Facilitate Fixing

RSA[®]Conference2019

11X

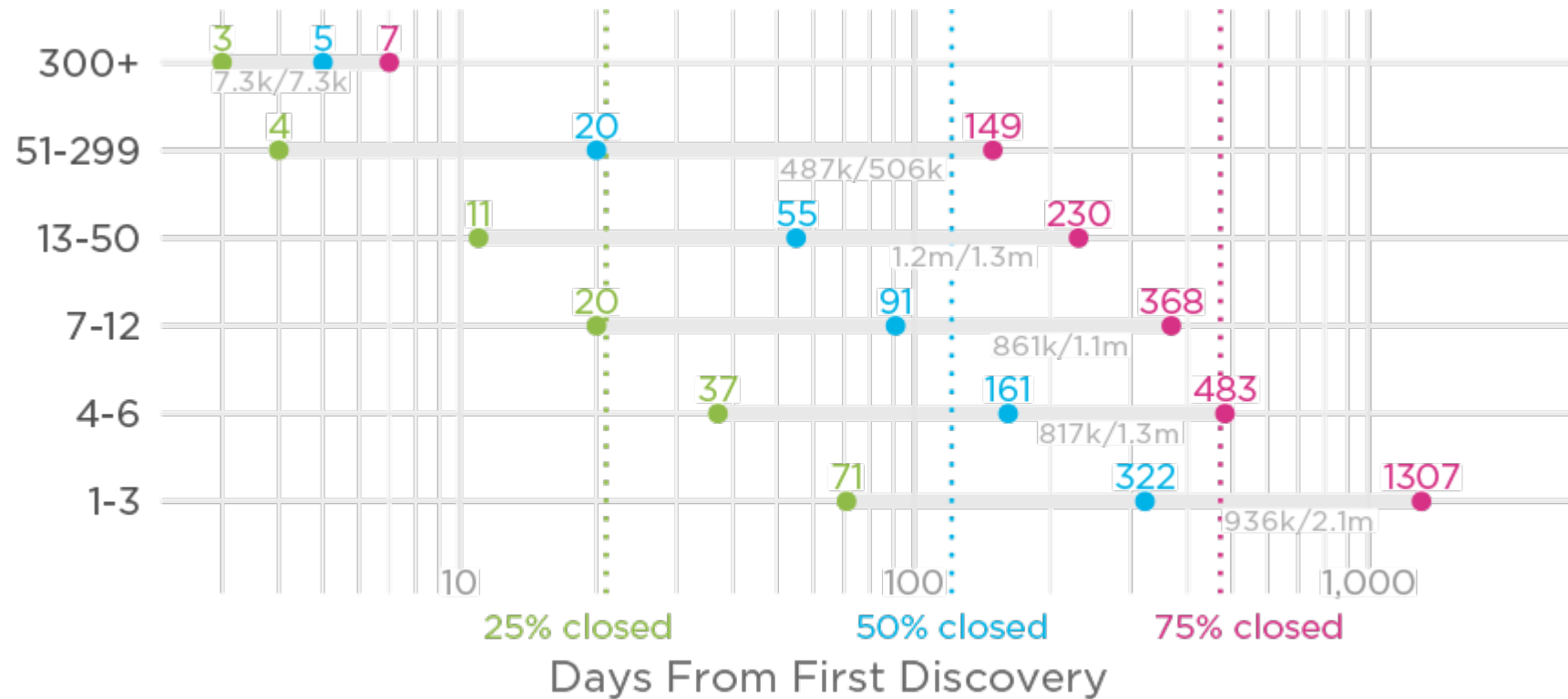
The DevSecOps Effect

#RSAC



Source: Veracode SOSS Volume 9

EFFECT OF SCAN FREQUENCY ON FLAW PERSISTENCE INTERVALS

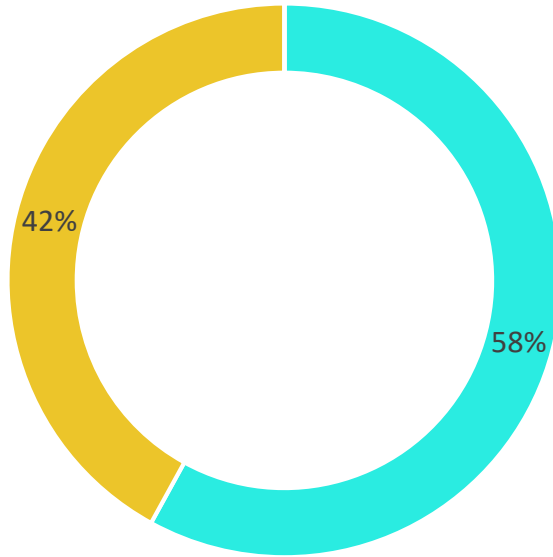


Source: Veracode SOSS Volume 9

CHAMPION

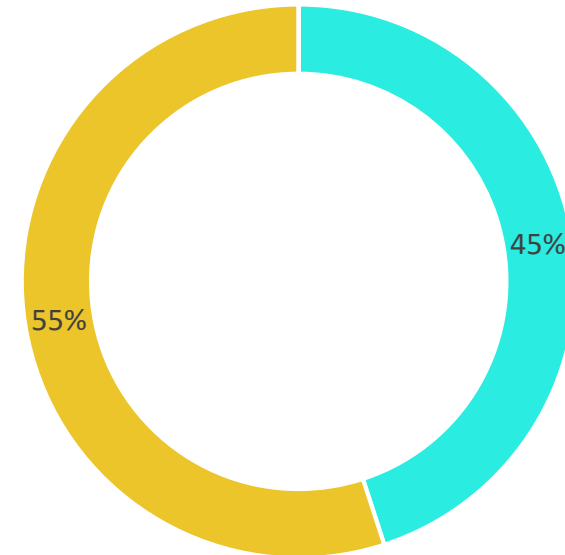
BOLDLY

DevSecOps shift is already changing the nature of the security-development relationship



Indicated that application development and security teams collaborate to prioritize security defects based on likelihood of exploitation

Indicated that the security team regularly participates in daily scrums and planning meetings



Source: Veracode AppSec and DevOps Trends Report

What does a security champion do?

- **Education.** Staying up-to-date with the latest practices through ongoing training with security
- **Inspiration.** Raising awareness of security issues within the development team
- **Review.** Reviewing code for security issues
- **Escalation.** Acting as the point person to elevate an issue for the security team to review
- **Resource.** Answering developer team questions about secure coding practices
- **Sharing.** Connecting with other security champions throughout the organization to share ideas and tips



What a does a developer champion do?

NEW RESPONSIBILITIES	NEW SKILL REQUIREMENTS	
	Enable developers to find and fix security-related code defects	Ability to provide remediation coaching and guidance on security-related code defects
	Govern the use of open source components	Basic understanding of application development and why and how third-party components are used
	Implement developer training on secure coding	Understanding of the basics of software development
	Manage and report on application security policy, KPIs and metrics	The ability to measure meaningful metrics at each point in the SDLC process
	Understand the requirements for security testing solutions in a DevSecOps environment — including the need for immediacy and accuracy of results to avoid impacting the delivery cycle — and enable dev to use these solutions	Basic understanding of developer role and tools, and the operation of a modern software delivery pipeline/factory
	Create developer security champions	Be empathetic and consultative

Creating Developer Champion

- Spend time in scrum and sprint meetings
- Develop a basic understanding of coding
- Learn how developers are using open source components
- Gain a firm grasp on development processes



OPERATE

BOLDLY

What Makes Good Software Security Hygiene

95%

Fix rate of high severity vulnerabilities compared to all vulnerabilities

19%

Improved fix rate with eLearning

88%

Improved fix rate with remediation coaching

48%

Improved fix rate with frequent scanning (Sandbox)

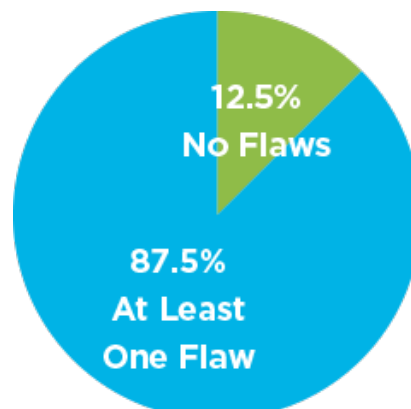
AT LEAST ONE FLAW IN A COMPONENT, BY LANGUAGE

75%

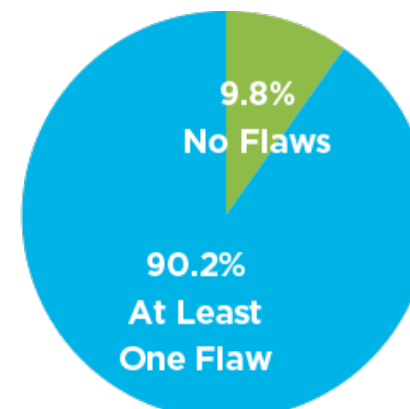
More than application is
made of components

28%

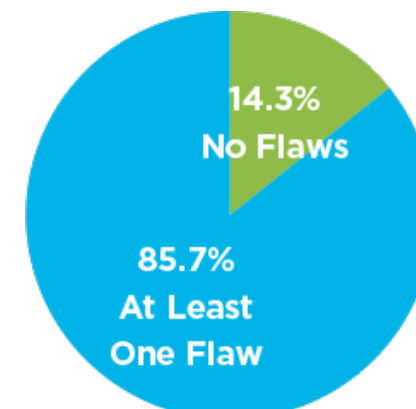
Conduct software
composition analysis



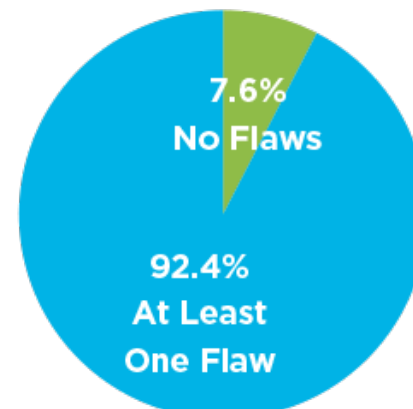
Java



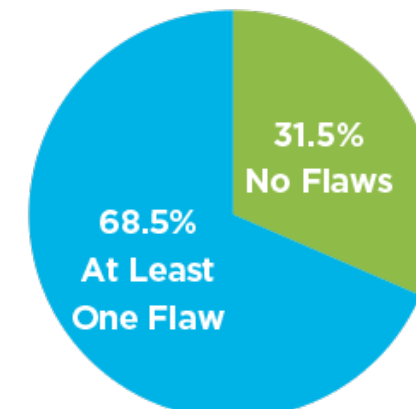
PHP



.Net



C++



JavaScript

Source: Veracode State of Software Security V9

COMPETE

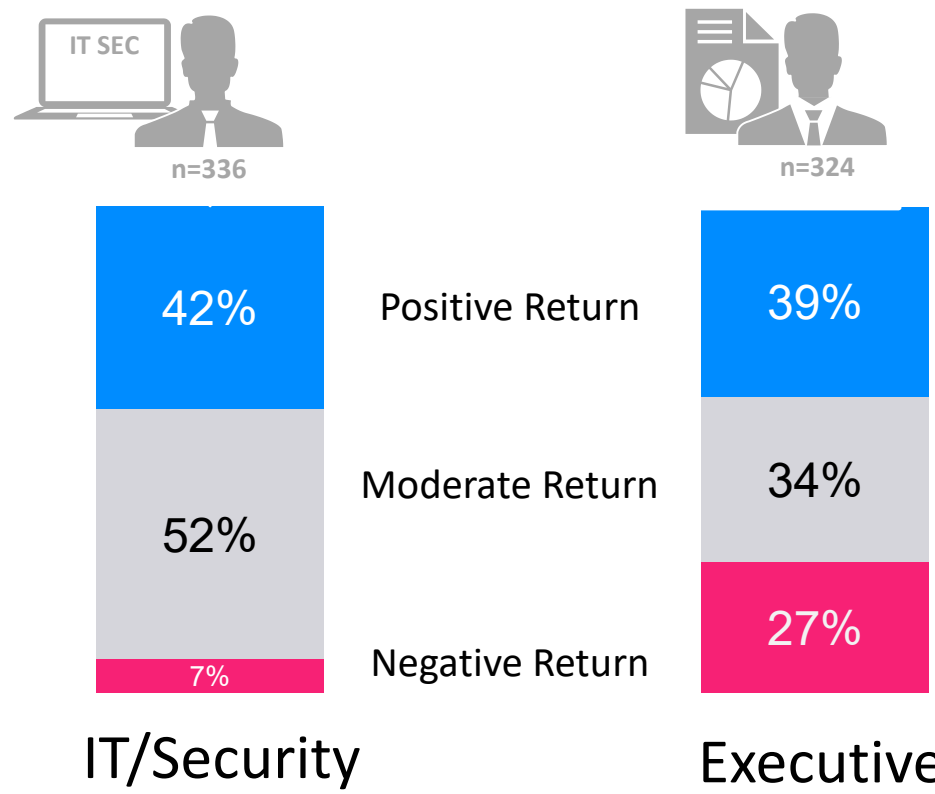
BOLDLY

Global top ten risks for doing business

- | | |
|----|---|
| 1 | Unemployment or underemployment |
| 2 | Failure of national governance |
| 3 | Energy price shock |
| 4 | Fiscal crises |
| 5 | Cyber-attacks |
| 6 | Profound social instability |
| 7 | Failure of financial mechanism or institution |
| 8 | Failure of critical infrastructure |
| 9 | Failure of regional and global governance |
| 10 | Terrorist attacks |

Business Execs more likely to think security has a negative ROI

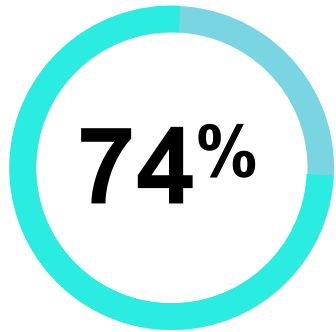
How Organizations Perceive Security Initiatives



Astonishingly, 76% of business executives who view security initiatives as having a negative ROI have also previously been involved in a publicly disclosed data breach.

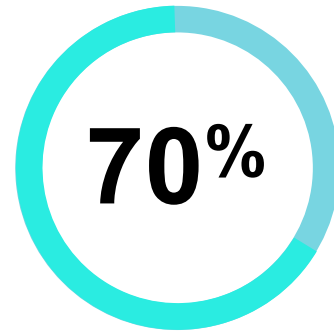
Base: All Business Respondents (n=1650)
Q22. When it comes to security of consumer data, do you perceive security initiatives as a...?

Customers are Concerned About Your Software Security



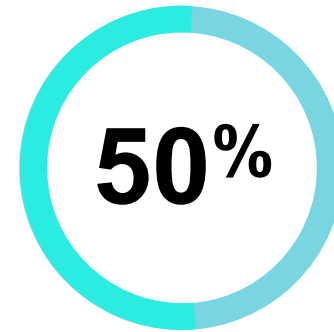
Concerned about sharing data with businesses

IPOS-MORI Study



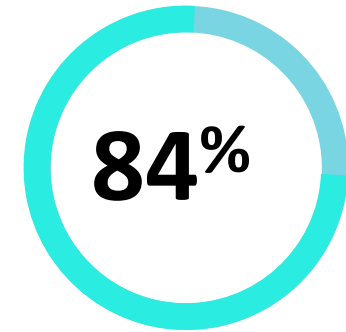
Have taken steps to reduce exposure online

IPOS-MORI Study



Have dropped a service after a publicized breach*

CA Digital Trust Survey

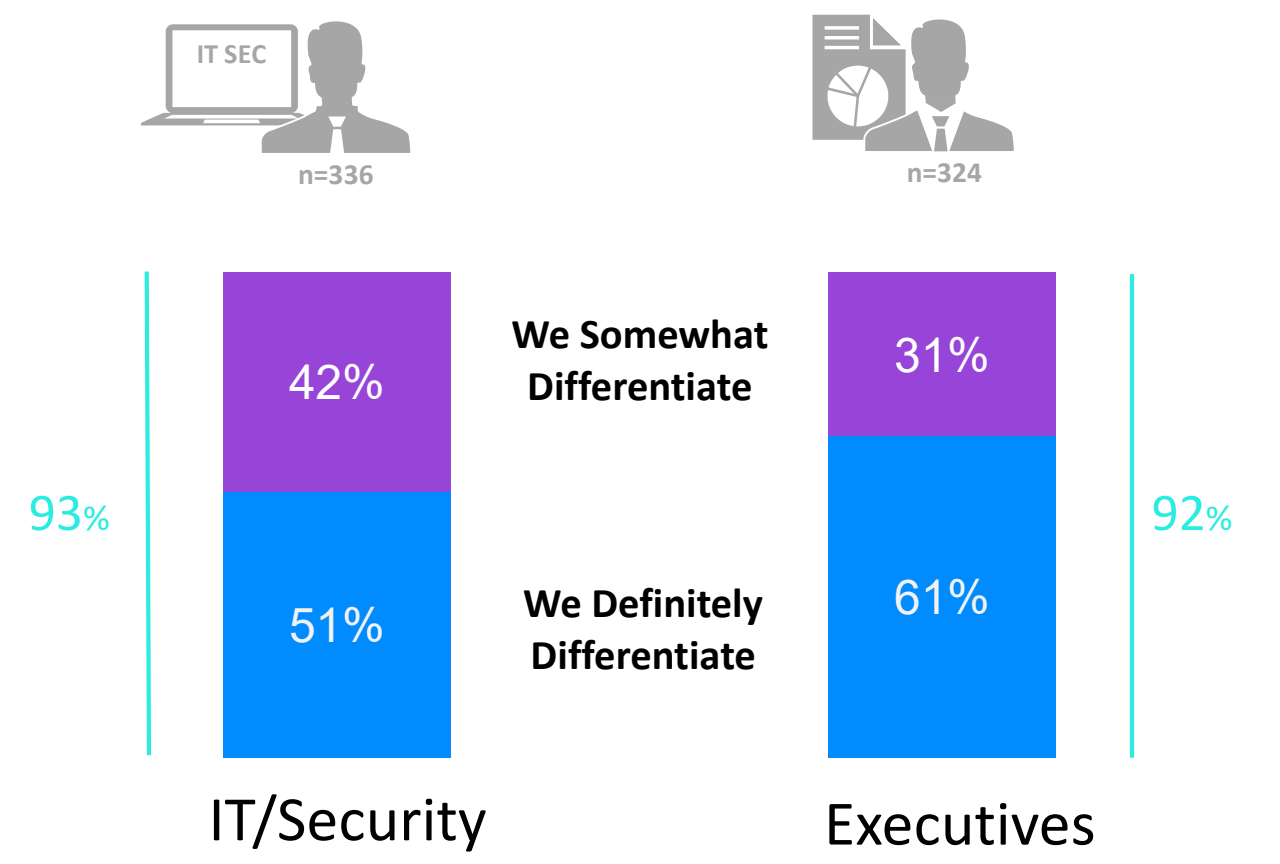


Organizations include security requirements into contracts

IDG Survey Report on Security as a Competitive Advantage

Nearly All Organizations Claim They Provide Better Data Privacy Than Their Competitors

Declared
Differentiation From
Competitors
By Claiming to
Provide Better
Consumer Data
Privacy



Base: All Business Respondents (n=660).
Q34. Does your organization differentiate itself from competitors by claiming to provide better consumer data privacy?

Verify your Security Processes

VERACODE
VERIFIED

STANDARD

VERACODE
VERIFIED

TEAM

VERACODE
VERIFIED

CONTINUOUS





VERACODE

You change the world, we'll secure it.

LEARN MORE AT **BOOTH N 6161**