Veracode Secure Development Survey

DEVELOPERS RESPOND TO APPLICATION SECURITY TRENDS

VERACODE

EXECUTIVE SUMMARY

Development teams face an onslaught of challenges from every direction as software development cycles accelerate and the responsibility for meeting operational requirements "shifts left" to developers. Add to this the growing importance of application security (AppSec) and an increased pressure on organizations to comply with regulations and reduce business risk from the ever-present threat of cyberattacks. Alongside these pressures, the DevOps model is disrupting software development and impacting development teams in ways both technical and cultural.

As developers and development managers, you're seeing this paradigm shift in real time. Your perspectives on the changing landscape are unique from IT operations and security teams, even as you share the goal of quickly deploying software that is both stable and secure. Yet you are the linchpin of any strategy to secure the applications that drive business innovation and revolutionary changes in technology.

That's why Veracode commissioned this survey of developers and development managers in the United States, United Kingdom and Germany. We're putting our finger on the pulse of development teams around the world, across industries and in organizations large and small. How are you responding to the changing methodologies of software development? And what does it mean for application security today and into the future?

The results of the Veracode Secure Development Survey show that most organizations haven't yet reached the gold standard of secure DevOps, although some have begun this journey, and the way forward is clear. Let's take a closer look at what developers and development managers are saying about the challenges many of you face every day and the current state of secure software development.

HERE ARE SOME HIGHLIGHTS FROM THE SURVEY:

36.8% of developers rank protecting applications from cyberattacks and data breaches as their top concern.

52% of developers say application security testing delays development and threatens deadlines.

24% of developers say their development team has no authority over application security.

Developers and Development Managers **Operate in a Pressure Cooker**

Security has become a non-functional requirement for development teams. Yet a majority of respondents to our survey say security testing slows development and threatens deadlines. In this pressure-cooker environment, something has to give.

Developers and development managers in the United States and Europe, and at every size company in every industry we surveyed, cite delays caused by application security testing as a challenge for development. Overall, 52.2 percent of developers say this challenge puts pressure on you. Managers in our survey are feeling the impact even more acutely — 66 percent of you in the U.S. say application security delaying production schedules is a challenge.

But not all developers see these challenges in the same way, with some differences across industries and regions. Developers within large enterprises (5,000 employees or more) cite legacy application security processes as a concern more than any other challenge, about 4 percent more than those citing application security testing (50 percent versus 45.9 percent). Development managers within large enterprises tend to agree with developers in organizations of that size, with more saying legacy application security processes are a challenge (54.1 percent) than delays caused by application security testing (43.2 percent). A majority of developers at manufacturing companies also cite legacy application security processes more than any other challenge (56.1 percent).

Interestingly, developers and development managers in the U.K. and Germany are less likely than their peers in the U.S. to cite any of these challenges as pressures.

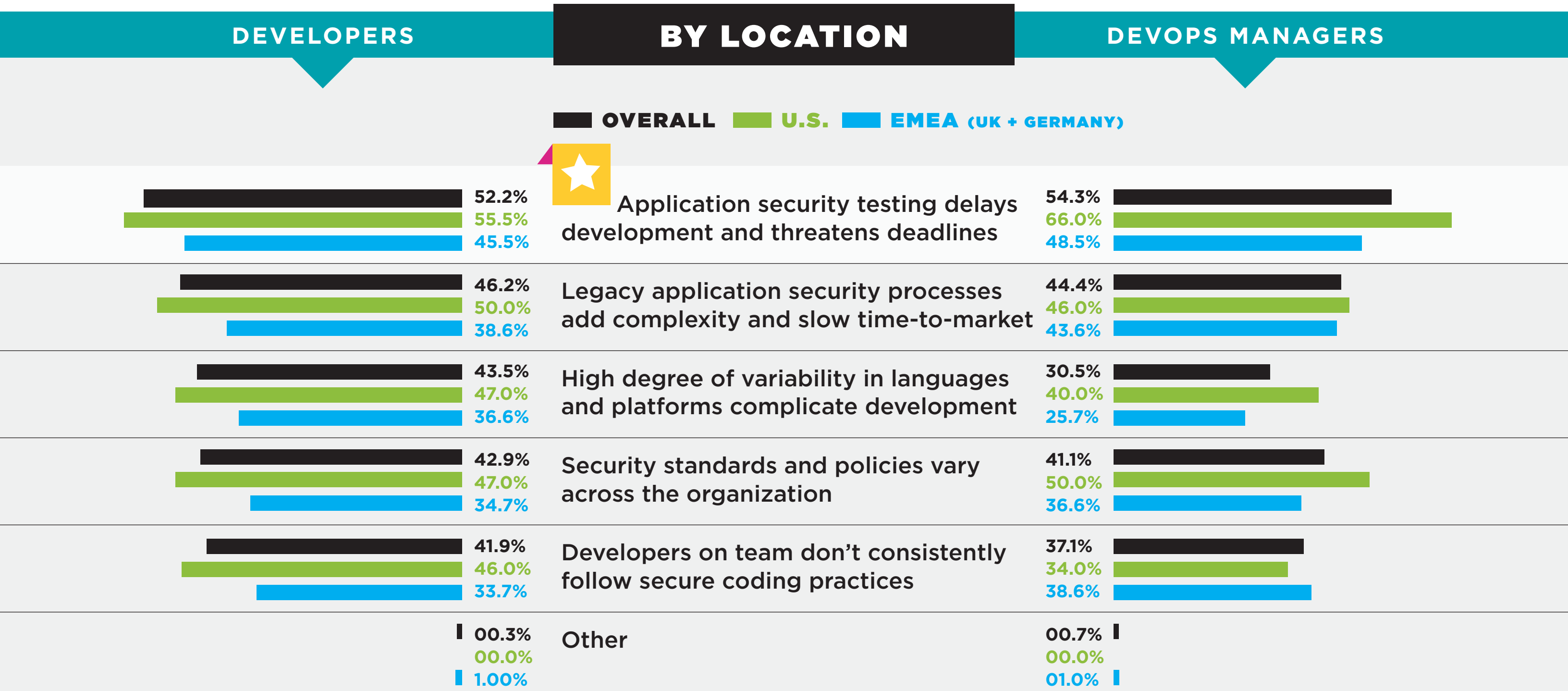
52%

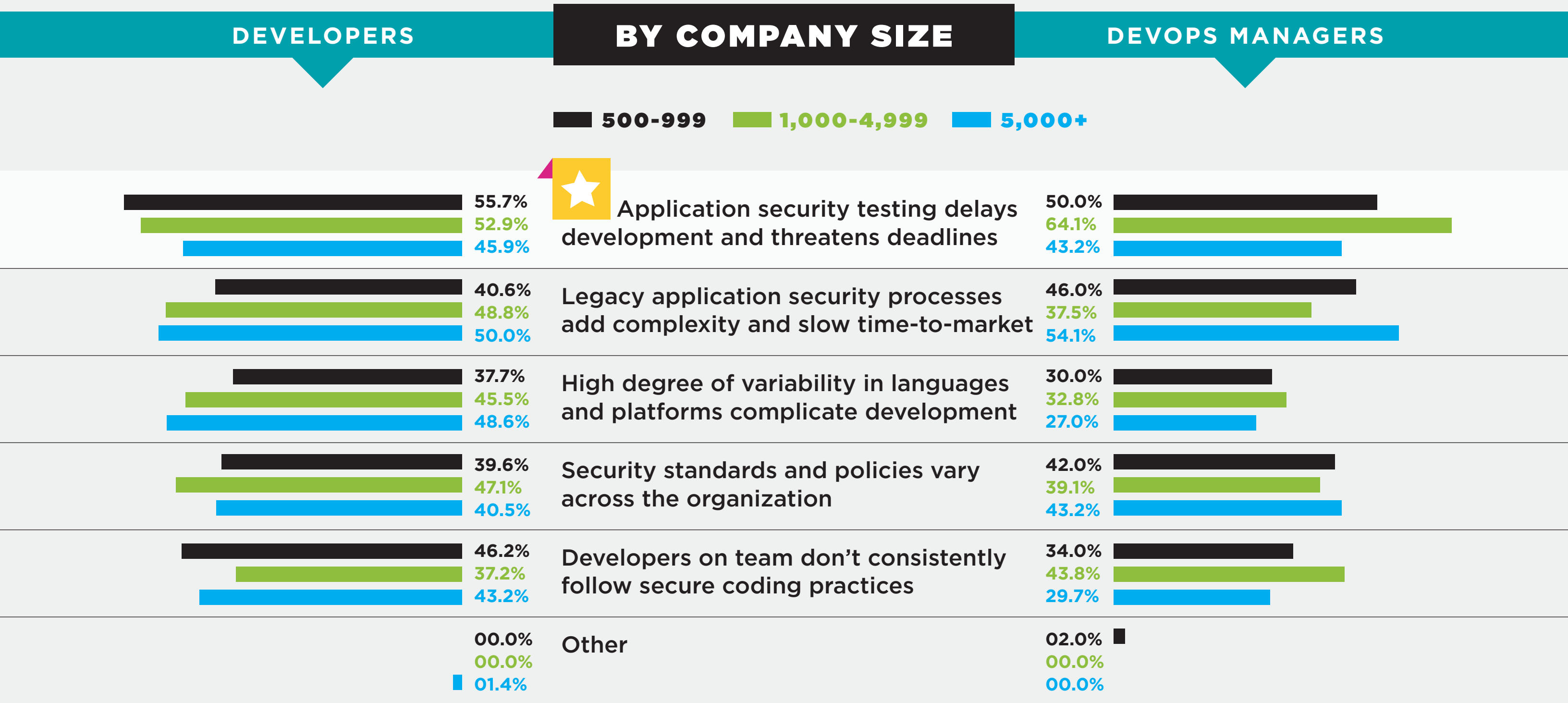
of developers say application security testing causes delays.

According to the Veracode-sponsored survey "Trends and Tactics: How IT Professionals Are Approaching AppSec Today," application security professionals have a slightly different view of development challenges than development managers. Overall, 43 percent of application security professionals say they see variability in languages and platforms as a challenge, versus just 30.5 percent of development managers. However, about 43.5 percent of developers cited languages and platform variability as a challenge, in line with AppSec professionals but out of sync with development managers.

WHAT KINDS OF PRESSURES/CHALLENGES DO YOU FEEL DURING THE DEVELOPMENT PROCESS?

(CHECK ALL THAT APPLY.)





The Number One Challenge: **Stopping Cyberattacks and Breaches**

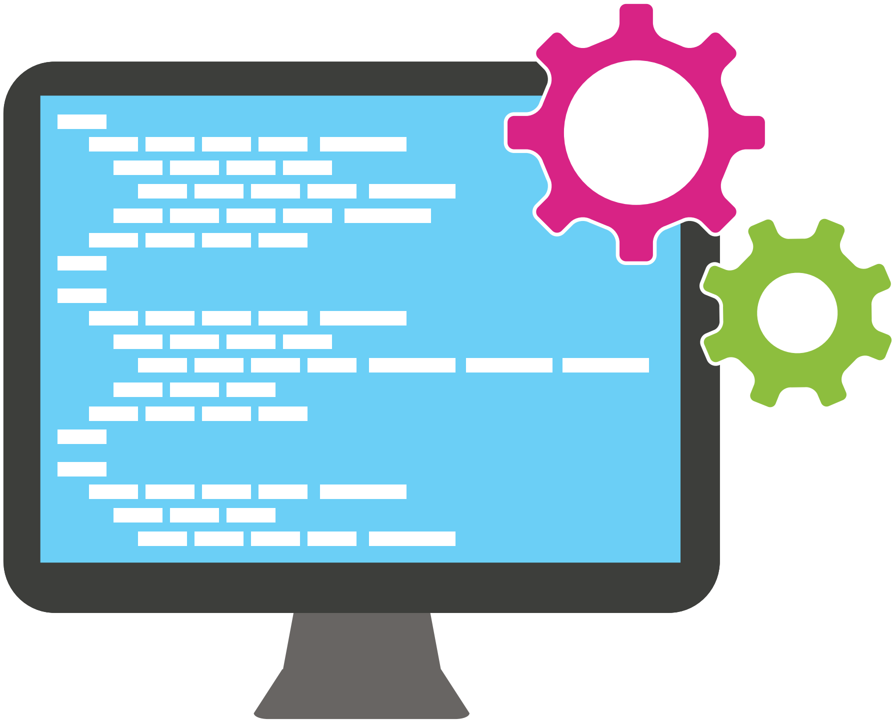
Developers and development managers know just how mission-critical application security is. When asked to choose their top concern out of four major challenges, more developers and development managers in this survey rated "protecting applications and data from cyberattacks and data breaches" as number one, by a wide margin over any other challenge.

However, development managers and developers in Germany and the U.K. diverge somewhat from their peers in the U.S. In Germany and the U.K., 40.5 percent of developers say stopping cyberattacks and breaches is their top concern, versus 37.6 percent of development managers. Meanwhile, in the U.S., the opposite is true: More development managers (42 percent) than developers (34.8 percent) say stopping cyberattacks and breaches is their top concern. In Germany and the U.K., 25.7 percent of development managers say meeting budget and delivery schedules is their top concern, compared to just 18 percent of development managers in the U.S.

Overall, the only industry where developers ranked another concern higher than stopping cyberattacks and breaches is healthcare, where meeting customer and/or regulatory compliance is an even greater concern (34.2 percent vs 28.9 percent).

36.8%

of developers say the number one concern is protecting applications from cyberattacks and data breaches.



WHAT IS YOUR NUMBER ONE SOFTWARE DEVELOPMENT CHALLENGE/CONCERN?

DEVELOPERS

BY LOCATION

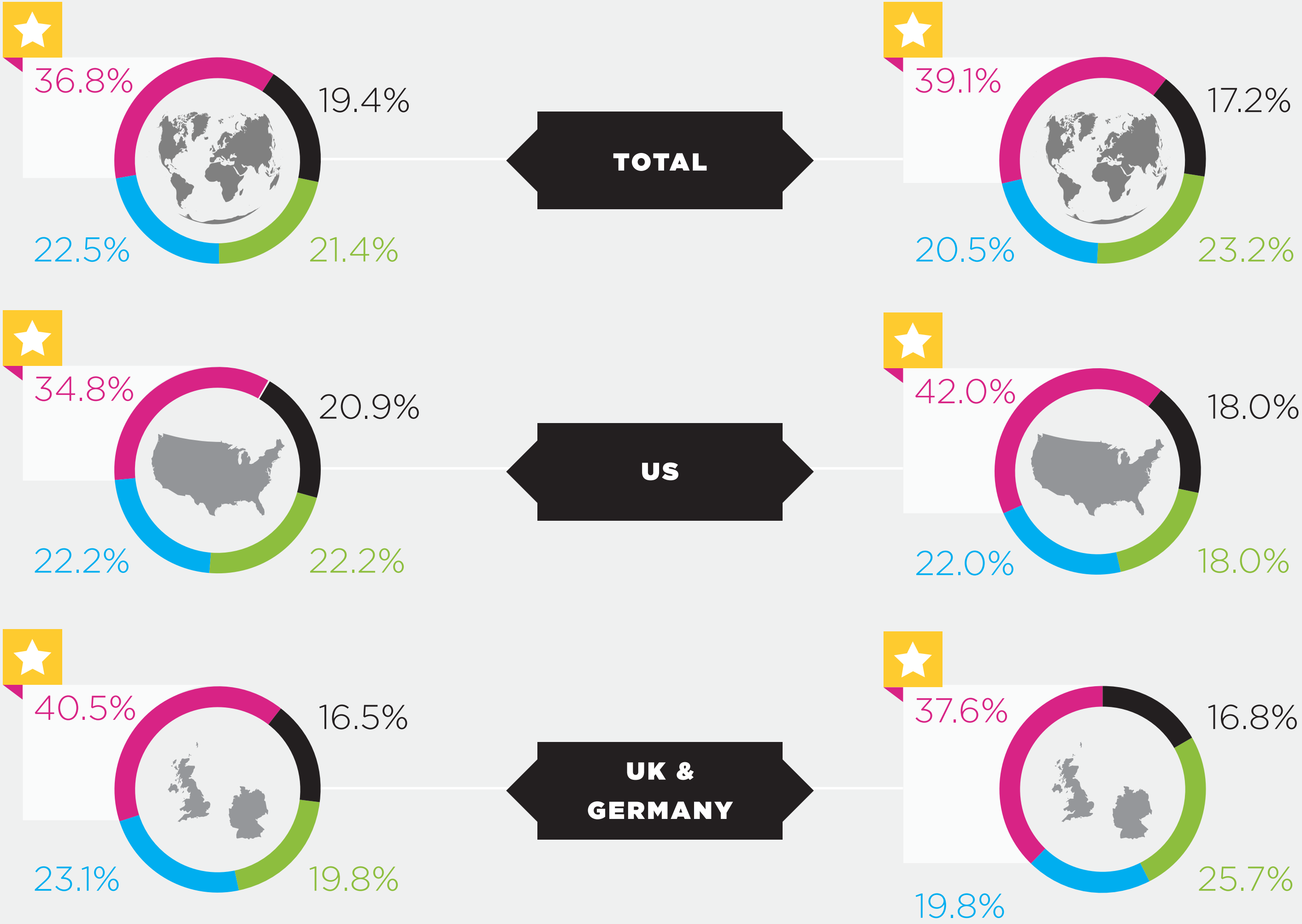
DEVOPS MANAGERS

■ DELIVERING SECURE CODE TO PASS INTERNAL AUDITS

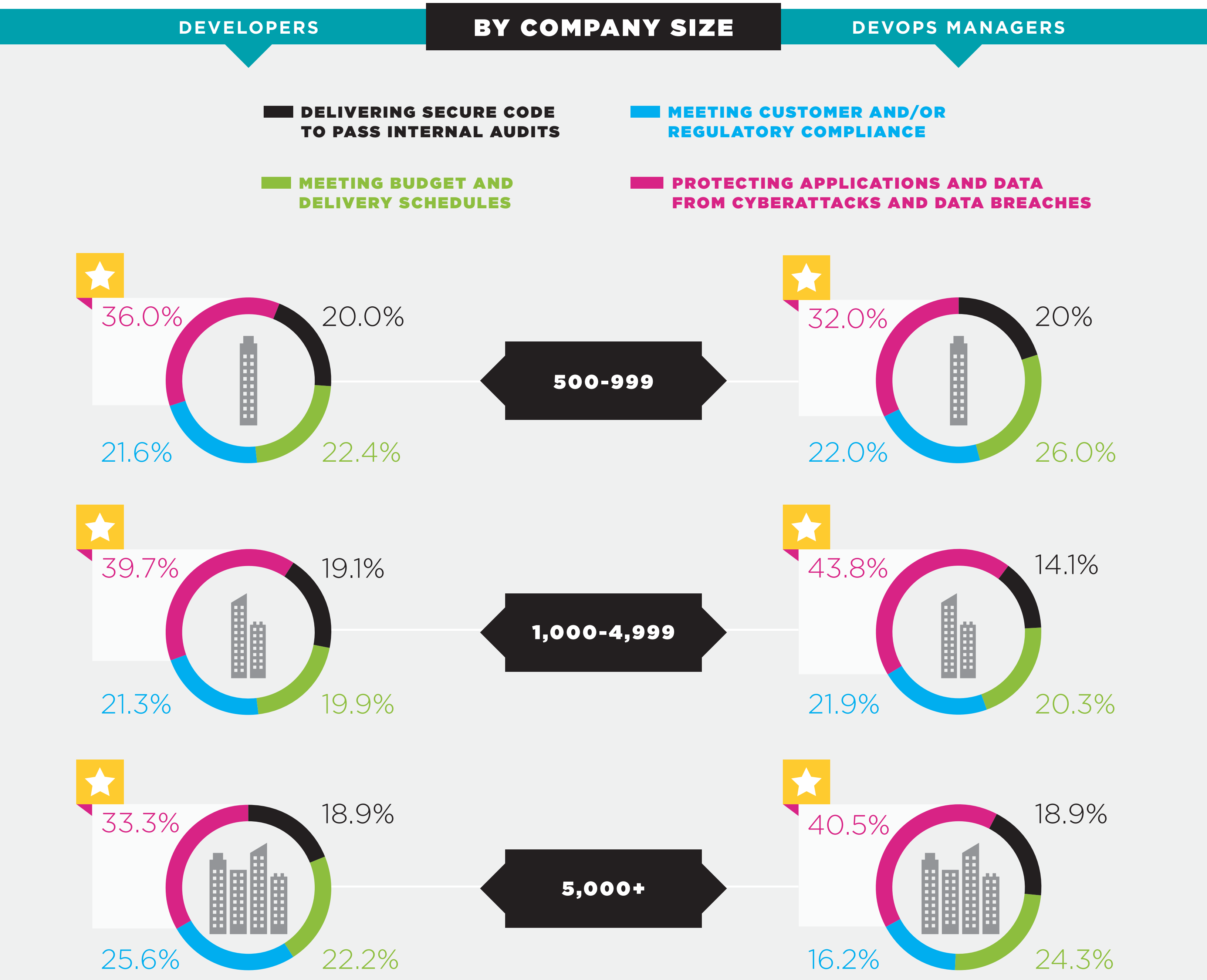
🟦 MEETING CUSTOMER AND/OR REGULATORY COMPLIANCE

🟩 MEETING BUDGET AND DELIVERY SCHEDULES

🟥 PROTECTING APPLICATIONS AND DATA FROM CYBERATTACKS AND DATA BREACHES



WHAT IS YOUR NUMBER ONE SOFTWARE DEVELOPMENT CHALLENGE/CONCERN?



Which Vulnerabilities **Scare You the Most?**

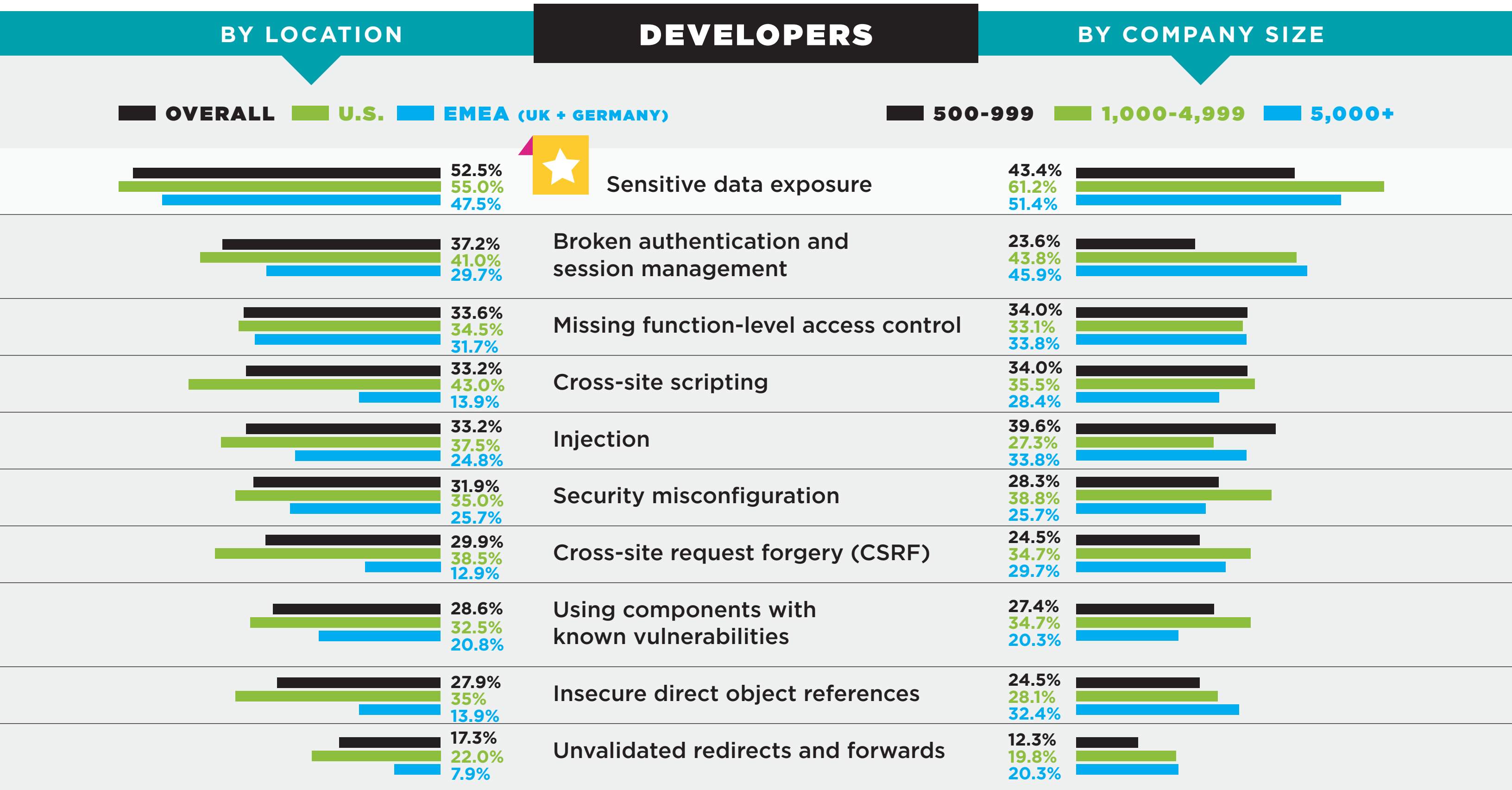
Which vulnerabilities concern developers the most? Sensitive data exposure is far and away the leader — 52.5 percent of you say this is a concern. An OWASP Top 10 vulnerability, sensitive data exposure is a broad category describing vulnerabilities that allow valuable data to be stolen or accidentally leaked from applications. Improperly implemented encryption or lack of encryption are the primary causes of sensitive data exposure. Sensitive data includes credentials and personally identifiable information (PII) that many organizations are legally required to protect, such as health data.

A distant second is broken authentication and session management, named by 37.2 percent of developers as a top concern. Missing function-level access control, Cross-Site Scripting and injection were all cited as top concerns by around 33 percent of developers.

52.5%

of all developers are worried about sensitive data exposure — the most frequently cited vulnerability.

WHICH TYPES OF VULNERABILITIES ARE YOU MOST CONCERNED ABOUT? (CHECK ALL THAT APPLY.)

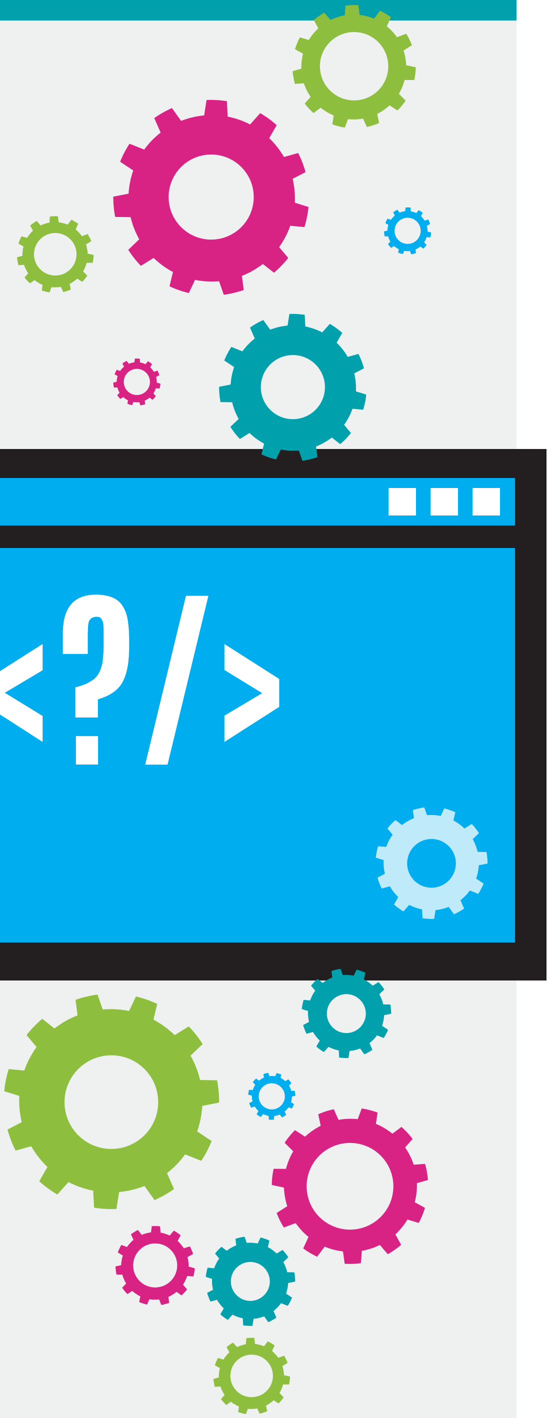


OPEN-SOURCE COMPONENTS:
Are Developers Underestimating the Risk?

Do developers' concerns about particular vulnerabilities match up with the risk? According to Veracode analysis in the State of Software Security 2016, 65 percent of applications have cryptographic issues and 41 percent have credentials management vulnerabilities, showing that developers' concerns about sensitive data exposure are well-placed.

However, fewer than one-third of developers (28.5 percent) cite using components with known vulnerabilities as a major concern, despite the high prevalence of vulnerabilities in open-source components. For example, Veracode analysis found that 97 percent of Java applications had at least one component with a known vulnerability.

As attackers increasingly target the application layer, risk from third-party and open-source components is growing, precisely because their use is so widespread and organizations aren't tracking what versions of components they're using and where. Worse still, failing to upgrade components increases the risk over time, as a vulnerability can quickly move from unknown to widely exploited.



97%

of Java applications had at least one component with a known vulnerability.

Application Security Expands to More Stages of the Development Lifecycle

Software development is undergoing major disruptive changes, as development teams are embracing Agile and, increasingly, DevOps processes. But rather than tacking on security at the end of the process, more organizations are incorporating security earlier in the software development lifecycle. Consistent with this trend, our survey found that a plurality of organizations (39.9 percent) integrate security at the programming stage. A smaller number of organizations are addressing security in the design stage, where potential issues can be identified and fixed where it is least costly to do so.

Large enterprises (25.7 percent) are moving application security into the design stage faster than their smaller counterparts, and the education (28 percent) and healthcare (28.9 percent) industries are slightly ahead here as well. A small percentage of organizations are shifting security even further "left," into the requirements and analysis stages.

But there are still some organizations addressing security late in the lifecycle. Overall, nearly 10 percent of organizations are integrating security in operations and 5.6 percent are doing so in testing. Those figures are higher in the U.K. and Germany, where 7.9 percent of developers say they integrate security in testing and 10.9 percent in operations. Large enterprises are more likely to integrate security into operations (13.5 percent), while 31.1 percent of large enterprises integrate security at the programming stage. By industry, our survey found that financial services (11.4 percent) and manufacturing (15.8 percent) are most likely to incorporate security late in the lifecycle (in operations).

39.9%

of organizations are incorporating security at the programming stage of the software development lifecycle.

Although it's a best practice to address security early in the software development lifecycle, the shift towards continuous delivery and DevOps is providing more opportunities to integrate security throughout the entire lifecycle. DevOps organizations can use a range of methods and technologies for integrating security at multiple stages, from static assessment during programming, to dynamic testing, web application firewalls and runtime application protection in production.

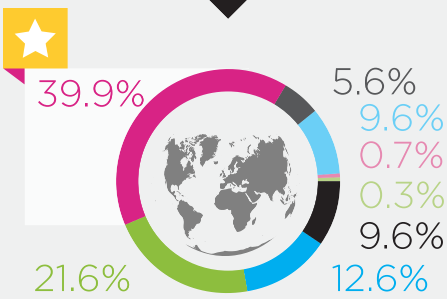
AT WHAT STAGE DO YOU INTEGRATE APPLICATION SECURITY INTO THE SOFTWARE DEVELOPMENT LIFECYCLE?

DEVELOPERS

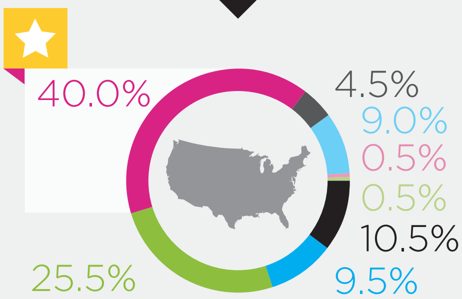
- ■ REQUIREMENTS
- ■ ANALYSIS
- ■ DESIGN
- ■ PROGRAMMING
- ■ TESTING
- ■ OPERATIONS
- ■ OTHER
- ■ WE DON'T FORMALLY INCORPORATE APPLICATION SECURITY INTO THE SDLC

BY LOCATION

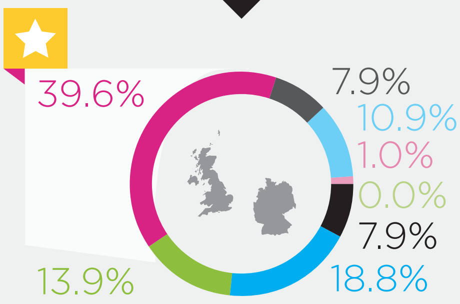
TOTAL



US

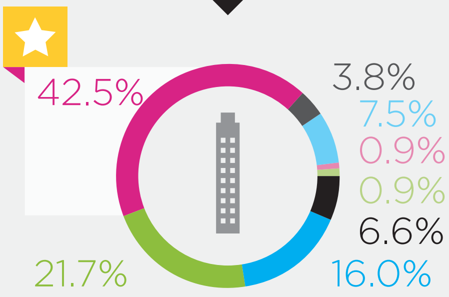


UK & GERMANY

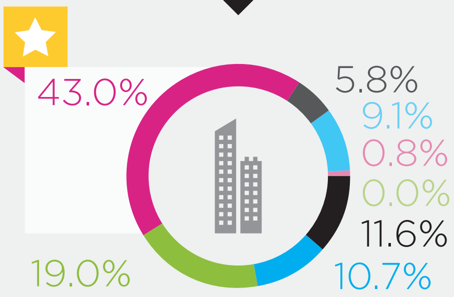


BY COMPANY SIZE

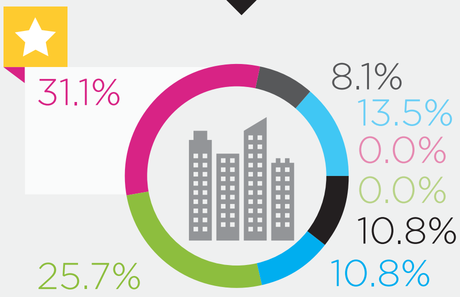
500-999



1,000-4,999



5,000+



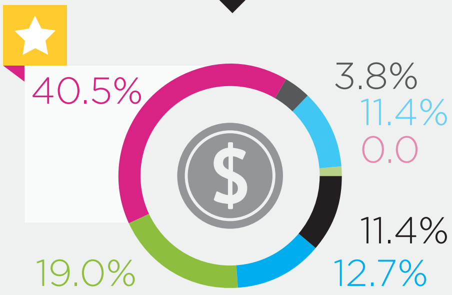
AT WHAT STAGE DO YOU INTEGRATE APPLICATION SECURITY INTO THE SOFTWARE DEVELOPMENT LIFECYCLE?

DEVELOPERS

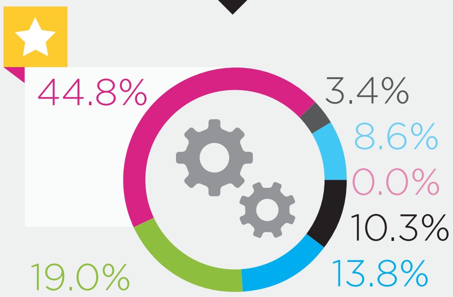
BY INDUSTRY

- ■ REQUIREMENTS
- ■ TESTING
- ■ ANALYSIS
- ■ OPERATIONS
- ■ DESIGN
- ■ PROGRAMMING
- ■ WE DON'T FORMALLY INCORPORATE APPLICATION SECURITY INTO THE SDLC

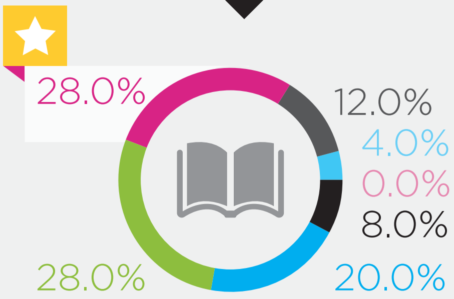
FINANCIAL SERVICES



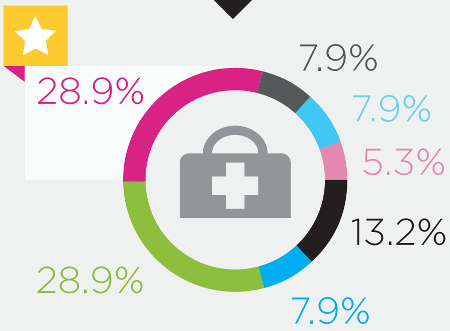
ARCHITECTURE & ENGINEERING



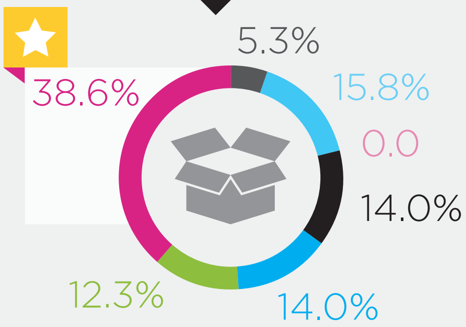
EDUCATION



HEALTHCARE



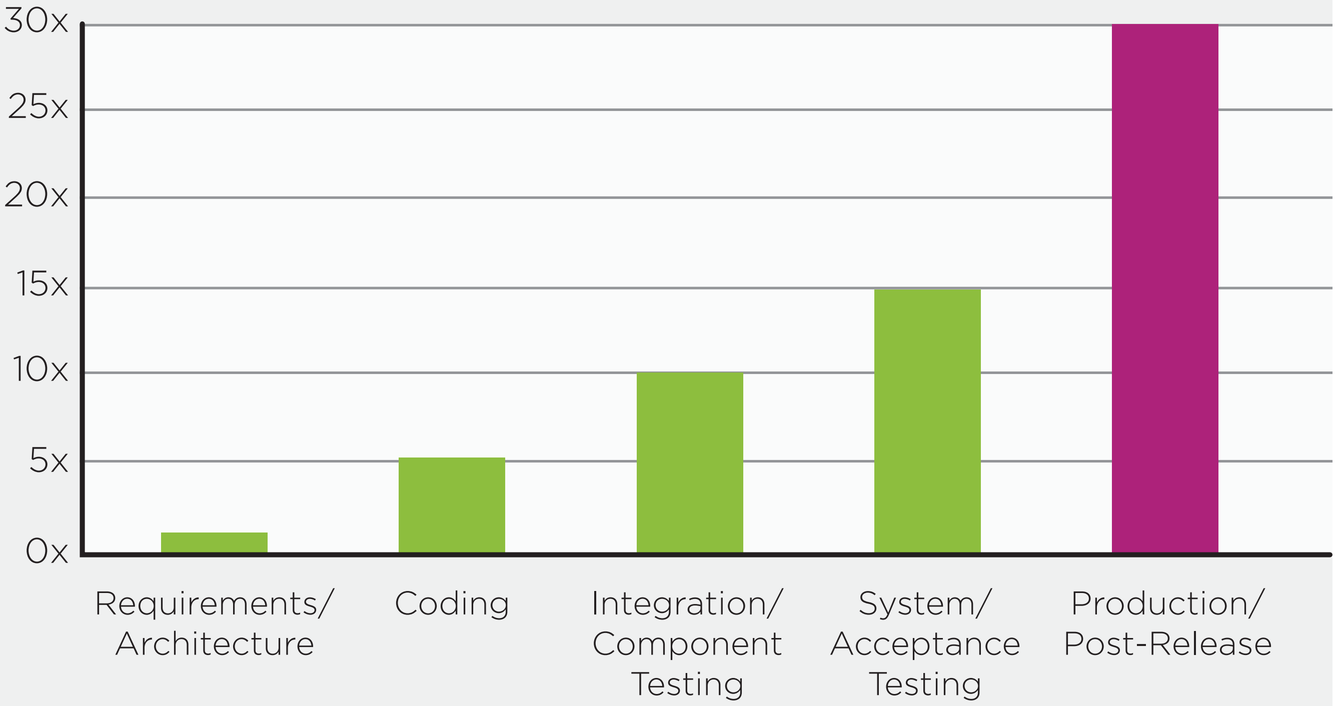
MANUFACTURING



SECURING SOFTWARE
at the End of the Lifecycle Causes Costly Delays

Conventional application security approaches, including manual penetration testing and on-premise tools, can't meet the demand for faster delivery. And they often deliver results too late in the development cycle. Studies from the National Institute of Standards and Technology have shown that fixing flaws in later stages of the development cycle costs significantly more than doing so early in the lifecycle – by orders of magnitude.[1] This might put pressure on development teams to knowingly ship vulnerable applications, or not test applications at all.

RELATIVE COST TO FIX, BASED ON TIME OF DETECTION



Source: National Institute of Standards and Technology

Most Organizations Employ **Web Application Firewalls to Protect Applications**

Although a large share of developers say their organizations are securing applications during development, web application firewalls (WAF) remain the most prevalent form of protection for applications — 55.8 percent of organizations use a WAF. Slightly more organizations in the financial services (60.8 percent) and engineering industries (60.3 percent) use a WAF. The rate of organizations using a WAF jumps to 78.9 percent in the healthcare industry.

Web application firewalls are the most prevalent protection for applications, used by **55.8%** of organizations.

Firewalls can be a vital layer of protection, by inspecting traffic and content, and making decisions to terminate sessions. However, perimeter firewalls can't see how traffic is being processed in applications. In addition, with mobile devices and cloud services proliferating, the perimeter is no longer clearly defined, making perimeter firewalls less effective. Recent successful attacks reveal that a single-solution approach creates an opening for attackers. Most of the large, widely publicized breaches in recent years targeted the application layer.[2] Attackers often don't directly target business-critical applications. Instead, they target overlooked, less-tested or third-party applications.

Securing the application layer requires a multi-tiered approach to protect the entire application landscape, from development to production. DevOps organizations are responding to this need by employing additional methods of security, including as-you-type solutions that help developers repeatedly test for flaws in their code as they write it without setting off alarms for the security or compliance team. And while manual penetration testing is popular (found in 43.9 percent of organizations), AppSec programs that combine static and dynamic testing with other techniques are more effective.

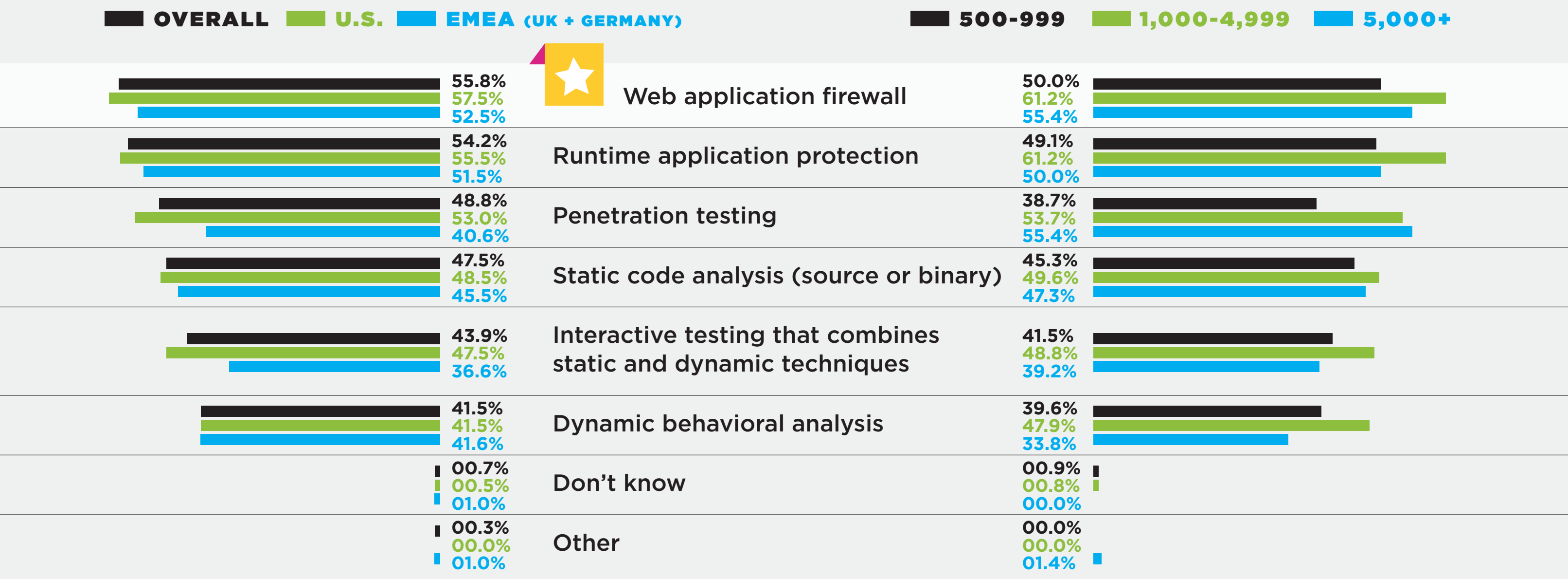
WHAT METHODS ARE YOU CURRENTLY USING TO ENSURE APPLICATION SECURITY?

(CHECK ALL THAT APPLY.)

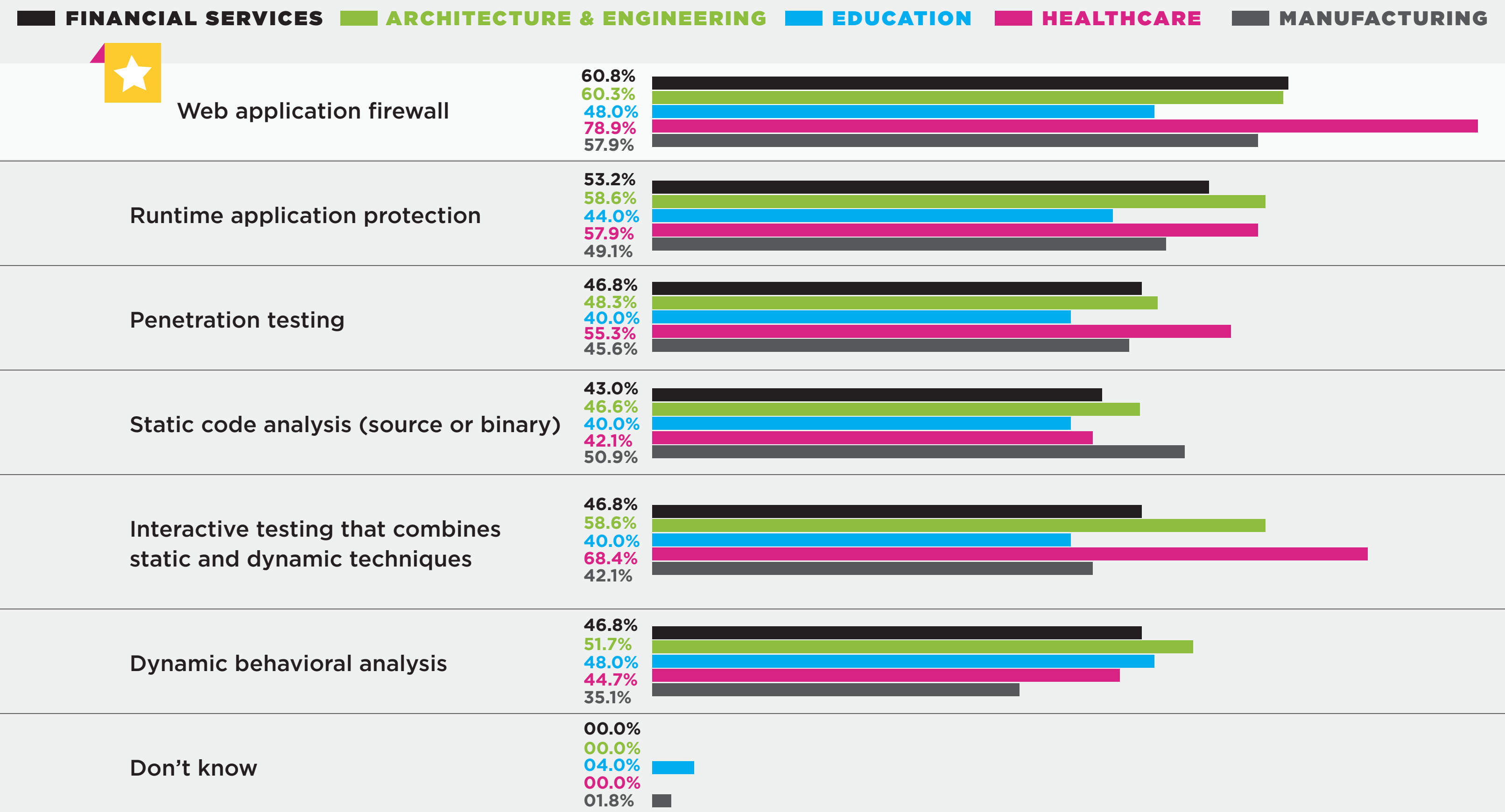
BY LOCATION

DEVELOPERS

BY COMPANY SIZE



BY INDUSTRY



Secure DevOps Is the Future — and the Future Is Here

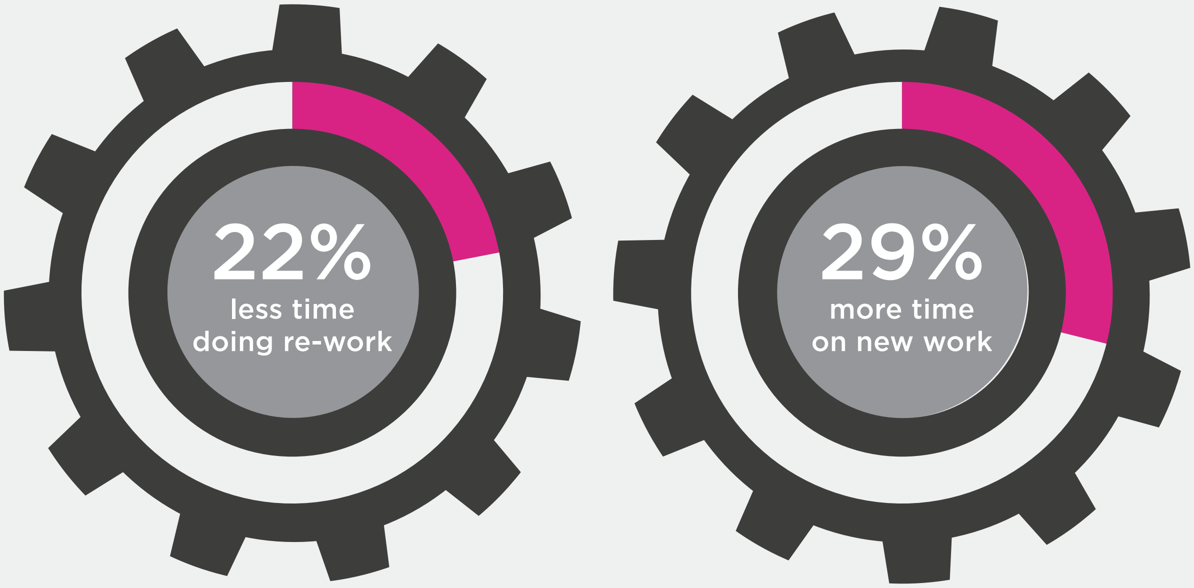
As developers and development managers, your role in application security continues to expand and increase in value. Although nearly a quarter of development teams don't have authority over application security (24.2 percent), nearly the same percentage of development organizations now share responsibility for AppSec with another team (22.2 percent). And in 15.7 percent of organizations, the security team now reports to development. This trend towards shared responsibility between development and security indicates that more organizations are shifting to integrated DevOps teams.

There's a clear benefit to making the move to DevOps. According to a study by Puppet, high-performing IT teams that apply security throughout the software development lifecycle spend 22 percent less time doing re-work and 29 percent more time on new work.[3] The less time you devote to security at the end of the lifecycle, the more time you have for developing features, and for driving innovation and profitability.

Not everyone is making progress at the same rate, however. For example, 36.8 percent of developers in manufacturing say they have no authority over application security. There are regional differences, too. In the U.K. and Germany, for instance, 18.2 percent of developers say the application security team reports to development, while security reports to development in just 14.3 percent of organizations in the U.S.

Even though most of you may not be there yet, you still understand that secure DevOps is the wave of the future. And the future is now in sight.

Teams that apply security throughout the development lifecycle spend:



HOW IS THE SECURITY TESTING PROCESS HANDLED AT YOUR ORGANIZATION?

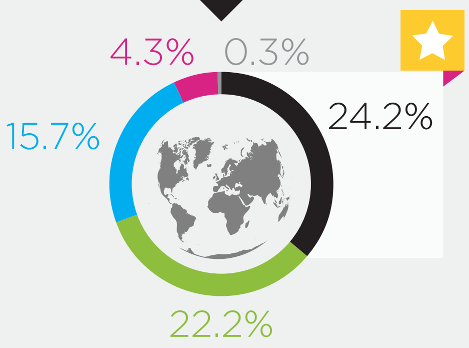
(CHECK ALL THAT APPLY.)

DEVELOPERS

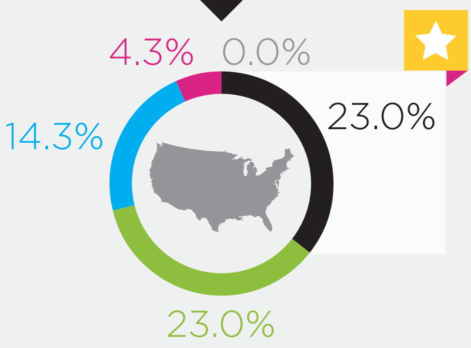
- ⬛ APPLICATION SECURITY IS PART OF A SEPARATE TEAM, AND DEVELOPMENT HAS NO AUTHORITY OVER IT
- 🟩 YOU SHARE RESPONSIBILITY FOR APPLICATION SECURITY WITH ANOTHER TEAM
- 🟦 SECURITY TEAM REPORTS TO DEVELOPMENT
- 🟪 YOU OUTSOURCE APPLICATION SECURITY
- ◼ DON'T KNOW

BY LOCATION

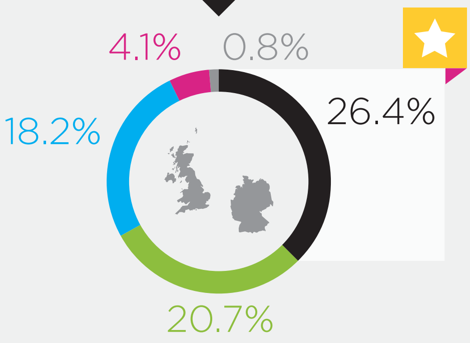
TOTAL



US

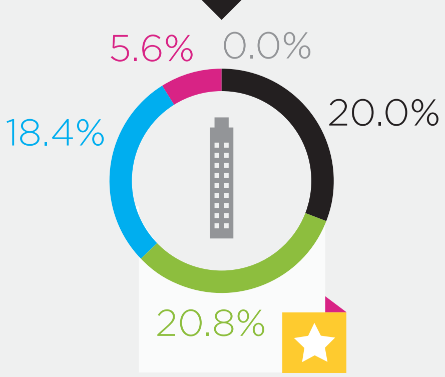


UK & GERMANY

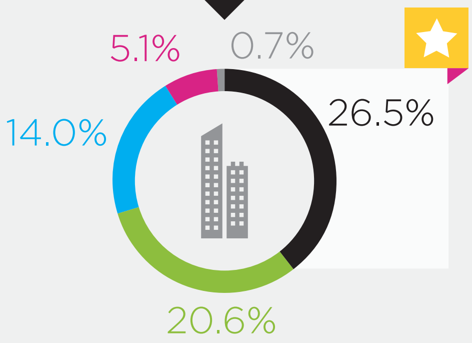


BY COMPANY SIZE

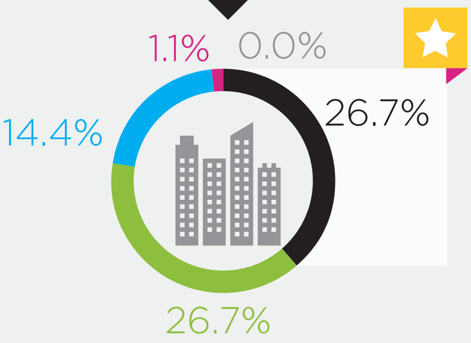
500-999



1,000-4,999



5,000+



HOW IS THE SECURITY TESTING PROCESS HANDLED AT YOUR ORGANIZATION?

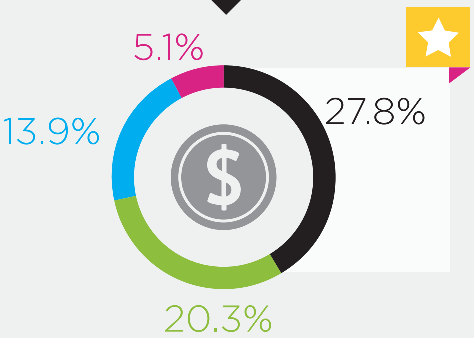
(CHECK ALL THAT APPLY.)

DEVELOPERS

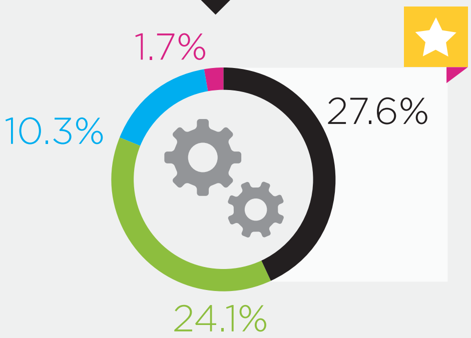
BY INDUSTRY

- ⬛ APPLICATION SECURITY IS PART OF A SEPARATE TEAM, AND DEVELOPMENT HAS NO AUTHORITY OVER IT
- 🟩 YOU SHARE RESPONSIBILITY FOR APPLICATION SECURITY WITH ANOTHER TEAM
- 🟦 SECURITY TEAM REPORTS TO DEVELOPMENT
- 🟥 YOU OUTSOURCE APPLICATION SECURITY

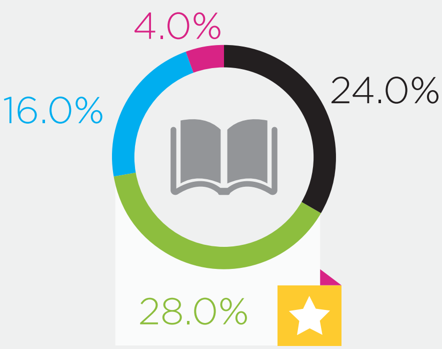
FINANCIAL SERVICES



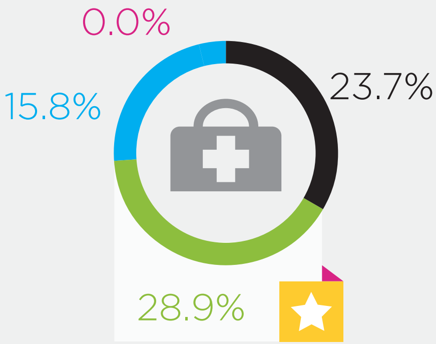
ARCHITECTURE & ENGINEERING



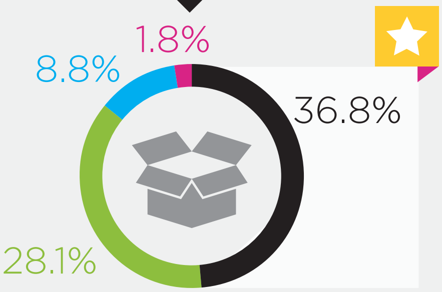
EDUCATION



HEALTHCARE



MANUFACTURING



METHODOLOGY

The survey was conducted on behalf of Veracode in September 2016. An independent research organization surveyed mid-level and senior software developers and development operations managers in a wide range of industries with a particular focus on financial services, architecture and engineering firms, education, healthcare and manufacturing.

A total of 351 developers completed the survey. Of the total, 230 were U.S.-based, 60 were from the U.K. and 61 were from Germany. For development operations managers, 151 people responded with 50 in the U.S., 50 in the U.K., and 51 in Germany.

Respondents were dispersed among mid-sized businesses and large enterprises. Companies were broken down into three categories: 500 to 999 employees, 1,000 to 4,999 employees and more than 5,000 employees.

Sources:

[1] "The Economic Impacts of Inadequate Infrastructure for Software Testing," NIST, 2002.

[2] "To Understand How a Secure Application Layer Can Prevent Disaster, Look No Further Than 2014's High-Profile Cyberattacks," Veracode, August 2015.

[3] "2016 State of DevOps Report," Puppet, March 2016.

ARE YOU READY FOR DEVOPS? DOWNLOAD OUR GUIDE:

FIVE PRINCIPLES FOR SECURING DEVOPS

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.

VERACODE

SECURING THE SOFTWARE THAT POWERS YOUR WORLD.