Provided at no cost to our Sales staff and Clients

CISO INVESTMENT BLUEPRINT FOR 2017

Demystifying the Role of Bug Bounties in Modern Application Security Programs

bugcrowd

We surveyed 100 CISOs and security decision makers across 17 industries and found that today's application security teams are facing resourcing issues that are making them vulnerable.

Why are organizations at a disadvantage?

The cybersecurity job gap is at an all-time high.

Attack surfaces are complex and large as ever.

Traditional application security testing methods just aren't cutting it, leaving organizations vulnerable.

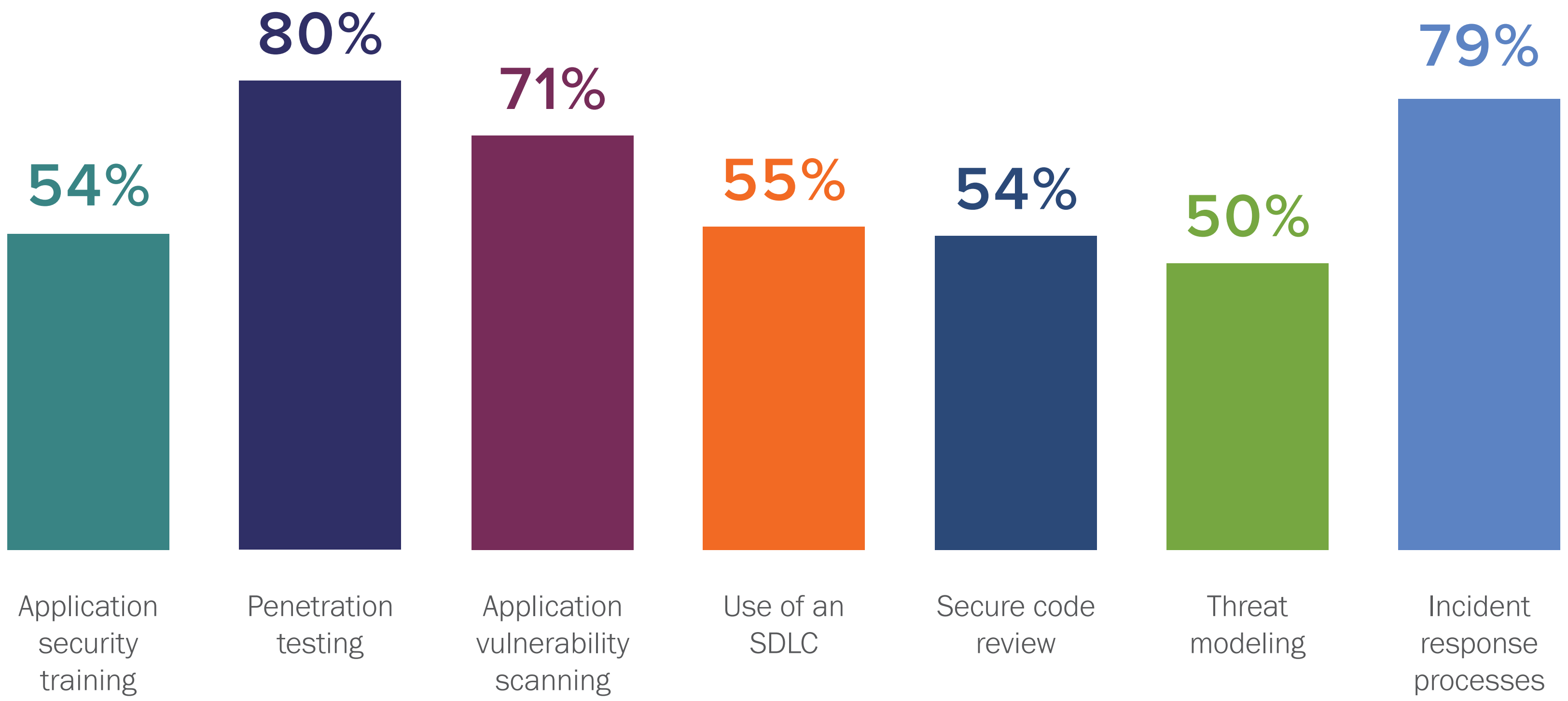
Bug bounty programs, however, are helping CISOs overcome these common application security challenges.

Hacking is the overwhelming leading cause of data breaches, and organizations are not equipped to prevent it.

According to the Identity Theft Resource Center, data breach incidents occurred as a result of hacking were up over 350% from 2007 to 2015.

CISOS UTILIZE **4.8** APPLICATION SECURITY TOOLS AND SERVICES ON AVERAGE.

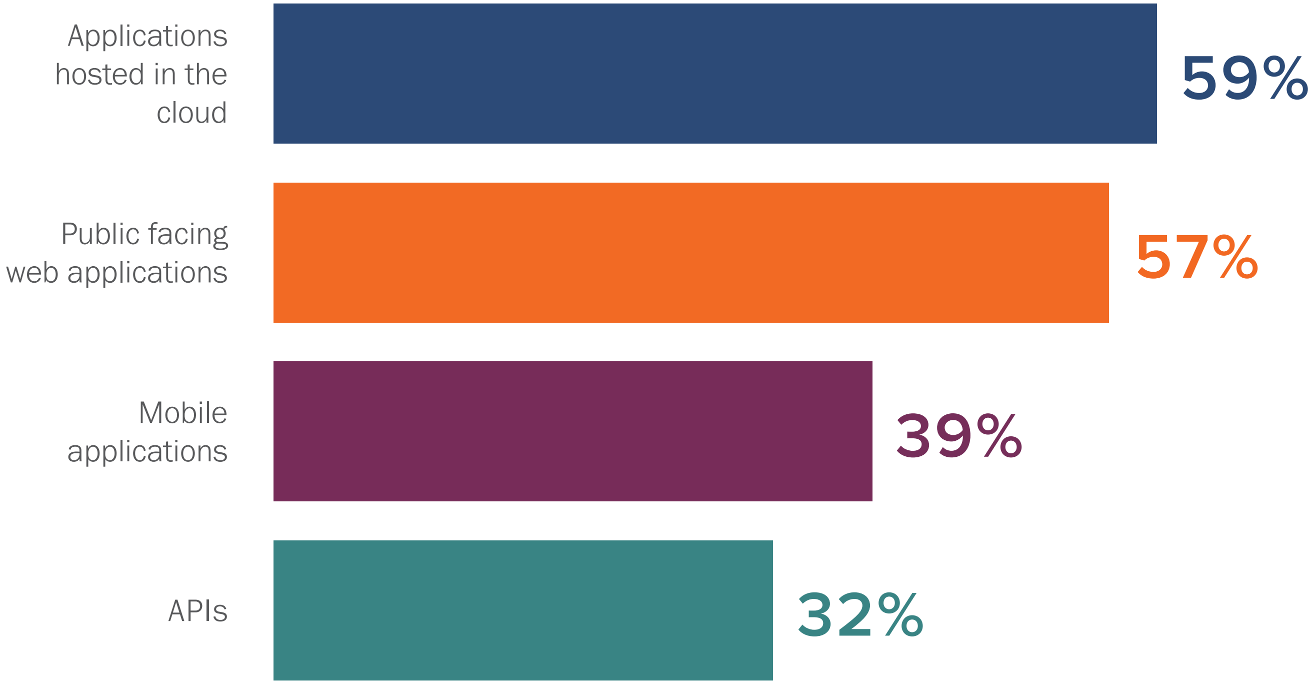
TOP 2017 APPLICATION SECURITY TOOLS AND PRACTICES

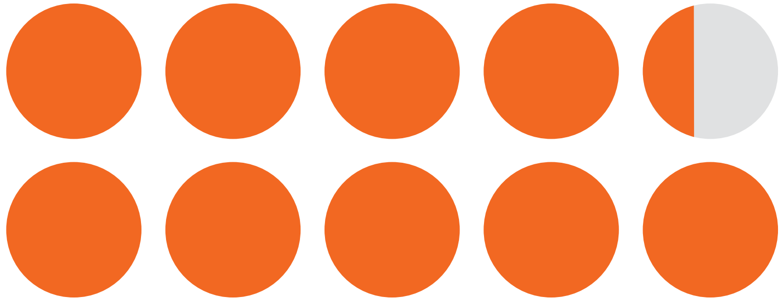


TOP AREAS OF SECURITY INVESTMENT FOR 2017

As more applications become publicly accessible, more breaches have occurred at the application level.

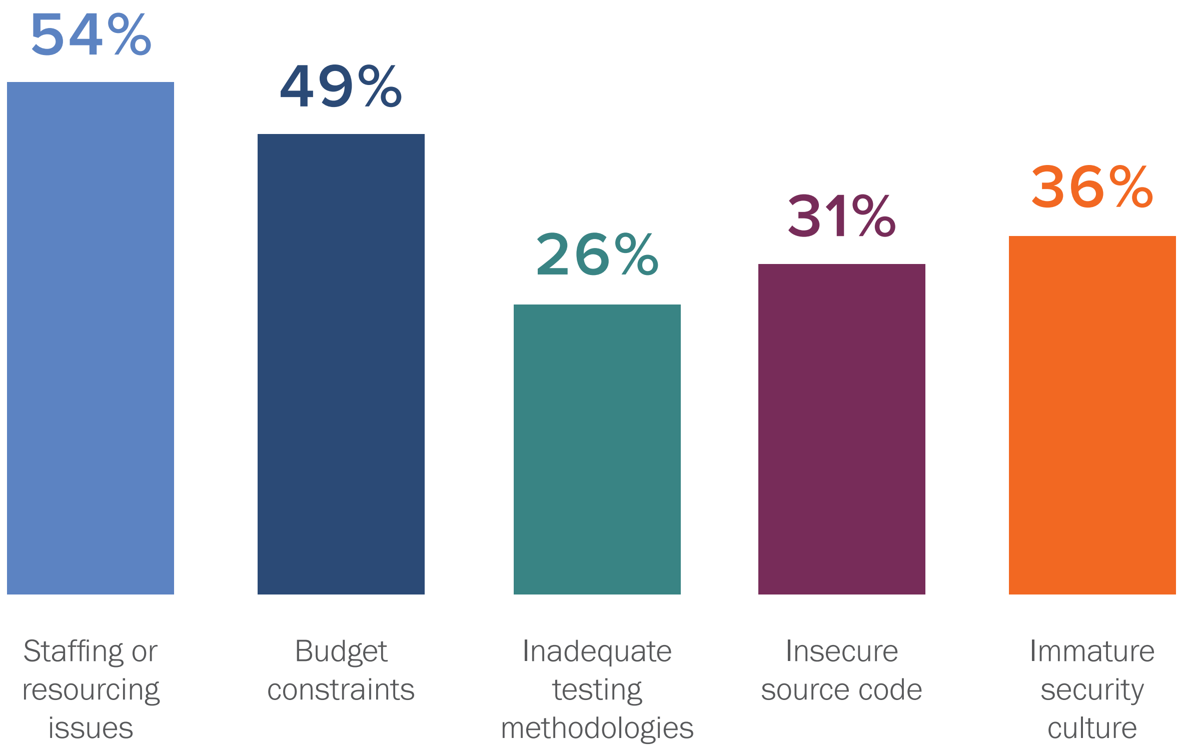
To keep up, IT organizations are continuing to prioritize application security spending. According to a SANS study, 76% of organizations list application security as a top spending priority for skills and technology.





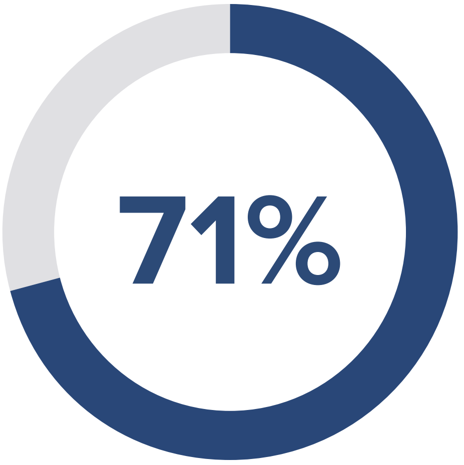
94% OF RESPONDENTS ARE CONCERNED ABOUT PUBLICLY FACING ASSETS OVER THE NEXT 12 MONTHS.

TOP 2017 APPLICATION SECURITY CHALLENGES



In 2017, modern application security teams will continue facing resourcing and budgeting issues while investment areas continue to diversify.

According to the Bureau of Labor Statistics, there are over 209,000 unfilled cybersecurity jobs in the U.S., and postings are up 74% over the past five years. **Our research shows that this will be the top issue over the next year along with budget constraints.**



71% OF RESPONDENTS ARE FACING APPLICATION SECURITY RESOURCING OR BUDGETING ISSUES.

Application security is getting harder. As organizations continue struggling to with keeping up with attackers, they are held back by additional organizational challenges.

In 2016, a record number of organizations have adopted bug bounty programs to overcome those challenges.

Bug bounties meet these application security challenges and secure modern businesses.

ADDRESSING STAFFING AND RESOURCING CHALLENGES

Bug bounty programs leverage volume of testers to improve overall coverage, multiplying the power of your security team and allowing your team to focus on other areas.

WORKING WITHIN APPSEC BUDGETING CONSTRAINTS

Bug bounty solutions have incredible ROI, and our recommendations make it easy and efficient to engage with the crowd through a powerful vulnerability disclosure and management platform, as well as full verification of all submissions.

IMPROVING SECURITY CULTURE THROUGHOUT ORGANIZATION

Through running a managed bug bounty program, our customers have seen improved understanding of secure coding best practices, and better application security accessibility and coverage throughout their organization.

Jon Green,
Aruba Networks

aruba
a Hewlett Packard
Enterprise company

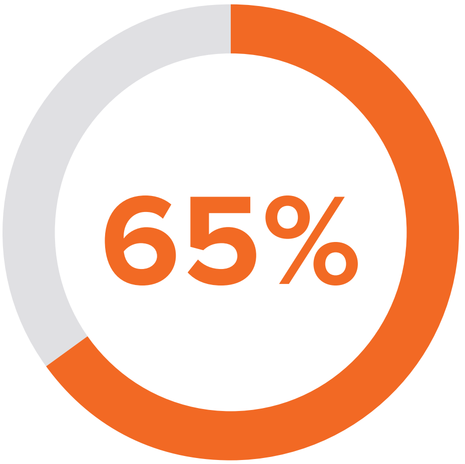
“We decided to run a bug bounty program in order to get access to a wide variety of security testers. Hiring security researchers is very difficult in today’s market, and even if you can find one, chances are good that person will be a specialist in only one or two areas.”

INCREASED BUG BOUNTY ADOPTION IN 2017

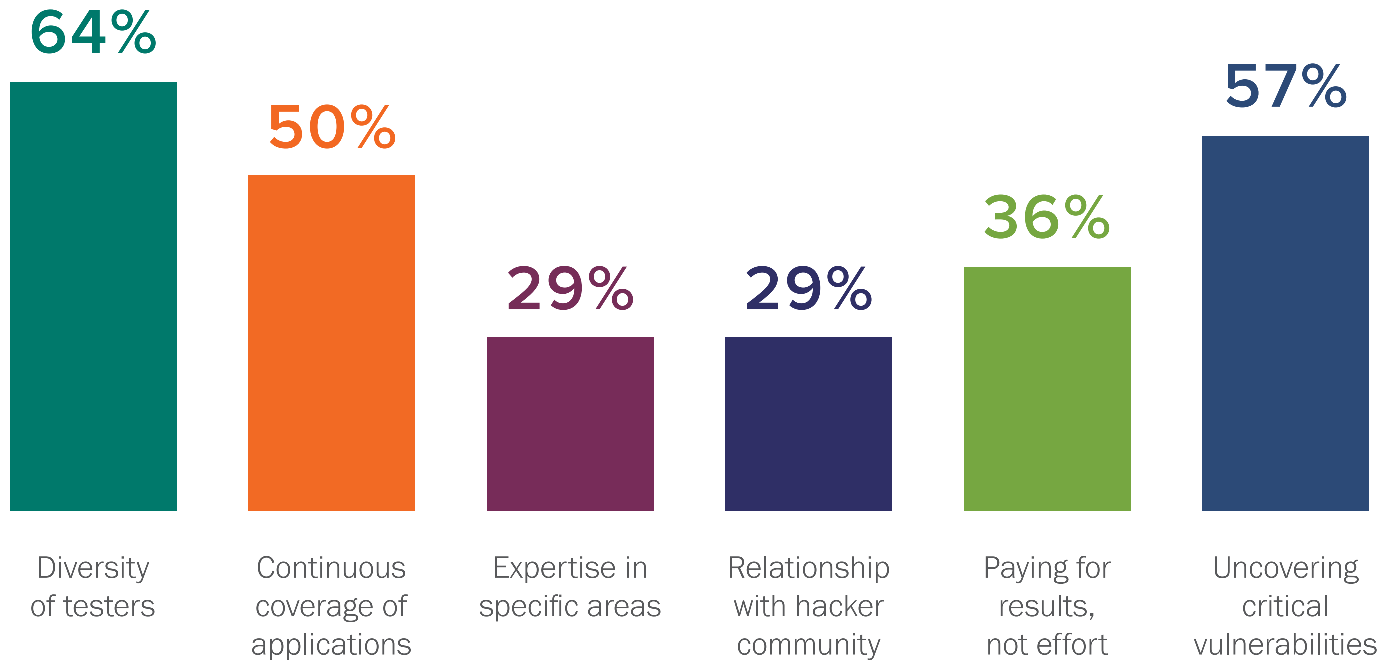
As they have continued to prove successful, bug bounty adoption has increased amongst enterprise organizations in 2016. We expect this trend to continue in 2017 with emphasis on financial services, e-commerce, automotive, and technology organizations.

The results-driven model and competitive nature of bug bounties drive success in the enterprise.

Why is the bug bounty model so valuable?



65% OF RESPONDENTS ARE CURRENTLY RUNNING OR PLANNING TO RUN A BUG BOUNTY PROGRAM.



MOST VALUABLE ASPECTS OF RUNNING A BUG BOUNTY

DIVERSITY OF TESTERS

The bug bounty model is successful in large part because of the diversity in background and experience of testers partaking in bug bounty programs. This diversity breeds the breadth and depth of findings typical for bug bounty programs.

Learn more about our bug hunters >

CONTINUOUS COVERAGE OF APPLICATIONS

For organizations with robust application security programs in place, it is invaluable to have a continuous stream of testing, which is nearly impossible with other testing methods.

Learn more about how bug bounties compare with traditional testing methods >

UNCOVERING CRITICAL VULNERABILITIES

The bug bounty model is fundamentally different from traditional testing methods in that it is results driven. This model drives the discovery of high-quality findings that are often missed by traditional testing methods.

Learn more about bug bounty results >

Richard Rushing,
Motorola

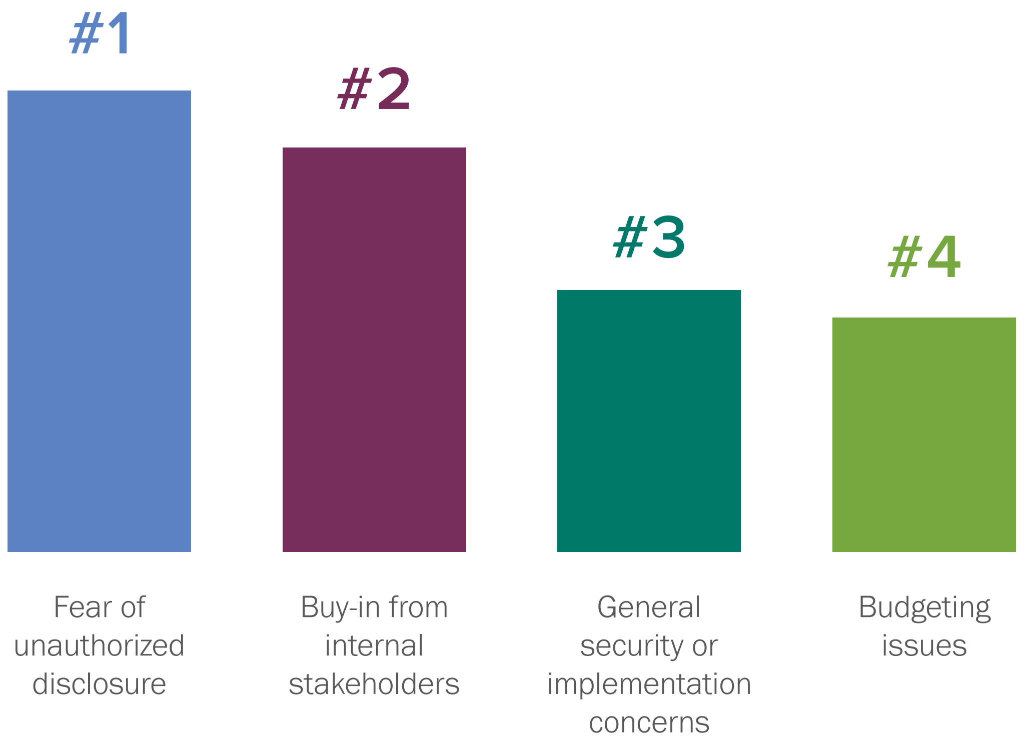
motorola
a lenovo company

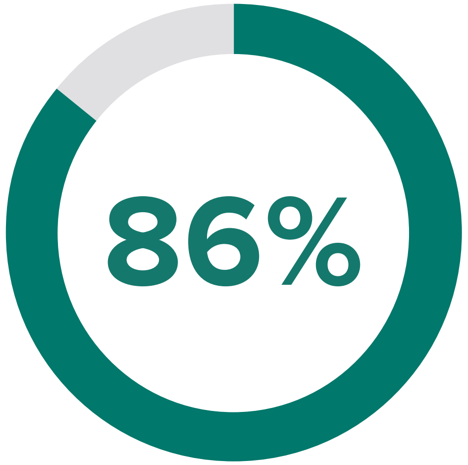
“Bug bounties are a great way to get a full product review versus a single point in time and are much better than website vulnerability scans. Bounty programs also allow me to continue to change my application over time and realize the cost savings versus a pen test for every version.”

PERCEIVED CHALLENGES IN RUNNING A BOUNTY PROGRAM

Although bug bounty adoption is at an all-time high, perceived challenges in implementing them remain.

To increase adoption of bug bounty programs across industries, organizations are overcoming misconceptions and combating real application security constraints. **Bugcrowd helps organizations implement and run successful bug bounty programs, overcoming internal hurdles and resourcing issues.**





86% OF THOSE WHO IMPLEMENTED A BUG BOUNTY PROGRAM HAD TO OVERCOME INTERNAL STAFFING, LEGAL, OR BUDGETING CHALLENGES.

Jim Hebert,
Fitbit

fitbit

> “We think of the bug bounty program as ‘part of this complete breakfast.’ You have all these internal activities, and the Bugcrowd program for us… is a nice supplement to those things, it catches bugs that our internal testing didn’t catch. it also gives us information in what it doesn’t report.”

You aren't alone. Bugcrowd helps CISOs and security decision makers combat modern application security challenges.

These challenges cannot be overcome with traditional security testing methods, nor in a silo. Bug bounty programs, however, have proven to break down many of those barriers.

Why is the bug bounty model so powerful?

MORE EYES

Bug bounties multiply the potential manpower of traditional security assessment methods exponentially, increasing the odds of finding more valid vulnerabilities at any given time.

Having such a large testing pool gets you as close to 24/7 human testing coverage as you can get.

COLLECTIVE CREATIVITY

A large, growing crowd naturally translates to a bigger pool of talent with varying backgrounds, skill sets, and perspectives.

Some researchers have an extensive breadth of skills and expertise, while others have mastery in a few specialized areas. Their creativity contributes to the wide range of vulnerabilities found in bug bounty programs.

BETTER RESULTS

Scanners are extremely limited -they are only able to detect what they have been programmed to recognize. Penetration testers are extremely limited by the knowledge of the few engaged testers and their specific skills.

By nature, crowdsourcing doesn't have those same limitations. More eyes + collective creativity = better results.

BETTER ROI

Bug bounties utilize a pay for results model, ensuring that only valid results are paid rather than effort.

With traditional testing methods, companies typically pay for the effort required to test their applications, regardless of what results are found.

GETTING STARTED

Want to learn more about how your organization can start discovering and fixing high-value vulnerabilities missed by traditional security testing?

Bugcrowd helps organizations leverage the bug bounty model through a full line of bug bounty solutions.

Visit bugcrowd.com/introduction to learn more.