2022

Cybersecurity
INSIDERS

# APPLICATION SECURITY REPORT


beyondsecurity
by HelpSystems

# INTRODUCTION

Business applications are increasingly under attack from advanced threats and malicious actors that are looking to gain access through vulnerable software. Organizations are trying to counter these threats by utilizing various controls for securing applications, such as vulnerability scanning, anti-malware software, penetration testing, and identity and access controls.

To gain deeper insights into the state of application security, Cybersecurity Insiders conducted an in-depth study in partnership with Beyond Security by HelpSystems in June 2022. The resulting report reveals the latest application security trends, how organizations protect critical applications, and what tools and best practices cybersecurity professionals prioritize to find, fix and prevent vulnerabilities in next-gen applications.

**Key findings include:**

- Forty-four percent of organizations have experienced application breaches or compromises in the past, and 20% have been attacked just within the last year.
- The biggest barriers to better defending against cyber threats include the lack of skilled personnel (39%), followed by low security awareness among employees (35%), and lack of budget (35%).
- Application security is gaining importance for most organizations as a majority (51%) project a budget increase over the next 12 months. About a third (34%) believe their application security budgets will remain flat.

We would like to thank Beyond Security, by HelpSystems, for supporting this important research.

We hope you enjoy this report.

Thank you,

Holger Schulze

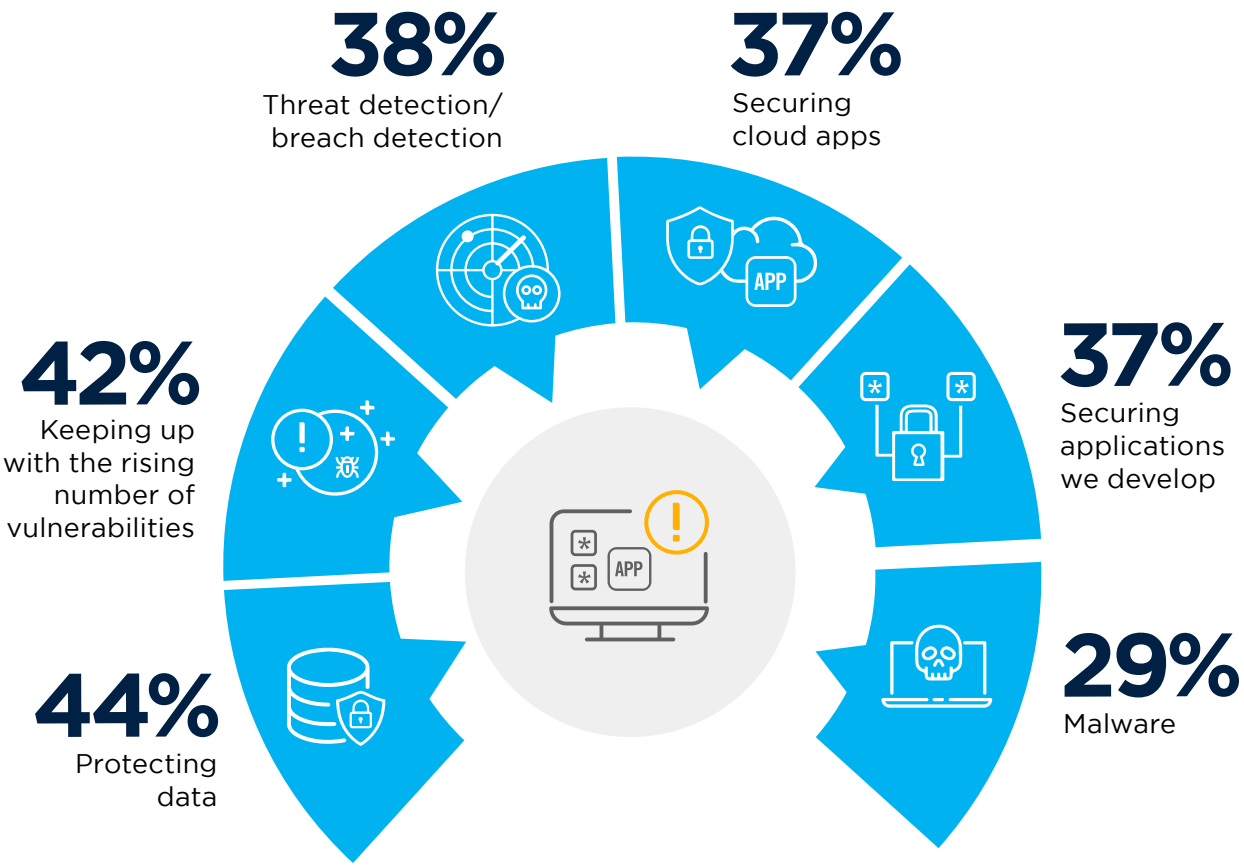
**Holger Schulze**
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

# APPLICATION SECURITY CONCERNS

When asked about their biggest application security concerns, cybersecurity professionals most frequently mentioned protecting data (44%) as their key concern. This is followed by the challenge of keeping up with the rising number of vulnerabilities (42%), threat and breach detection (38%) and securing cloud apps (37%).

### What are your biggest application security concerns?

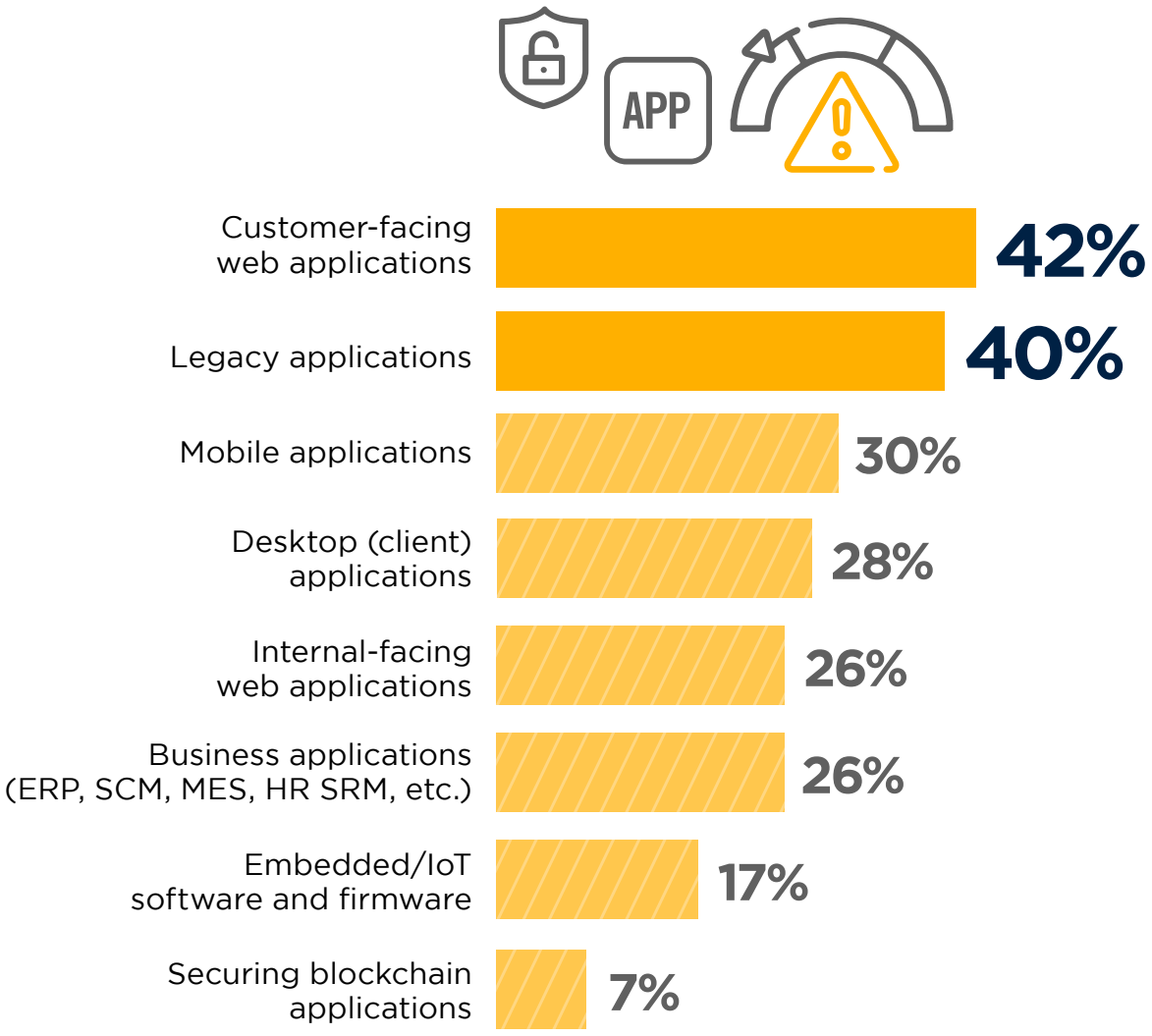



Effective threat modeling 27% | Effectively prioritizing and remediating vulnerabilities that pose the most risk 26% | Meeting regulatory/compliance requirements 26% | Securing mobile apps 26% | Securing business apps (ERP, etc.) 23% | Meeting customers' security needs and requirements 21% | Securing open source software 20% | Securing Embedded/IoT/hardware 17% | Securing commercial off-the-shelf software 16% | Securing Blockchain 6% | Don't know/other 6%

# APPLICATIONS AT RISK

So, which types of applications present the highest security risks? Customer-facing web applications tops the list (42%), followed by legacy apps (40%). Less frequently mentioned are mobile apps (30%), desktop applications (28%), and internal-facing web apps (26%).

**Which types of applications present the highest security risk to your business?**




Don't know/other 12%

# BARRIERS TO BETTER DEFENSES

A variety of barriers are inhibiting organizations from adequately defending against cyberthreats, and none of them has to do with security technologies directly. At the top of the list are two "people issues": the perennial lack of skilled personnel (39%) followed by low security awareness among employees (35%). Next are lack of budget (35%), lack of collaboration between departments (29%), and lack of management support (26%).

**Which of the following barriers inhibit your organization from adequately defending against cyberthreats?**

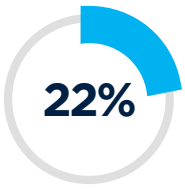
**39%** Lack of skilled personnel

**35%** Low security awareness among employees

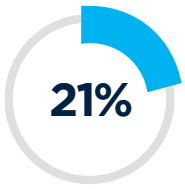
**35%** Lack of budget

**29%** Lack of collaboration between separate departments

**26%** Lack of management support/ awareness



**22%** Too much data to analyze



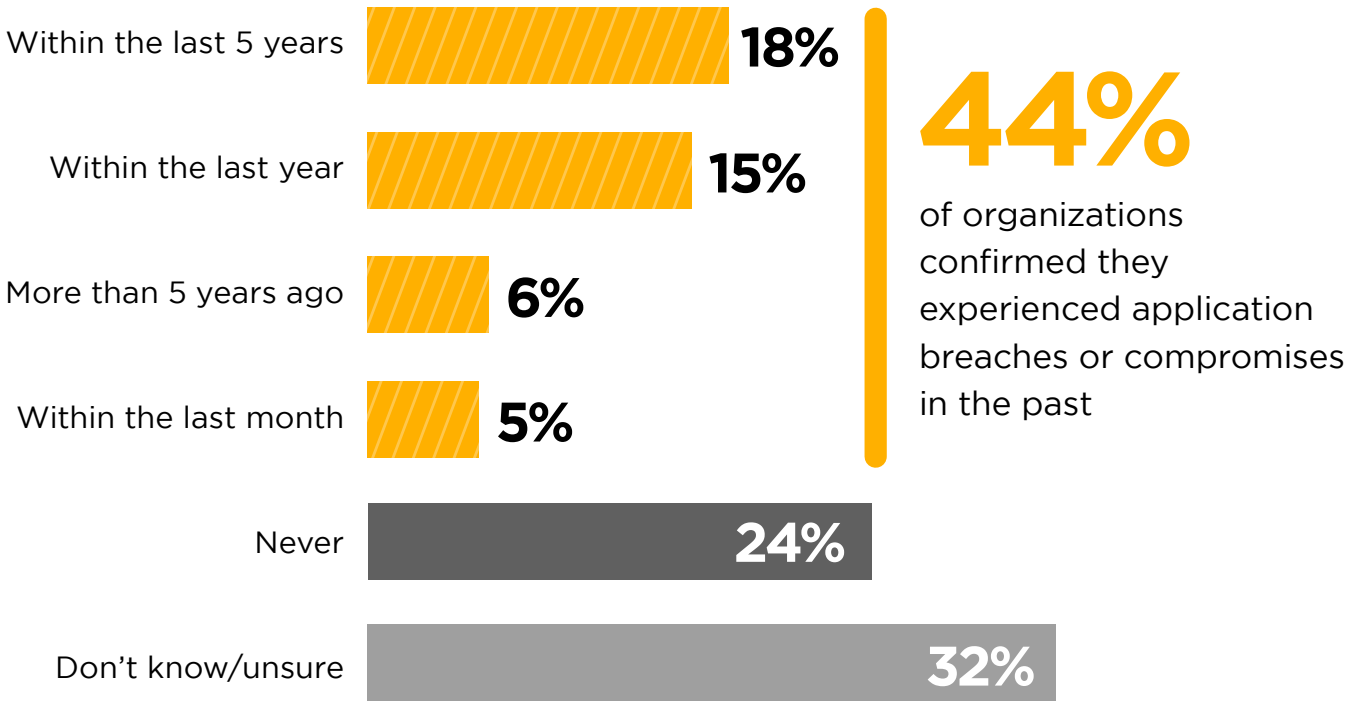
**21%** Poor integration/ interoperability between security solutions

Lack of investment in effective solutions 20% | Inability to prioritize vulnerabilities based on risk 20% | Lack of contextual information from security tools 13% | Inability to justify additional investment 13% | None 7% | Not sure/other 10%

# COMPROMISED APPS

Forty-four percent  of surveyed organizations have experienced application breaches or compromises in the past, and of those, 20% had been attacked just within the last year. The alarming news is that one third of survey participants (32%) are not sure if they have experienced a security attack against applications.

**When was the last time that one of your company's applications was breached/compromised?**

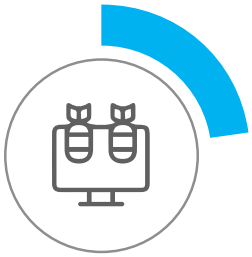



# ATTACKS AGAINST APPLICATIONS

Recent years have seen rapid growth in volume and sophistication of attacks, and the survey answers reflect this trend. Not surprisingly, malware remains the most common attack vector against applications (31%), followed by distributed denial-of-service attacks (23%) and application misconfiguration (21%). Other common types of attacks include stolen credentials (20%), exploits of software vulnerabilities (18%), and brute force attacks (17%).

**Which of the following security attacks against applications has your organization experienced over the past 12 months?**

**31%**
Malware



**23%**
DDoS

**21%**
Application misconfiguration


**20%**
Stolen credentials

**18%**
Software vulnerability exploit

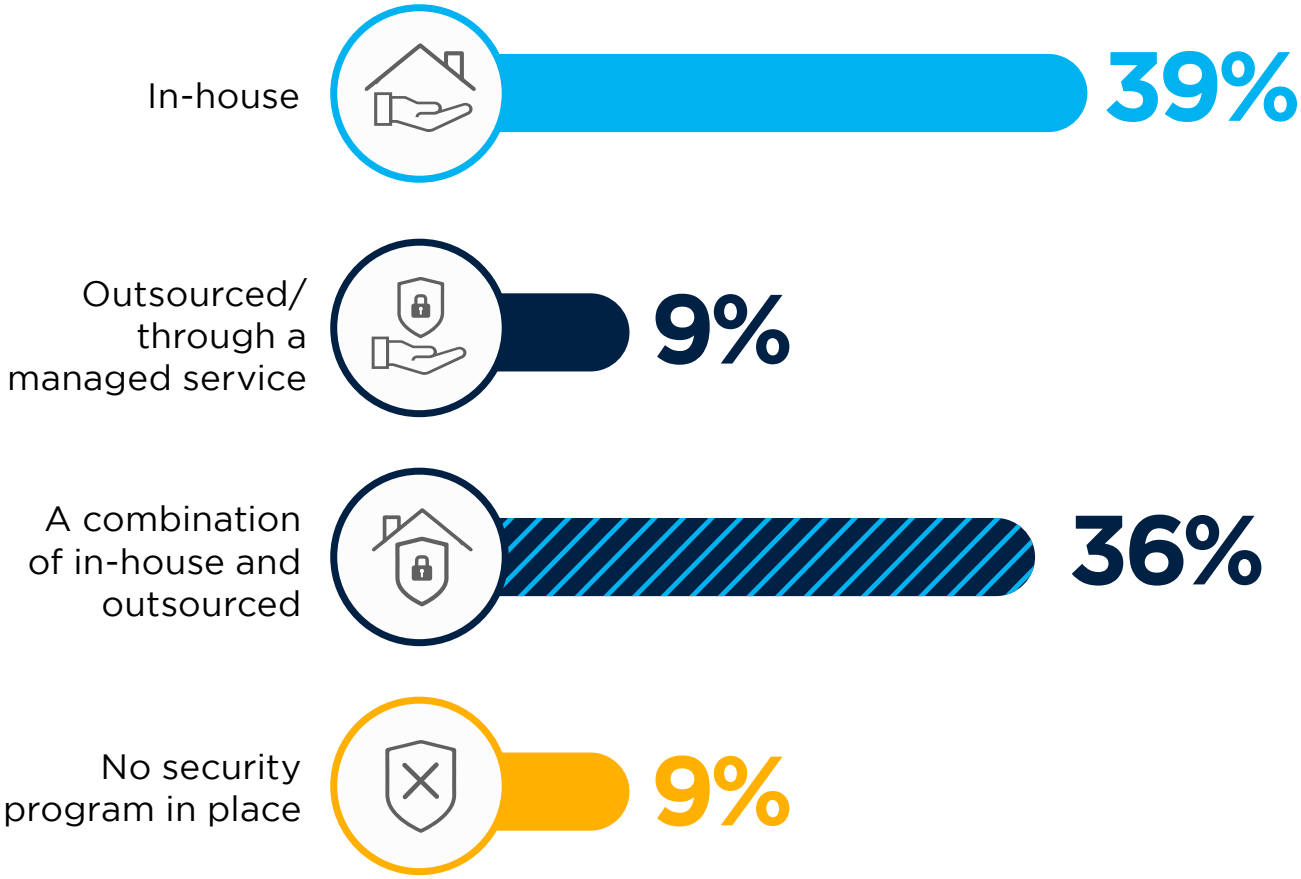
**17%**
Brute force

Cross-site scripting 16% | Unpatched library 15% | Information leakage 15% | Web fraud 14% | SQL injection 13% | Content spoofing 10% | Clickjacking 7% | Cross-site registry 7% | MitM/MitB 4% | Other 6%

# APPLICATION SECURITY PROGRAM

For organizations that have a dedicated application security program in place, in-house management remains the favorite option (39%). Nearly as common is a combination of in-house and outsourced application security. Only a minority (9%) rely exclusively on outsourcing for their application security. A minority of organizations (9%) rely exclusively on outsourcing for their application security needs.

### How is your application security program sourced?

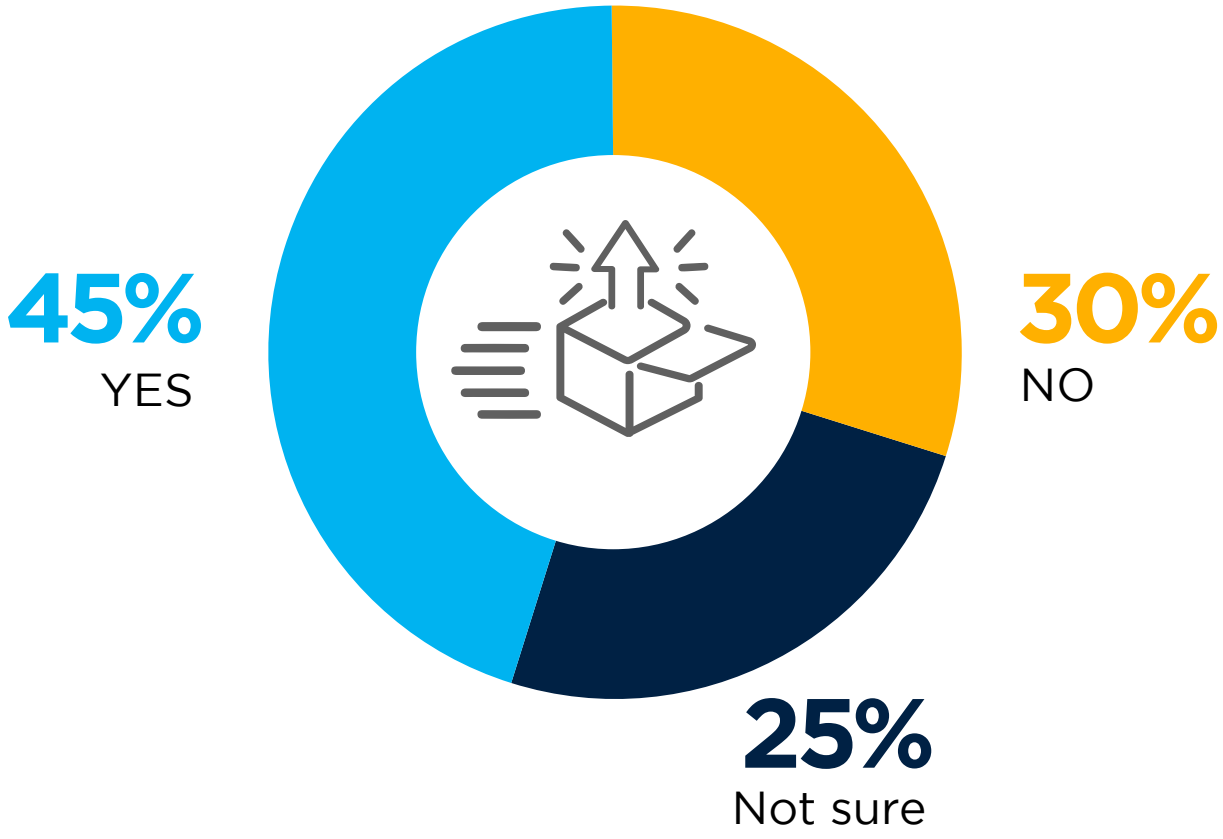



Don't know/unsure 7%

# SECURE CODING PROCESSES

Many companies are facing pressure to get new software developed quickly. But does the "rush to release" cause application developers to neglect secure coding procedures and processes? The most common answer is yes, according to 45% of the respondents. Only 30% said they do not neglect secure coding processes, and 25% are not sure.

**Does the "rush to release" cause application developers in your organization to neglect secure coding procedures and processes?**

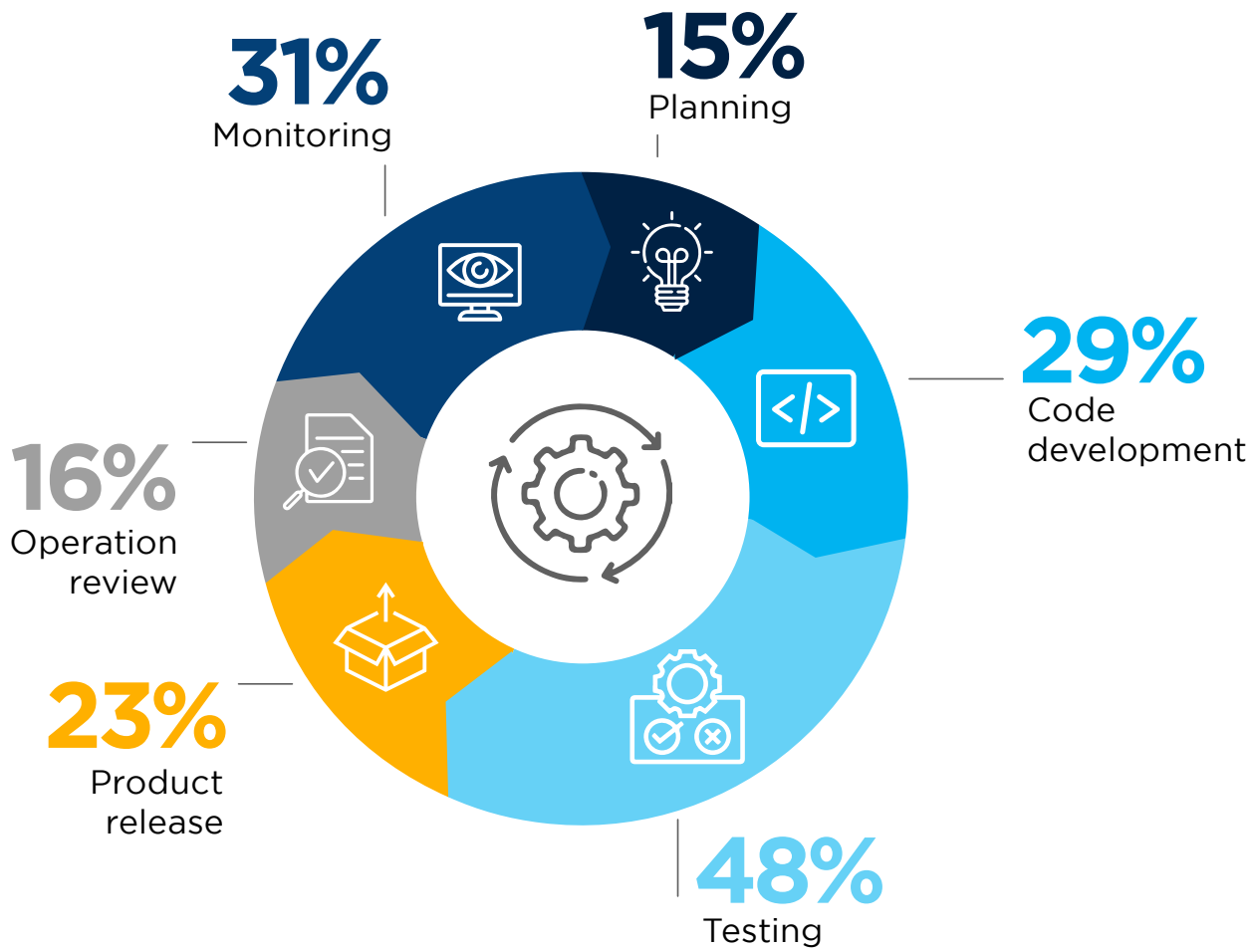


# AUTOMATIC SECURITY TESTING

Forty-six percent of organizations do not automate security testing during their software lifecycle. Of the 54% of organizations that automate security testing, it is done at multiple stages of the software release lifecycle. The most popular stage is during the software testing phase (48%). This is followed by automatic security testing during monitoring (31%) and code development (29%).

### Do you automate security testing in your software release lifecycle?

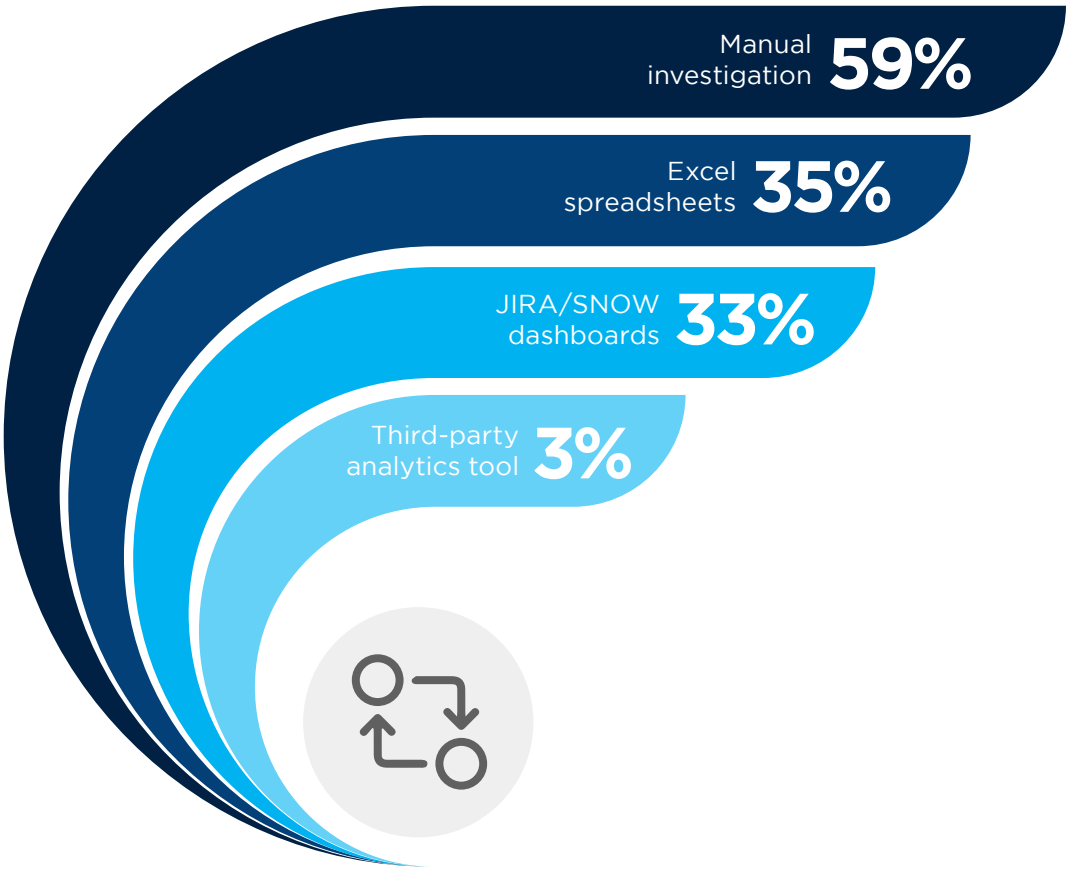

### What stage in your software release lifecycle do you automate security testing?



# MULTIPLE SECURITY SCANNERS

Utilizing multiple security scanners creates the challenge of correlating and triaging alerts and vulnerabilities. For most organizations, this means manual inspection of logs and alerts (59%) – a time and resource intensive approach. More than a third use excel spreadsheets for tracking (35%), closely followed by JIRA/SNOW dashboards (33%).

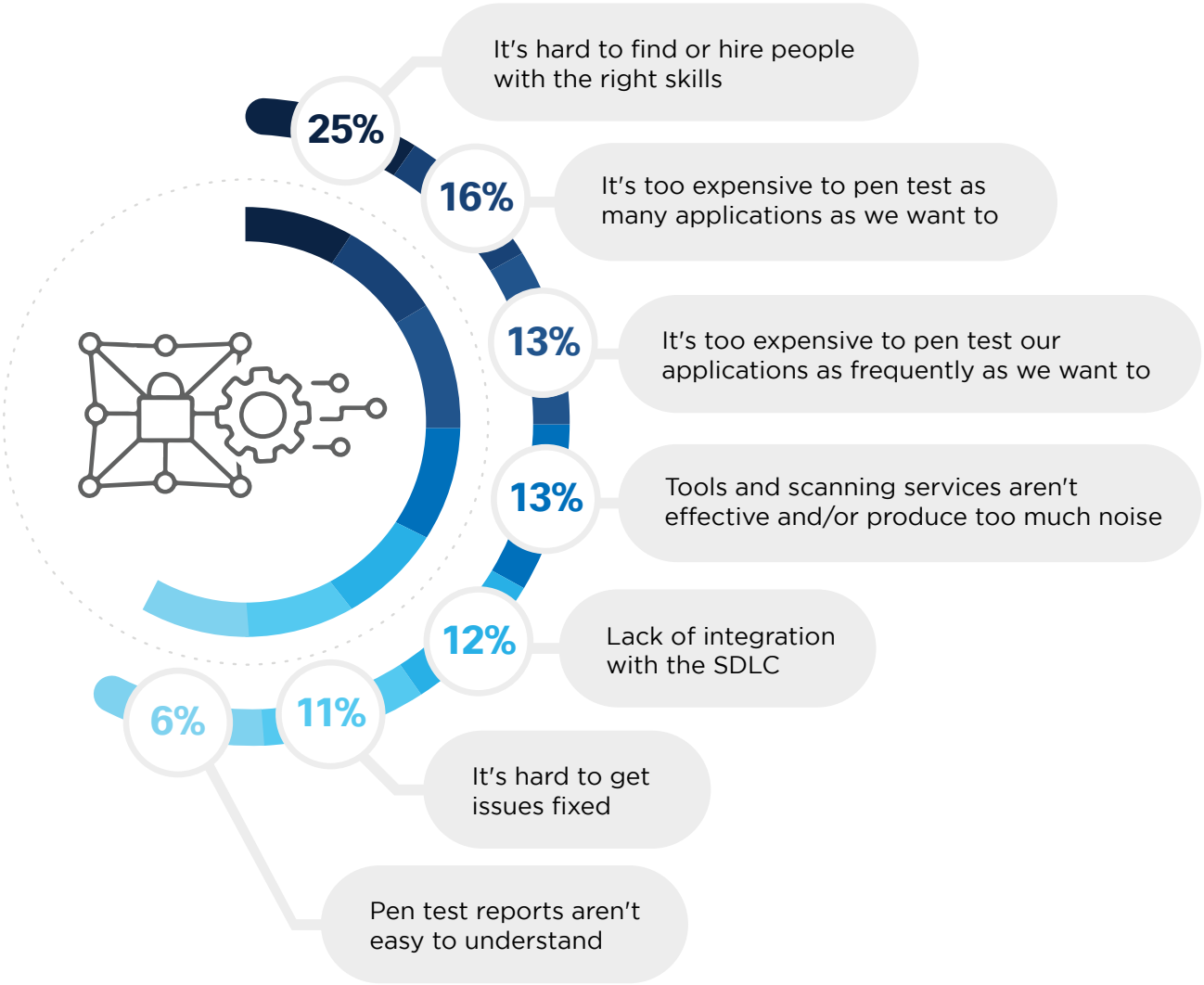
**How do you correlate and triage vulnerabilities from multiple scanners?**



# PEN TESTING CHALLENGES

The most challenging aspect of penetration testing applications continues to be finding people with the right skillset, according to 25% of survey respondents. This is followed by cost barriers preventing organizations from pen testing as many applications as they would like (16%) and as frequently as desired (13%).

### What is the biggest challenge regarding pen testing applications?

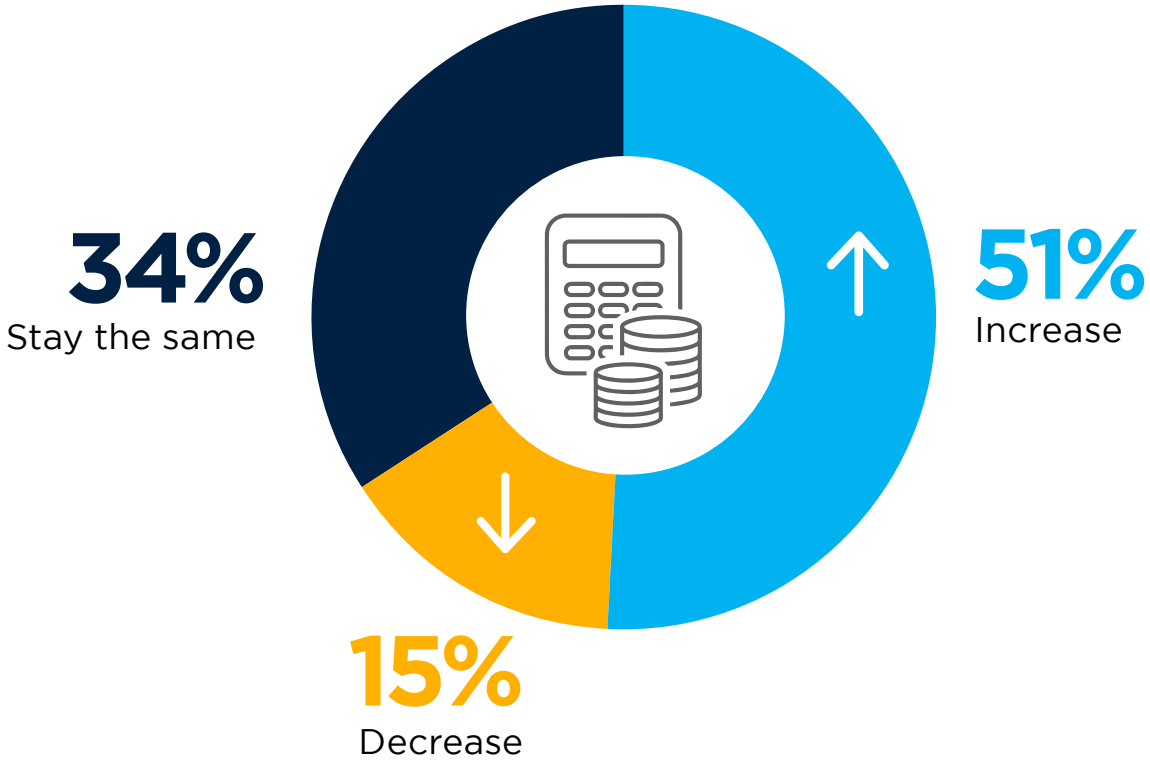



Other 4%

# APPLICATION SECURITY BUDGET

A fairly reliable indicator for the importance of a program in an organization is the allocation of resources to the program. By that measure, application security is gaining in importance for most organizations - a majority (51%) projects a budget increase over the next 12 months. About a third believe their appsec budgets will remain the flat (34%). Only 15% say their budget is likely to decline.

**How is the budget for securing your applications changing over the next 12 months?**

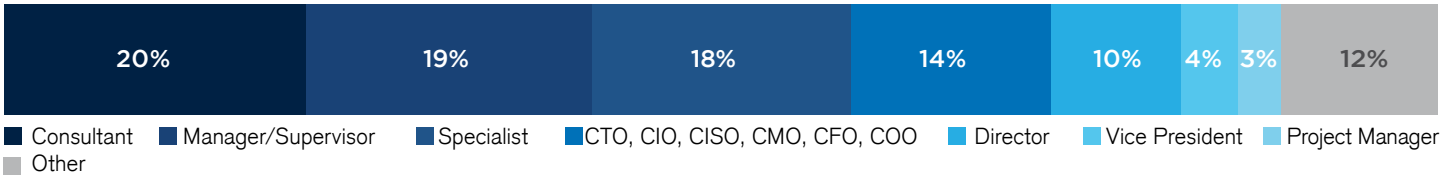



**If the budget for securing your application will increase, indicate by how much.**

# METHODOLOGY & DEMOGRAPHICS

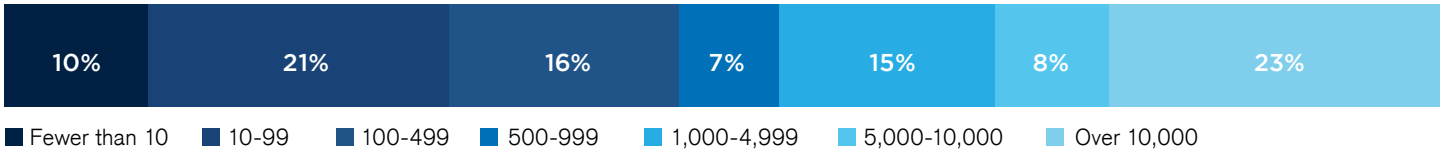
The 2022 Application Security Report is based on the results of a comprehensive online global survey of 325 cybersecurity professionals, conducted in June 2022, to gain deep insight into the latest trends, key challenges, and solutions for application security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

## CAREER LEVEL

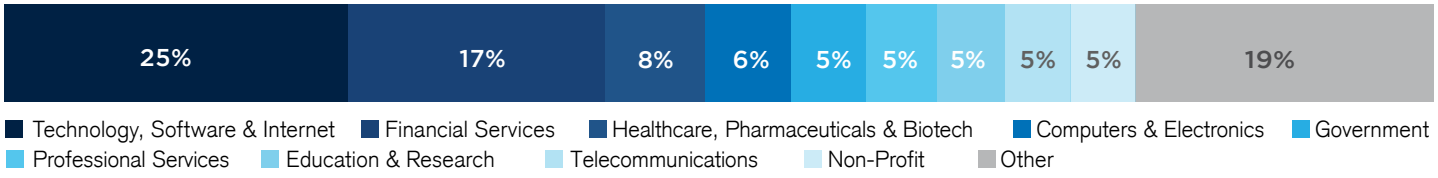



## DEPARTMENT

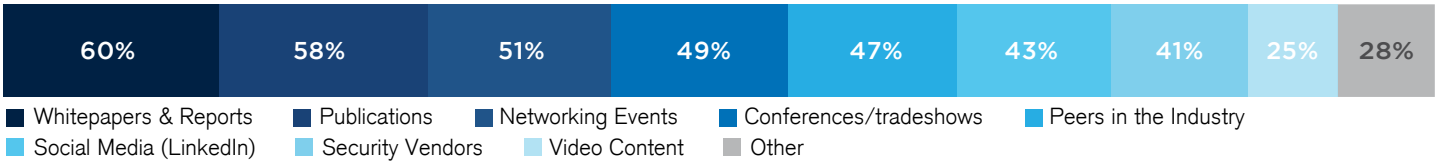

## COMPANY SIZE




## INDUSTRY




## RESOURCES



beyondsecurity
by HelpSystems

Beyond Security is a global leader in automated vulnerability assessment and compliance solutions – enabling businesses and governments to accurately assess and manage security weaknesses in their networks, applications, industrial systems, and networked software.

www.beyondsecurity.com

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

**For more information please visit www.cybersecurity-insiders.com**