Cybersecurity
INSIDERS

2022

Application Security Report

CISCO

INTRODUCTION

Business applications are increasingly under attack from advanced threats and malicious actors that are looking to exploit software vulnerabilities. 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 Cisco in July 2022. The resulting report reveals the latest application security trends, how organizations protect critical applications, and the tools and best practices cybersecurity professionals prioritize.

Key findings include:

- Cybersecurity professionals most frequently mention protection of data (44%) as their key application security 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%).
- Customer-facing web applications tops the list of applications introducing the highest security risks (42%), followed by legacy apps (40%). Less frequently mentioned are mobile apps (30%), desktop applications (28%), and internal-facing web apps (26%).
- About a third (36%) of cybersecurity professionals confirm encrypted traffic is a security risk to their environment due to the inability to inspect all traffic and detect threats quickly before they can cause damage. Specifically, cyber professionals are most concerned about hidden malware (63%), lack of visibility (58%), and data loss through exfiltration (37%) as the main problems caused by encrypted traffic.

We would like to thank Cisco for supporting this important research.

We hope you enjoy this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SECURITY BARRIERS

Various barriers inhibit organizations from adequately defending against cyber threats and an effective security posture. 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%). Organizational issues are also a contributing factor.

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

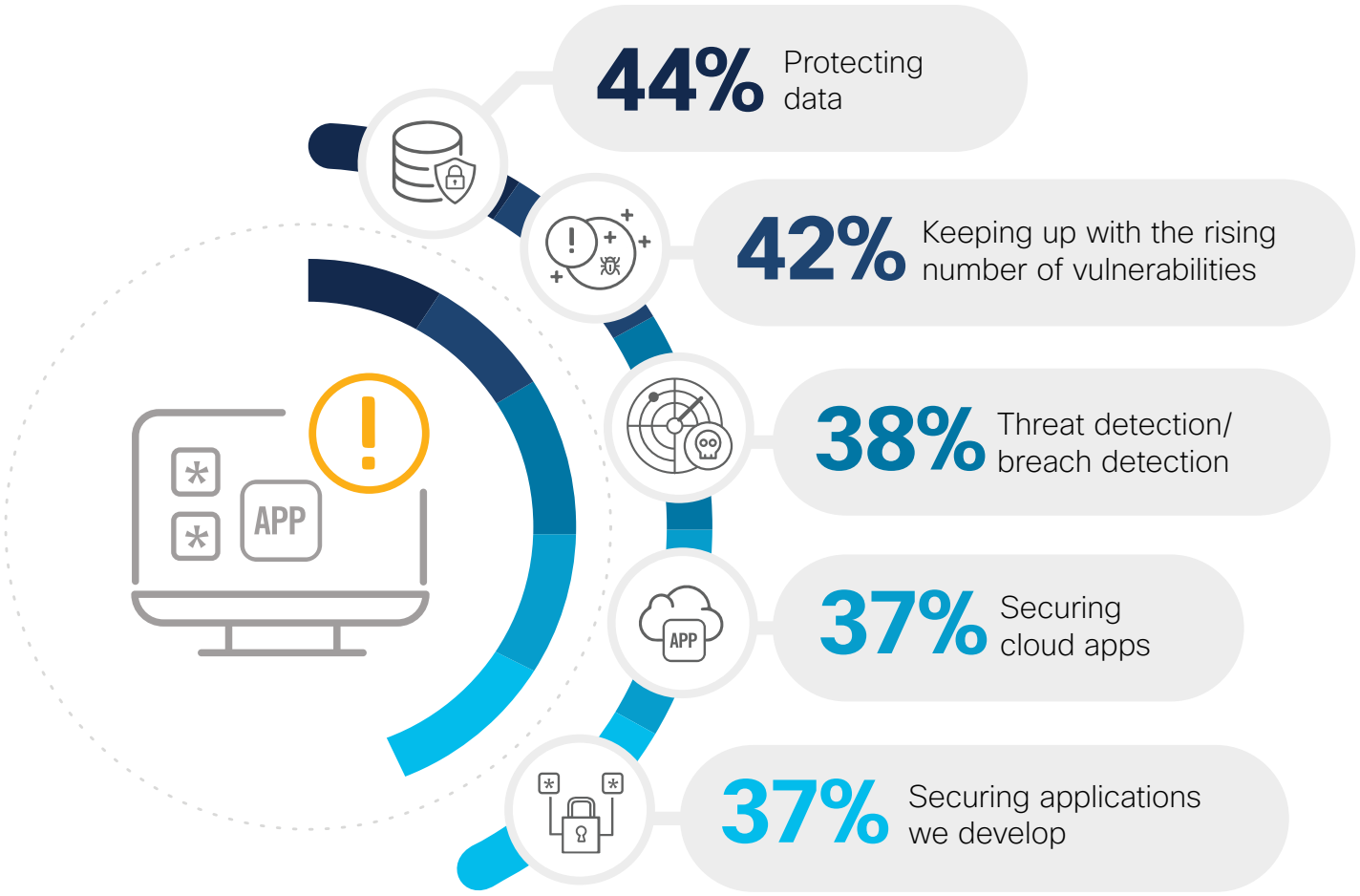
21% Poor integration/ interoperability between security solutions

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%

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?

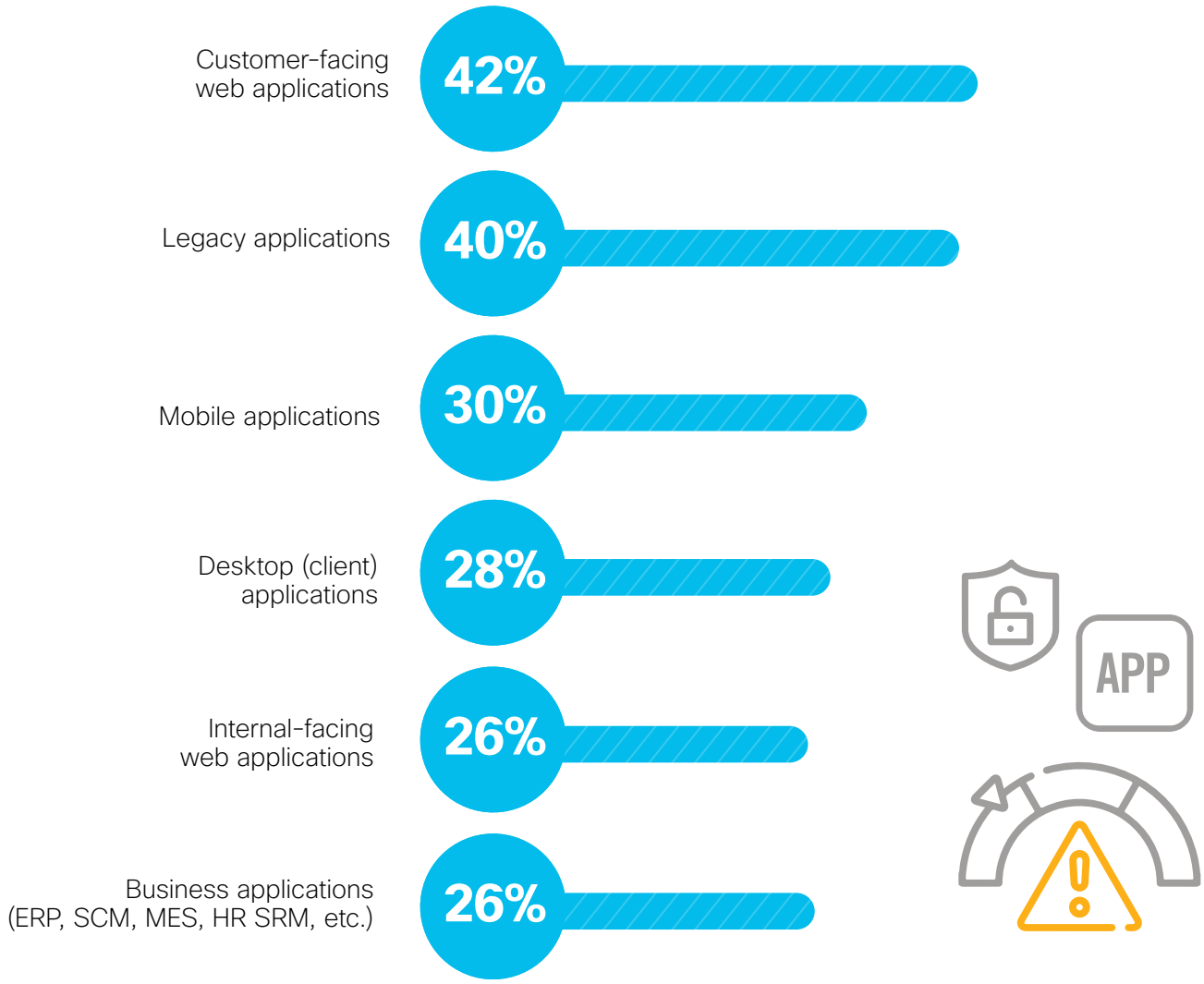


Effective threat modeling 27% | Effectively prioritizing and remediating vulnerabilities that pose the most risk 26% | Meeting regulatory/ compliance requirements 26% | Securing mobile apps 26% | Securing business apps (ERP, etc.) 23% | Meeting customers' security needs and requirements 21% | Securing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

RISKIEST APPLICATIONS

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

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

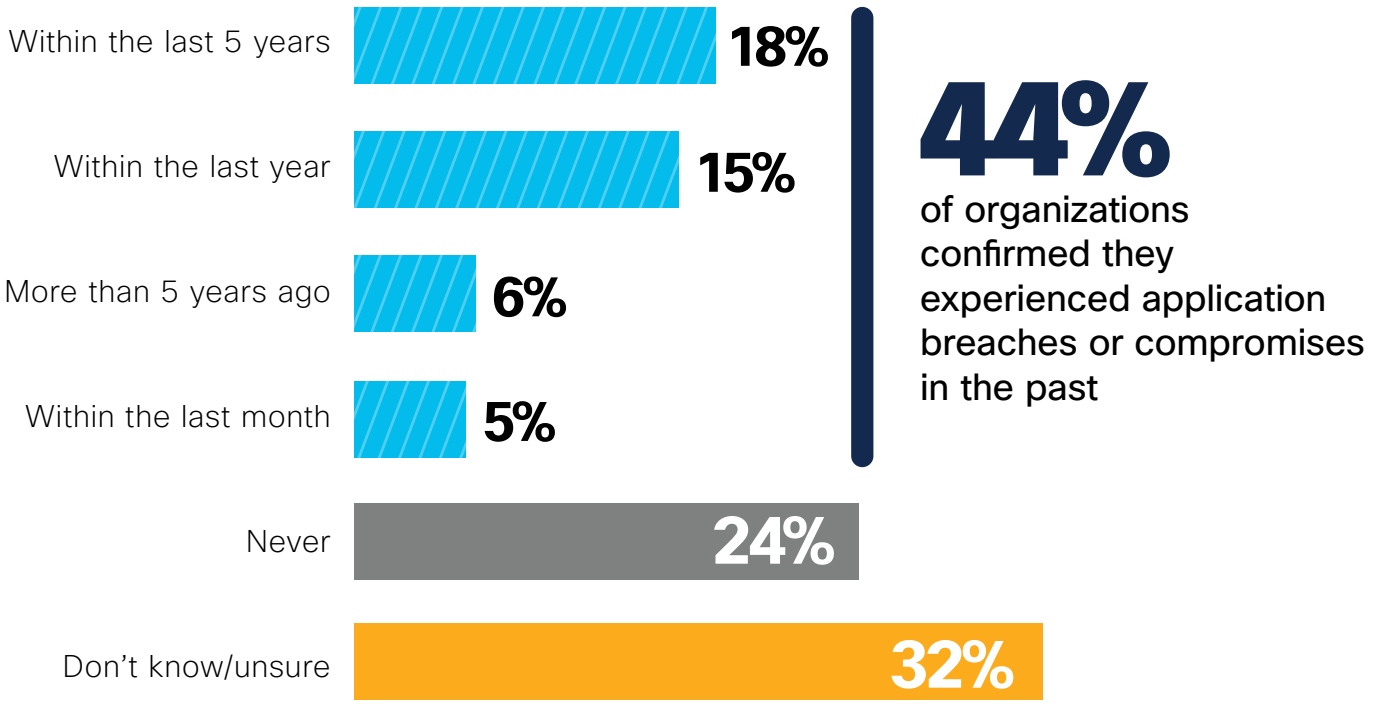


Embedded/IoT software and firmware 17% | Securing Blockchain applications 7% | Don't know/unsure/other 12%

LAST BREACH

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

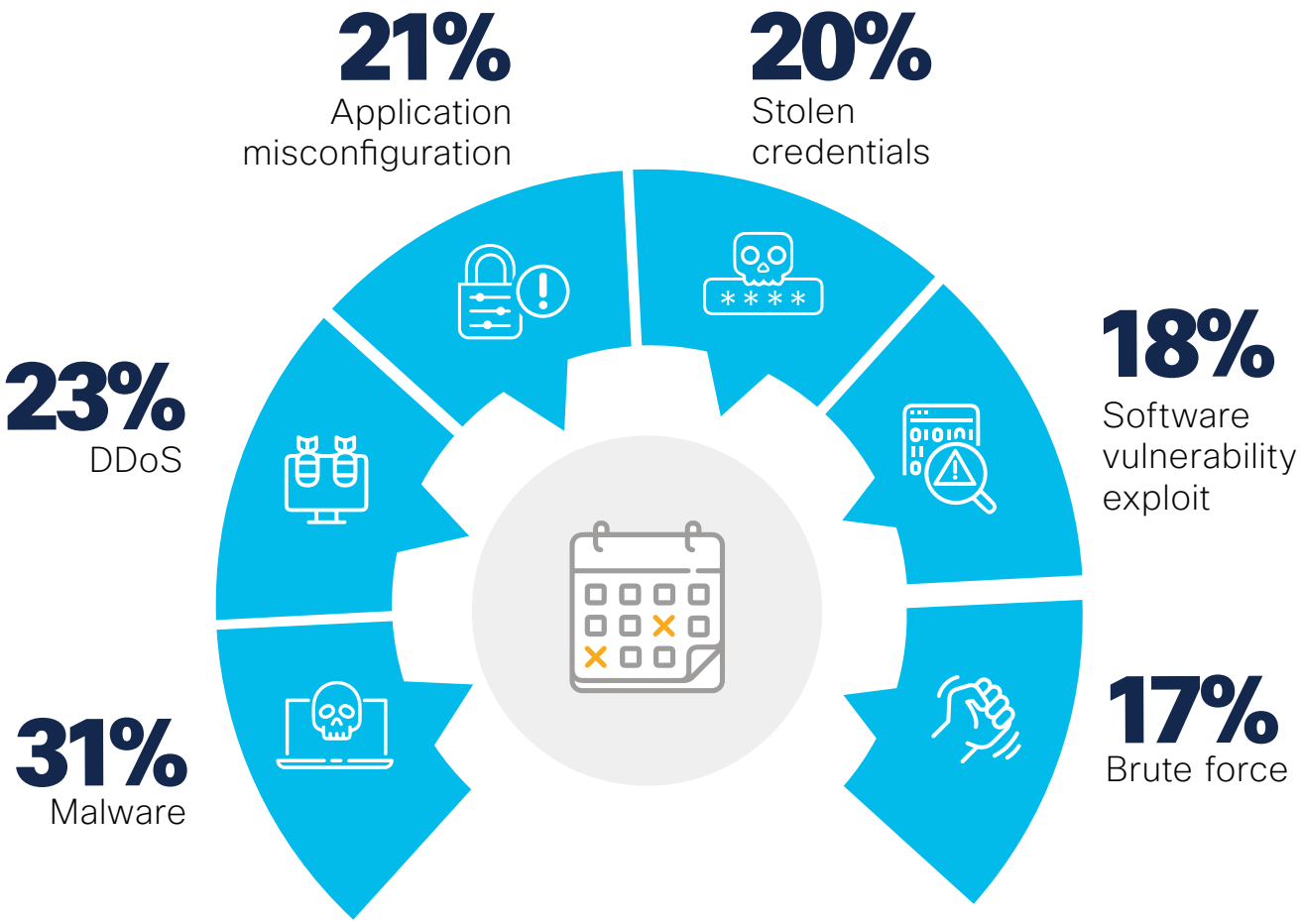
When was the last time that one of your company's applications was breached/ compromised?



ATTACKS AGAINST APPS

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?

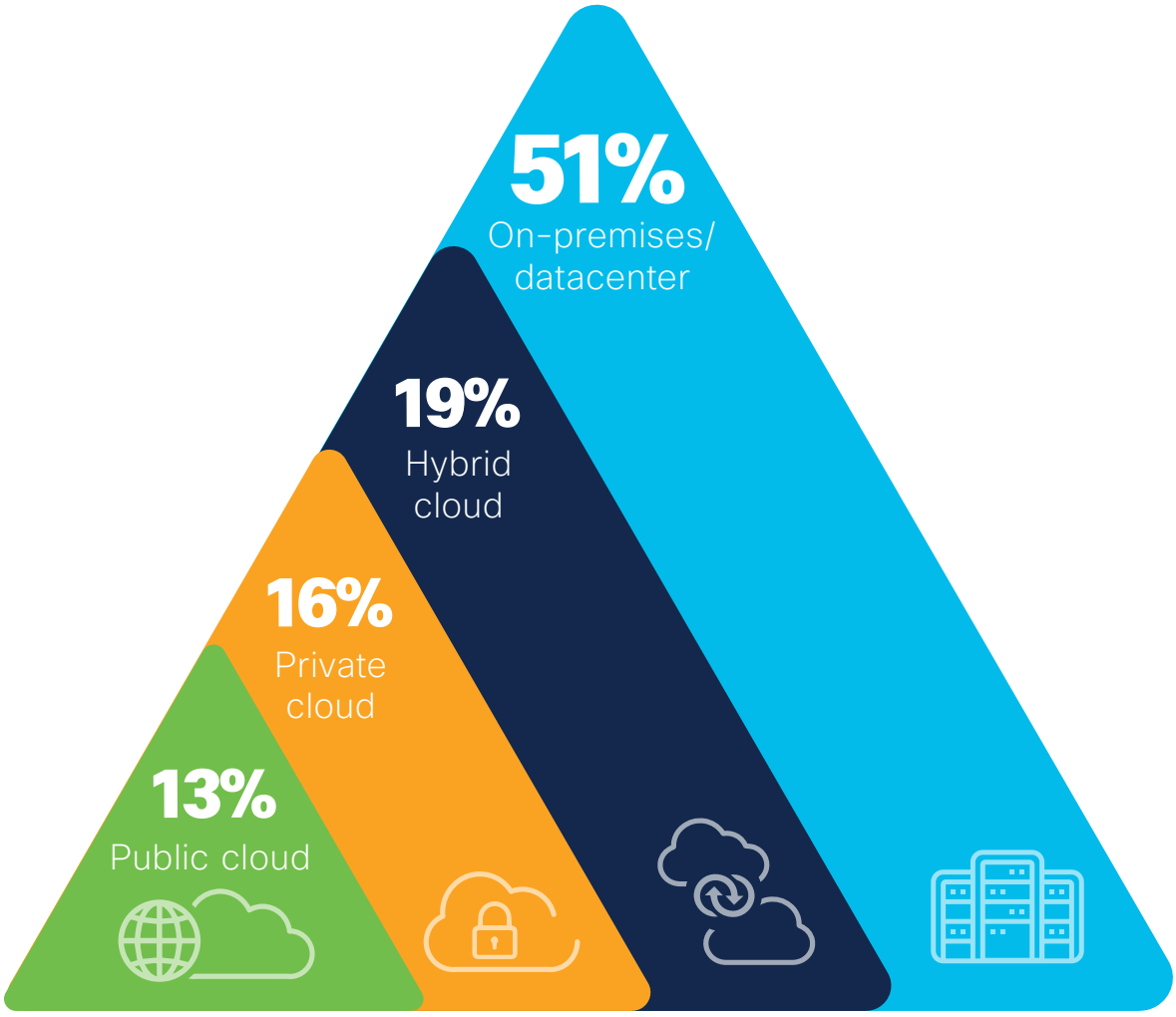


Cross-site scripting 16% | Unpatched library 15% | Information leakage 15% | Web fraud 14% | SQL injection 13% | Content spoofing 10% | Clickjacking 7% | Cross-site registry 7% | MitM/MitB 4% | Other 6%

WHERE THE APPS ARE

Despite rapid adoption of cloud computing in the last years, most business applications are still hosted on-premises (51%), followed by hybrid cloud environments (19%), private clouds (16%) and public clouds (13%).

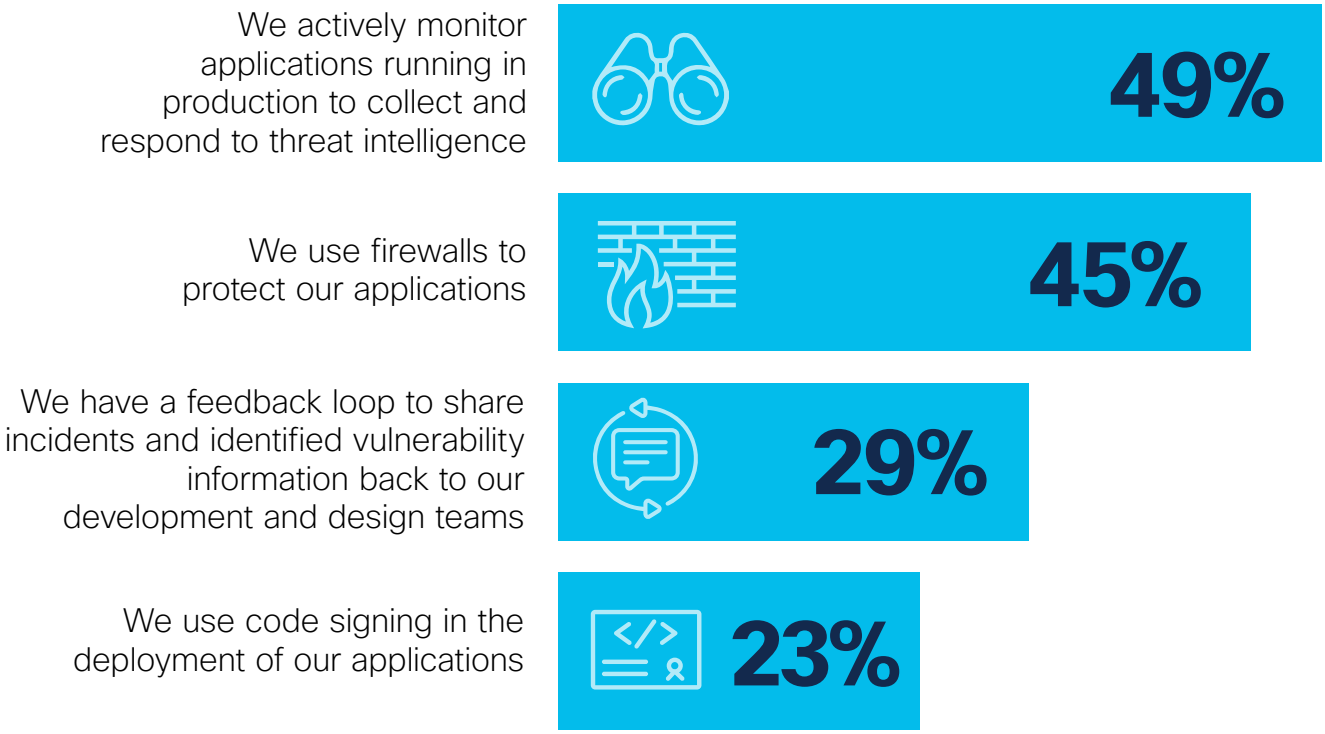
Where are the majority of your applications hosted?



APPLICATION MONITORING

How are organizations monitoring their apps for security issues? About half of organizations (49%) are actively monitoring applications in production to collect and respond to threat intelligence. They're using a variety of methods to monitor security issues, with Web Application Firewalls (WAF) being one of the primary solutions (45%).

How are you currently monitoring applications for security issues?

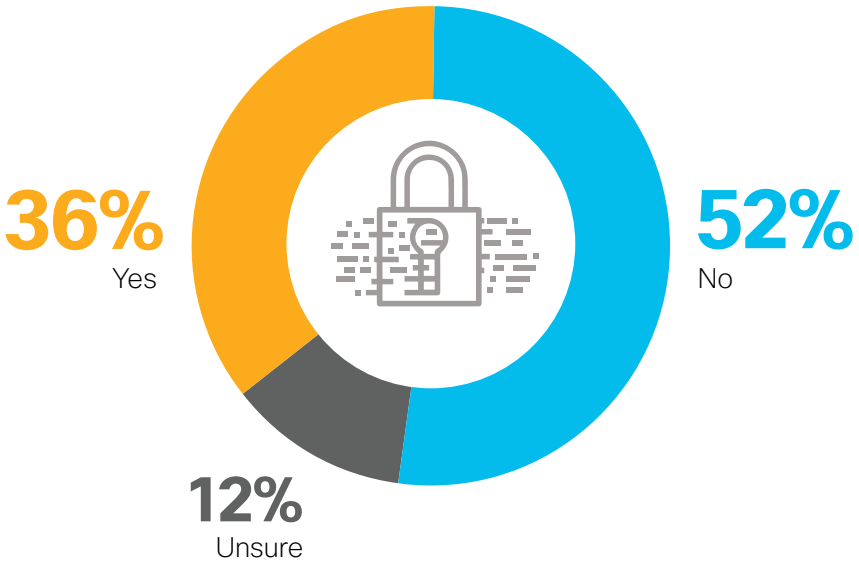


None of the above 10% | We use endpoint security to protect our applications 5% | We use the embedded security provided by our cloud provider 3% | We use a workload security product to protect our applications 1% | Don't know/unsure/other 17%

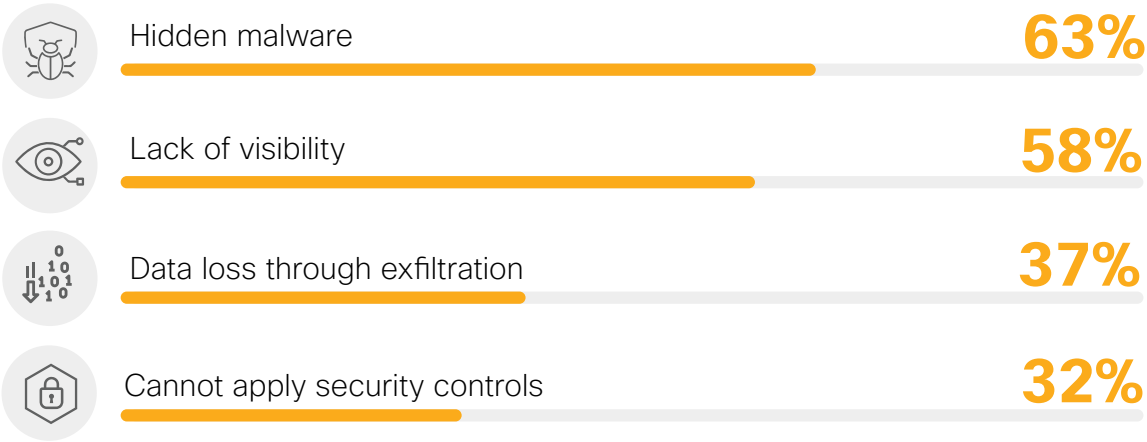
ENCRYPTED TRAFFIC RISKS

About a third (36%) of cybersecurity professionals confirm encrypted traffic is a security risk to their environment due to the inability to inspect all traffic and detect threats quickly before they can cause damage. Specifically, cyber professionals are most concerned about hidden malware (63%), lack of visibility (58%), and data loss through exfiltration (37%) as the main risks amplified by encrypted traffic.

Do you view encrypted traffic as a security risk in your environment?



If yes, what problems does encrypted traffic cause?

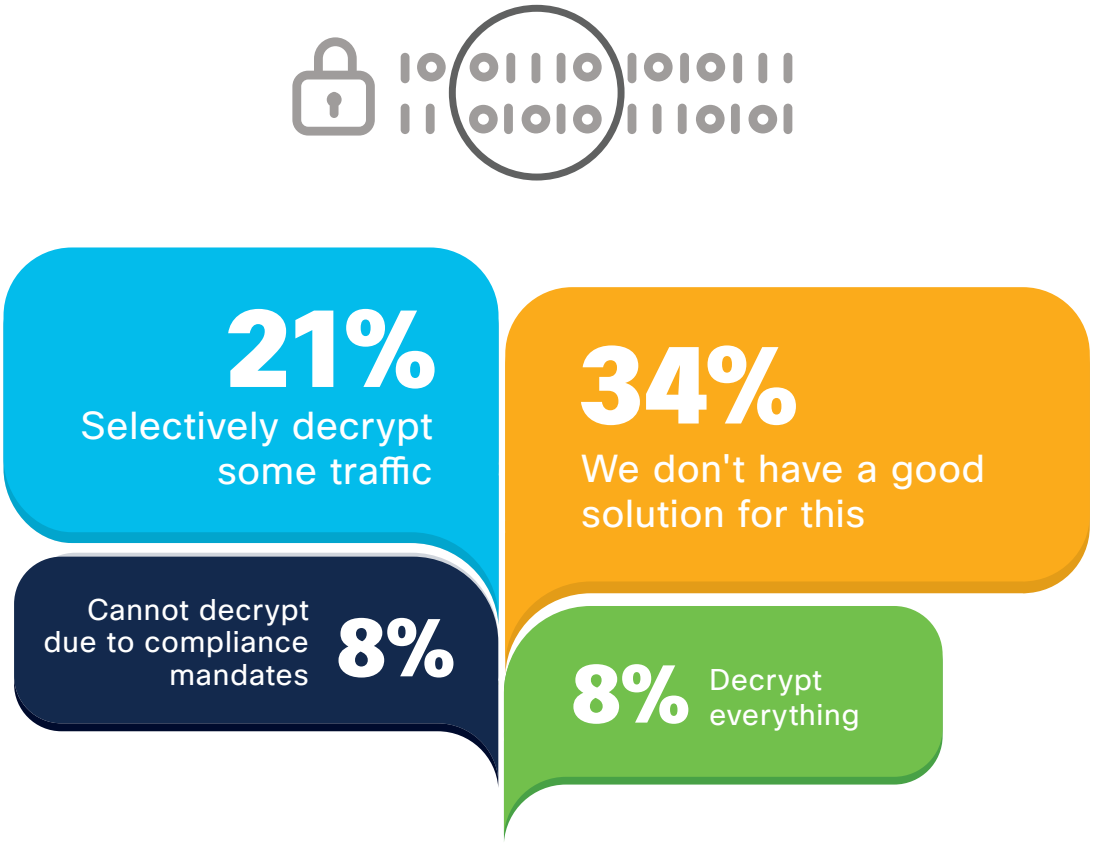


Other 5%

HANDLING ENCRYPTED TRAFFIC

How do organizations handle the challenges created by encrypted network traffic? A third of organizations (34%) don't have a good solution for encrypted traffic while 21% selectively decrypt some traffic.

How do you deal with encrypted traffic in your environment?



Unsure 25% | Other 4%

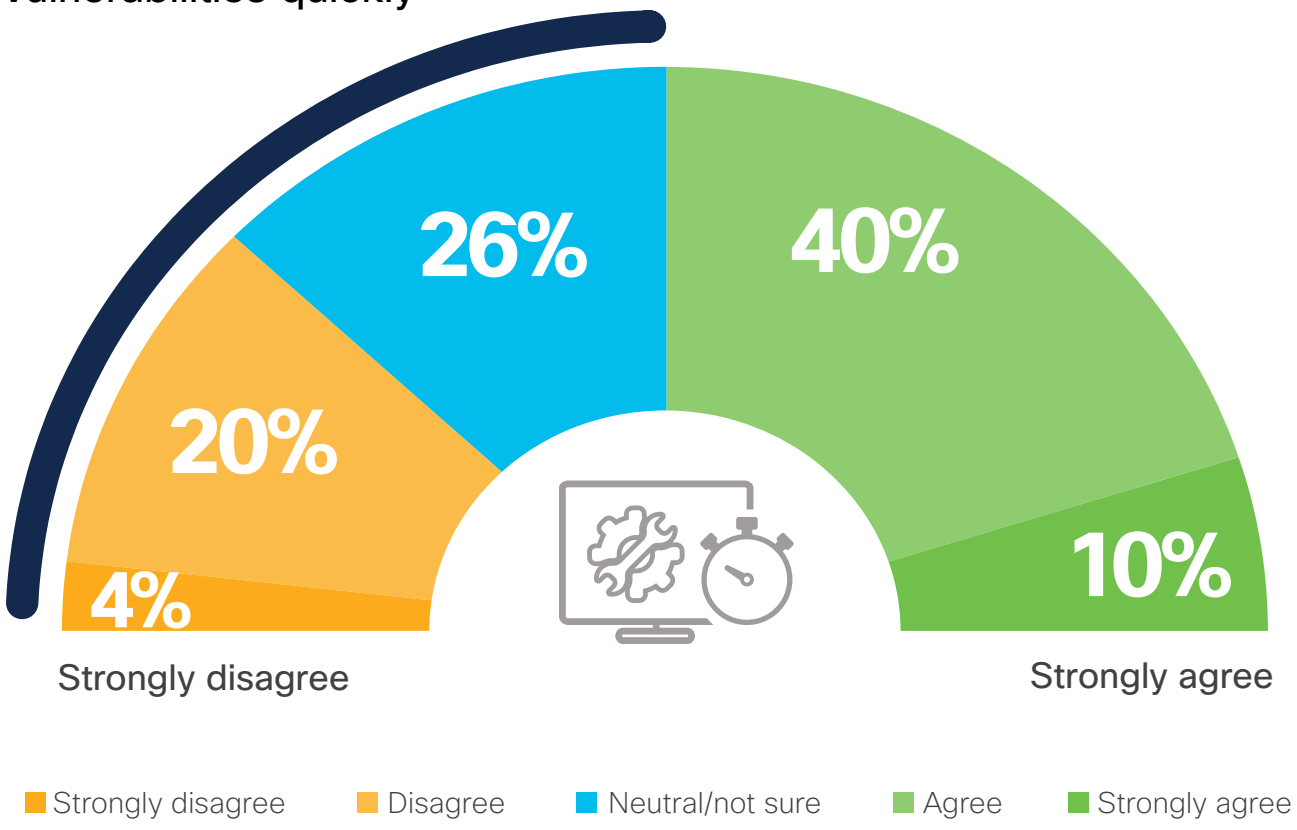
APPLICATION VULNERABILITIES

Only half of organizations (50%) agree they have sufficient resources to detect and remediate vulnerabilities in a timely manner. That leaves the other half without the necessary funds and staff to address application security issues quickly.

My organization has ample resources to detect and remediate vulnerabilities in applications in a timely manner

50%

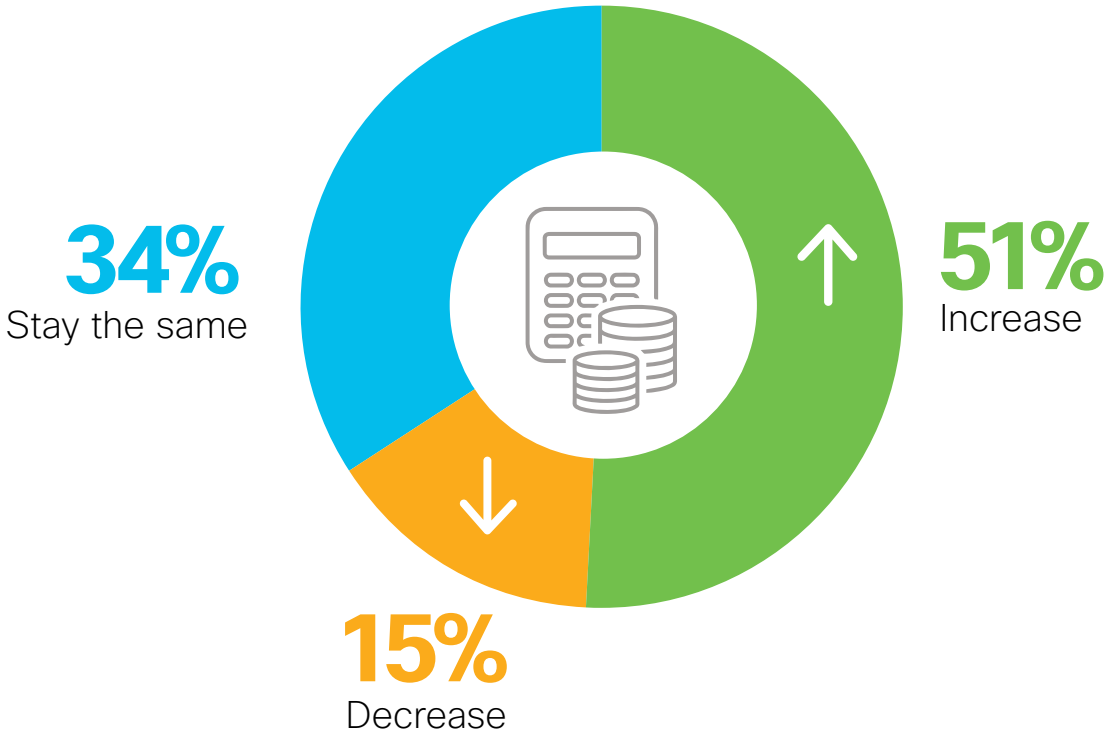
organizations are lacking sufficient resources to detect and remediate application vulnerabilities quickly



APPSEC BUDGETS ON THE RISE

For most organizations (51%), budgets dedicated to application security are increasing over the next 12 months. Only 15% expect a decline.

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

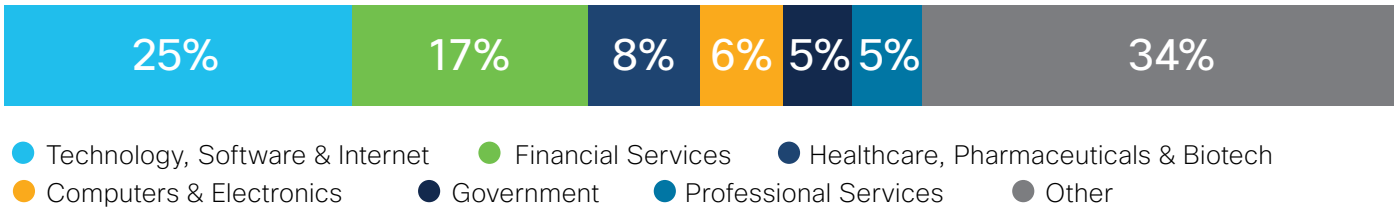


If the budget for securing your application will increase, indicate by how much.

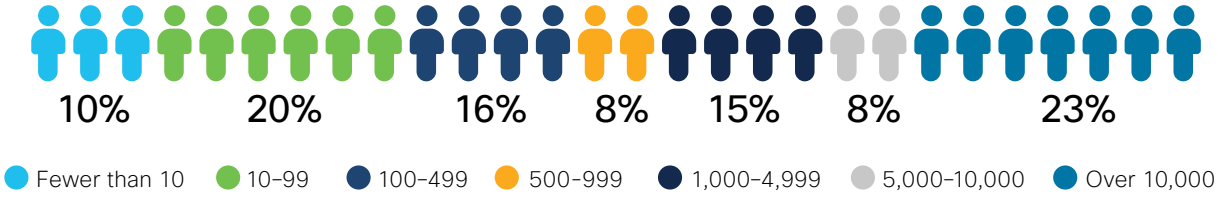
DEMOGRAPHICS

The 2022 Application Security Report is based on the results of a comprehensive online global survey of 386 cybersecurity professionals, conducted in July 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.

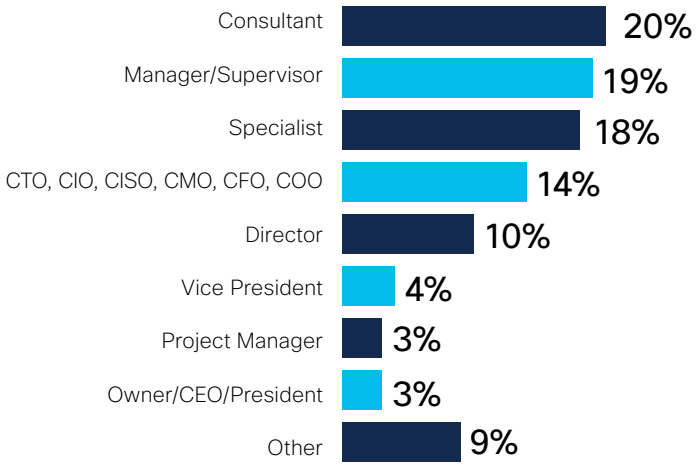
What is your organization's industry?



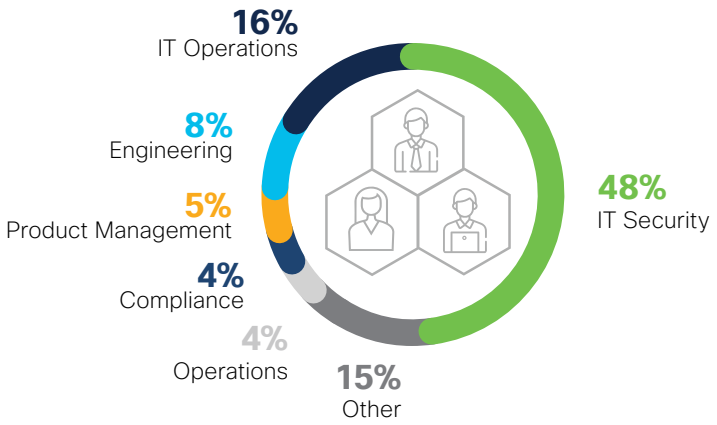
What is your company size?



What department do you work in?



What organizational level best describes your current position?



Cisco has long established itself as the worldwide leader in technology that powers the internet, while building an open, integrated portfolio of cybersecurity solutions along the way. We believe that security solutions should be designed to act as a team. They should learn from each other. They should listen and respond as a coordinated unit. When that happens, security becomes more systematic and effective. Our customers have trusted us for years as both the world's largest provider of IT infrastructure and networking services and the world's largest enterprise cybersecurity business.

Cisco Secure is built on the principle of better security, not more. It delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use – and that it all works together. We're driven by the fact that people and our customers are at the heart of what we do. We understand that customers want to cut through the complexity and noise and feel confident in their security, focusing on outcomes. This requires simplification without being simplistic. Our cloud-native platform is a giant leap forward in that.

We empower the security community with the reliability and confidence that they're safe from threats now and in the future with the Cisco SecureX platform. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Learn more about Cisco Secure

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