

Cloud Detection and Response: Market Growth as an Enterprise Requirement

Melinda Marks, Senior Analyst Jon Oltsik, Distinguished Analyst and ESG Fellow

JULY 2023



۲

Research Objectives

Increasingly dynamic cloud environments are presenting visibility challenges for security. Indeed, the majority of organizations claim that lack of access to physical networks, the dynamic nature of cloud-native applications, and elastic cloud infrastructure create blind spots, making security monitoring challenging. SOC teams need to address this cloud visibility gap by collecting, processing, monitoring, and acting upon information from an assortment of cloud security telemetry sources.

Additionally, nearly all organizations experienced a cloud security incident in the last year, resulting in application downtime, unauthorized access, data loss, and compliance fines. Thus, cloud security limitations can impact the business. Understanding this risk, executives and corporate boards are demanding measurable progress. Given the rise of digital transformation applications and cloud-native software development, CISOs must align threat detection and response spending with an increasing array of cloud-based business-critical workloads.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 393 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for evaluating or purchasing cloud security technology products and services.

This study sought to:



Determine the challenges security teams face resulting from threats to cloud workloads, identities, and application development processes.



Assess the state of cloud detection and response (CDR) skills, processes, and technologies.





Establish how CDR tools are used today and where they fit into the broader security plans, strategies, and established security operations technologies.

Understand why security teams are prioritizing CDR and the benefits they are seeing from these tools and services.





CLICK TO FOLLOW



Production Workloads Are Migrating to Multiple CSPs at an Accelerating Pace

PAGE 4



Cloud Detection and Response Is a Work in Progress

PAGE 17



DevOps Is Pervasive While DevSecOps Lags Behind



Cloud Security Operations Are Increasingly Automated But Remain Challenging

PAGE 14

PAGE 8



Cloud Detection and Response Is a Shared Responsibility That Requires Continuous Training



CDR Spending Is Growing as Cloud Security Professionals' List of Technology Requirements Expands

PAGE 28

PAGE 25





Production Workloads Are Migrating to Multiple CSPs at an Accelerating Pace

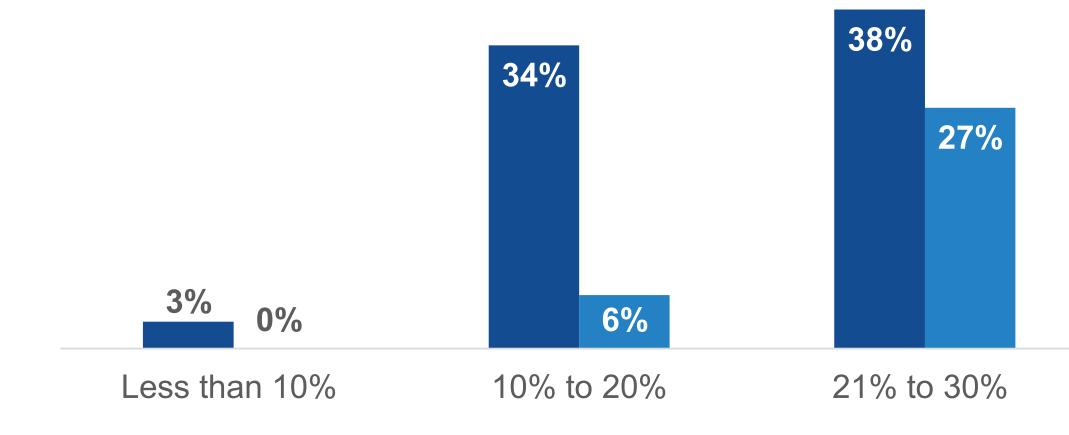


Production Workloads Moving to the Cloud

A majority (83%) of organizations have "lifted and shifted" applications to the public cloud. Today, one-quarter of organizations run more than 30% of their production workloads on public cloud infrastructure, but this is expected to increase dramatically over the next two years. Specifically, by 2025, nearly six in ten anticipate that more than 30% of their production workloads will run on public cloud infrastructure. To prepare for this shift, security teams will need CDR solutions that support scale and process automation.

Percentage of production applications that are cloud-hosted.

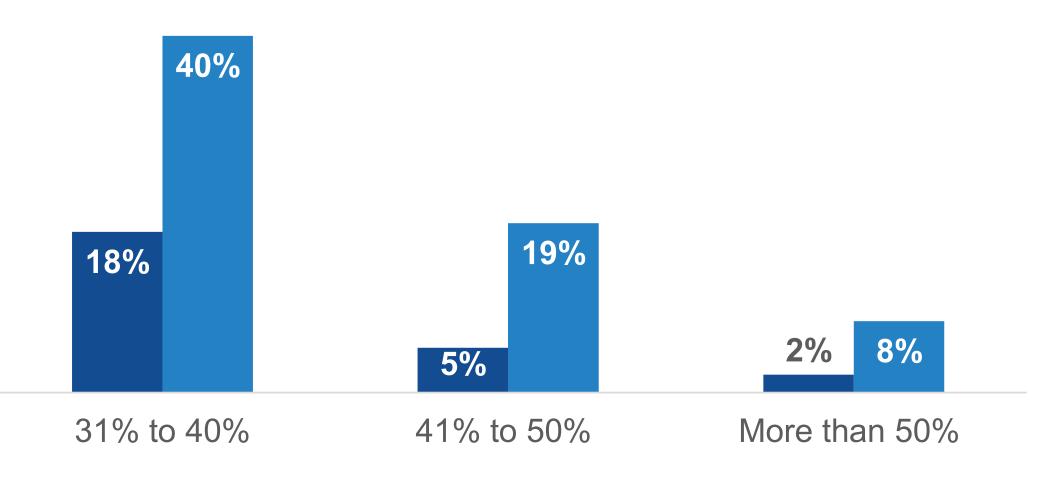
- Percentage of production workloads run on public cloud infrastructure services today



83%

have lifted and shifted existing production applications and server workloads to run on cloud infrastructure and/or platform services.

Percentage of production workloads run on public cloud infrastructure services 24 months from now



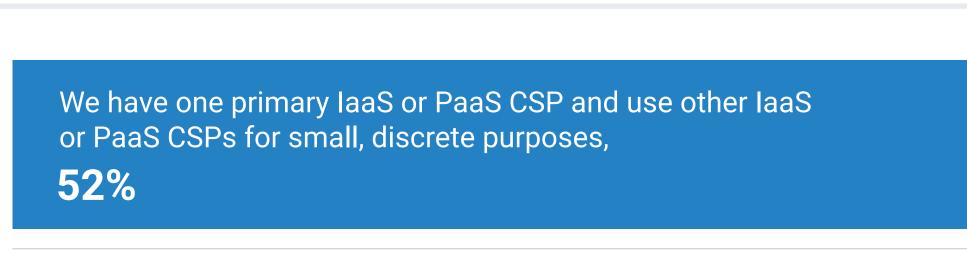
Drivers of Multi-cloud Strategies

Many (69%) organizations utilize at least 3 different cloud service providers. More than half (52%) of organizations claim to have a primary CSP, while 48% use multiple CSPs in a meaningful way. Firms choose different CSPs for business units or applications using CSP products or product suites, based on software developer skills and relationships, or based on the existing relationships of business units or acquired companies. Using multiple CSPs poses several challenges for cybersecurity. Security teams must be well versed in each CSP's technology, with a strong understanding of services, security tooling, log sources, and hosted applications. Additionally, they must understand the interrelationships between CSPs, while maintaining visibility across all public clouds to manage risk and detect/respond to threats.



Number of unique CSPs in use.

How multiple CSPs are being used.



0%

We use multiple laaS or PaaS CSPs in a meaningful way, 48%

100%

Reasons for using multiple unique CSPs.

To choose different CSPs for business units or applications that are mostly using products or product suites from the same vendor

To choose different CSPs for different business units or applications depending on the skills and relationships of different software developers

Certain business units or acquired companies have existing relationships or preferences for CSPs other than our primary CSP

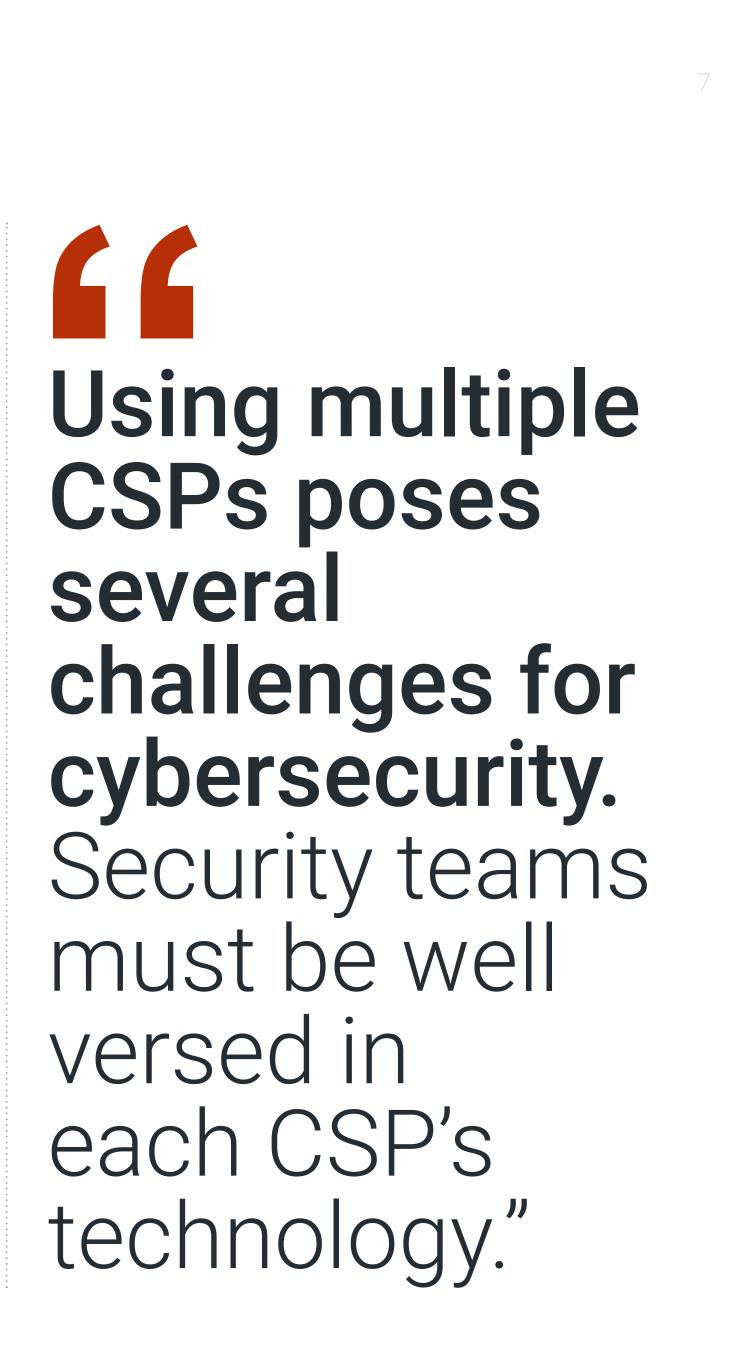
To supplement the primary CSP we use for most of our needs with another that is more adept at working in our industry

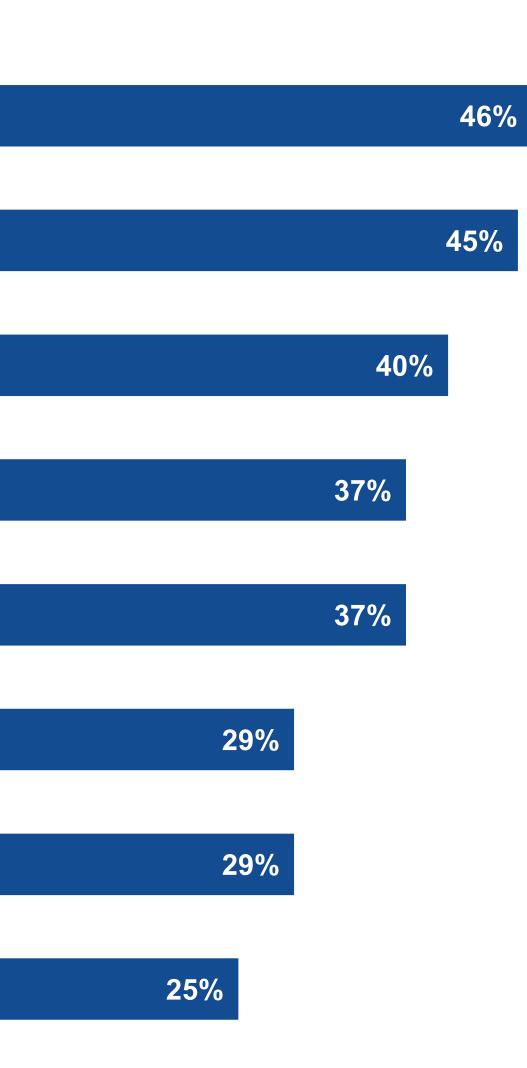
To choose different CSPs based on SLA and feature alignment with application needs

Preexisting relationships with several CSPs that we continue to work with

So that we aren't reliant on a single vendor

To negotiate better pricing



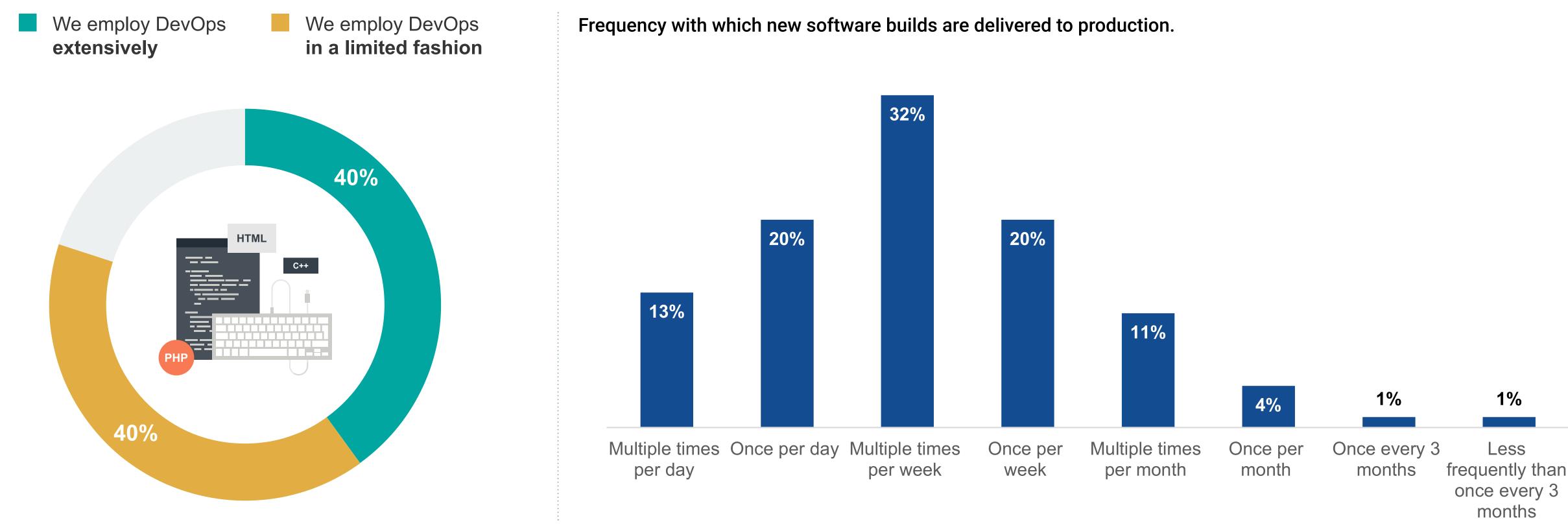


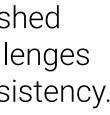
DevOps Is Pervasive While DevSecOps Lags Behind



Faster Software Release Cycles Cause Security Challenges

The majority of organizations employ a DevOps model extensively (40%) or at least on a limited basis (40%). This embrace of DevOps has led to a rapid cadence of software pushed to production, with 85% of organizations deploying new builds to production at least once per week. From a security perspective, rapid application changes introduce many challenges such as a lack of visibility and control in development processes, software being released without going through security checks and testing, and a lack of security process consistency. Alarmingly, one-third (33%) of survey respondents claim they are challenged because developers are skipping security processes in order to meet deadlines.





Security challenges caused by faster development cycles of CI/CD.

Security lacks visibility and control in development processes

Software is released without going through security checks and/or testing

Lack of consistency of security processes across different development teams

Developers are skipping security processes in order to meet deadlines

New builds are deployed to production with misconfigurations, vulnerabilities, and other security issues

Developers lack security visibility in the development process

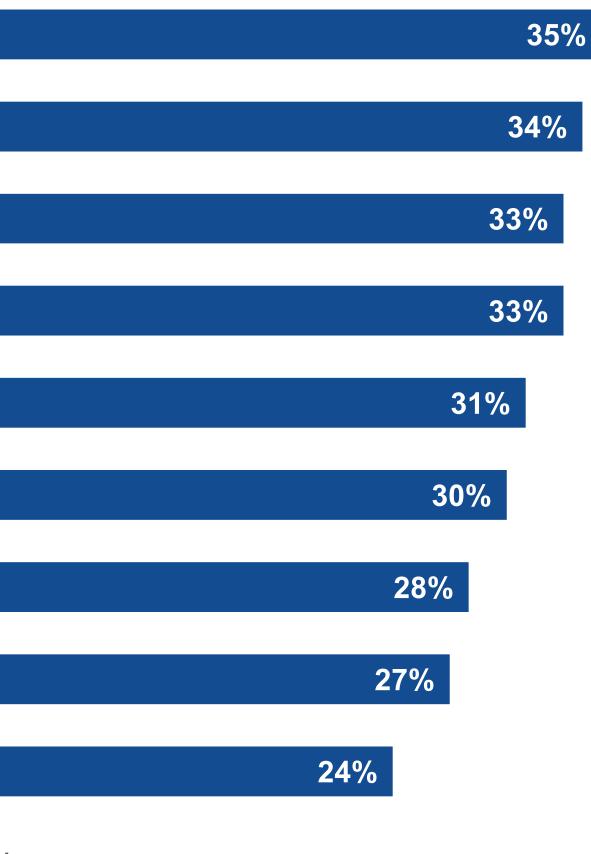
Developers don't know what security actions to take or prioritize

Security team can't keep pace with release cadences

Developers don't want to work with security

None of the above 1%

From a security perspective, rapid application changes introduce many challenges."







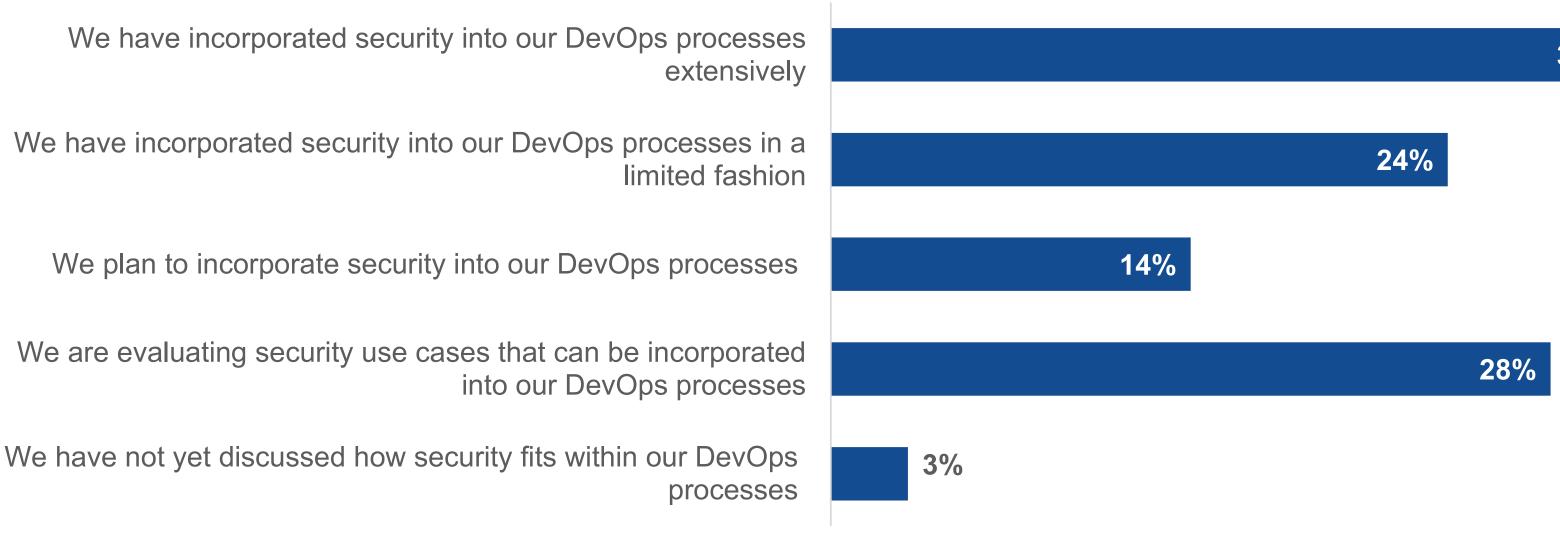


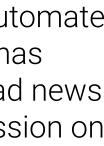
The good news is that 31% of security pros claim their organization has incorporated security into their DevOps process extensively, while another 24% have done so on a limited basis.

Incorporating Security into DevOps

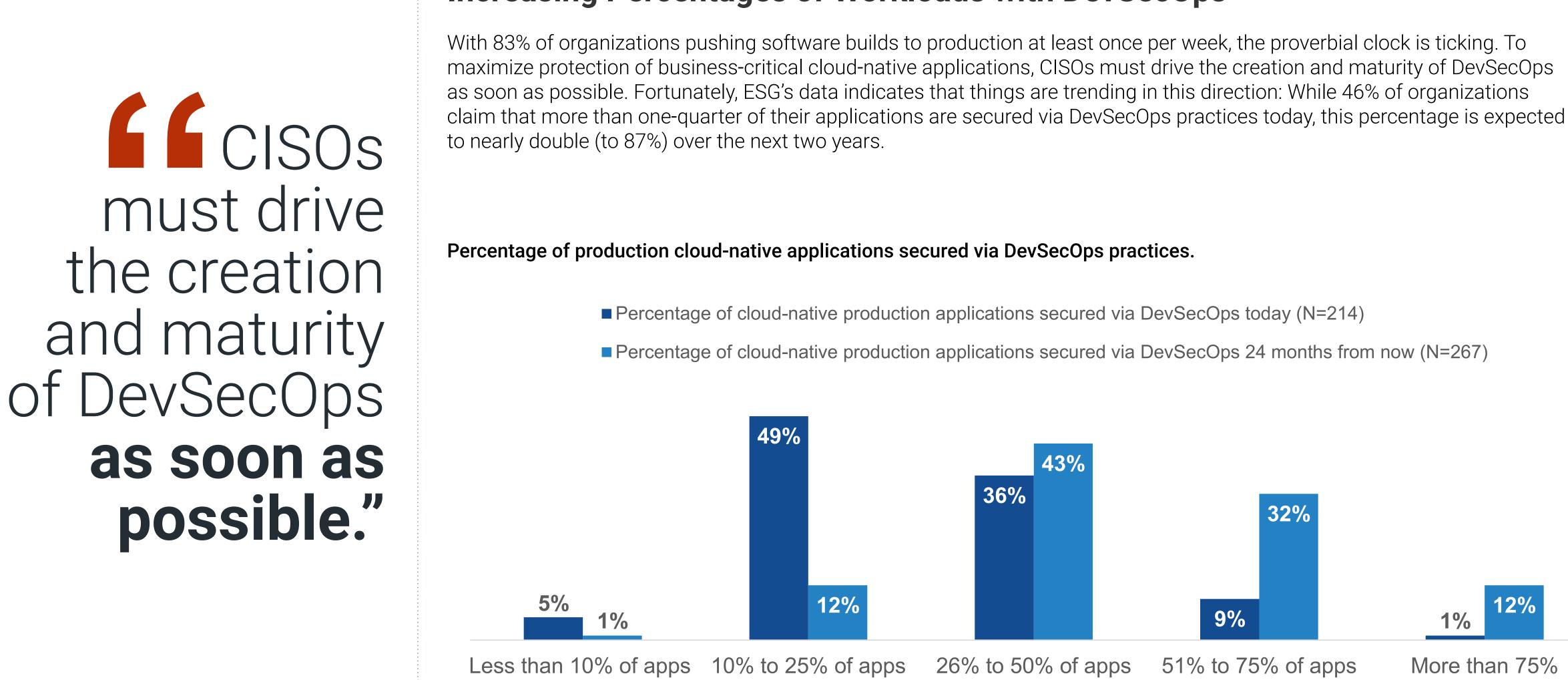
To keep up with the pace of software "pushes" to production, security teams must continually scan the entire cloud application environment, integrate tooling and testing into CI/CD pipelines, and work with cloud operations teams to automate remediation actions. This equates to DevSecOps. The good news is that 31% of security pros claim their organization has incorporated security into their DevOps process extensively, while another 24% have done so on a limited basis. The bad news is that 31% are still evaluating how security can be incorporated into DevOps processes or haven't even begun a discussion on DevSecOps.

Extent to which organizations plan to incorporate security processes and controls into DevOps processes.









Increasing Percentages of Workloads with DevSecOps

Cloud Detection and Response: Market Growth as an Enterprise Requirement

Organizations **Recognize How DevSecOps Helps** with CDR

Aside from adding security to the development process, security professionals agree that DevSecOps can bolster cloud detection and response in several ways. For example, DevSecOps includes threat modeling, introducing an adversary perspective and countermeasures to the development process. DevSecOps also requires advanced security training for developers and cloud operations groups, accelerates remediation activities amid a cyber-attack, and drives improved collaboration.

How DevSecOps processes align with cloud detection and response.

The included threat modeling helps us imagine

The required advanced security training for

Helps us accelerate remediation activities if we

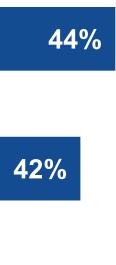
Drives better collaboration, which helps

Helps us automate remediation activities if we

We can use the included detailed application

Helps us discover and fix software vuln

e how adversaries might attack so we can build adequate countermeasures	
or developers and cloud operations groups helps with cloud detection and response	
e experience a cloud-focused cyber-attack	
accolorate threat detection and reasons	
accelerate threat detection and response processes	39%
e experience a cloud-focused cyber-attack	38%
on behavior visibility for security purposes	36%
Inerabilities, decreasing the attack surface	32%





Cloud Security **Operations** Are Increasingly Automated But Remain Challenging



Is Cloud Easing Traditional Security Operations Issues?

As cloud adoption and usage evolves, some see improvements with security operations. Cloud security operations are typically more comprehensive than traditional security operations, with opportunities to ease the burden on security teams. It follows then that half of survey respondents believe that security operations are easier today than they were two years ago. These individuals are focused on cloud security, so these results could be related to factors like organizations' adoption of DevSecOps, security automation through CI/CD pipelining, and the tight integration between CDR and CSPM.



31%

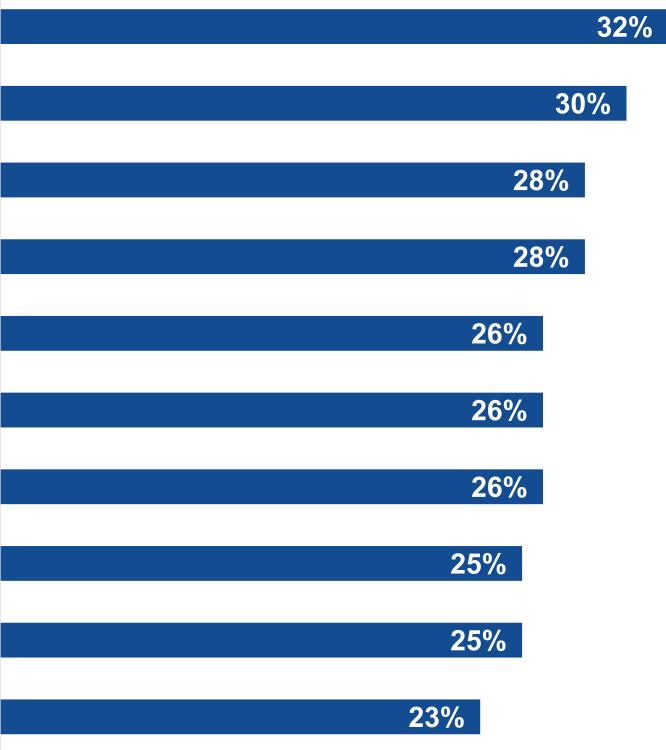
believe that security operations are **more** difficult than they were two years ago.

Top 10 reasons security operations have become more difficult.

We have been unable to automate complex tasks We have gaps in our security monitoring tools and processes leading to scalability problems The volume and complexity of security alerts have increased My organization's increased use of public cloud services The threat landscape is evolving and changing rapidly

The attack surface has grown and/or is continuously changing and evolving Security operations are based upon a significant number of manual processes, It is difficult for my organization to develop detection rules in a timely manner We collect and process more security data today than we did two years ago It is difficult for my organization to tune security controls in a timely manner

While this is a net positive, nearly one-third (31%) believe that security operations are more difficult than they were two years ago, due to factors like the inability to automate processes, a growing attack surface, and monitoring gaps. This could be from trying to manage cloud security with traditional tools that aren't made for the complexity of how the applications run in the cloud. Since these issues greatly increase cybersecurity risk and ultimately business risk, rectifying them should be a high priority across the organization.





Biggest SecOps Challenges for Cloud Applications

Similarly, SecOps is challenged with the complexity of securing cloud-native applications because of the higher speed and volume of releases, plus highly distributed applications with microservices-based architectures using dynamic, ephemeral resources. While some organizations have improved security operations, all firms still face a number of SecOps challenges like keeping up with accelerated application change velocity, dealing with attack surface complexity, collaborating with new/more stakeholders, and an increasing volume of cloud application vulnerabilities. Clearly, cloud security demands greater scale, rapid data analysis, and more process automation.

Biggest SecOps challenges for organizations' cloud applications.

Increasing change velocity (i.e., shift-left, DevOps, and speed and volume of releases) is requiring us to prepare different skills and engage more deeply with application development teams

The complexity of the attack surface and the ephemeral nature of modern cloud workloads is not well supported by our existing technology

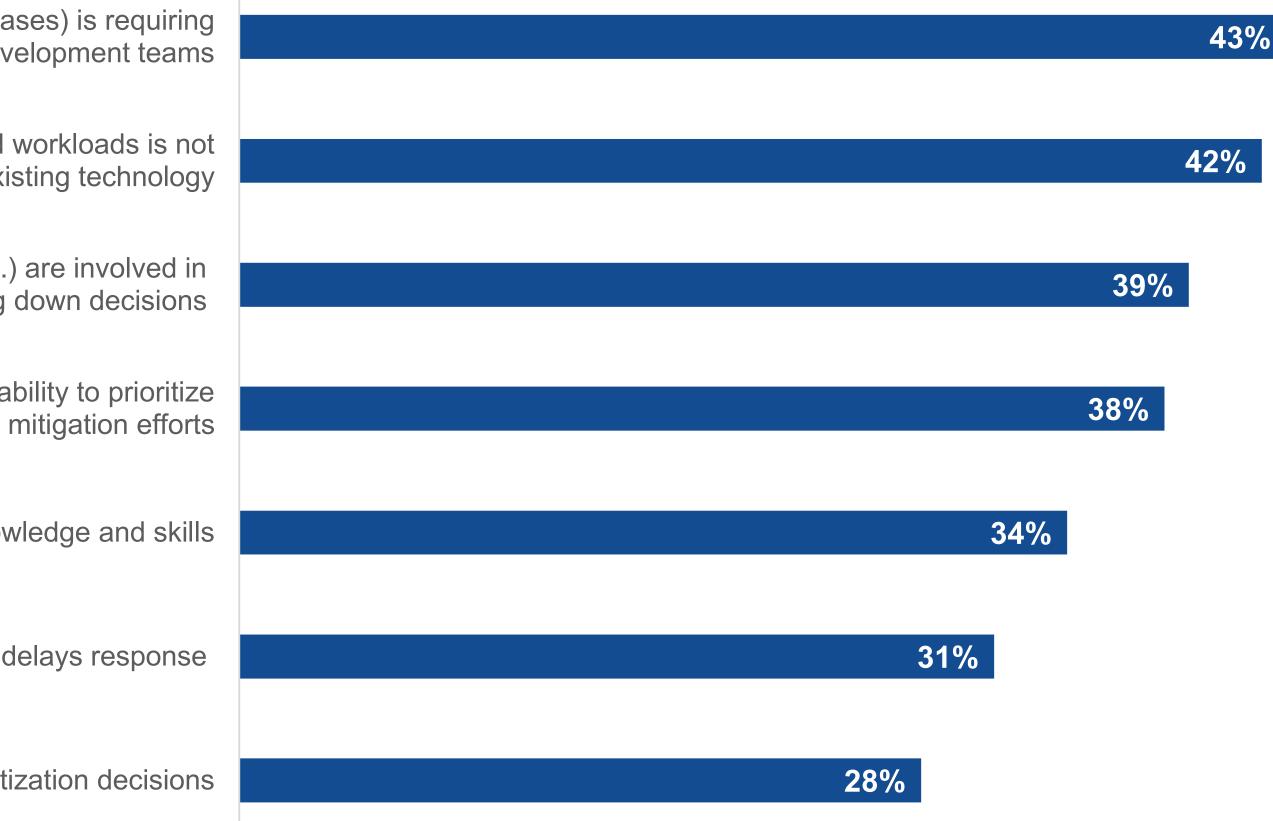
New/more stakeholders (e.g., cloud architects, shift-left-app developers, etc.) are involved in security decisions, adding complexity and slowing down decisions

The increased number of vulnerabilities and security alerts challenges our ability to prioritize

The security operations team lacks adequate cloud security knowledge and skills

Attack surface complexity slows investigations and response decisions and delays response

Visibility gaps across the attack surface make it challenging to make risk and prioritization decisions







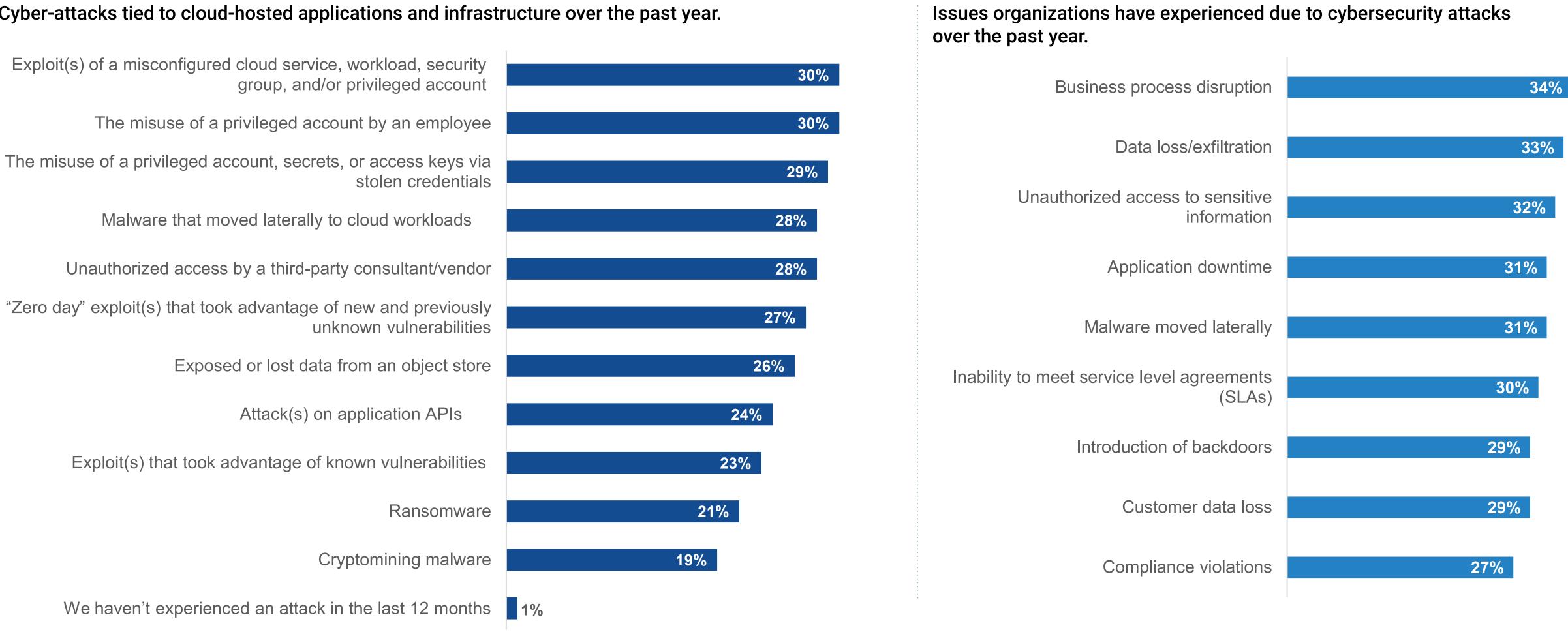
Cloud Detection and Response Is a Work in Progress



Impacts of Cybersecurity Attacks Occurring During Response Time

Nearly all organizations have suffered at least one cyber-attack over the past 12 months, including those caused by exploitation of a misconfigured cloud service; the misuse of a privileged account by an employee; the misuse of a privileged account, secrets, or access keys via stolen credentials; and unauthorized access by a third party. These incidents can be costly, resulting in business process disruption, data loss or exfiltration, unauthorized access to sensitive data, or application downtime.

Cyber-attacks tied to cloud-hosted applications and infrastructure over the past year.

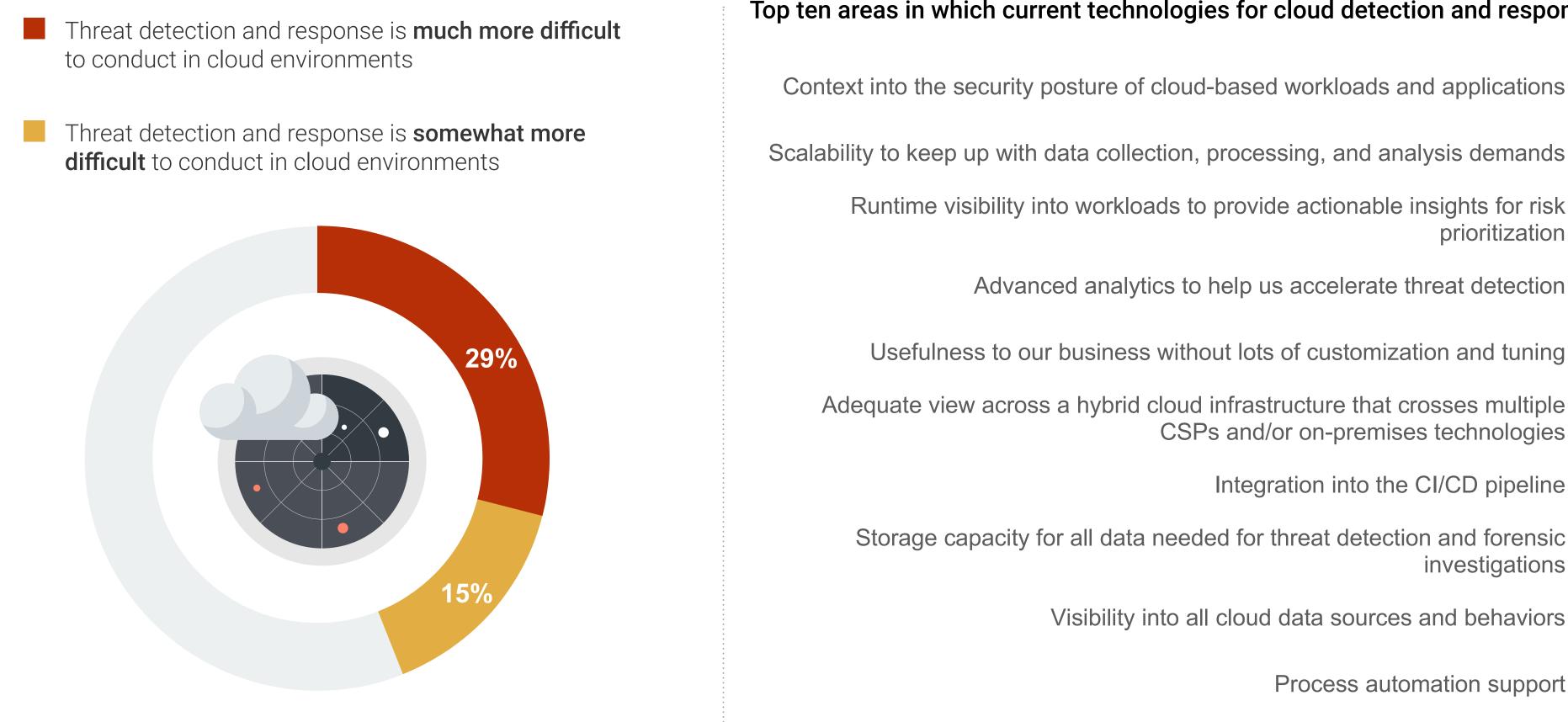




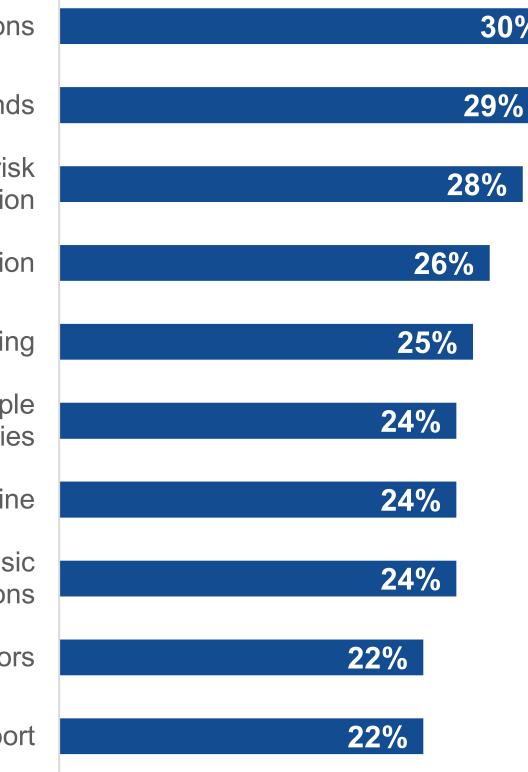
Areas Lacking for CDR

Combating cyber-attacks requires strong CDR, but it's worth noting that 44% of respondents claim that threat detection and response is more difficult for their organizations to conduct in cloud environments. Why? Aside from the use of a multitude of different tools, cloud security professionals identified specific areas where their current CDR tools are lacking. The list includes cloud-based security posture context, scalability, runtime visibility into risk prioritization, advanced analytics, and intuitive business value.

To address these deficiencies, CISOs should make them requirements for all RFIs and RFPs. Alternatively, CDR vendors should address every lacking area as part of marketing communications and sales presentations.



Top ten areas in which current technologies for cloud detection and response are lacking.



Scalability to keep up with data collection, processing, and analysis demands Runtime visibility into workloads to provide actionable insights for risk

prioritization

Advanced analytics to help us accelerate threat detection

Usefulness to our business without lots of customization and tuning

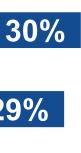
Adequate view across a hybrid cloud infrastructure that crosses multiple CSPs and/or on-premises technologies

Integration into the CI/CD pipeline

Storage capacity for all data needed for threat detection and forensic investigations

Visibility into all cloud data sources and behaviors

Process automation support



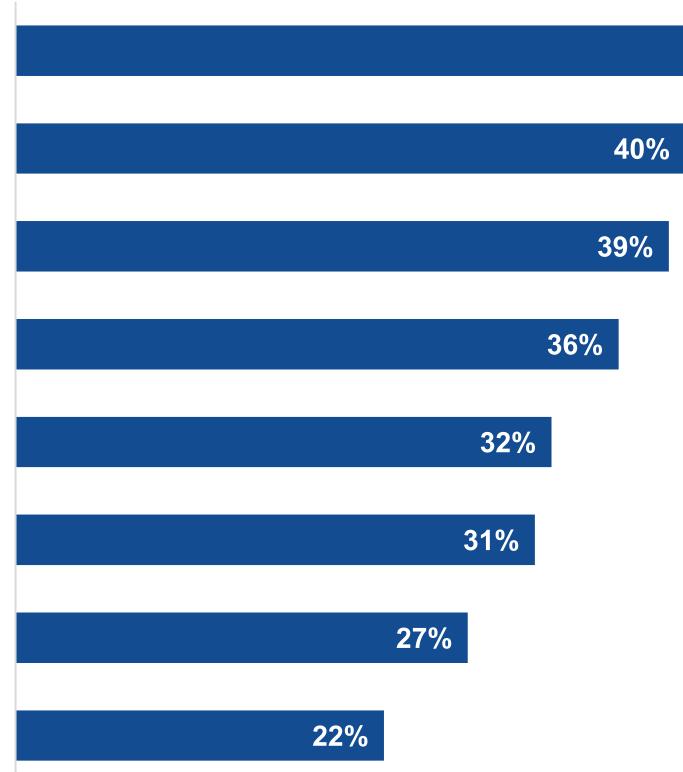
Organizations are using a plethora of tools for cloud threat detection and response today, such as XDR, a dedicated SIEM (i.e., one dedicated to cloud security operations), a central SIEM (i.e., a SIEM with coverage that spans hybrid IT), thirdparty tools, CSP security tools, and dedicated CDR tools."

Organizations Use a Variety of Tools for Cloud Threat Detection and Response

Tools used for cloud threat detection and response.

Extended detection and response tools A dedicated SIEM platform A central SIEM platform A dedicated cloud detection and response tool Multiple SIEM platforms and/or data lakes Open source tools

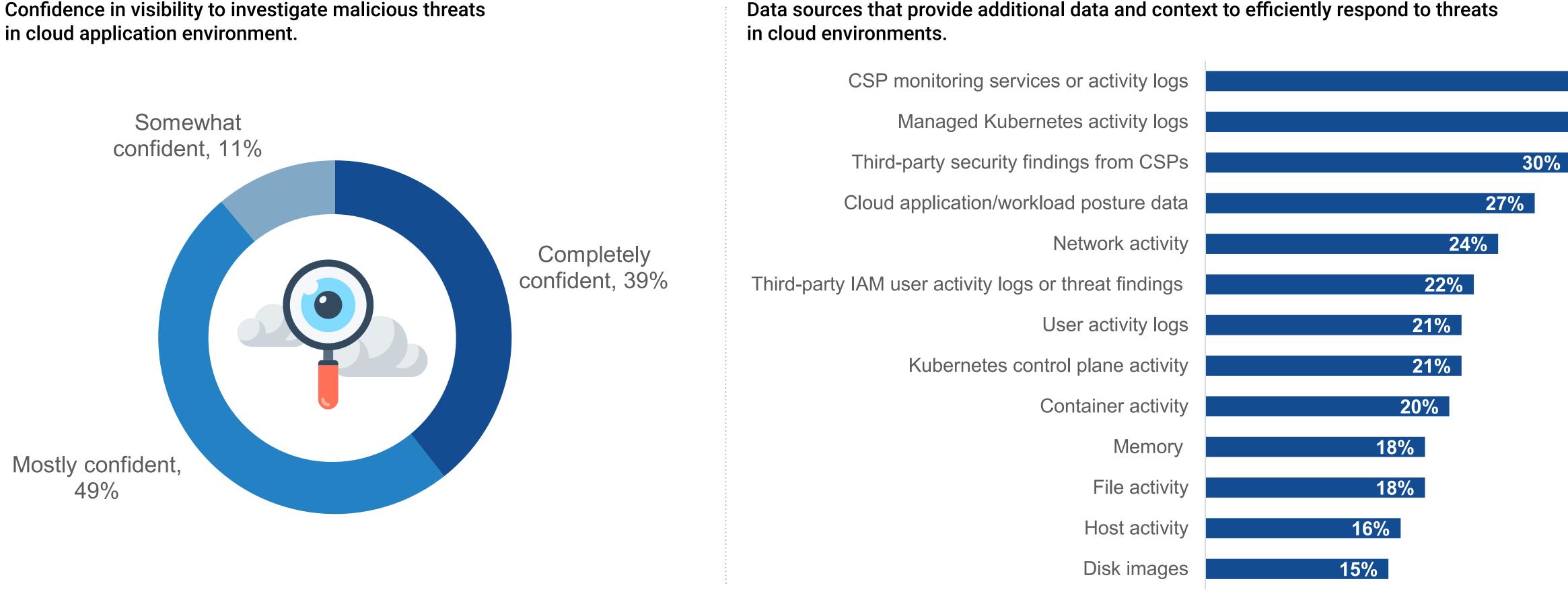
Third-party security solutions for cloud detection and response Security solutions native to the cloud service provider's platform



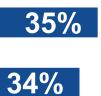


Data Sources with the Most Insight for CDR

The majority of organizations are only mostly (49%) or somewhat (11%) confident in their ability to investigate a cloud-focused cyber-attack, demonstrating that they likely have some issues with data sources. The most common of these include CSP monitoring services/logs, managed Kubernetes activity logs, third-party findings from CSPs, CSPM, network activity, IAM logs, and user activity logs.



Data sources that provide additional data and context to efficiently respond to threats



Monitoring Cloud Environments with Agents

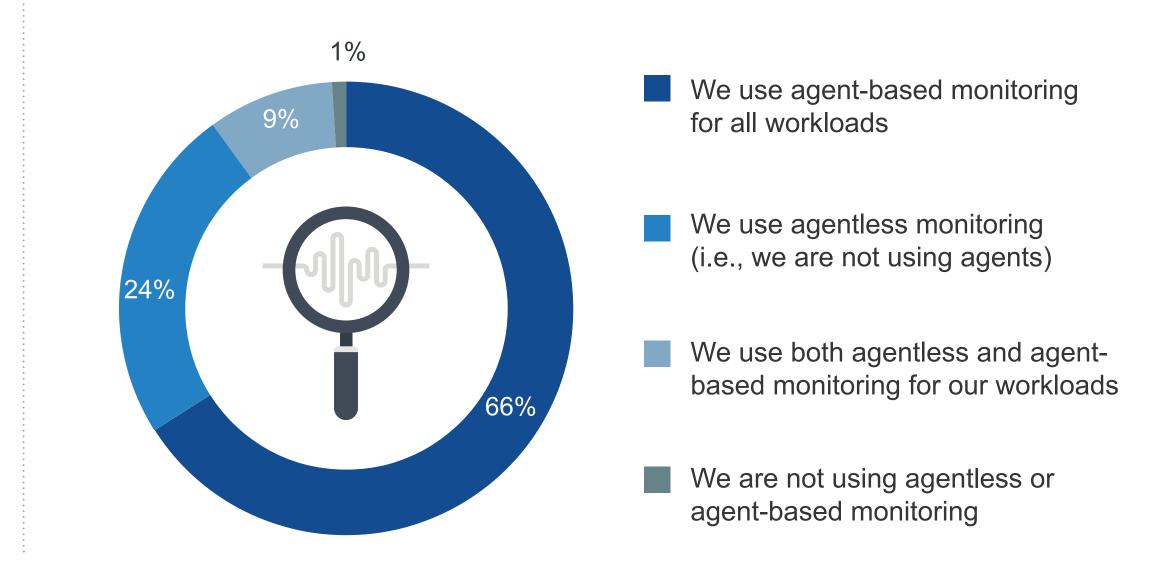
Most organizations are using agent-based monitoring for their cloud applications. Specifically, two-thirds take an agent-based approach for all applications/workloads, while 9% use a combination of agent-based and agentless monitoring. For organizations using agents, the majority find them mostly (39%) or completely (57%) effective in helping with detection, investigation, and response. Agent technology can certainly provide deep and specific visibility into cloud workloads, but using agents comes with some compromises. Cloud security professionals should use them prudently to gain strong visibility but understand that they may require extra care and feeding.

Effectiveness of agent-based detection and monitoring in cloud applications/workloads.

It is completely effective, 57%

An additional 3% said it is somewhat effective.

Use of agent-based or agentless approaches to monitor and/or detect security issues in cloud applications/workloads.

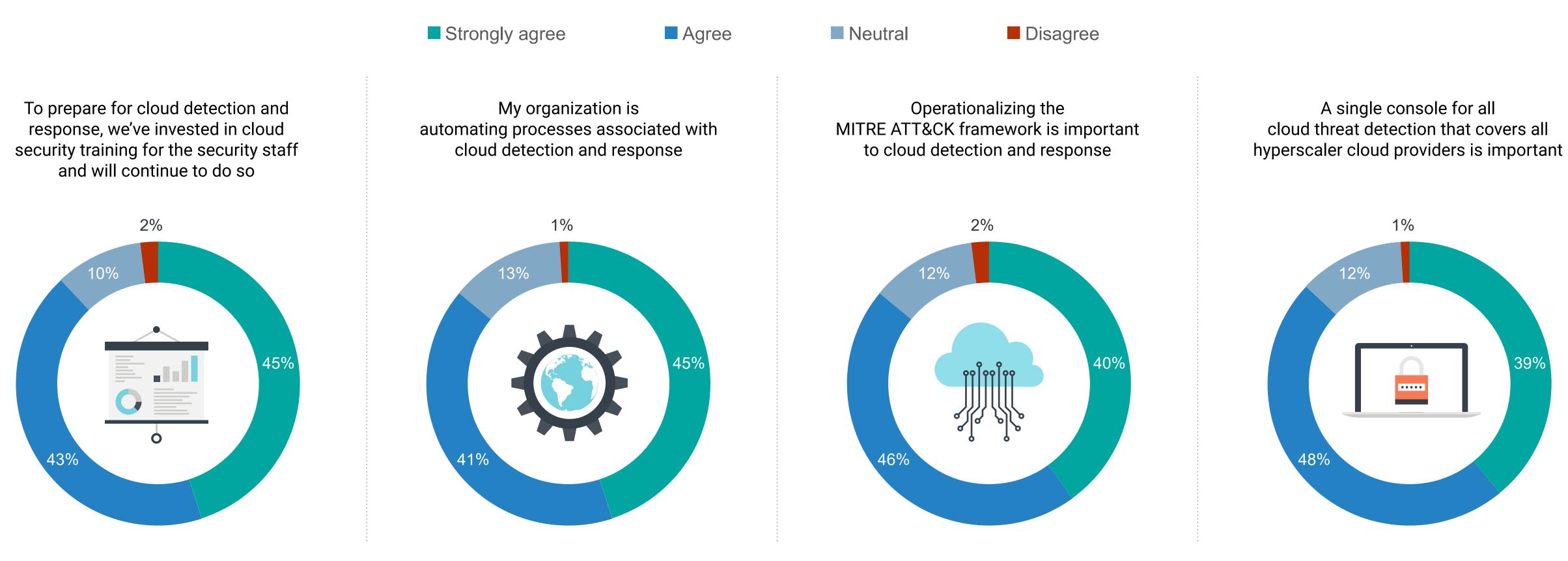


It is mostly effective, 39%

1009

Opinions on Improving CDR

Cloud security professionals have strong opinions on what their organizations are doing and need to do to improve cloud detection and response. For example, organizations have increased cloud security training and automated CDR processes, and they also believe it is important to operationalize the MITRE ATT&CK framework and move to a single CDR console that can span multiple hyperscale cloud providers. CDR tools will need strong support of these requirements.





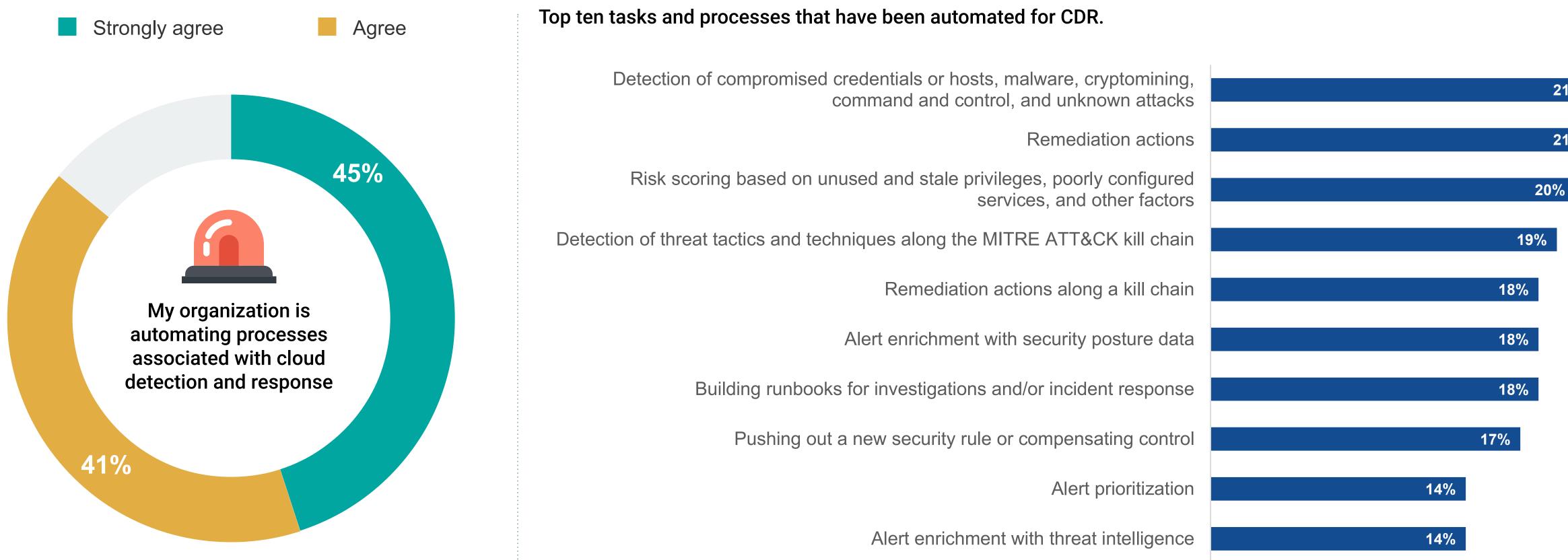




Using Automation for CDR

Eighty-six percent of cloud security professionals say that their organizations are automating processes for CDR. Processes being automated include detection of compromised assets, remediation actions, risk scoring, and threat detection based on the MITRE ATT&CK framework.

Process automation is already well established in DevSecOps in an effort to "shift left," but that is not enough on its own. Security operations should plan for inevitable cyber-attacks by automating CDR activities like data enrichment, alert correlation, and incident response. It appears cloud security operations teams have begun this endeavor.











24

Cloud Detection and Response Is a Shared Responsibility That Requires Continuous Training

-18,22 -18,37 pg tepert (ert* treamy* treamy*

ClocksPerSec - Float64(138)

03:40:44:21



CDR Responsibilities Are Commonly Shared by Cloud **Engineering and SOC Teams**

Just who owns cloud detection and response processes? The data shows an assortment of models in which SOC teams and cloud teams share responsibility evenly, where cloud engineering and security teams take the lead, and where SOC teams have primary responsibility. In some cases, CDR is ceded to security engineering or application owners.

Responsibility for CDR processes and activities.



45%

Our SOC team and cloud engineering and security teams share responsibility evenly



37% Our security engineering and security teams



45% Our cloud engineering and security teams with some help from the SOC team



39%

Our SOC team with some help from cloud engineering and security teams



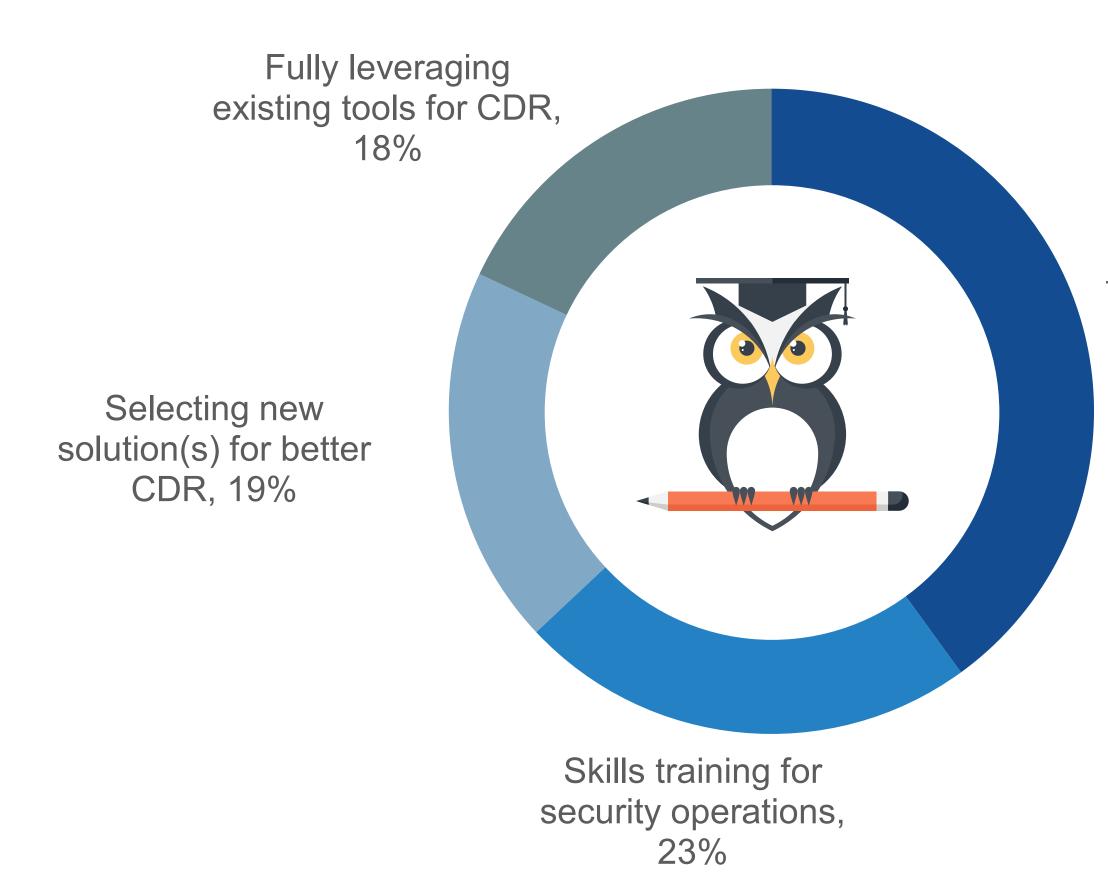
33% Cloud application owners



27% Our SOC team

Highest Priority for CDR Is Training

Highest priority task for cloud detection and response.



Cloud security training for security operations, 40%

When asked to identify their organization's highest priority for CDR, respondents pivoted sharply to skills improvement, with 40% saying cloud security training for security operations and 23% citing skills training for security operations."



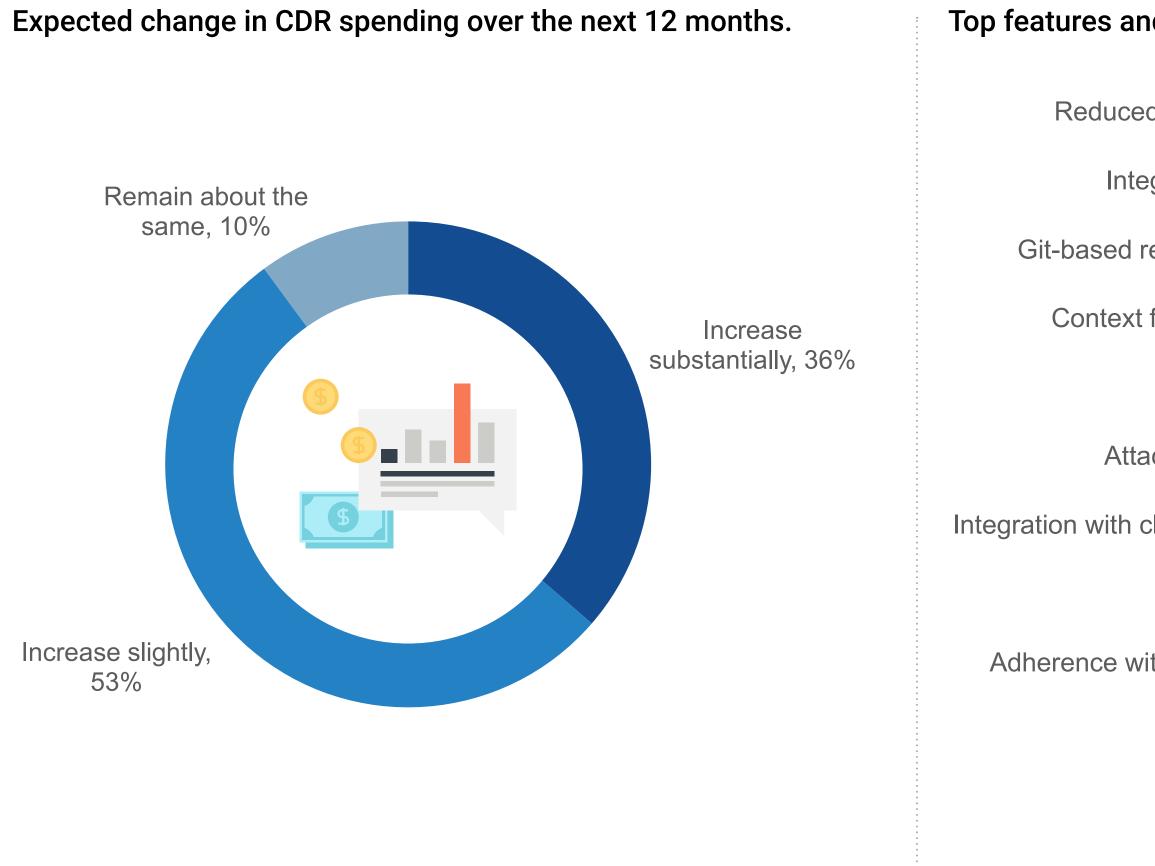


CDR Spending Is Growing as **Cloud Security** Professionals' List of Technology Requirements Expands



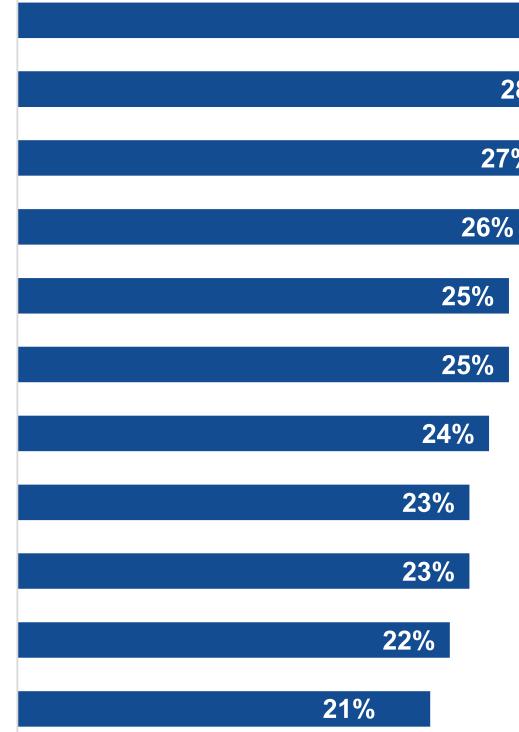
Most Organizations Are Increasing CDR Spending for Features Driving Increased Efficiency and Speed

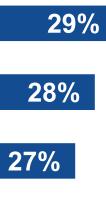
The majority of organizations plan to increase CDR spending in the next 12 months either substantially (36%) or at least slightly (53%). As they do, they will look for CDR solutions that can automate manual tasks, integrate with application security and DevSecOps practices, offer git-based remediation features, and provide context for alerts and threat prioritization, among other needs.



Top features and capabilities needed to improve CDR.

Reduced/automation of manual tasks for security operations teams Integration with application security and DecSecOps practices Git-based remediation features to better enable developer's workflows Context for alert and threat prioritization from different data sources Workflow automation to speed response activities Attack path modeling to predict vulnerability/exposure to attack Integration with cloud security posture management solution and/or CNAPP Threat research/threat intelligence Adherence with best practices and frameworks such as MITRE ATT&CK Tools for forensic investigation Automation of data capture and processing











Sysdig

Sysdig helps companies secure and accelerate innovation in the cloud. Powered by runtime insights, the cloud security platform stops threats in real time and reduces vulnerabilities by up to 95%. Rooted in runtime, the company created Falco, the open source solution for cloud threat detection. By knowing what is running in production, Dev and security teams can focus on the risks that matter most. From shift left to shield right, the most innovative companies around the world rely on Sysdig to prevent, detect, and respond at cloud speed.

LEARN MORE

ABOUT ENTERPRISE STRATEGY GROUP

TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

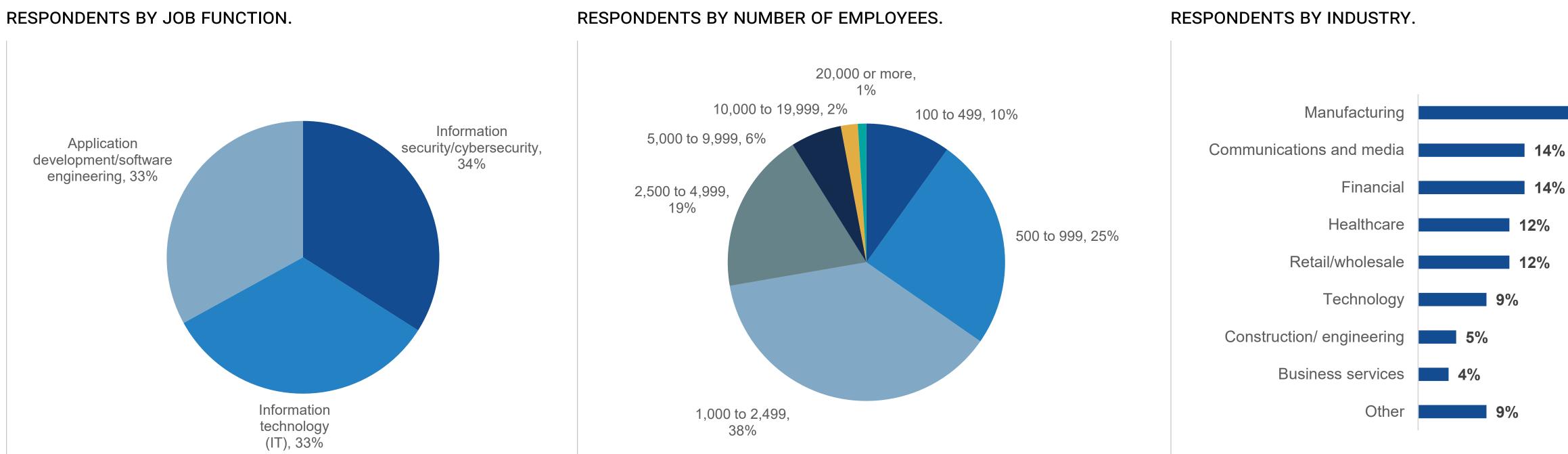




Research Methodology and Demographics

To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between May 23, 2023 and June 2, 2023. To qualify for this survey, respondents were required to be responsible for evaluating or purchasing cloud security technology products and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 393 IT and cybersecurity professionals.





21%

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations ir currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statement.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2023 TechTarget, Inc. All Rights Reserved.

get, Inc. light of ements