CLOUD SECURITY REPORT

CHECK POINT™

YOU DESERVE THE BEST SECURITY

INTRODUCTION

Cloud adoption continues to permeate throughout organizations as they embrace agile software development. While they are seeing great dividends in cost-effectiveness and flexibility, building security throughout the software development lifecycle is proving to be difficult, citing increased misconfigurations from user error. At the moment, there is a severe learning curve around DevSecOps and organizations are struggling to find the right expertise to plug this knowledge gap.

Key Survey Findings Include:

- Up 10% from last year, a quarter of organizations (27%) have experienced a public cloud security incident. This year misconfigurations (23%) have clinched the top position as the number one security-related incident, surpassing exposed data by user (15%) and account compromise (15%) from last year.

- Organizations continue to rely on multi-cloud solutions with 76% of respondents using two or more cloud providers, compared to just 62% from the previous year. While cost (61%) and ease of use (58%) initially drove their security decision between cloud-native versus independent cloud security solutions, managing multiple cloud vendors has created a greater complexity than first imagined.

- It's clear organizations are embracing more agile software development. Today, 35% of respondents have more than 50% of their workloads in the cloud, with 29% stating that they anticipate moving this number up to 75% of workloads in the cloud in the next 12-18 months.

- 61% of respondents have already integrated their DevOps toolchain into cloud deployments, yet organizations are still struggling with the lack of expertise that bridges security and DevOps. Only 16% of respondents have comprehensive DevSecOps in place, with 37% starting to incorporate some aspect of DevSecOps within the organization.

We would like to thank CheckPoint for supporting this important industry research project. We hope you'll find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
I N S I D E R S
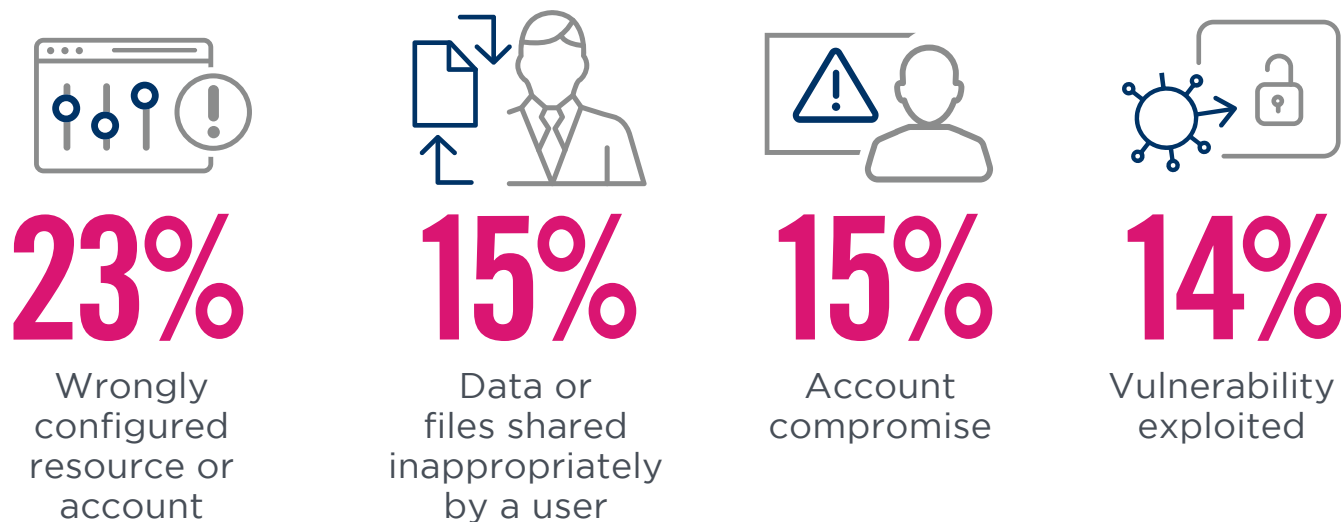
BACKGROUND

Current state of cloud and workloads

CLOUD SECURITY INCIDENTS

A quater of organizations (27%) have experienced a public cloud related security incident; up 10% from last year. This year misconfigurations (23%) have clinched the top position as the number one security related incident, surpassing exposed data by user (15%) and account compromise (15%) from last year.

▶ **Did your organization experience a public cloud related security incident in the last 12 months?**

27%
YES

73%
NO

▶ **If yes, what type of incident was it?**

23%
Wrongly configured resource or account

15%
Data or files shared inappropriately by a user

15%
Account compromise

14%
Vulnerability exploited

Data or files uploaded to an unsanctioned cloud resource 12% | Malware infection 9% | Data or files downloaded to an unsafe device 9% | Other 8%

CLOUD PROVIDERS AND PRIORITIES

With 76% of respondents using two or more cloud providers, top security priorities, such as preventing misconfigurations, securing cloud apps, and reaching regulatory compliance are multiplied, resulting in multiple threats, work and headcount.

▶ **How many cloud providers does your organization currently use?**

76% use two or more cloud providers

22%	34%	18%	24%	2%

■ One ■ Two ■ Three ■ More than 3 ■ None
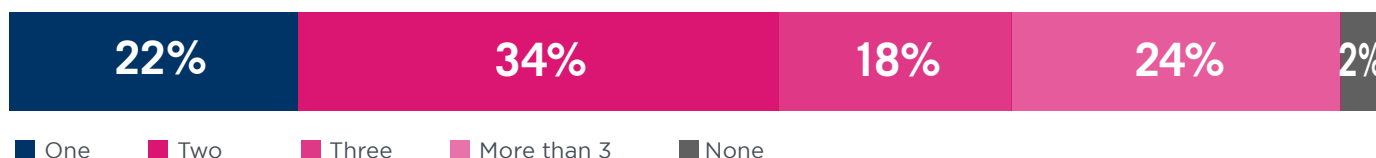
▶ **What are your cloud security priorities for your company this year?**

20%
Preventing cloud misconfigurations

16%
Securing major cloud apps already in use

16%
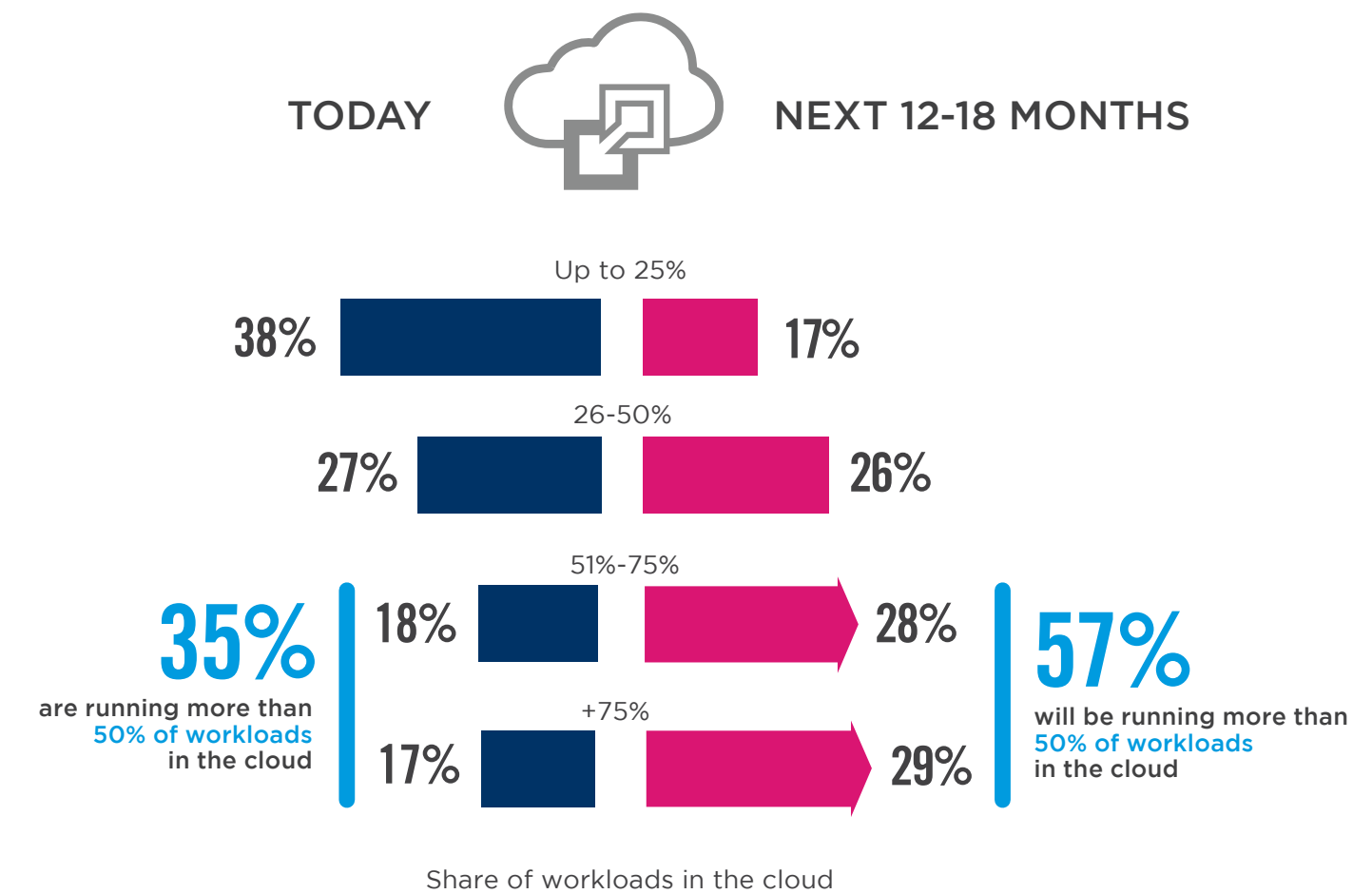Reaching regulatory compliance

13%
Defending against malware

Cloud security training 11% | Securing mobile devices 7% | Discovering unsanctioned cloud apps in use 7% | Securing BYOD (bring your own device) 6% | Securing less popular cloud apps already in use 5%

WORKLOADS IN THE CLOUD

Organizations moving workloads to the cloud are the way forward for most companies. Today, 35% of respondents have more than 50% of their workloads in the cloud, with 29% stating that they anticipate moving this number up to 75% of workloads in the cloud in the next 12-18 months.

▶ **What percentage of your workloads are in the cloud today?**

▶ **What percentage of your workloads will be in the cloud in next 12-18 months?**

TODAY   NEXT 12-18 MONTHS

Up to 25%

38%   17%

26-50%

27%   26%

51%-75%

35%   18%   28%   **57%**
are running more than   will be running more than
50% of workloads   **50% of workloads**
in the cloud   in the cloud

+75%

17%   29%

Share of workloads in the cloud

CLOUD SECURITY CAPABILITIES

With the shift of moving workloads to the cloud, we see that more and more organizations are deploying application protection in the cloud. This security capability has moved up 11% in just a year, clinching the number 3 spot with 53%.

▶ **What security capabilities have you deployed in the cloud?**

72%
Access control

60%
Anti-virus/
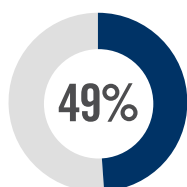anti-malware/
Advanced Threat
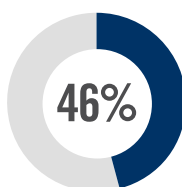Protection (ATP)

53%
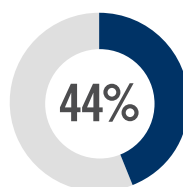Application
protection
(e.g., WAF,
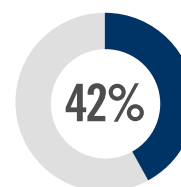scanners, etc.)

53%
Multi-factor
authentication

49%
Data
encryption

46%
Cloud data
backup

44%
Firewalls/
NAC

42%
Vulnerability
assessment

Enpoint security 38% | Network encryption (VPN, packet encryption, transport encryption) 37% |
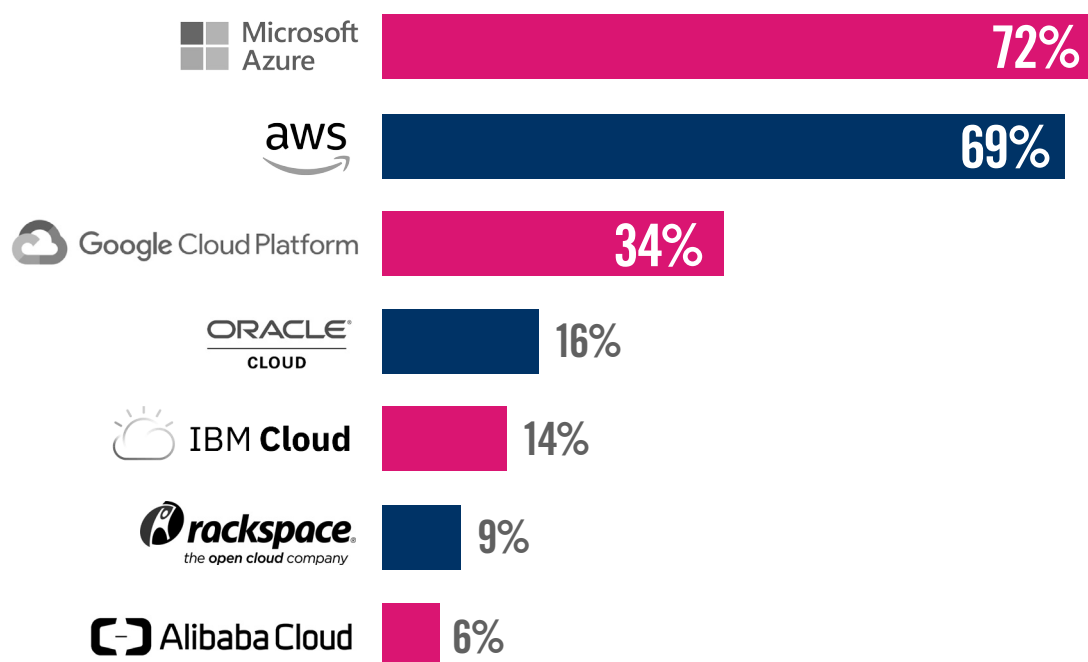Single sign-on/user authentication 37%

MULTI CLOUD CHALLENGES

CLOUD SECURITY PROVIDERS

Seventy-two percent (72%) of respondents are using Microsoft Azure, 69% are using AWS and 34% are using GCP as their IaaS providers, yet 54% of this audience conceded to the fact that cloud security from an independent security vendor is better than these cloud vendors.

▶ **What cloud IaaS provider(s) do you currently use?**

Provider	%
Microsoft Azure	72%
aws	69%
Google Cloud Platform	34%
ORACLE CLOUD	16%
IBM Cloud	14%
rackspace the open cloud company	9%
Alibaba Cloud	6%

▶ **How do you think cloud security from a 3rd-party security vendor compares with cloud security from a cloud vendor?**

54% think that cloud security from an independent security vendor is better than these cloud vendors

11%	43%	41%	4%	1%

Much better   Much worse
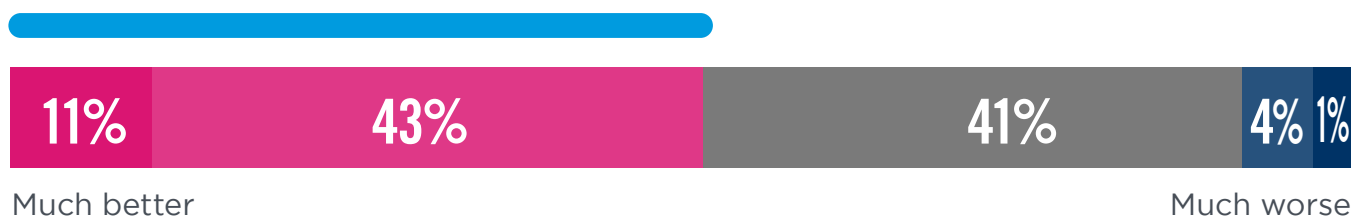
■ Much better   ■ Better   ■ Similar   ■ Worse   ■ Much worse

MULTI-CLOUD SECURITY CHALLENGES

Ensuring data protection and privacy for each environment (57%), having the right skills to deploy and manage a complete solution across all cloud environments (56%), and understanding service integration options (50%) are among the top three multi-cloud challenges. While cost (61%) and ease of use (58%) initially drove respondents' security decision between cloud-native versus independent cloud security solutions, managing multiple cloud vendors has created a greater complexity than first imagined.

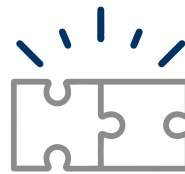▶ **What are your biggest challenges securing multi-cloud environments?**

57%
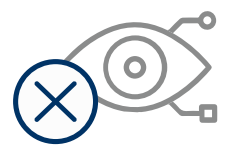Ensuring data protection and privacy for each environment

56%
Having the right skills to deploy and manage a complete solution across all cloud environments

50%
Understanding how different solutions fit together

46%
Loss of visibility and control

Understanding how different solutions fit together 41% | Keeping up with the rate of change 41% | Selecting the right set of services 33%
Providing seamless access to users based on their credentials 33% | Managing the costs of different solutions 30% | Other 3%

▶ **What criteria are most important to you when deciding between cloud native vs. independent cloud security solutions?**
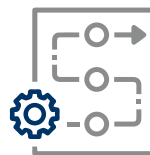
61%
Cost

58%
Ease of use

56%
Less solution complexity and already well integrated

48%
Performance

Quicker deployments 33% | No need to manage another vendor 29% | Cloud vendor security is good enough, why would I need anything else? 13% | Other 8%
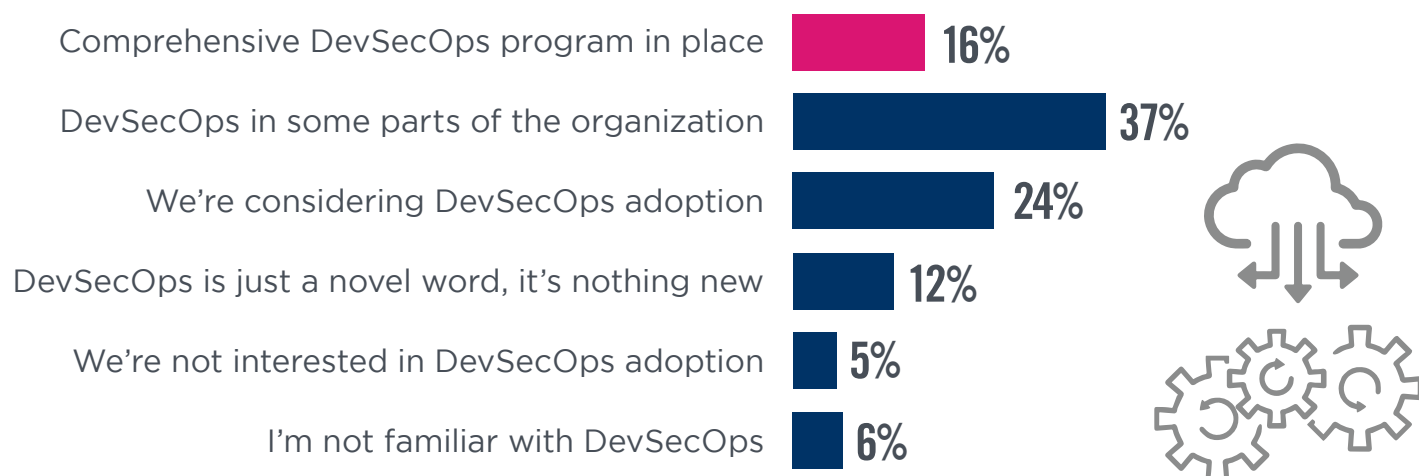
NEED FOR DEVSEC TEAMS

DEVSECOPS ADOPTION

It's clear organizations are embracing more agile software development. Sixty-one percent (61%) of respondents have already integrated their DevOps toolchain into cloud deployments, yet organizations are still struggling with the lack of expertise that bridges security and DevOps.

Only 16% of respondents have comprehensive DevSecOps in place, with 37% starting to incorporate some aspect of DevSecOps within the organization.

▶ **Do you integrate your DevOps toolchain into your cloud deployments?**

61% ⊘	39% ⊗
YES	NO

▶ **What is your organization's current position on DevSecOps?**

Comprehensive DevSecOps program in place **16%**

DevSecOps in some parts of the organization **37%**

We're considering DevSecOps adoption **24%**

DevSecOps is just a novel word, it's nothing new **12%**

We're not interested in DevSecOps adoption **5%**

I'm not familiar with DevSecOps **6%**

AUTOMATION AND ORCHESTRATION TOOLS

Infrastructure-as-a-code (48%), serverless (44%), and plugins for continuous integration and delivery (44%) are the top automation and orchestration tools organizations leverage to aid in security control implementation.

▶ **Which of the following automation and orchestration tools are you leveraging to aid in security controls implementation or processes?**
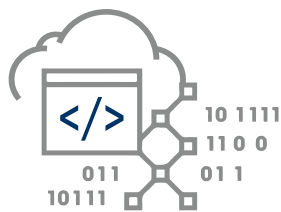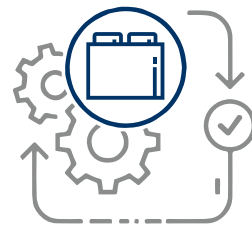
48%
Infrastructure-as-a-code (and security as-a-code) in templates (e.g. Terraform and AWS CloudFormation)
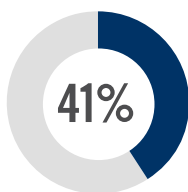
44%
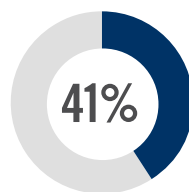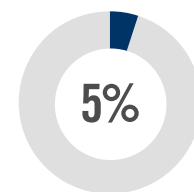Serverless technologies (e.g. Lambda or Azure Functions)

44%
Plugins for Continuous Integration (CI)/ Continuous Delivery (CD) tools (e.g. Jenkins or TeamCity)

41%
Security orchestration, automation and response (SOAR) tools

41%
Configuration orchestration tools (e.g. Chef and Ansible)

5%
Web application firewalls

Microservices (serverless and containers) 4% | Security Information Event Management (SIEM) 4% | Microsegmentation 2% | Cloud Infrastructure and Entitlements Management (CIEM) 1% | Other 5%

DEVOPS SECURITY CHECKS

When asked what stage(s) of your Software Development Life Cycle (SDLC) do you have DevOps security and/or compliance checks, respondents indicated the following: system testing and production (52%), feature development and unit testing (42%), and staging (42%).

▶ **In what stage(s) of your Software Development Life Cycle (SDLC) do you have DevOps security and/or compliance checks?**

52%
System testing
and production

42%
Feature development
and unit testing

42%
Staging

We don't have security or compliance checks 10% | Other 27%

KNOWLEDGE AND SKILLS GAP

OPERATIONAL SECURITY HEADACHES

Forty-five percent (45%) of respondents cited lack of qualified staff as their biggest day-to-day headache trying to protect cloud workloads. Followed by compliance (39%) and lack of visibility into infrastructure security (35%).

▶ **What are your biggest operational, day-to-day headaches trying to protect cloud workloads?**
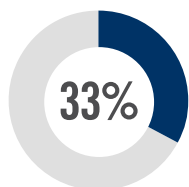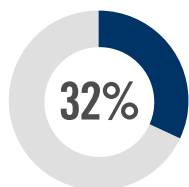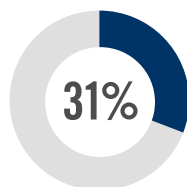
45%
Lack of qualified staff

39%
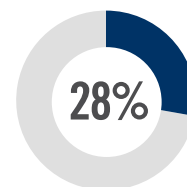Compliance

35%
Lack of visibility into infrastructure security

33%
Can't identify misconfigurations quickly

32%
Setting consistent security policies

31%
Implementing continuous and automated security controls in the cloud

28%
Automatically enforcing security across multiple clouds

Setting the correct user access privileges 27% | Security can't keep up with the pace of changes to new/existing applications 25% | Securing access from personal and mobile devices 25% | Justifying more security spend 24% | Lack of integration with on-prem security technologies 24% | Securing traffic flows 24% | Complex cloud to cloud / cloud to on-prem security rule matching 23% | Reporting security threats 21% | No automatic discovery/visibility/control to infrastructure security 21% | Remediating threats 21% | Understanding network traffic patterns 19% | Lack of feature parity with on-prem security solution 14% | Not sure/other 14%

CLOUD COMPLIANCE CHALLENGES

Lack of qualified staff and knowledge (55%) was also echoed as the most challenging aspect of cloud compliance currently.

▶ **Which part of the cloud compliance process is the most challenging?**

55%
Lack of staff expertise/ knowledge

43%
Continuously staying in compliance, as cloud environment changes

42%
Going through audit/ risk assessment within the cloud environment
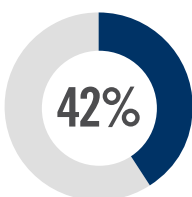
42%
Monitoring for compliance with policies and procedures
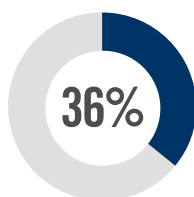
36%
Staying up to date about new/changing compliance and regulatory requirements
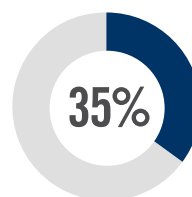
35%
Monitoring for new vulnerabilities in cloud services that must be secured
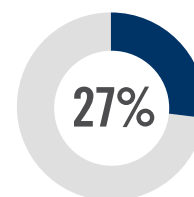
27%
Scaling and automating compliance activities

Data quality and integrity in regulatory reporting 22% | Applying/following the Shared Responsibility Model 22% |
Not sure/other 9%

SINGLE PLATFORM TO SUPPORT NATIVE CLOUD

SECURITY IN PUBLIC CLOUDS

Being able to streamline cloud security would help greatly, considering that 72% of organizations are still concerned about the security of public clouds, with 52% of organizations only moderately confident in their cloud security posture.

▶ **How concerned are you about the security of public clouds?**

72% of organizations are extremely to very concerned about cloud security

30%	42%	23%	4%	1%
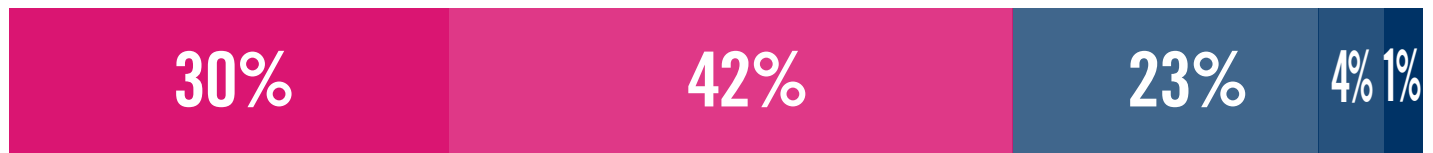
Extremely concerned   Not at all concerned

■ Extremely concerned ■ Very concerned ■ Moderately concerned ■ Slightly concerned ■ Not at all concerned

▶ **How confident are you in your organization's cloud security posture?**

52% of organizations are moderately confident in their cloud security posture

6%	24%		12%	6%

Extremely confident   Not at all confident

■ Extremely confident ■ Very confident ■ Moderately confident ■ Slightly confident ■ Not at all confident

SINGLE DASHBOARD PLATFORM

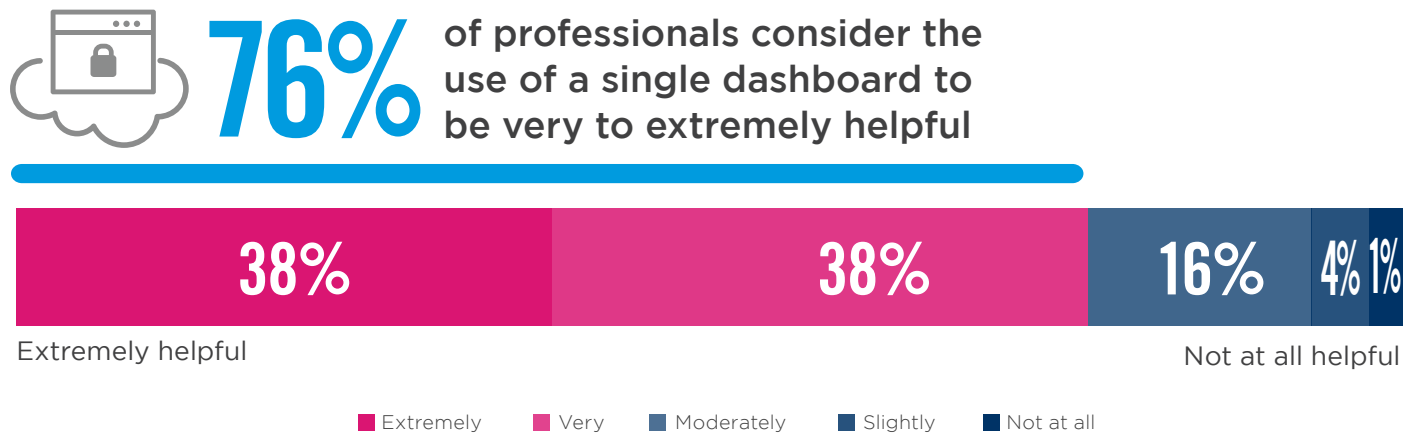It's no surprise that over 75% of respondents cited the need for a single cloud security platform with a single dashboard where they could configure all of the policies needed to protect data consistently and comprehensively across their cloud footprint. Currently, 80% of users have to access 3 or more separate security solutions dashboards to configure their enterprise's cloud policies.

▶ **How helpful would it be to have a single cloud security platform with a single dashboard where you could configure all of the policies needed to protect data consistently and comprehensively across your cloud footprint?**

76%
of professionals consider the use of a single dashboard to be very to extremely helpful

38%	38%	16%	4%	1%

Extremely helpful   Not at all helpful

■ Extremely   ■ Very   ■ Moderately   ■ Slightly   ■ Not at all
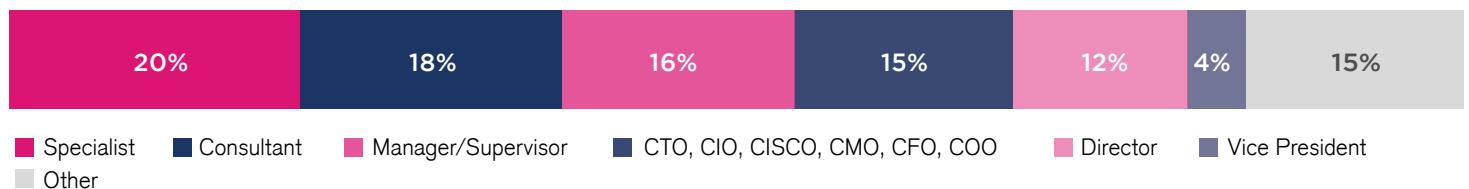
Not sure 3%

▶ **How many separate security solutions do your users have to access to configure the policies that secure your enterprise's entire cloud footprint?**

80%
have to access 3 or more dashboards to configure their enterprise's cloud policies

20%	41%	24%	6%	3%	6%

■ 1-2   ■ 3-4   ■ 5-6   ■ 7-8   ■ 9-10   ■ More than 10
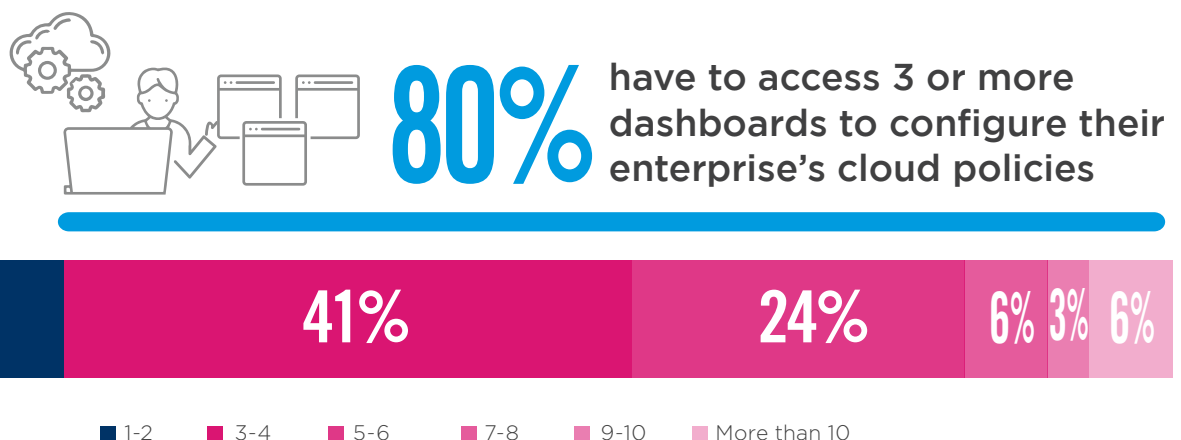
METHODOLOGY & DEMOGRAPHICS

The 2022 Cloud Security Report is based on a comprehensive survey of 775 cybersecurity professionals conducted in January 2022, to uncover how cloud user organizations are responding to security threats in the cloud, and what training, certifications, and best practices IT cybersecurity leaders are prioritizing in their move to the cloud. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.
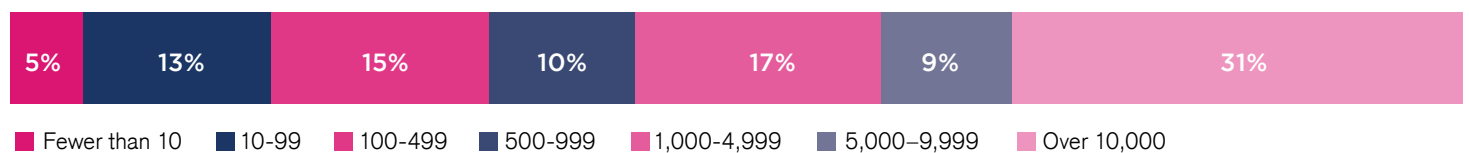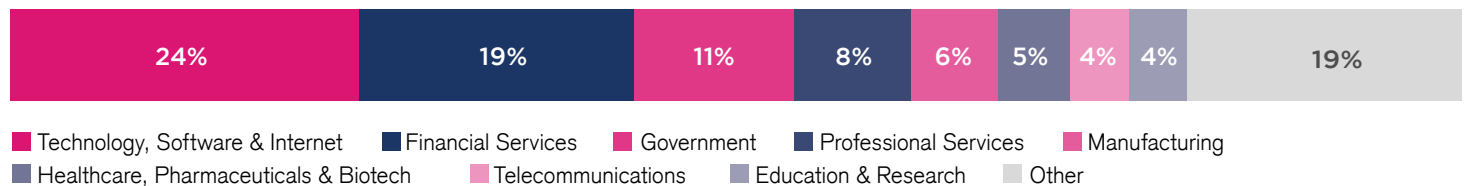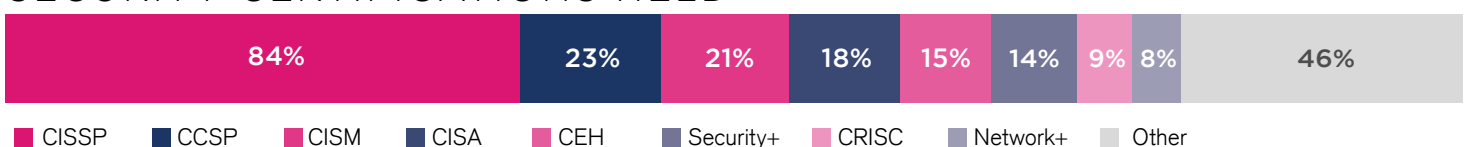
CAREER LEVEL

20%	18%	16%	15%	12%	4%	15%

■ Specialist ■ Consultant ■ Manager/Supervisor ■ CTO, CIO, CISCO, CMO, CFO, COO ■ Director ■ Vice President
■ Other

DEPARTMENT

54%	16%	7%	4%	3%	3%	13%

■ IT Security ■ IT Operations ■ Engineering ■ Operations ■ Product Management ■ Compliance ■ Other

COMPANY SIZE

5%	13%	15%	10%	17%	9%	31%

■ Fewer than 10 ■ 10-99 ■ 100-499 ■ 500-999 ■ 1,000-4,999 ■ 5,000–9,999 ■ Over 10,000

INDUSTRY

24%	19%	11%	8%	6%	5%	4%	4%	19%

■ Technology, Software & Internet ■ Financial Services ■ Government ■ Professional Services ■ Manufacturing
■ Healthcare, Pharmaceuticals & Biotech ■ Telecommunications ■ Education & Research ■ Other

SECURITY CERTIFICATIONS HELD

84%	23%	21%	18%	15%	14%	9%	8%	46%

■ CISSP ■ CCSP ■ CISM ■ CISA ■ CEH ■ Security+ ■ CRISC ■ Network+ ■ Other

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry-leading catch rate of malware, ransomware, and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network, and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Process efficiencies and increased network agility are driving SaaS, PaaS and IaaS technology adoption at a rapid pace. This new infrastructure is also presenting businesses with a unique set of security challenges. Check Point CloudGuard provides unified cloud native security for all your assets and workloads, giving you the confidence to automate security, prevent threats, and manage posture – everywhere – across your multi-cloud.

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**