2020

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

Check Point®
SOFTWARE TECHNOLOGIES LTD

INTRODUCTION

As organizations migrate more workloads from on-premises and datacenters to the cloud, security concerns remain high as the adoption of public cloud computing continues to surge in the wake of the 2020 COVID crisis and the resulting accelerated shift to remote work environments.

Key survey findings include:

- Security remains a key issue for cloud customers, despite continued rapid adoption of cloud computing. 75% of cybersecurity professionals confirm they are very concerned about public cloud security, a small increase from last year's cloud security survey.
- When asked about what are the biggest security threats facing public clouds, organizations ranked misconfiguration of the cloud platform (68%) highest, up from the third spot on last year's survey. This is followed by unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%).
- Among the key barriers to cloud adoption, organizations mention a lack of qualified staff (37%) as the biggest impediment to faster adoption – up from the fifth spot on last year's survey.
- When selecting a cloud security provider, most organizations look at cost-effectiveness (63%), ease of deployment (53%), and that the security tools are cloud-native (52%) as their key priorities.
- When asked what criteria organizations consider most important when evaluating a cloud security solution they prioritize product features (66%), cost (65%), and vendor experience (55%) as the most important considerations.
- Organizations rely on multi-cloud solutions with most organizations deploying more than three cloud solutions in their environment.

This 2020 Cloud Security Report has been produced by Cybersecurity Insiders to explore how organizations are responding to the evolving security threats in the cloud and the continued shortfall of qualified security staff.

Many thanks to Check Point Software Technologies for supporting this important research project. We hope you find this report informative and helpful as you continue your efforts in securing your cloud environments.

Thank you,

Holger Schulze

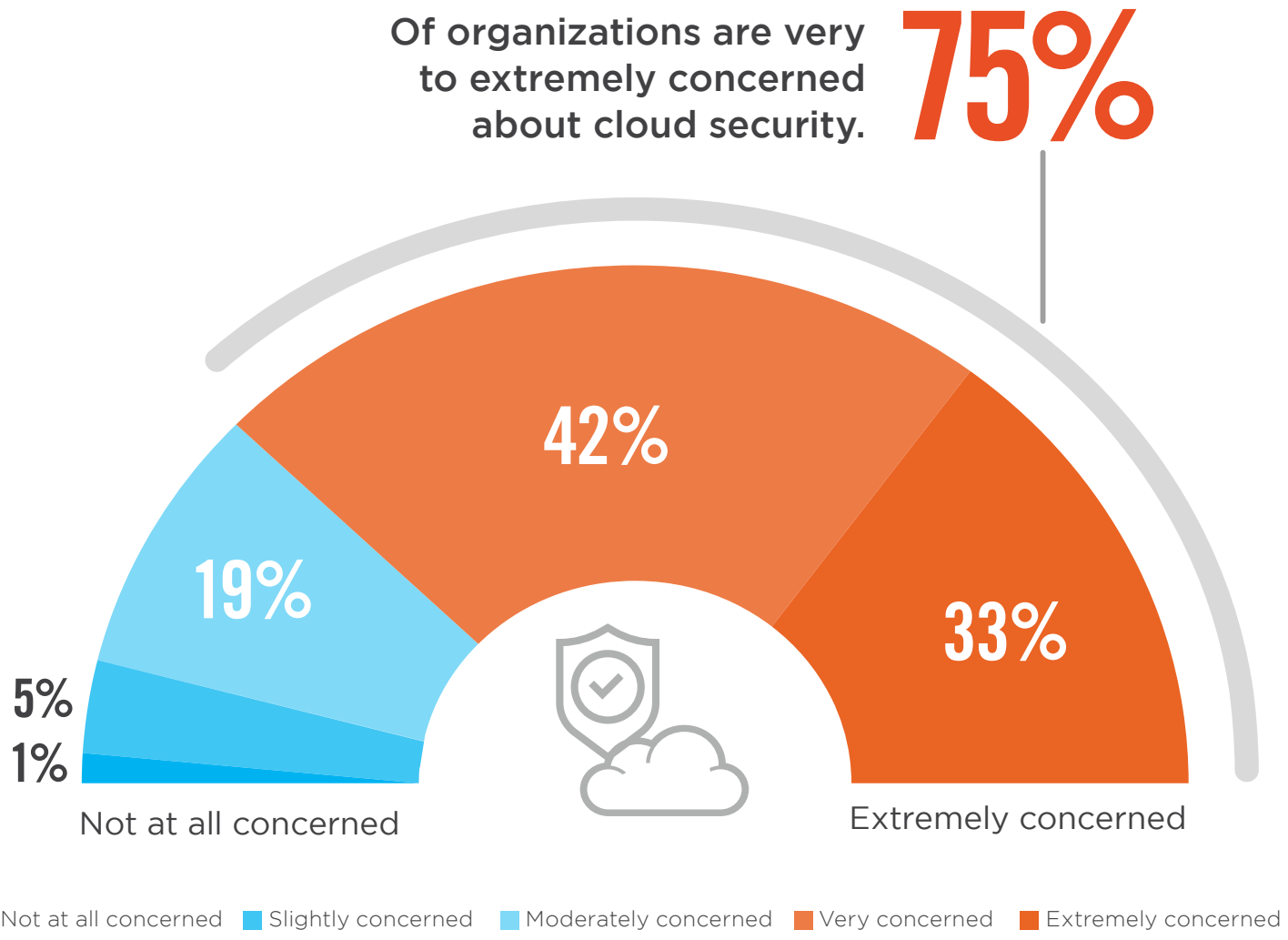
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SECURITY IN PUBLIC CLOUDS

Security remains a key issue for cloud customers, despite continued rapid adoption of cloud computing. Seventy-five percent of cybersecurity professionals confirm they are at least very concerned about public cloud security, a small increase from last year's cloud security survey.

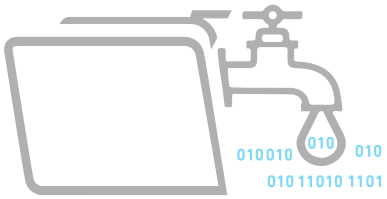
How concerned are you about the security of public clouds?



CLOUD SECURITY CONCERNS

Cloud providers offer increasingly robust security measures as part of cloud services, but customers are ultimately responsible for securing their workloads in the cloud. The top cloud security challenges highlighted in our survey are about data loss/leakage (69% - up five percentage points since last year) and data privacy/confidentiality (66% - up four percentage points). This is followed by concerns about accidental exposure of credentials and incident response (tied at 44%).

What are your biggest cloud security concerns?

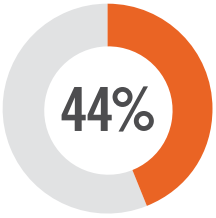


69%

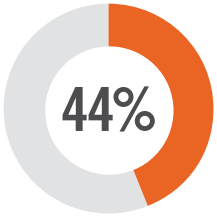
Data loss/leakage

66%

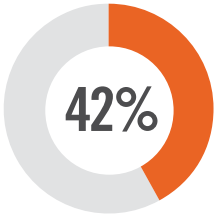
Data privacy/ confidentiality



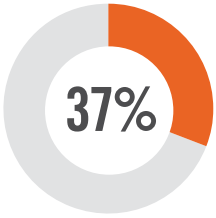
Accidental exposure of credentials



Incident response



Legal and regulatory compliance



Data sovereignty/ residency/control

Visibility & transparency 30% | Availability of services, systems and data 28% | Lack of forensic data 27% | Business continuity 26% Liability 24% | Fraud (e.g., theft of SSN records) 24% | Disaster recovery 23% | Having to adopt new security tools 21% | Performance 19% | Not sure/other 8%

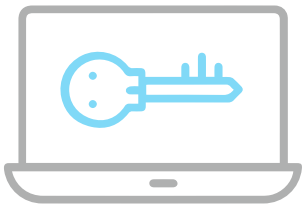
BIGGEST CLOUD SECURITY THREATS

When asked about what are the biggest security threats facing public clouds, organizations ranked misconfiguration of the cloud platform (68%) highest, up from the third spot on last year's survey. This is followed by unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%).

What do you see as the biggest security threats in public clouds?

68%

Misconfiguration of the cloud platform/ wrong setup



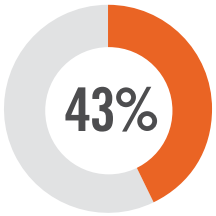
58%

Unauthorized access

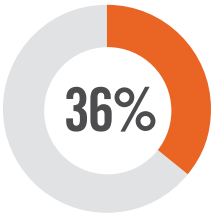
52%

Insecure interfaces/ APIs

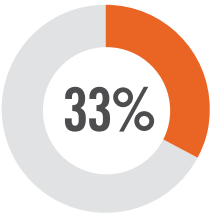
Hijacking of accounts, services or traffic



External sharing of data



Malicious insiders



Foreign state-sponsored cyber attacks

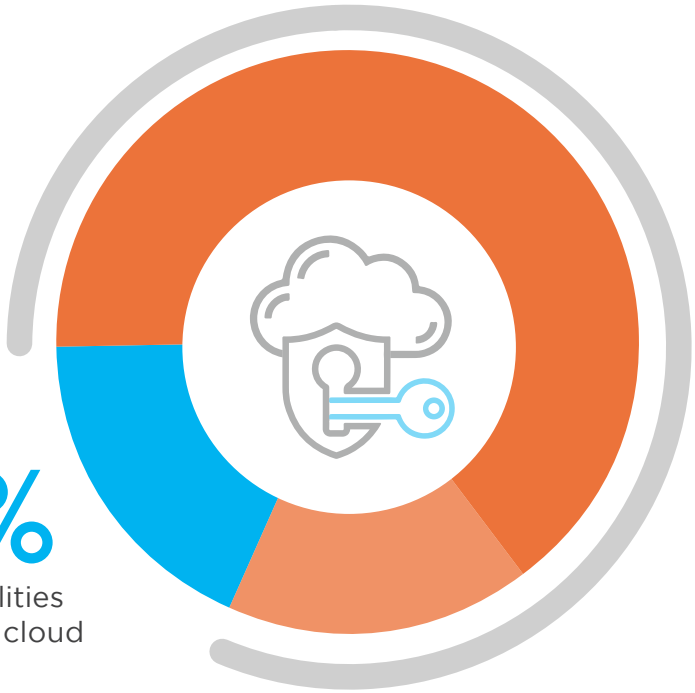
Denial of service attacks

TRADITIONAL TOOLS IN THE CLOUD

As workloads continue to move to the cloud, organizations are faced with unique security challenges presented by cloud computing. Most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. Eighty-two percent of respondents say traditional security solutions either don't work at all in cloud environments or have only limited functionality.

How well do your traditional network security tools/appliances work in cloud environments?

82% **Claim traditional security solutions either don't work at all or have limited functionality.**



65%
Limited functionality

18%
All capabilities work in the cloud

17%
Our traditional network security tools don't work in the cloud

DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

Organizations recognize several advantages of deploying cloud-based security solutions, including faster time to deployment and cost savings (both tied at 41%). This is followed by reduced efforts around patches and software updates (40%).

What are the main drivers for considering cloud-based security solutions?

41%

Faster time to deployment

41%

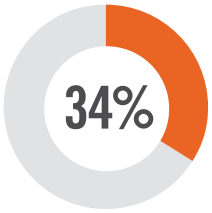
Cost savings

40%

Reduced efforts around patches and upgrades of software

Better visibility into user activity and system behavior

Need for secure app access from any location



Our data/workloads reside in the cloud (or are moving to the cloud)

Meet cloud compliance expectations

Better performance 30% | Easier policy management 26% | Reduction of appliance footprint in branch offices 21% | Other 5%

BARRIERS TO CLOUD-BASED SECURITY ADOPTION

Despite the significant advantages offered by cloud-based security solutions, barriers to adoption still exist. Our survey reveals that the biggest challenge organizations are facing is not technology, but people and processes. Staff expertise and training (55%) continues to rank as the highest barrier to faster adoption, followed by budget challenges (46%), data privacy concerns (37%), and lack of integration with on-premises platforms (36%).

What are the main barriers to migrating to cloud-based security solutions?

55%

Staff expertise/ training

46%

Budget

37%

Data privacy

Lack of integration with on-premises security technologies

Solution maturity

Regulatory compliance requirements

Data residency

Sunk cost into on-premises tools 24% | Integrity of cloud security platform (DoS attack, breach) 17% | Limited control over encryption keys 15% | Scalability and performance 12% | Not sure/other 10%

CLOUD MIGRATION SECURITY NEEDS

Training and certifying IT staff (61%) continues to rank as the primary tactic organizations deploy to assure their evolving security needs are met. Fifty-eight percent of respondents rely on their cloud provider's native security tools, and 34% are looking to hire more staff dedicated to cloud security.

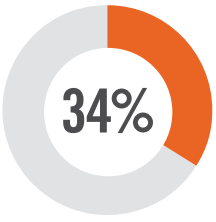
When moving to the cloud, how do you handle your changing security needs?

61%

Train and/or certify existing IT staff

58%

Use native cloud provider security tools*



Hire staff dedicated to cloud security

Deploy security software from independent software vendors

Partner with a Managed Security Services Provider (MSSP)

Other 5%
*(e.g., Azure Security Center, AWS Security Hub, Google Cloud Command Center)

CLOUD PROVIDER CRITERIA

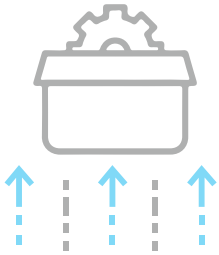
When selecting a cloud security provider, most organizations look at cost-effectiveness (63%), ease of deployment (53%), and that the security tools are cloud-native (52%) as their key priorities. A notable trend year-over-year is the increase in the importance of automation. In 2019, 37% of organizations wanted a provider with automation tools versus this year 52% of organizations seek these capabilities.

What do you look for in your cloud security provider?

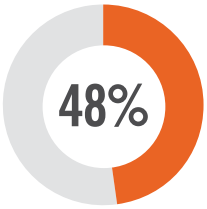
63% Cost effectiveness

53%
Ease of deployment

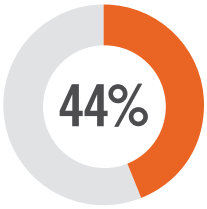
52%
Security tools are cloud native



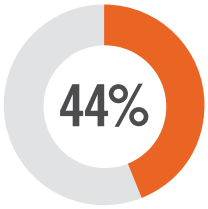
52%
Deploy tools with automation



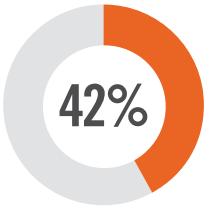
Interoperable with on-premises solutions



Policy customization



Integrates seamlessly with cloud platforms



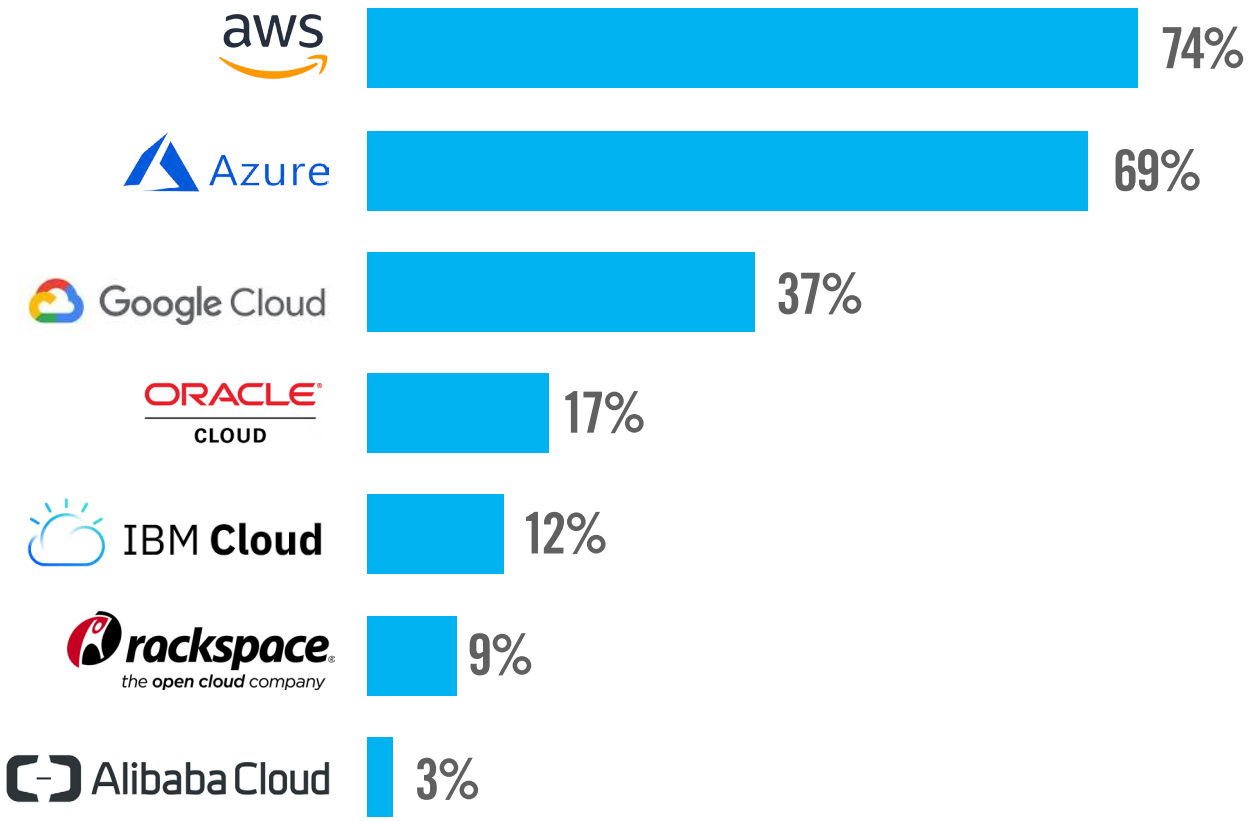
Multi-cloud support

Demonstrates cloud knowledge 39% | Extends on-premises policies to the cloud 38% | Other 4%

CLOUD PROVIDER PREFERENCES

We asked organizations what IaaS cloud providers they are currently using, and not surprisingly, the results mostly reflect the overall rankings of cloud market share among the three biggest cloud service providers. Amazon web services (AWS) lead the list, followed by Microsoft Azure, and Google Cloud Platform. Interesting to point out is the growth of Azure (65% in 2019 vs. 69% in 2020). Also interesting to point out was usage for Google (48% in 2019 versus 37% in 2020,) and Oracle (28% in 2019 vs 17% in 2020).

What cloud IaaS provider(s) do you currently use or plan to use in the future?



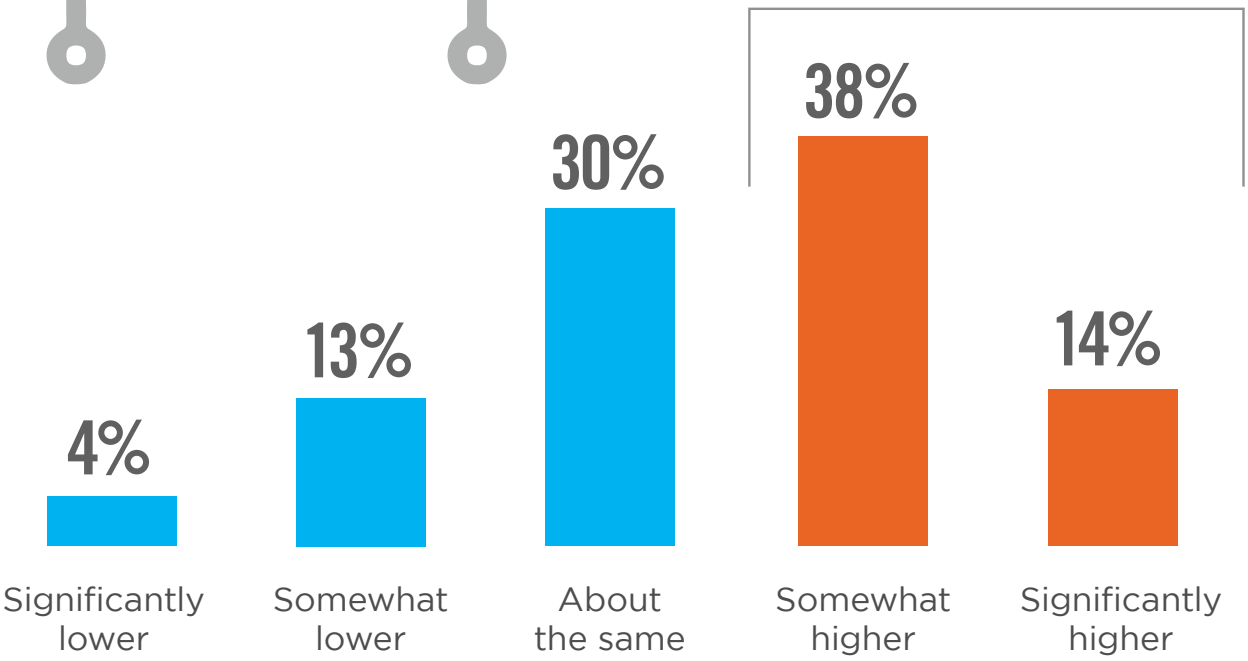
SECURITY RISK IN THE CLOUD

Organizations in our survey consider the risk of security breaches in public cloud environments higher (52%) than in traditional, on-premises IT environments. Only 17% see lower risks, and 30% believe the risks are about the same between the two computing models.

Compared to traditional, on-prem IT environments, would you say the risk of security breaches in a public cloud environment is …

52%

Consider the risk of security breaches in public cloud environments higher than in traditional, on-premises IT environments.



CLOUD SECURITY CAPABILITIES

Among the hundreds of security controls and technologies to protect cloud infrastructure and workloads, the most widely deployed cloud security capabilities include access control (69%) and antivirus/anti-malware (53%), followed by multifactor authentication (49%).

What security capabilities have you deployed in the cloud?

69%

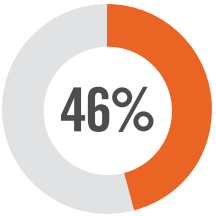
Access control

53%

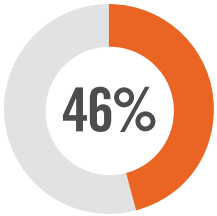
Anti-virus/anti-malware/ Advanced Threat Protection (ATP)

49%

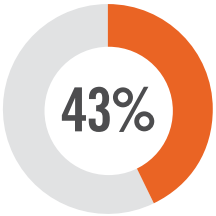
Multi-factor authentication



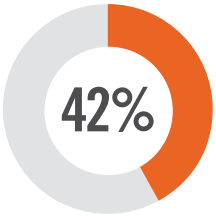
Data encryption



Cloud data backup



Firewalls/ NAC



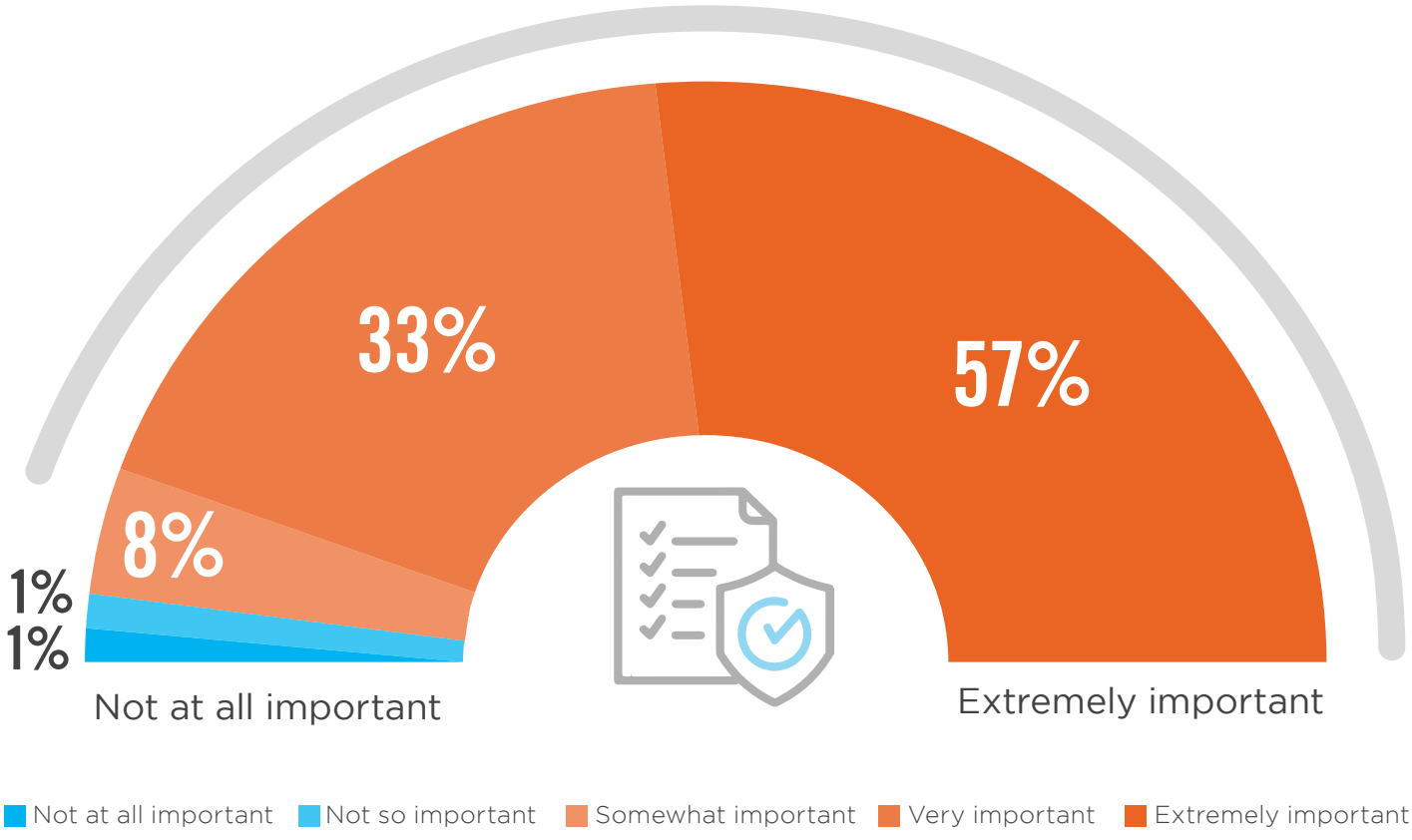
Application protection (e.g., WAF, scanners, etc.)

Single sign-on/user 40% | Network encryption (VPN, packet encryption, transport encryption) 37% | Enpoint security 36% | Other 4%

COMPLIANCE CONTINUITY

An overwhelming majority of 90% considers it very important or extremely important to ensure continuous compliance when migrating secure workloads from on-prem to cloud environments.

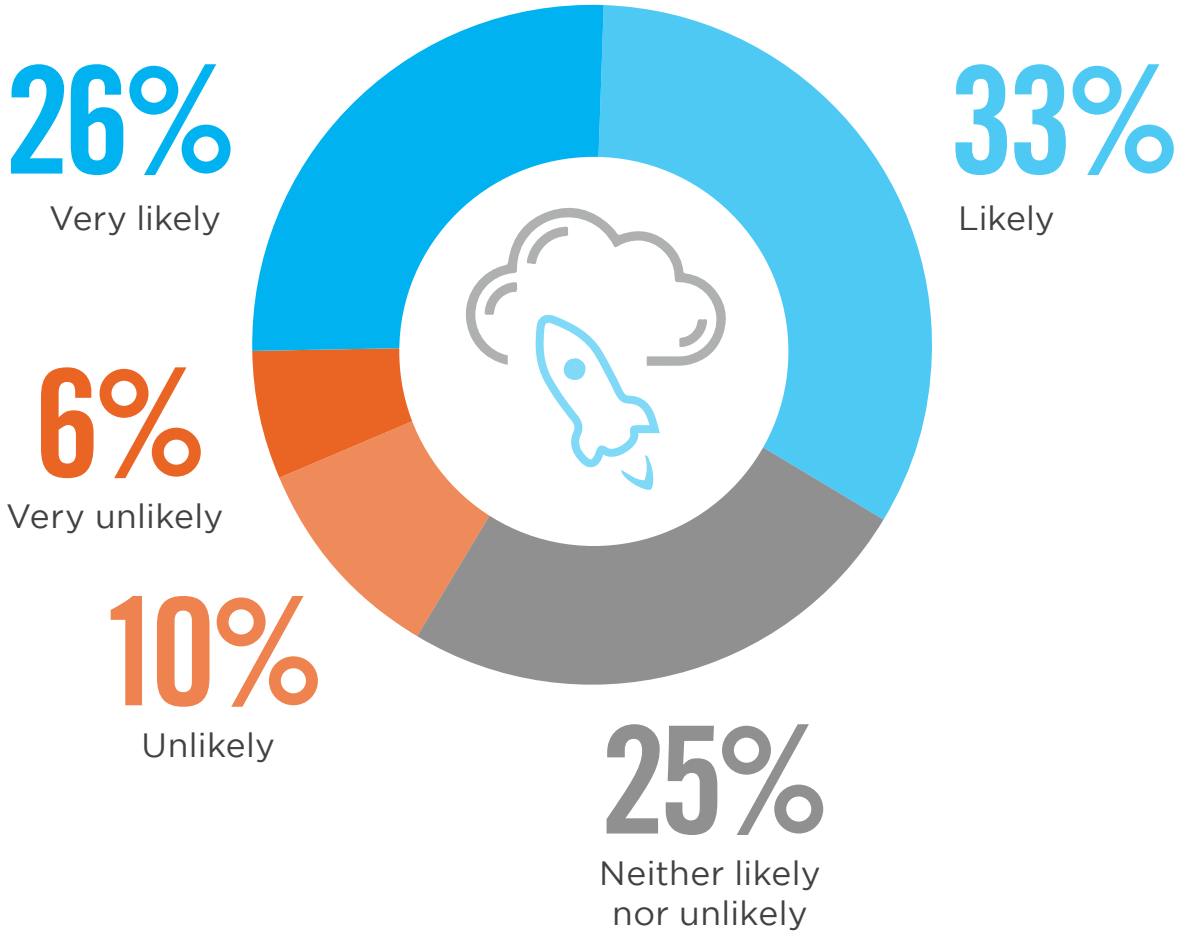
If you secure your workloads (VMs, containers, and serverless instances) on-prem, how important is continuous compliance when they migrate to the cloud?



DEPLOYING CLOUD SECURITY

A majority of 59% says it is likely to very likely that they will deploy a new cloud security solution within the next 12 months.

How likely is your organization to deploy a new cloud security solution within the next 12 months?



CLOUD SECURITY SOLUTION CRITERIA

When asked what criteria organizations consider most important when evaluating a cloud security solution they prioritize product features (66%), cost (65%), and vendor experience (55%) as the most important considerations.

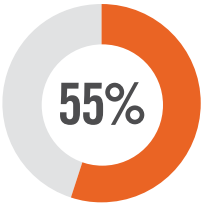
What criteria do you consider most important when evaluating a cloud security solution?

66%

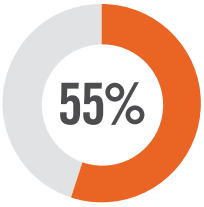
Product features/ functionality

65%

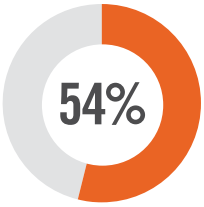
Cost



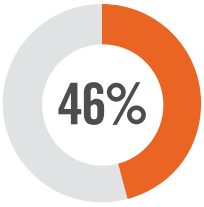
Vendor experience and reputation



Product performance



Support



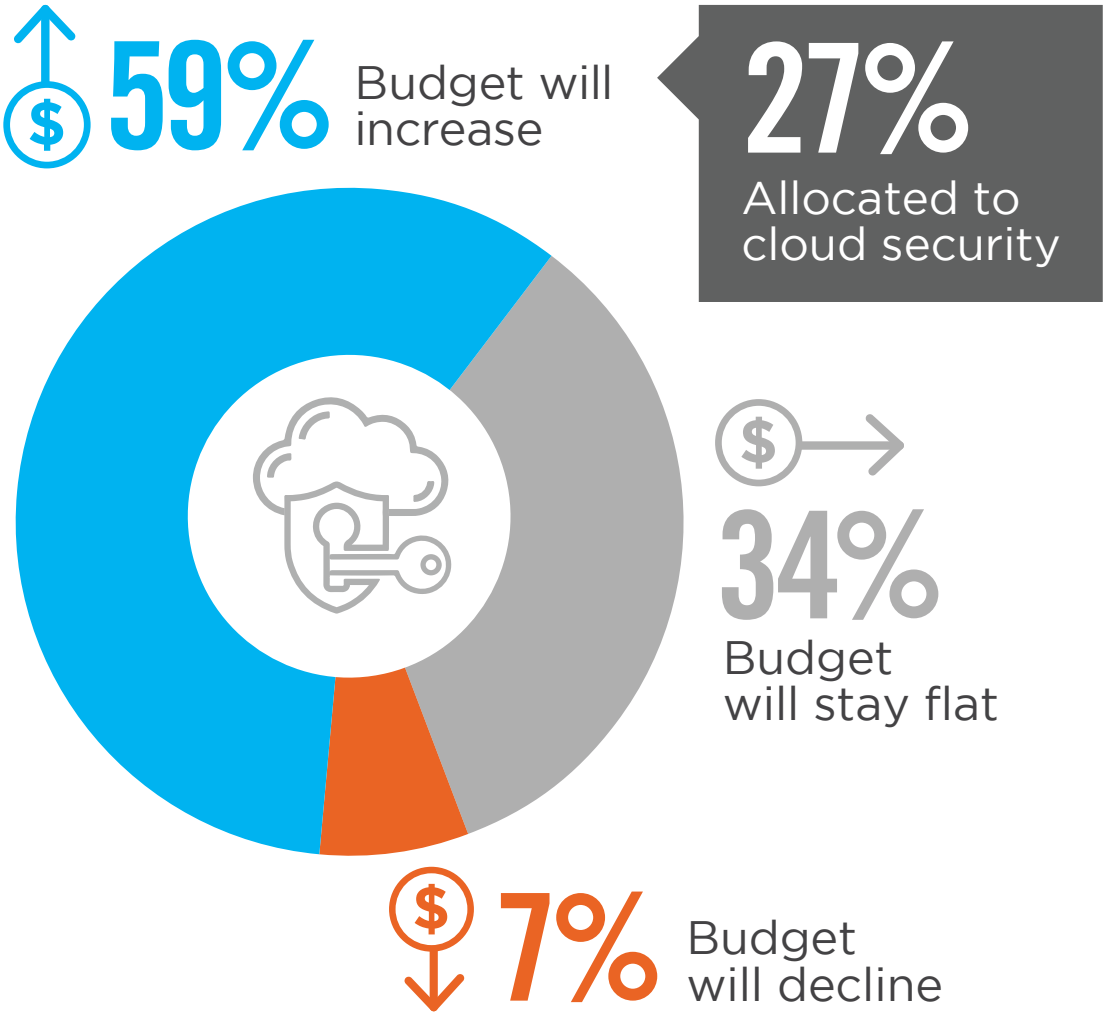
Provider's willingness to adapt and address our use case

Product ease of use 44% | Contract/term 27% | Customer reviews 13% | Other 5%

CLOUD SECURITY BUDGET

Nearly 60% of organizations expect their cloud security budget to increase over the next twelve months. On average, organizations allocate 27% of their security budget to cloud security.

How is your cloud security budget changing in the next 12 months?



CLOUD SOLUTION CRITERIA

We asked what criteria organizations prioritize when deciding between cloud security solutions offered by independent third-party providers and the cloud-native security solutions offered by the cloud platform. The most mentioned factor is cost of the security solution (61%). This is followed by ease of use (55%), solution complexity (53%), and performance (49%).

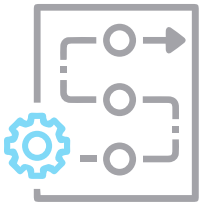
What criteria are most important to you when deciding between cloud native vs independent cloud security solutions?

61%

Cost

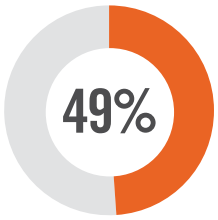
55%

Ease of use

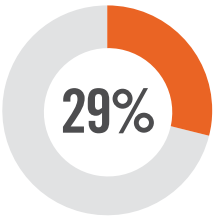


53%

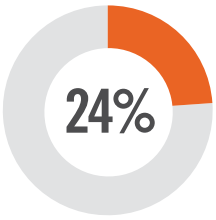
Less complexity and well integrated



Performance



Quicker deployments



Cloud vendor security is good enough, why would I need anything else?

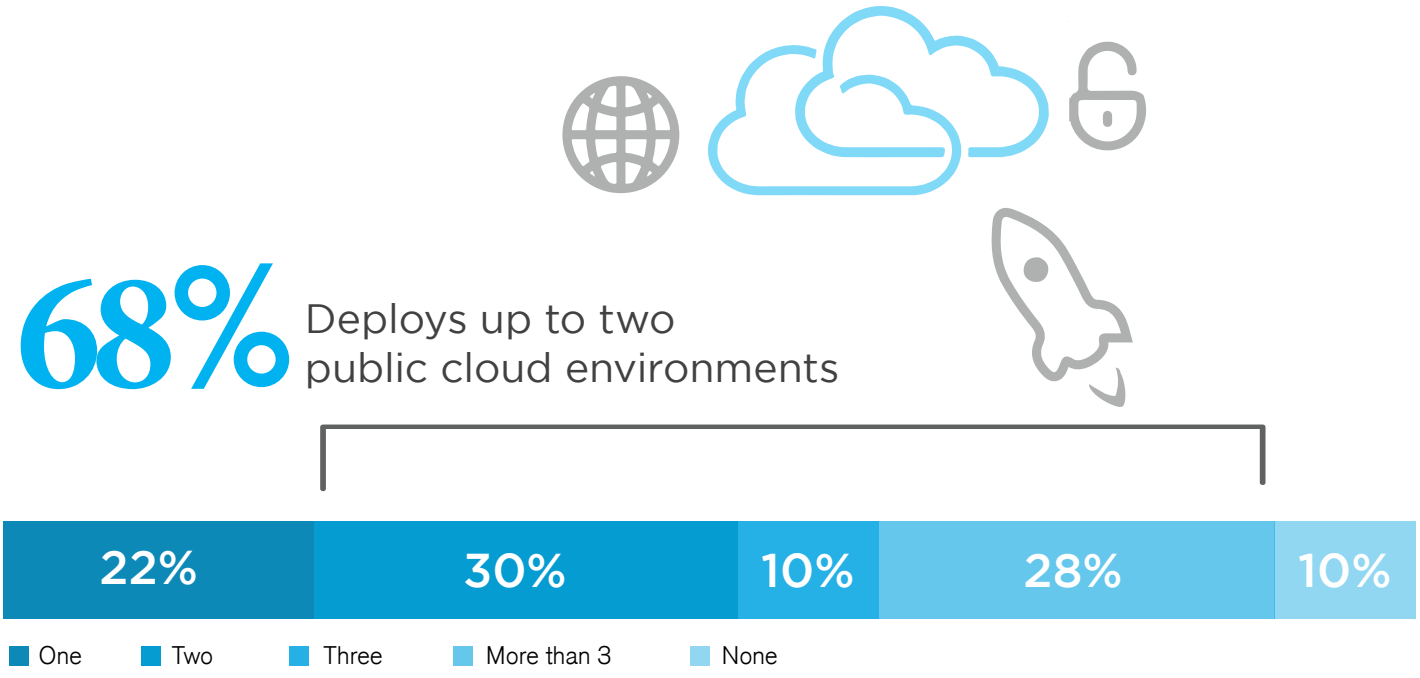
No need to manage another vendor

Other 4%

CLOUD SOLUTION CRITERIA

A majority of organizations deploys up to two public cloud environments (52%).

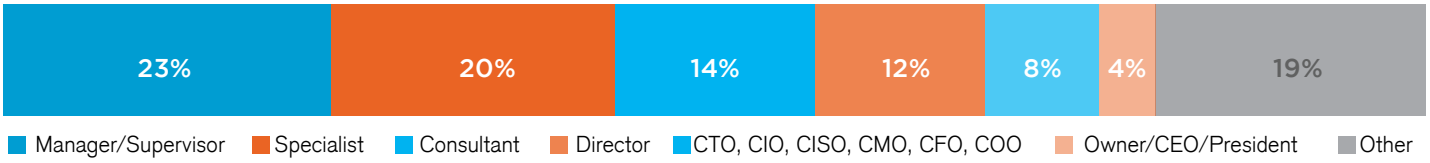
How many cloud providers does your organization currently use?



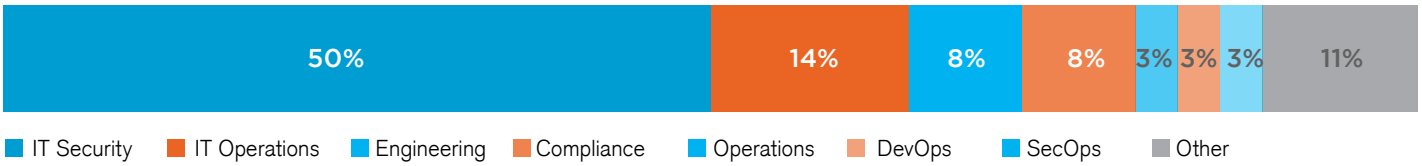
METHODOLOGY & DEMOGRAPHICS

The 2020 Cloud Security Report is based on a comprehensive survey of 653 cybersecurity professionals conducted in July 2020 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.

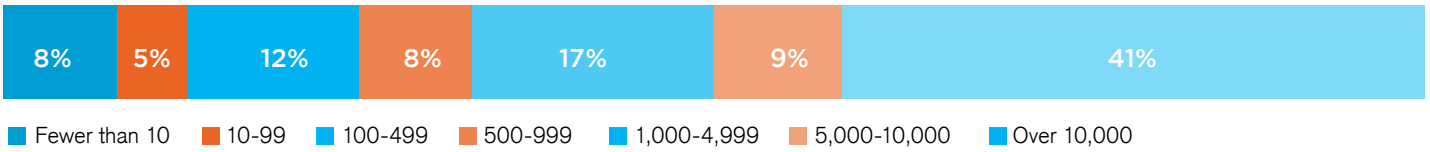
CAREER LEVEL



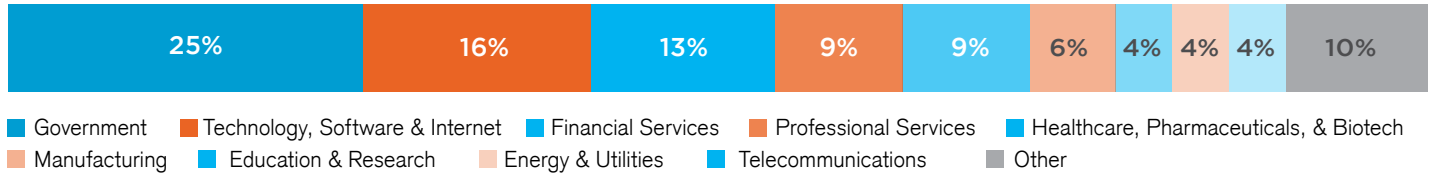
DEPARTMENT

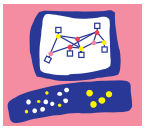


COMPANY SIZE



INDUSTRY





Check Point®
SOFTWARE TECHNOLOGIES LTD

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.

www.checkpoint.com