2021

Cybersecurity INSIDERS

CLOUD SECURITY REPORT

FORTINET®

INTRODUCTION

Organizations continue to rapidly migrate workloads from datacenters to the cloud, and the trend has been accelerating during the recent Covid pandemic.

However, cloud security concerns remain high as the adoption of public cloud computing continues to surge in the wake of the pandemic and the resulting massive shift to remote work.

The 2021 Cloud Security Report is based on a comprehensive global survey of 572 cybersecurity professionals to reveal how organizations are responding to security threats in the cloud, and what tools and best practices IT cybersecurity leaders are prioritizing in their move to the cloud.

Key survey findings include:

- Most organizations are pursuing a hybrid or multi-cloud strategy (71%). They are doing this for integration of multiple services, scalability, or business continuity reasons. Few companies rely on a single cloud deployment (27%) for their business needs.
- Seventy-six percent of organizations are using two or more cloud providers.
- Among the key barriers to faster cloud adoption, survey participants mentioned lack of visibility (53%), lack of control (46%), lack of staff resources or expertise (39%), and high cost (35%) as the most significant negative factors.
- Misconfiguration of cloud security remains the biggest cloud security risk according to 67% of cybersecurity professionals in our survey. This is followed by exfiltration of sensitive data (59%) and tying at 49% are unauthorized access and insecure interfaces/APIs.
- Multi-cloud environments add complexity and security challenges. In our survey, organizations are most concerned with data protection (58%) followed by a lack of security skills (57%) and understanding how different solutions fit together (52%).
- Seventy-eight percent of surveyed cybersecurity professionals would find it very helpful to extremely helpful to have a single cloud security platform offering a single dashboard while allowing for configuration of policies to protect data consistently and comprehensively across the cloud.

We would like to thank Fortinet for supporting this important industry research project. We hope you find this report informative and helpful as you continue your efforts in securing your journey to the cloud.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

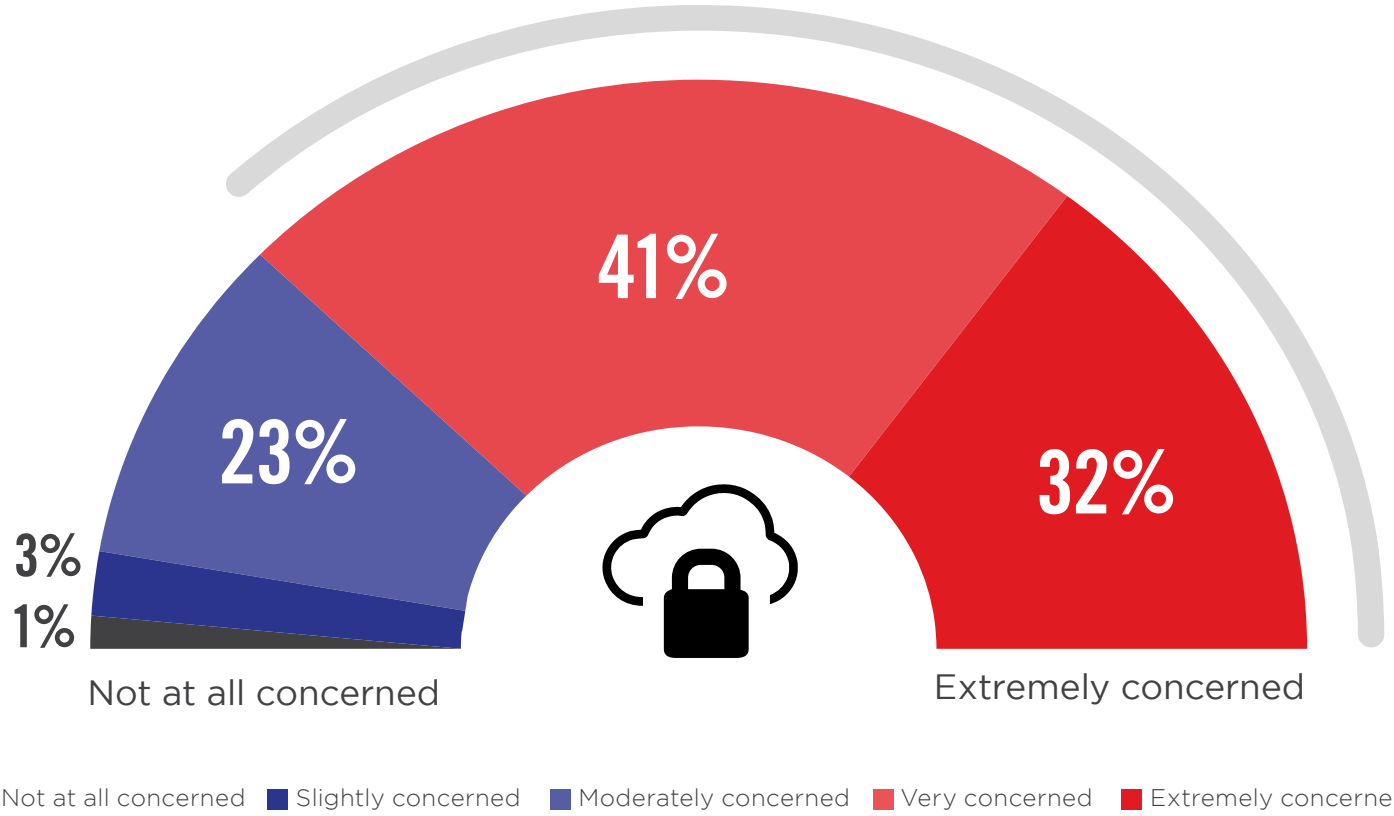
Cybersecurity
INSIDERS

PUBLIC CLOUD SECURITY

Cloud security continues to be a significant concern for cybersecurity professionals. Almost all respondents in our survey are at least moderately concerned (96%) and a third are extremely concerned (32%).

How concerned are you about the security of public clouds?

73% Of organizations are very to extremely concerned about cloud security.



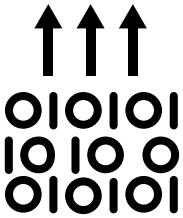
BIGGEST SECURITY THREATS

Misconfiguration of cloud security remains the biggest cloud security risk according to 67% of cybersecurity professionals in our survey. This is followed by exfiltration of sensitive data (59%) and tying at 49% are unauthorized access and insecure interfaces/APIs.

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

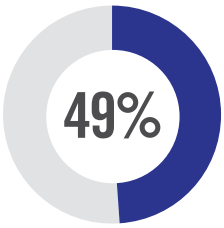
67%

Misconfiguration of the cloud platform/wrong set-up

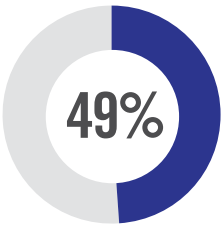


59%

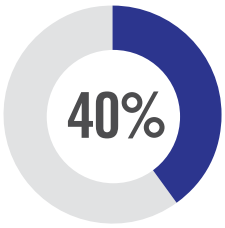
Exfiltration of sensitive data



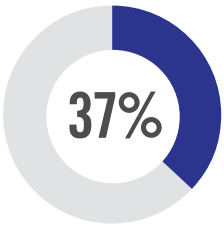
Unauthorized access



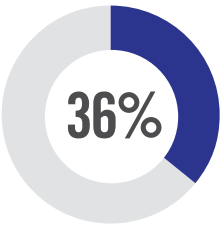
Insecure interfaces/APIs



External sharing of data



Hijacking of accounts, services, or traffic



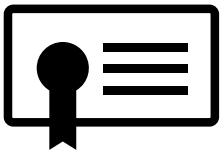
Malicious insiders

Foreign state-sponsored cyber attacks 34% | Malware/ransomware 31% | Denial of service attacks 26% | Cloud cryptojacking 16% | Theft of service 13% | Lost mobile devices 8% | Don't know/other 7%

CLOUD SECURITY FACTORS

We asked cybersecurity professionals what features they find most useful in a cloud security solution. The most requested capability is third-party security certifications (54%) followed by integration with security scanner tools (52%) and the ability to write custom rules and remediation actions (49%).

What features do you find most useful in a cloud security solution?

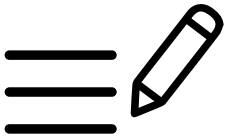


54%

Third-party security certifications
(e.g., SOC2, FedRAMP, etc.)

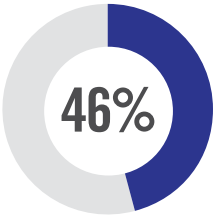
52%

Integration with security scanner tools
(e.g., Rapid7, Qualys, Tenable)

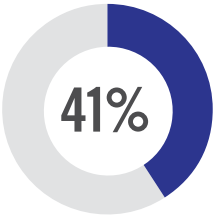


49%

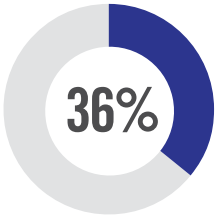
Ability to write custom rules and remediation actions



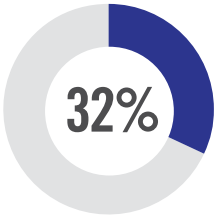
Integration with change management platforms
(e.g., ServiceNow, Remedy, JIRA, etc.)



Integration with end-to-end vulnerability remediation tools
(e.g., TrueSight Server Automation, IBM BigFix, TrueSight Vulnerability Manager, Chef, Puppet, etc.)



Research-based policies
(e.g., content beyond the CIS best practices)



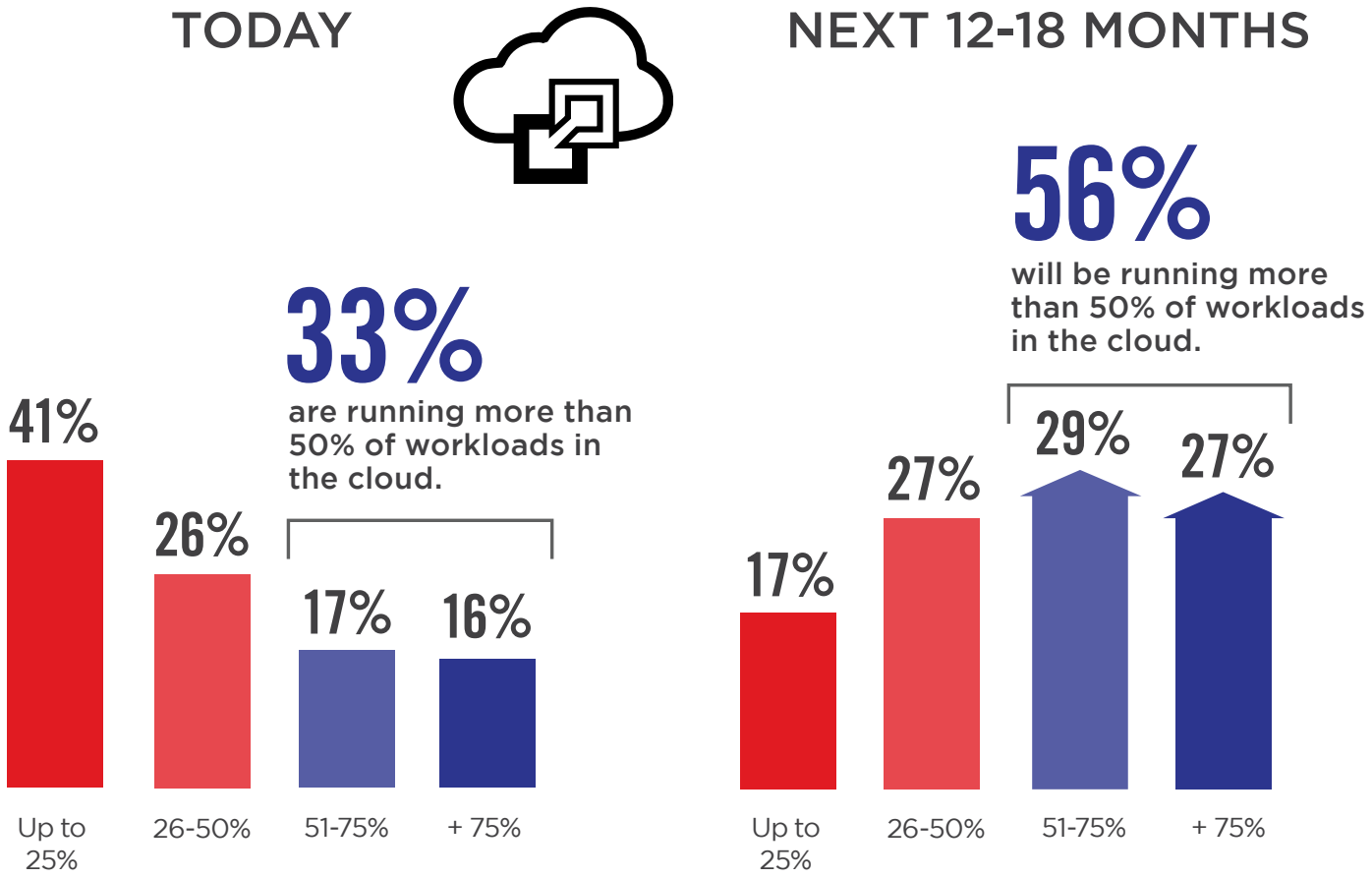
Billing model
(monthly, yearly, flat)

Billing by usage instead of number of accounts 31% | Integration with alerting tools (i.e., OpsGenie that support integration with phone, messaging, Slack, email, etc. 30% | User community support 20% | Other 2%

WORKLOADS IN THE CLOUD

When asked what percentage of workloads organizations already have in the cloud, today 33% are running more than 50% of workloads in the cloud; in the next 12-18 months, that grows to 56%.

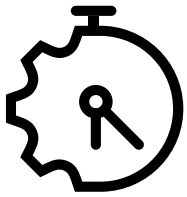
What percentage of your workloads are in the cloud today compared to how it will be in the next 12-18 months?



BUSINESS RESULTS

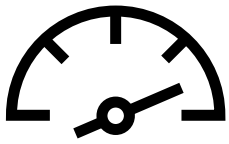
The outcomes organizations have realized from cloud computing are in line with the original promise of the cloud: faster time to market (53%), increased responsiveness (51%), and cost reductions (41%) lead the list.

What business outcomes have you realized by moving to the cloud?



53%

Accelerated time to market

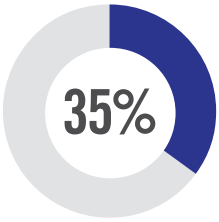


51%

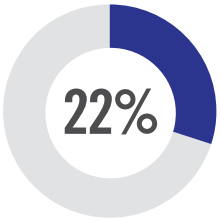
Increased responsiveness to customer needs

41%

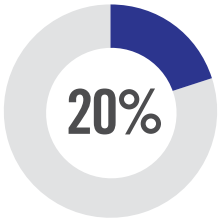
Saved money



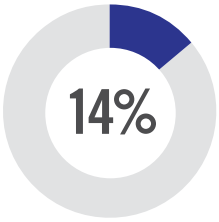
Reduced risk and improved security



Expanded market reach to new markets



Accelerated revenue growth in existing markets



Gained parity with competitors

Other 7%

CLOUD DEPLOYMENT STRATEGIES

Most organizations are pursuing a hybrid or multi-cloud strategy (71%) for integration of multiple services, scalability, or business continuity reasons. Few companies rely on a single cloud deployment (27%) for their business needs. Seventy-six percent are utilizing two or more cloud providers.

What is your primary cloud deployment strategy?

HYBRID
(e.g., integration between private and public clouds)

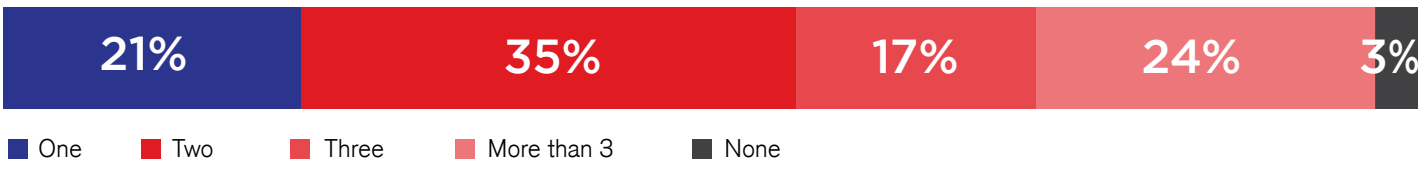
MULTI-CLOUD
(e.g., multiple providers without integration)

SINGLE CLOUD

Other 2%

How many cloud providers does your organization currently use?

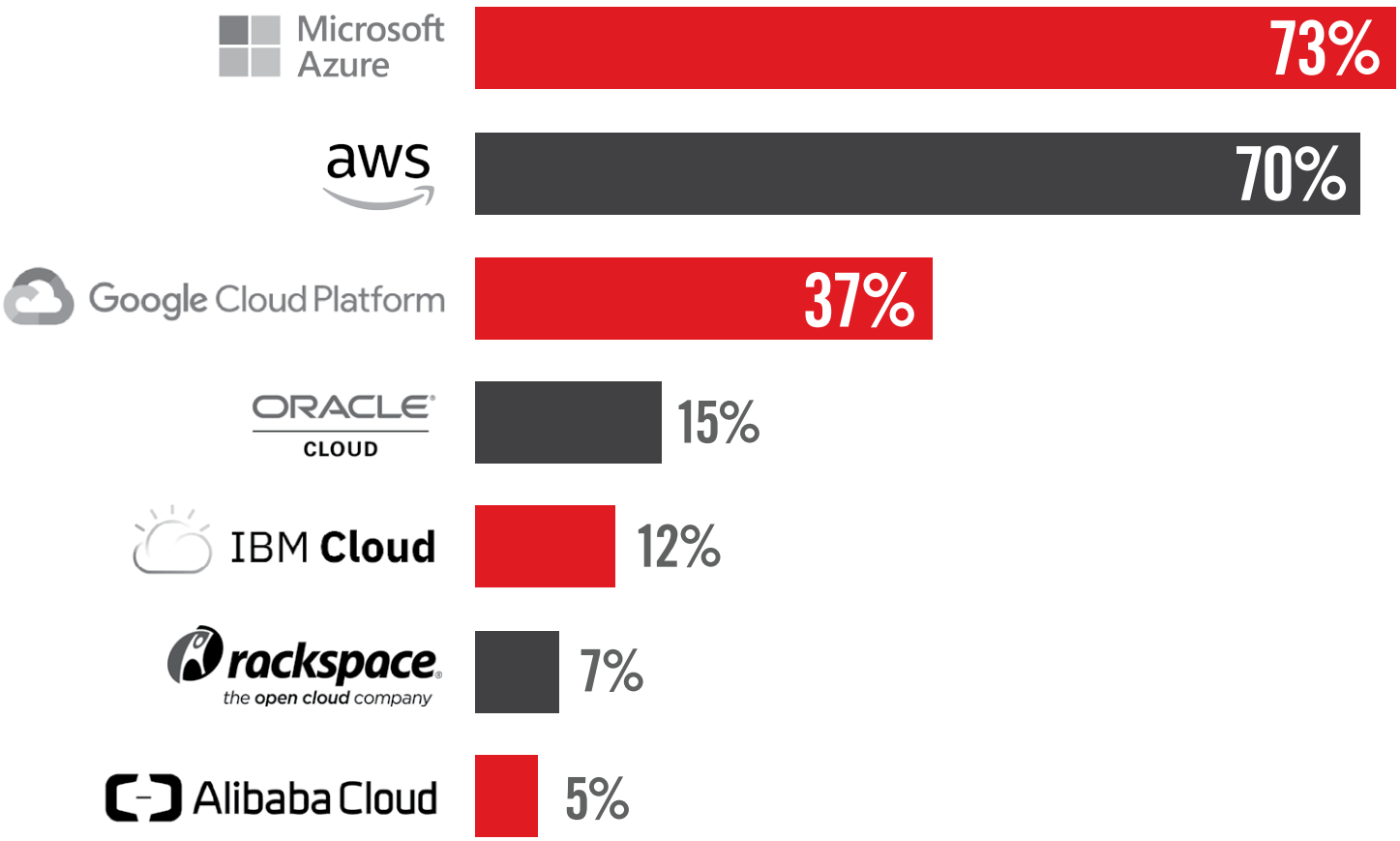
76% Use two or more cloud providers.



POPULAR CLOUD PROVIDERS

Among the organizations surveyed, Microsoft Azure is the most popular cloud provider (73%) followed by Amazon Web Services (70%) and the Google Cloud Platform (37%).

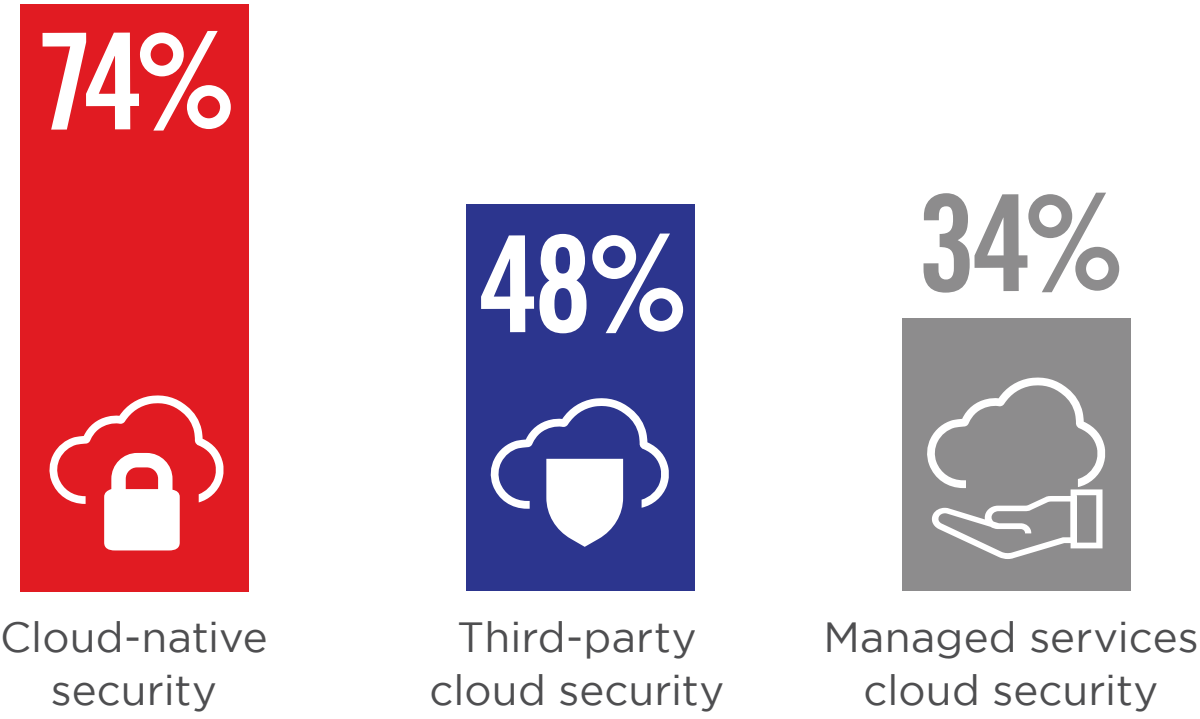
What cloud IaaS provider(s) do you currently use?



CLOUD SECURITY PATH

When asked how organizations source their cloud security, the vast majority said they prefer cloud-native security (74%). This is followed by third-party cloud security solutions (48%) and managed service providers delivering security services (34%).

How do you source cloud security?



Cloud-native security tools: are defined as solutions that can ingest and make sense of the rich APIs offered by the cloud platforms

Security ISV/Third Party: vendor-supplied or outsourced software is any program or application that is not written exclusively by employees belonging to the company for which the software was created.

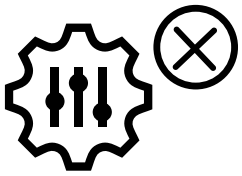
CLOUD ADOPTION BARRIERS

Among the barriers to faster cloud adoption, survey participants mentioned lack of visibility (53%), lack of control (46%), lack of staff resources or expertise (39%), and high cost (35%) as the most significant negative factors.

What are the biggest barriers holding back cloud adoption in your organization and what surprises did you uncover that may slow/stop cloud adoption?

53%

Lack of visibility



46%

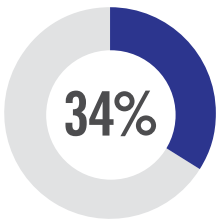
Not enough control

39%

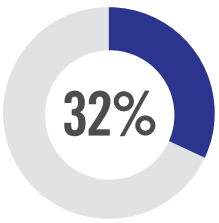
Lack of staff resources or expertise

35%

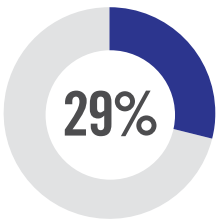
Too expensive



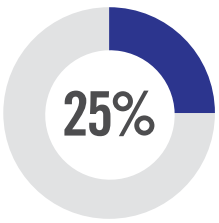
Data security, loss & leakage risks



Legal & regulatory compliance



Integration with existing IT environment



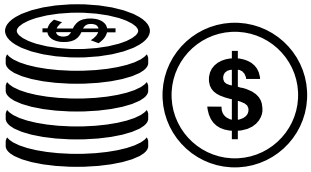
General security risks

Fear of vendor lock-in 24% | Loss of control 22% | Internal resistance and inertia 21% | Complexity managing cloud deployment 21% | Lack of budget 20% | Cost/lack of ROI 19% | Not secure 16% |

CLOUD SECURITY CRITERIA

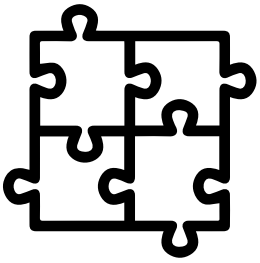
We asked what factors organizations prioritize when deciding between cloud security solutions offered by independent third-party providers and the cloud-native security solutions offered by the cloud platform. The most mentioned factor is cost of the security solution (60%). This is followed by low solution complexity (59%) and ease of use (52%).

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



60%

Cost

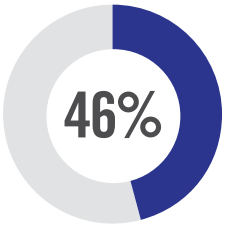


59%

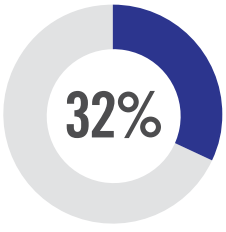
Less solution complexity and already well integrated

52%

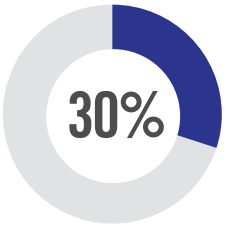
Ease of use



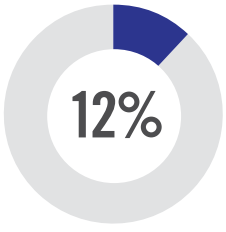
Performance



Quicker deployments



No need to manage another vendor



Cloud vendor security is good enough: "Why would I need anything else?"

Other 5%

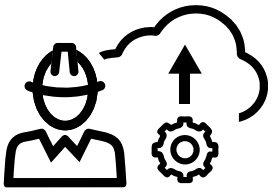
MULTI-CLOUD SECURITY CHALLENGES

Multi-cloud environments add complexity and security challenges. In our survey, organizations are most challenged with data protection (58%) followed by a lack of security skills (57%) and understanding how different solutions fit together (52%).

What are your biggest challenges securing multi-cloud environments?

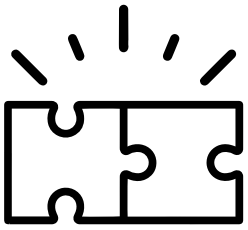
58%

Ensuring data protection and privacy for each environment



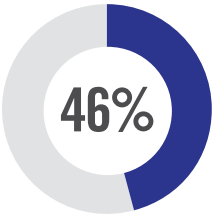
57%

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

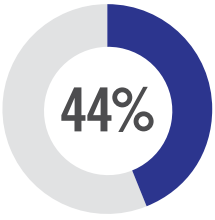


52%

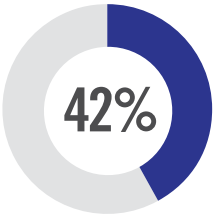
Understanding how different solutions fit together



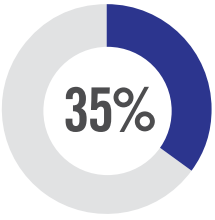
Loss of visibility and control



Keeping up with the rate of change



Understanding service integration options



Selecting the right set of services

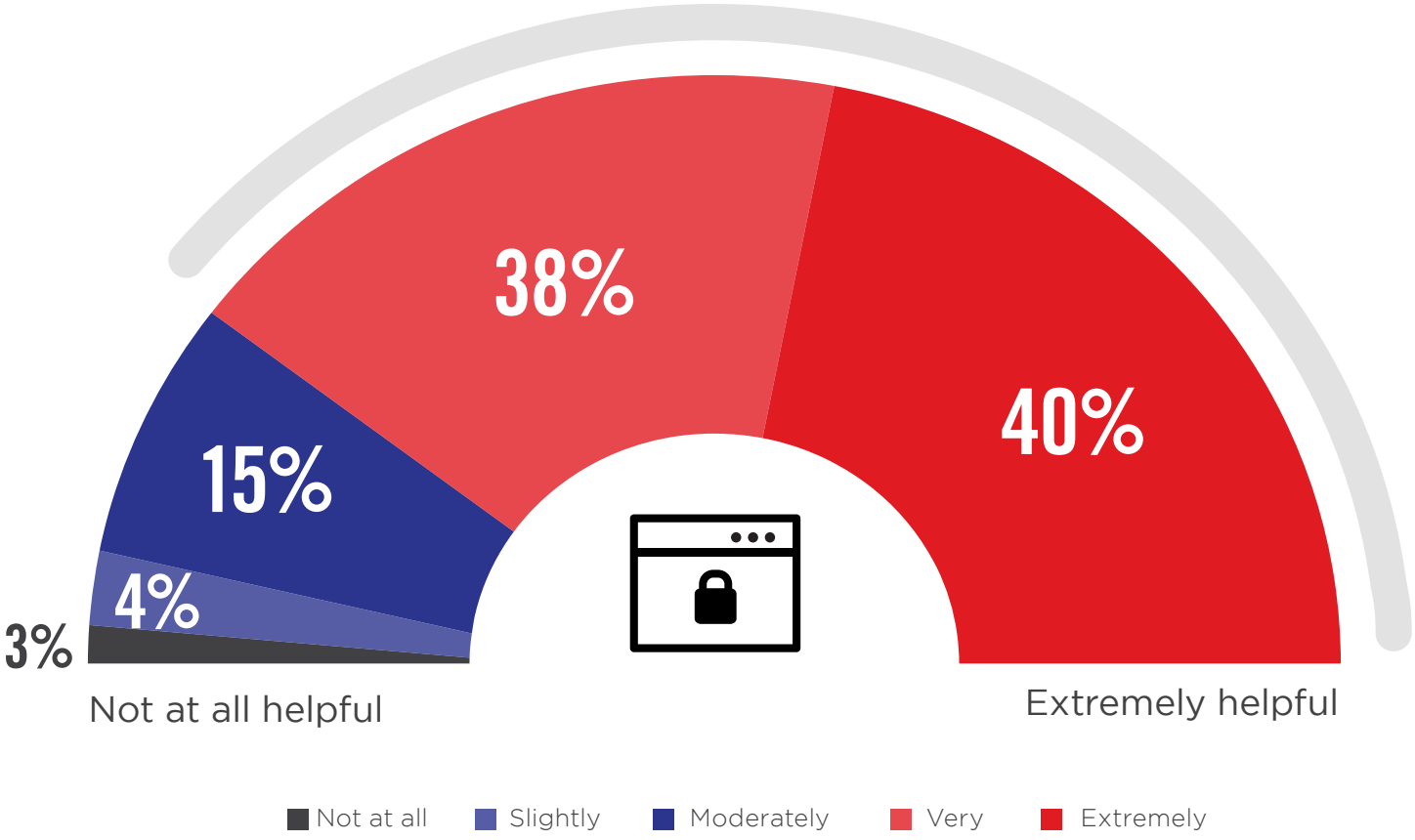
Providing seamless access to users based on their credentials 28% | Managing the costs of different solutions 28% | Other 3%

SINGLE CLOUD SECURITY PLATFORM

Seventy-eight percent of surveyed cybersecurity professionals would find it very helpful to extremely helpful to have a single cloud security platform offering a single dashboard while allowing for configuration of policies to protect data consistently and comprehensively across the cloud.

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?

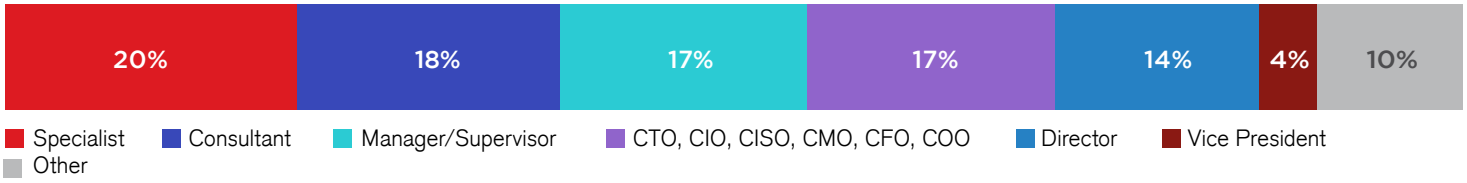
78% Of professionals would consider it very to extremely helpful to have a single cloud security dashboard.



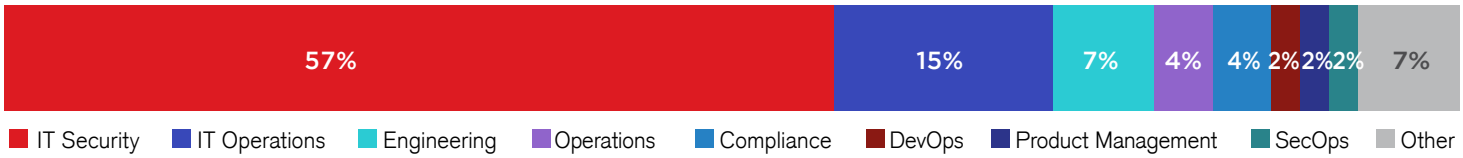
METHODOLOGY & DEMOGRAPHICS

The 2021 Cloud Security Report is based on the results of a comprehensive online global survey of 572 cybersecurity professionals, conducted in April 2021, to gain deep insight into the latest trends, key challenges, and solutions for cloud security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

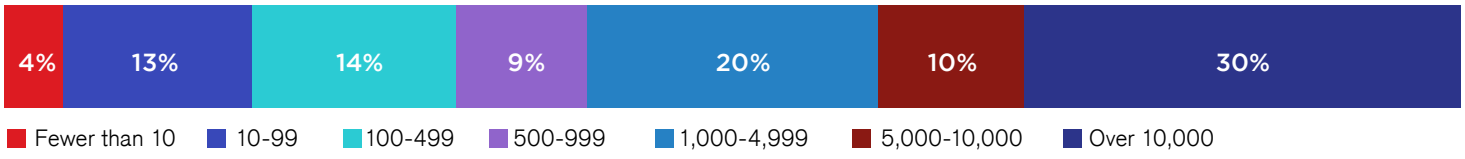
CAREER LEVEL



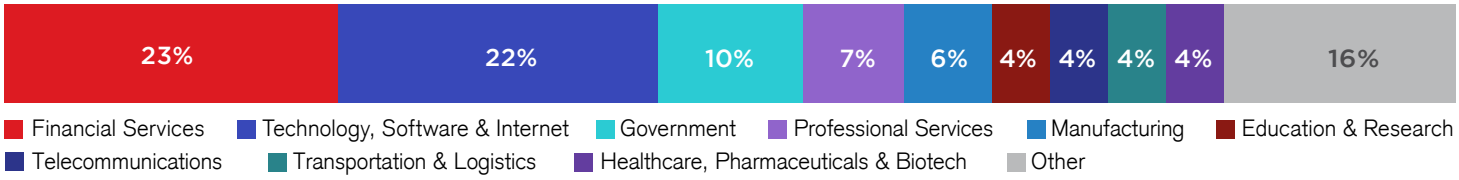
DEPARTMENT



COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as the company with the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

www.fortinet.com