

2021

Cybersecurity  
INSIDERS

# CLOUD SECURITY REPORT



bitglass

# INTRODUCTION

Companies continue to rapidly migrate workloads to the cloud to benefit from increased efficiency, better scalability, and faster deployments from cloud computing.

This 2021 Cloud Security Report, based on a comprehensive survey of cybersecurity professionals, reveals that cloud security concerns remain high as the adoption of public cloud computing continues to surge, especially in the wake of the 2020 COVID crisis and the resulting accelerated shift to remote work environments.

However, we find that many organizations are not yet fully prioritizing the appropriate security solutions required to keep up with the new normal, including mobile device management for mobile devices, endpoint cloud protection, or data loss prevention (DLP) solutions.

## Key findings include:

- Security remains a key issue for cloud customers, despite the continued rapid adoption of cloud computing. Seventy-three percent of cybersecurity professionals confirm they are at least very concerned about public cloud security.
- Employees increasingly use personal devices to access data in the cloud. To protect this use case, 40% of organizations install MDM agents on mobile devices to manage them remotely. 23% block all personal devices from accessing the cloud, both through policy or access controls. 17% use a model that only allows access by trusted devices.
- When asked about the technologies organizations use to protect against malware, 65% prioritize endpoint protection solutions, followed by built-in cloud protections (57%) and secure web gateways (31%).
- Among the hundreds of security controls and technologies to protect cloud infrastructure and workloads, the most widely deployed cloud security capabilities include access control (68%) and anti-virus/anti-malware (54%), followed by multifactor authentication (47%).

This 2021 Cloud Security Report has been produced by Cybersecurity Insiders to explore how organizations are responding to the evolving security threats in the cloud.

We would like to thank [Bitglass](#) 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

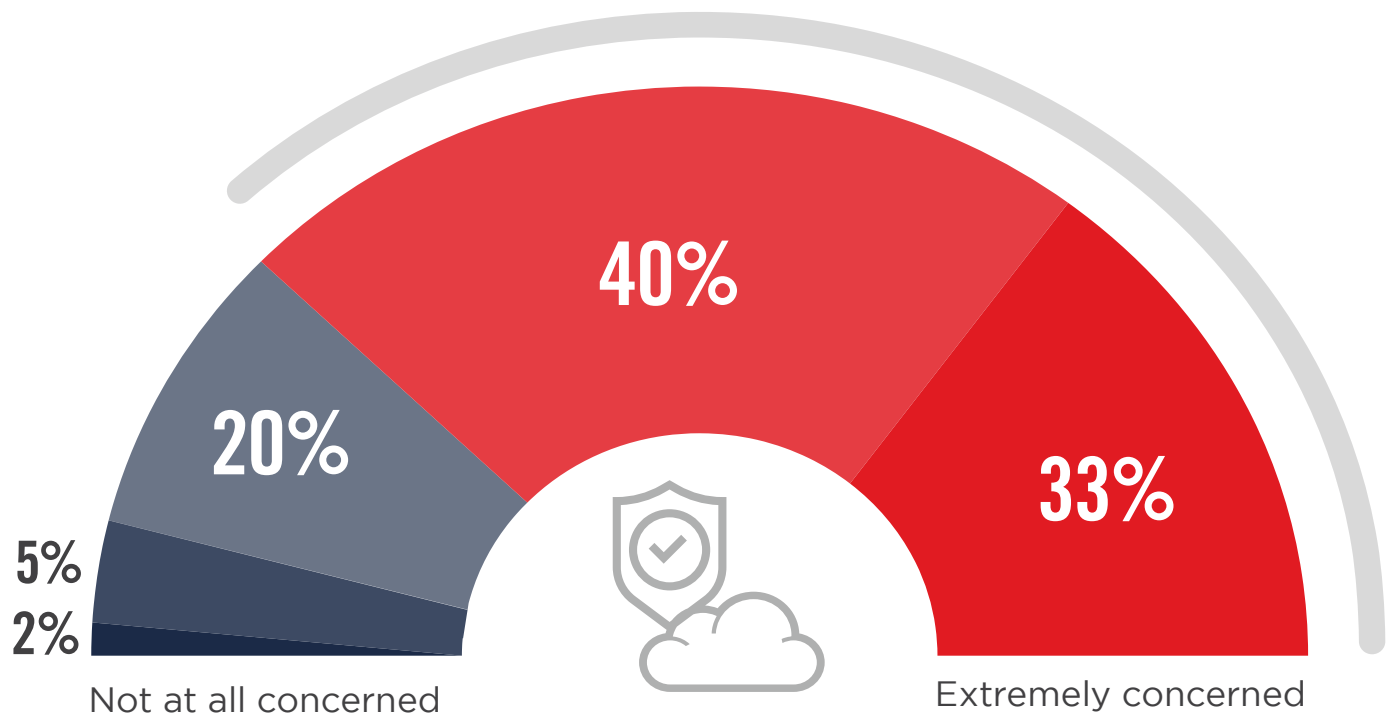
**Cybersecurity**  
INSIDERS

# SECURITY IN PUBLIC CLOUDS

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

## ► How concerned are you about the security of public clouds?

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

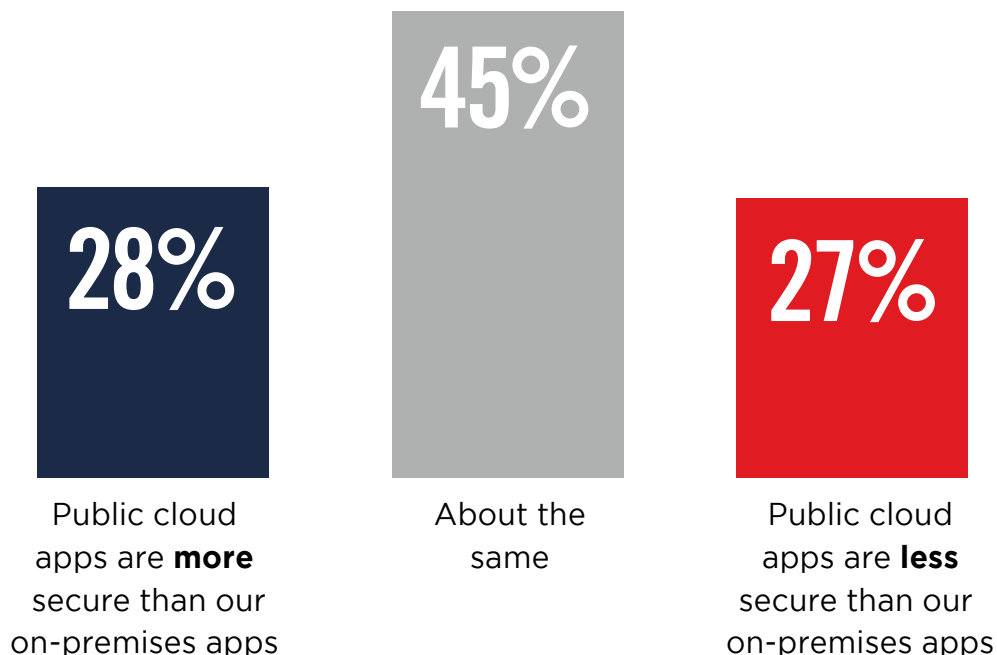
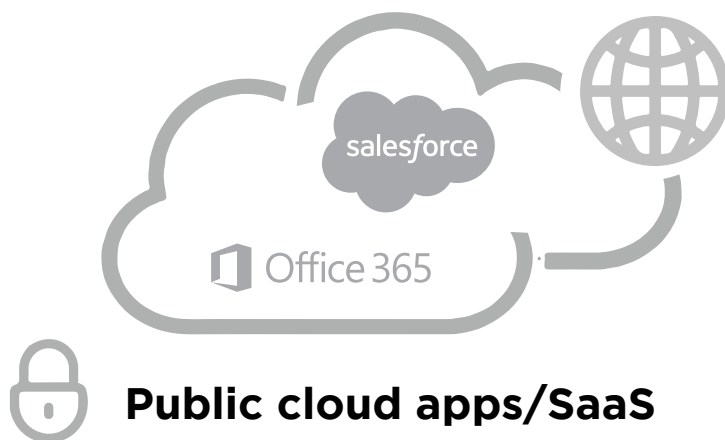


■ Not at all concerned ■ Slightly concerned ■ Moderately concerned ■ Very concerned ■ Extremely concerned

# SECURITY OF SAAS VS ON-PREMISES APPS

A majority of 73% believe that cloud apps are as secure or more secure than on-premises applications, up from 67% in last year's survey.

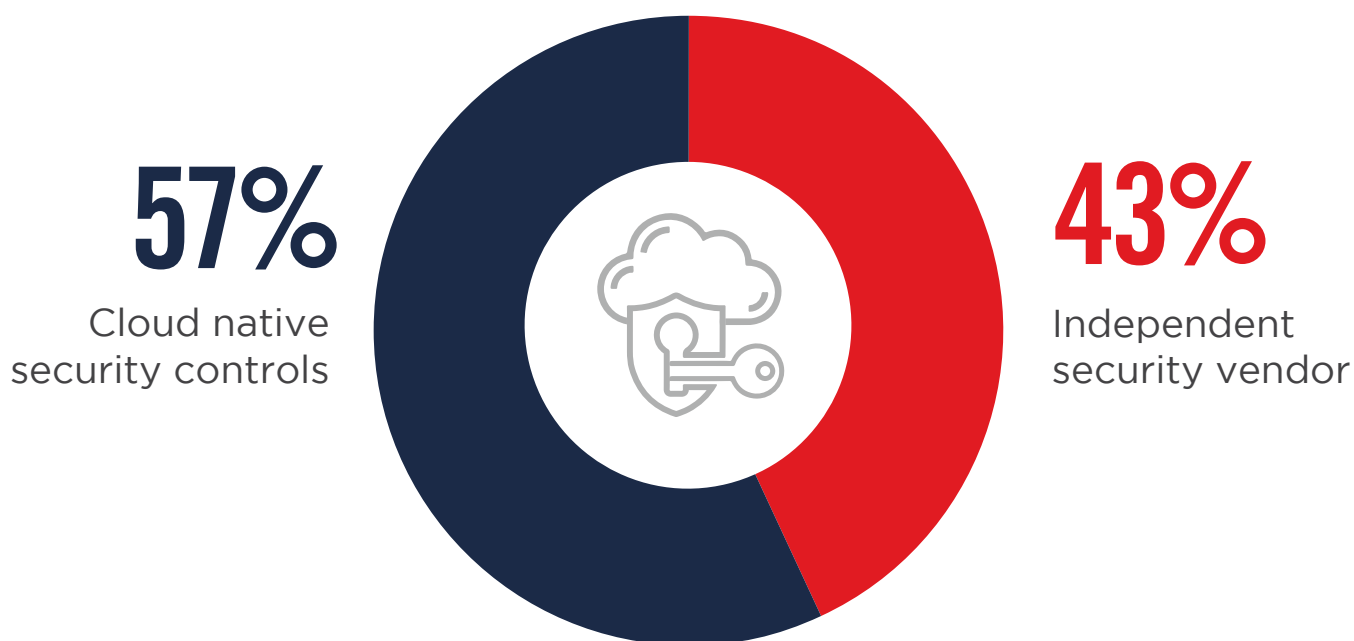
- ▶ Are public cloud apps/SaaS (such as Salesforce and Office 365) more or less secure than on-premises applications?



# CLOUD-NATIVE VS **VENDOR SECURITY**

When asked whether they prefer cloud-native security controls or using an independent security vendor for their cloud security needs, a majority of 57% prioritized cloud-native security controls.

- ▶ **Do you prefer cloud native security controls or using an independent security vendor for your cloud security needs?**



# 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 (68%). This is followed by ease of use (59%) and performance (52%).

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



**68%**

Cost



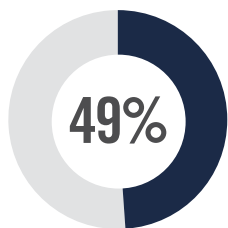
**59%**

Ease of use

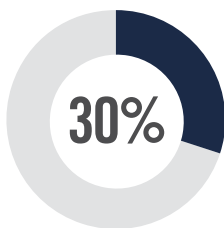


**52%**

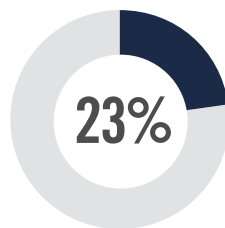
Performance



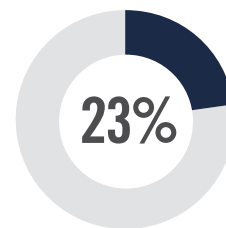
Less complexity and well integrated



Quicker deployments



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



No need to manage another vendor

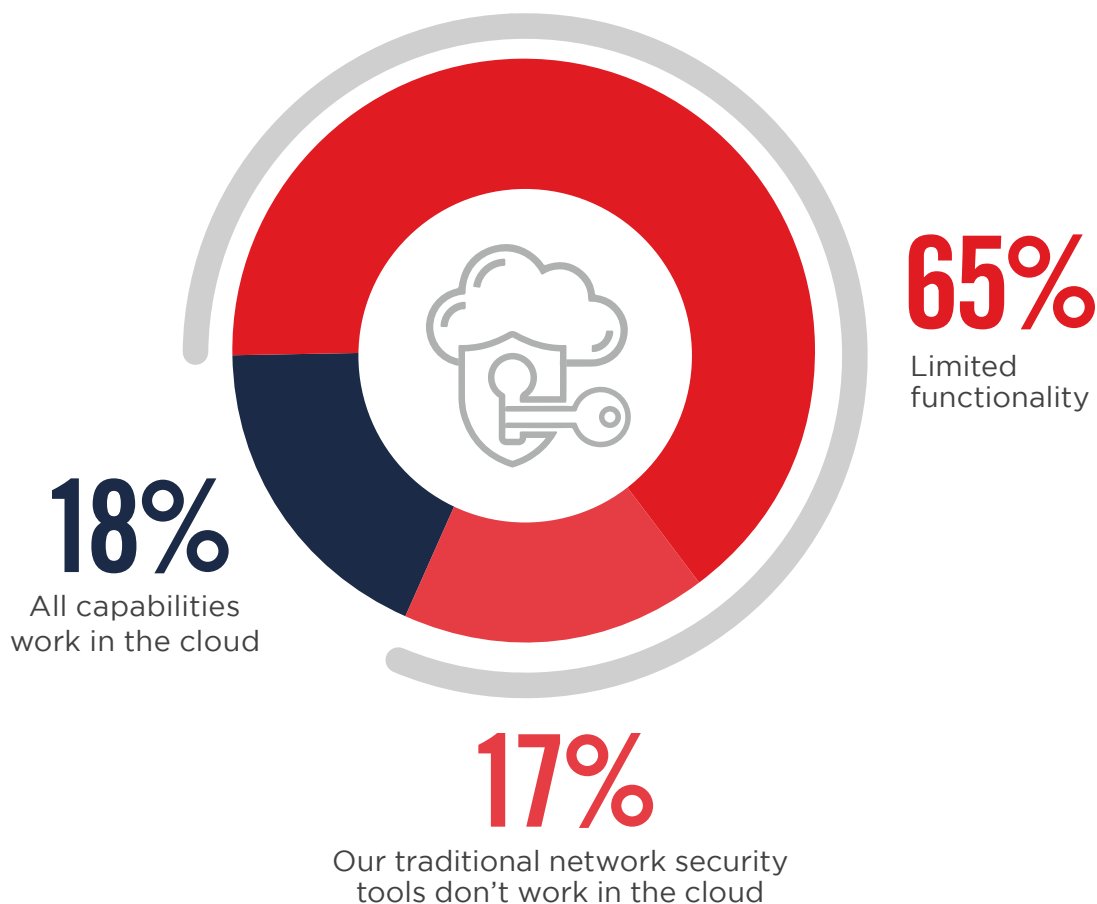
Other 5%

# 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?

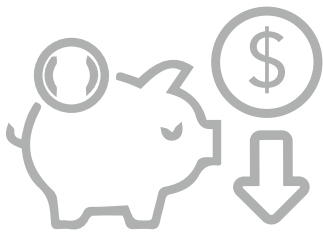
**82%** Say traditional security solutions either don't work at all in the cloud or have limited functionality.



# DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

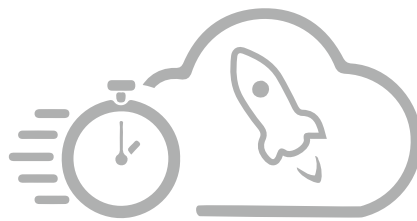
Organizations recognize several advantages of deploying cloud-based security solutions, including cost savings (55%), faster time to deployment (51%), and reduced efforts around patches and software updates (43%).

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



**55%**

Cost savings



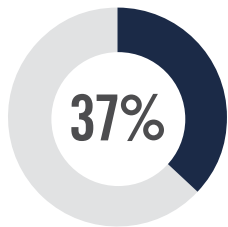
**51%**

Faster time to deployment

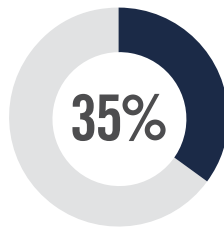


**43%**

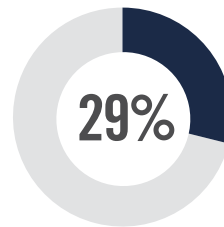
Reduced efforts around patches and upgrades of software



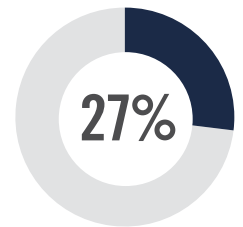
Reduction of appliance footprint in branch offices



Need for secure app access from any location



Better visibility into user activity and system behavior



Better performance

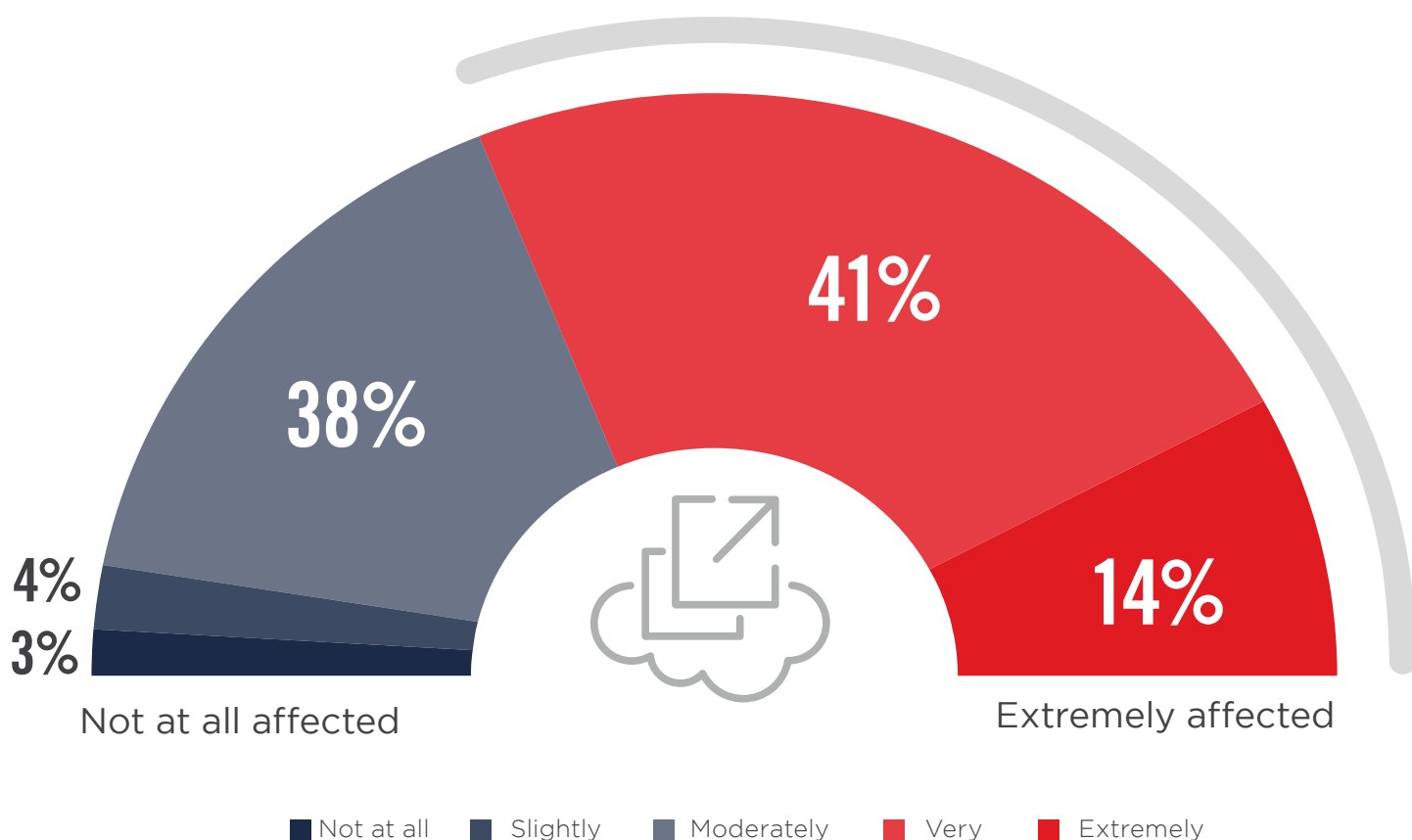
Easier policy management 24% | Better scalability 24% | Meet cloud compliance expectations 20% | Better uptime 20% | Our data/workloads reside in the cloud (or are moving to the cloud) 16%

# IMPACT OF CLOUD ARCHITECTURE

When asked how much architecture affects cloud security solutions, over half of the organizations (55%) confirm that cloud security scalability, performance, and uptime are very to extremely affected by cloud architecture.

- ▶ How much does architecture affect cloud security solution scalability, performance, and uptime? For example, comparing solutions built in the public cloud vs. security vendors' private data centers.

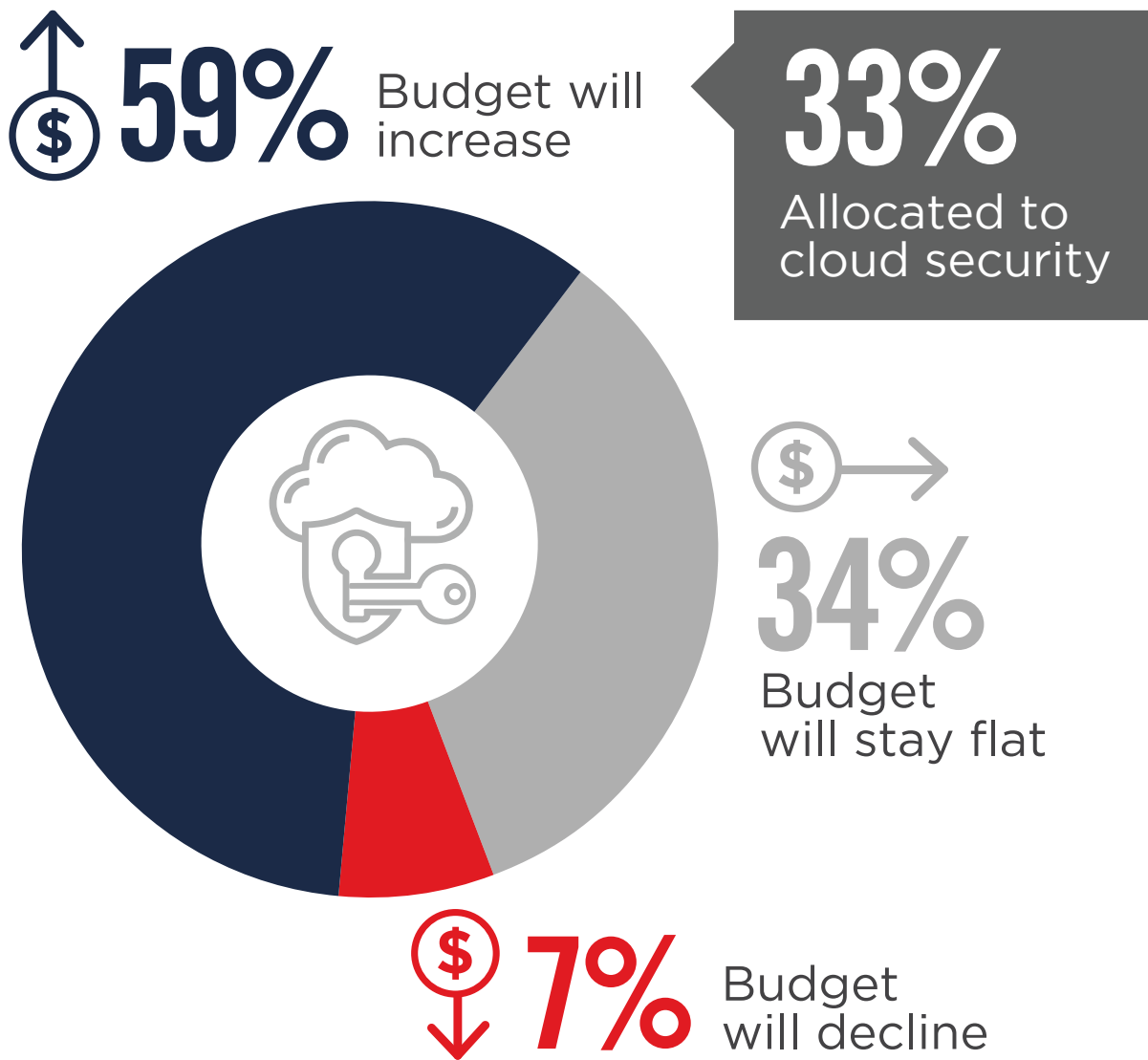
**55%** Confirm that cloud security scalability, performance, and uptime are very to extremely affected by cloud architecture.



# CLOUD SECURITY BUDGET

Nearly 60% of organizations expect their cloud security budget to increase over the next 12 months. On average, organizations allocate 33% of their security budget to cloud security.

- ▶ How is your cloud security budget changing in the next 12 months and what percentage of your IT security budget is allocated to cloud security?



# 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 (66%) and data privacy/confidentiality (63%). These are followed by concerns about accidental exposure of credentials (43%) and incident response (42%).

## ► What are your biggest cloud security concerns?



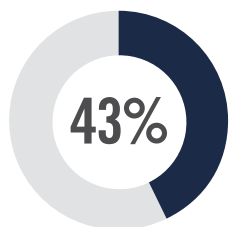
# 66%

Data loss/leakage

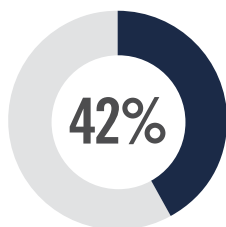


# 63%

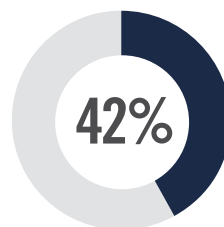
Data privacy/  
confidentiality



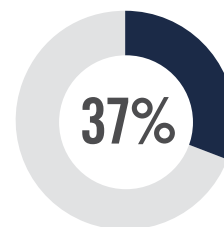
Accidental exposure of credentials



Incident response



Legal and regulatory compliance



Data sovereignty/  
residency/control

Visibility & transparency 29% | Availability of services, systems, and data 29% | Business continuity 28% | Lack of forensic data 27% | Disaster recovery 26% | Liability 24% | Fraud (e.g., theft of SSN records) 24% | Performance 21% | Having to adopt new security tools 21% | Not sure/other 7%

# 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 (68%) and anti-virus/anti-malware (54%), followed by multifactor authentication (47%).

## ► What security capabilities have you deployed in the cloud?



**68%**

Access control



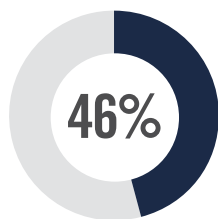
**54%**

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

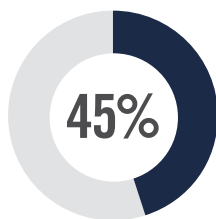


**47%**

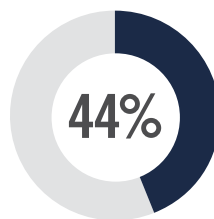
Multi-factor  
authentication



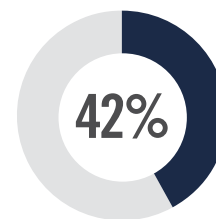
Cloud data  
backup



Data  
encryption



Firewalls/  
NAC



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

Single sign-on/user 37% | Network encryption (e.g., VPN, packet encryption, transport encryption) 36% | Endpoint security 35% | Log managements and analytics 32% | Configuration management 30% | Container security 30% | Other 4%

# CLOUD VISIBILITY

User logins (72%), file downloads (55%), and file uploads (50%) are the most frequently mentioned cloud activities administrators have visibility into. These concerns are followed by DLP policy violations (high-risk download/upload) (49%) and external sharing (45%).

## ► Which of the following cloud activities do you have visibility into?



**72%**

User logins



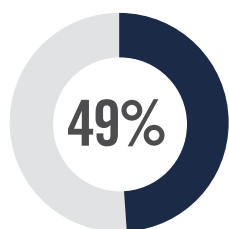
**55%**

File downloads

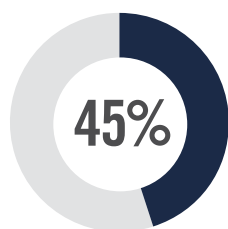


**50%**

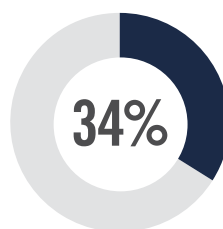
File uploads



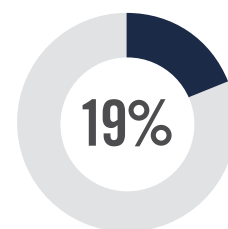
DLP policy violations  
(high-risk  
download/upload)



External  
sharing



User access to  
unmanaged  
applications/  
shadow IT



Cross-app  
anomalous  
behavior

Other 6%

# SECURITY DASHBOARDS

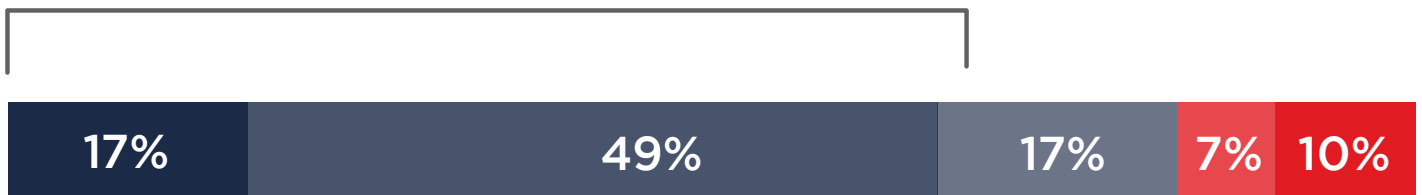
A majority of 66% of cloud administrators need to access at least four dashboards to configure cloud security policies today.

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



**66%**

Need to access at least 4 dashboards to configure cloud security policies.



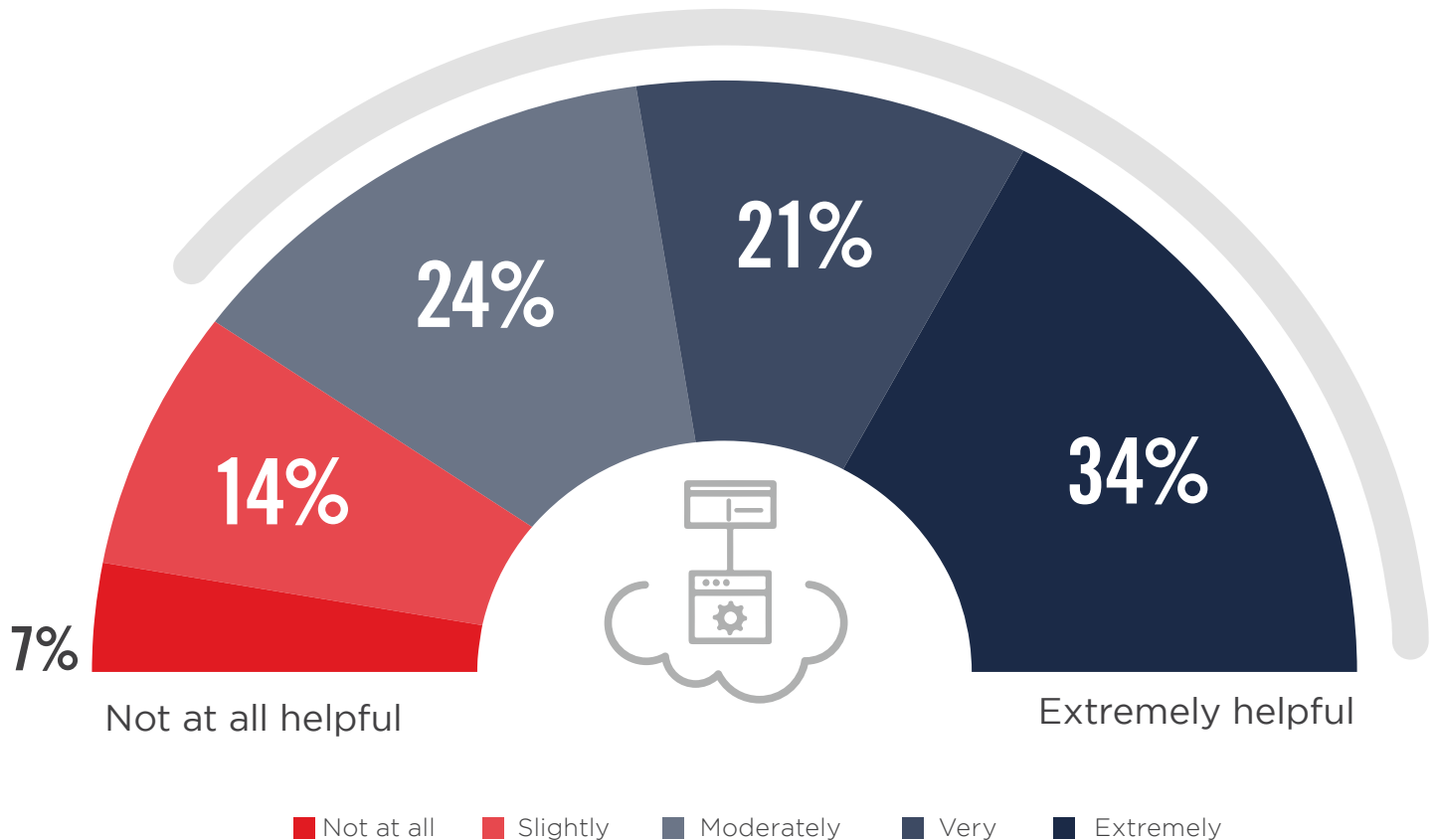
■ 1-2 ■ 3-4 ■ 5-6 ■ 7-8 ■ More than 10

# PREFERENCE FOR SINGLE DASHBOARD

Cloud administrators are increasingly overwhelmed with the proliferation of dashboards to manage different aspects of cloud security policy. A majority of 79% would consider it moderately to extremely helpful to have only a single dashboard to configure all of the policies needed to protect data consistently and comprehensively across their cloud footprint.

- ▶ 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?

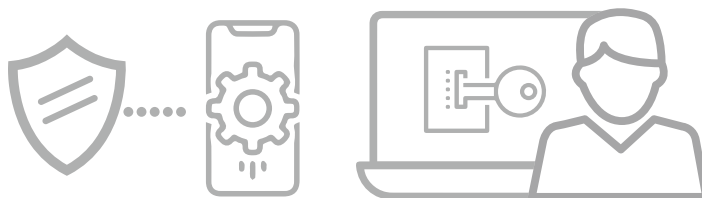
**79%** Would consider it moderately to extremely helpful to have a single cloud security dashboard.



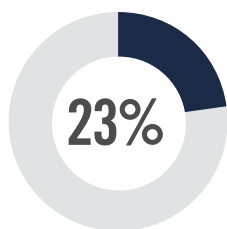
# PERSONAL DEVICE SECURITY

Employees increasingly use personal devices to access data in the cloud. To protect this use case, 40% of organizations install MDM agents on mobile devices to manage them remotely, 23% block all personal devices from accessing the cloud, both through policy or access controls, and 17% use a model that only allows access by trusted devices.

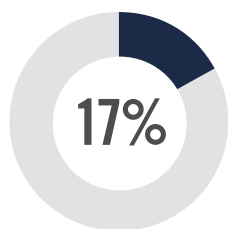
## ► What does your organization do for securing cloud data on employees' personal devices?



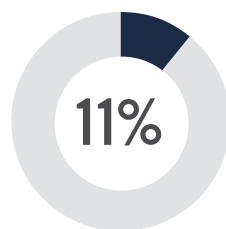
**40%** Install agents (MDM) on all personal devices



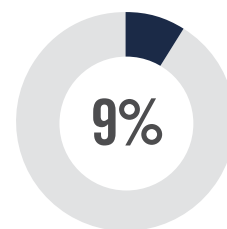
Block all personal devices



Use a trusted devices model



Grant access to any device

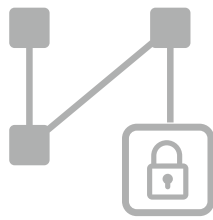


Apply DPL at upload or on download

# ANTI-MALWARE SOLUTIONS

When asked about the technologies organizations use to protect against malware, 65% prioritize endpoint protection solutions, followed by built-in cloud protections (57%) and secure web gateways (31%).

## ► What anti-malware tool does your organization currently use to secure cloud data?



**65%**

Endpoint protection



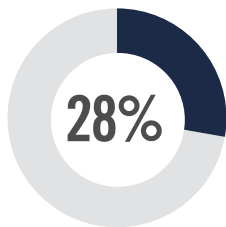
**57%**

Built-in protections in cloud apps such as G Suite and Office 365

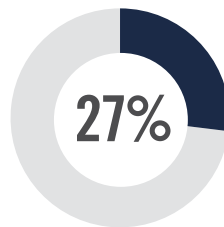


**31%**

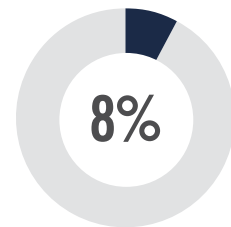
Secure Web Gateway (SWG)



Other third-party ATP solutions for cloud apps



Cloud access security browser

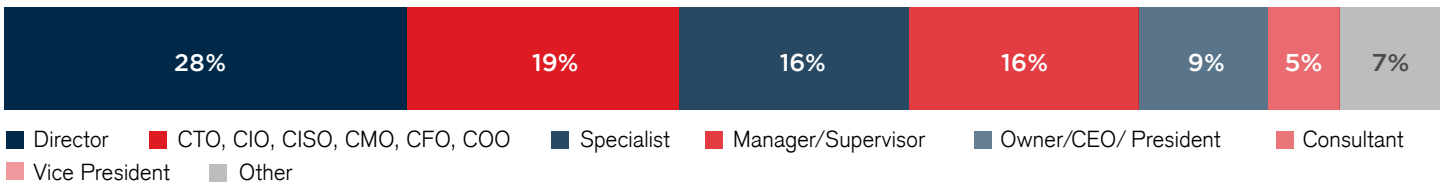


None of the above

# METHODOLOGY & DEMOGRAPHICS

The 2021 Cloud Security Report is based on the results of a comprehensive online survey of 351 cybersecurity professionals, conducted in October 2020, 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.

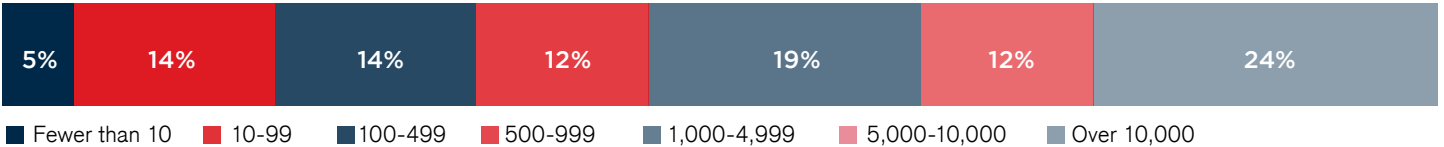
## CAREER LEVEL



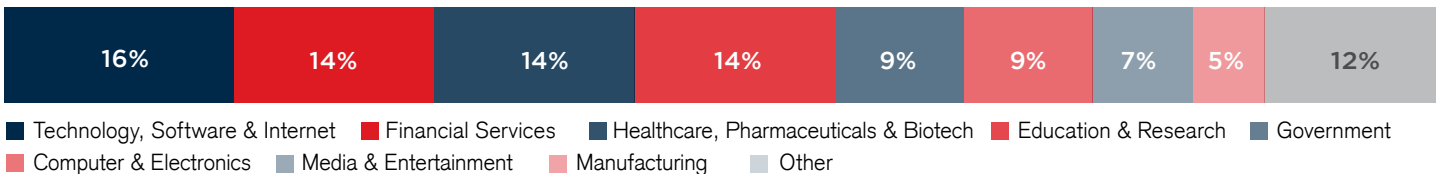
## DEPARTMENT



## COMPANY SIZE



## INDUSTRY





Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

[www.bitglass.com](http://www.bitglass.com)