SOPHOS

THE STATE OF CLOUD SECURITY 2020

The results of an independent study of 3,521 IT managers hosting data and workloads in the public cloud

A Sophos whitepaper July 2020

Introduction

Thanks to growing demand for remote working and public cloud services, on-premises infrastructure is shifting from asset to liability. But moving to the cloud comes at a cost: increasing every organization's attack surface. The numerous and well-publicized breaches of data storage services have raised cloud security awareness, but cybercriminals work diligently to stay one step ahead.

To understand the reality behind the headlines, Sophos commissioned an independent survey of 3,251 IT managers across 26 countries who are using the public cloud. The findings provide brand new insights into the concerns for security teams that host data and workloads in the public cloud; how attackers are changing the rules to find new ways into environments; and how to find the visibility you need – and perhaps the security gaps you never knew you had.

About the survey

Sophos commissioned research specialist Vanson Bourne to survey 3,521 IT managers currently hosting data and workloads in the public cloud about their experiences with cloud security. By public cloud we mean organizations using at least one of the following providers: Azure, Oracle Cloud, AWS, VMWare Cloud on AWS, and Alibaba Cloud. In addition, they may also have used Google Cloud and IBM Cloud. Sophos had no role in the selection of respondents and all responses were provided anonymously. The survey was conducted during January and February 2020.

48% of survey respondents using the public cloud were from small organizations (100-1000 employees), and 52% were from larger organizations (1001-5000 employees).

Respondents came from 26 countries across six continents:

COUNTRY	# RESPONDENTS
Australia	148
Belgium	66
Brazil	136
Canada	131
China	162
Colombia	120
Czech Republic	63
France	203
Germany	194

COUNTRY	# RESPONDENTS
India	227
Italy	128
Japan	126
Malaysia	79
Mexico	140
Netherlands	150
Nigeria	65
Philippines	62
Poland	53

COUNTRY	# RESPONDENTS
Singapore	158
South Africa	158
Spain	139
Sweden	72
Turkey	72
UAE	65
UK	191
US	413

Respondents came from a range of sectors, both public and private.

SECTOR	# RESPONDENTS	% RESPONDENTS
IT, technology and telecoms	735	21%
Manufacturing and production	466	13%
Retail, distribution and transport	449	13%
Financial services	409	12%
Business and professional services	357	10%
Public sector	308	9%
Construction and property	177	5%
Energy, oil/gas and utilities	125	4%
Media, leisure and entertainment	120	3%
Other	375	11%

Executive summary

The survey provides fresh new insights into the experiences of organizations hit by cybercriminals in the public cloud, including:

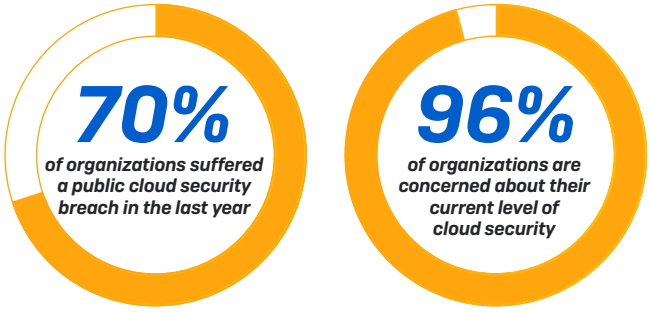
- **Almost three-quarters of organizations hosting data or workloads in the public cloud experienced a security incident in the last year.** Seventy percent of organizations reported they were hit by malware, ransomware, data theft, account compromise attempts, or cryptojacking in the last year.
- **Data loss/leakage is the number one concern for organizations.** Data loss and leakage topped our list as the biggest security concern, with 44% of organizations seeing data loss as one of their top three focus areas.
- **Ninety-six percent of organizations are concerned about their current level of cloud security.** Data loss, detection and response, and multi-cloud management top the list of the biggest concerns among organizations.
- **Multi-cloud organizations reported more security incidents in the last 12 months.** Seventy-three percent of the organizations surveyed were using two or more public cloud providers and reported more security incidents as those using a single platform.
- **European organizations may have the General Data Protection Regulation (GDPR) to thank for the lowest attack rates of all regions.** The GDPR guidelines' focus on data protection, and well-publicized ransomware attacks have likely led to these lucrative targets becoming harder for cybercriminals to compromise in Europe.
- **Only one in four organizations see lack of staff expertise as a top concern despite the number of cyberattacks reported in the survey.** When it comes to hardening security postures in the cloud, the skills needed to create good designs, develop clear use cases, and leverage third-party services for platform tools are crucial but underappreciated.
- **Two-thirds of organizations leave back doors open to attackers.** Accidental exposure through misconfigurations continues to plague organizations. Security gaps in misconfigurations were exploited in 66% of attacks (either through attackers exploiting a flaw in the web application firewall to access account credentials or attackers taking advantage of a misconfigured resource), while 33% of attacks used stolen credentials to get into cloud provider accounts.

Use of data and charts in this report

Part 1: The prevalence of cloud attacks

Seven in 10 organizations have been hit by a cyberattack

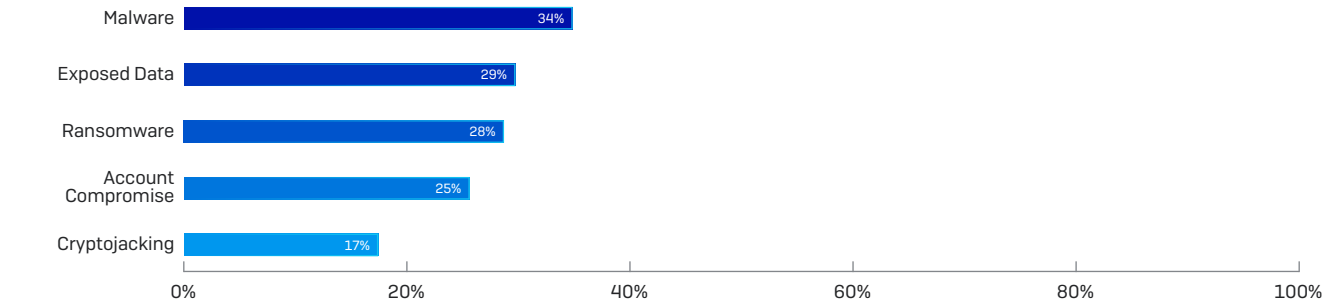
Seventy percent of respondents said they had suffered a public cloud security breach in the last year. This is extremely worrisome for organizations, with 96% of the 3,521 respondents expressing concern about their current level of security across the six major public cloud platforms listed, including Amazon Web Services, Microsoft Azure, and Google Cloud Platform.



As you move, so does the target

Among organizations suffering a cyberattack in the cloud, the breakdown of attack types reads like the usual suspects: 50% of organizations were hit by malware of some form, including ransomware (respondents could select multiple options).

Organizations suffering security incidents in the last year

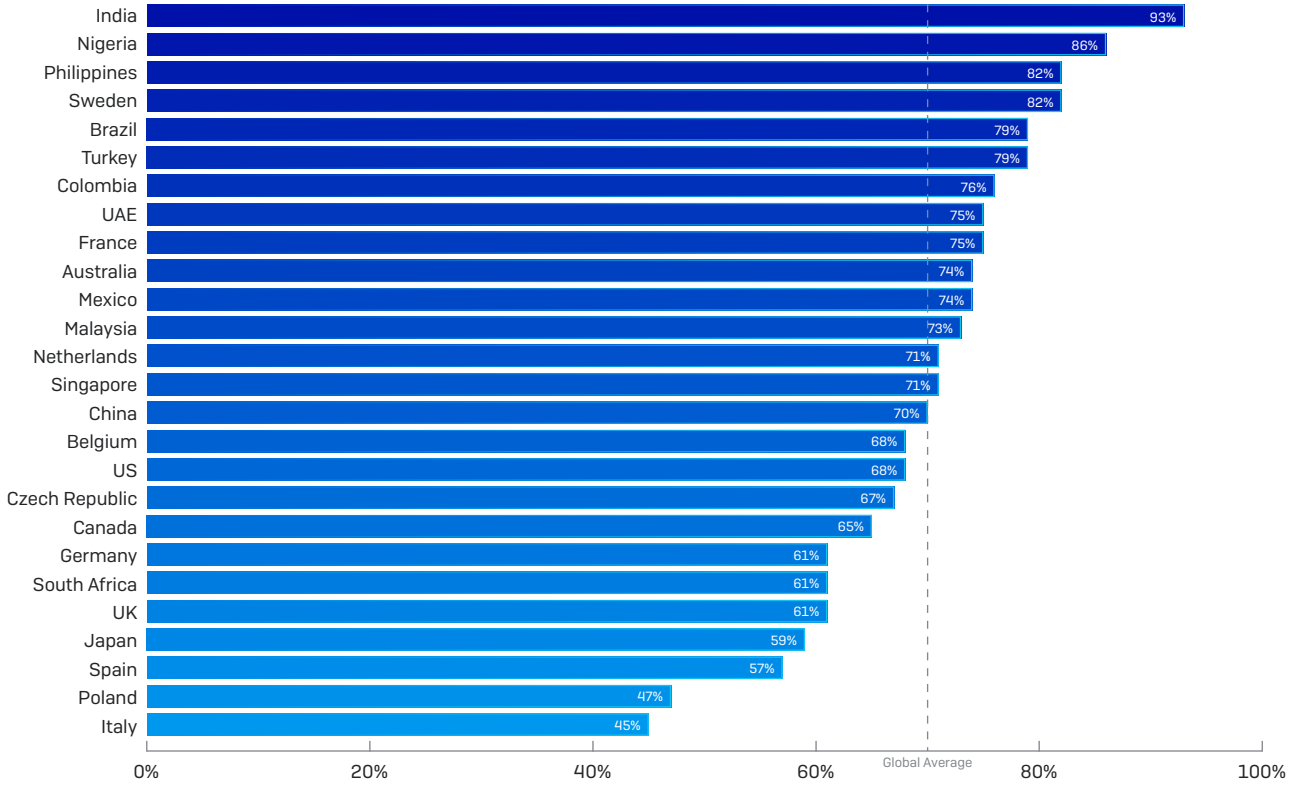


Has your organization suffered a public cloud security incident in the last 12 months? Base 3,521 respondents

Attack levels vary across the globe

Looking at the number of public cloud attacks across the globe reveals interesting variations. This is likely due to criminals focusing their efforts where they see the greatest opportunity for return. Country-level analysis also showed differing levels of protection and visibility of cloud environments, and awareness of cloud security responsibilities and best practices.

Organizations suffering public cloud security incidents in the last year



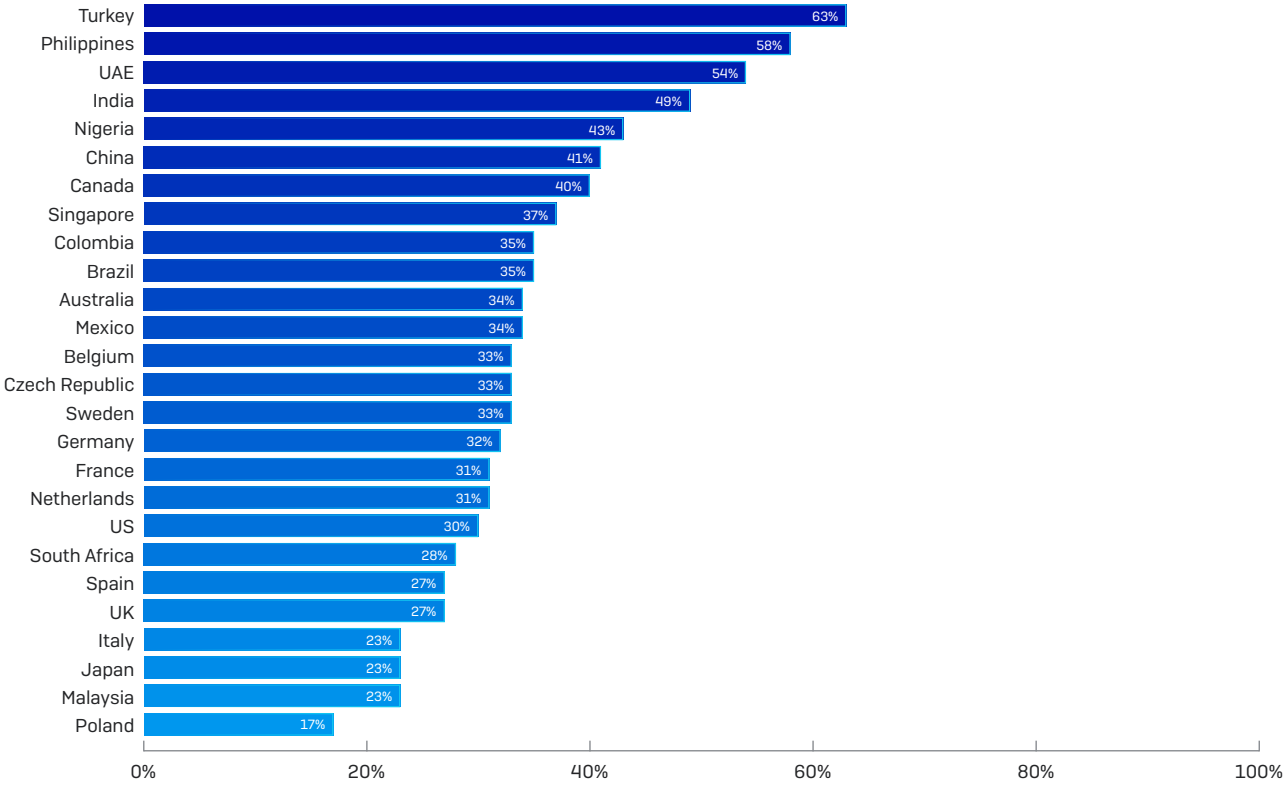
Has your organization suffered a public cloud security incident in the last 12 months? Combination of "Yes" answers ("Yes Malware", "Yes, Exposed Data", "Yes, Ransomware", "Yes, Account Compromise", and "Yes, Cryptojacking." Base 3,521 respondents

- **India** (227 respondents) tops the list with 93% of organizations reporting being hit by a cyberattack in the last year, despite 92% of organizations reporting they had complete visibility of all cloud assets. This indicates a lack of complete cyber hygiene, creating weaknesses in cloud security configurations which make organizations vulnerable to attack.
- This trend of the highest proportion of attacks echoes throughout the **Asia-Pacific (APAC)** region, with the highest regional rates of exposed data (35%), ransomware attacks (37%), and account compromise (33%) among the survey respondents.
- **Europe** (1259 respondents) may have GDPR to thank for its low attack rate, with European respondents suffering the lowest percentage of security incident rates of all respondents in the last year. This includes Italy (45%), Poland (47%), Spain (57%), UK (61%) and Germany (61%).

The focus on protection of data and well-publicized ransomware attacks have likely led to these lucrative targets being better protected than other regions. As a result, Europe shows the lowest rates of malware infections (29%), exposed data (24%), and ransomware attacks (22%) among the survey respondents. This also explains the higher comparative levels of account compromise incidents (21%) and cryptojacking (15%), as attackers move to exploit resource misconfigurations and over-privileged IAM roles to compromise cloud environments.

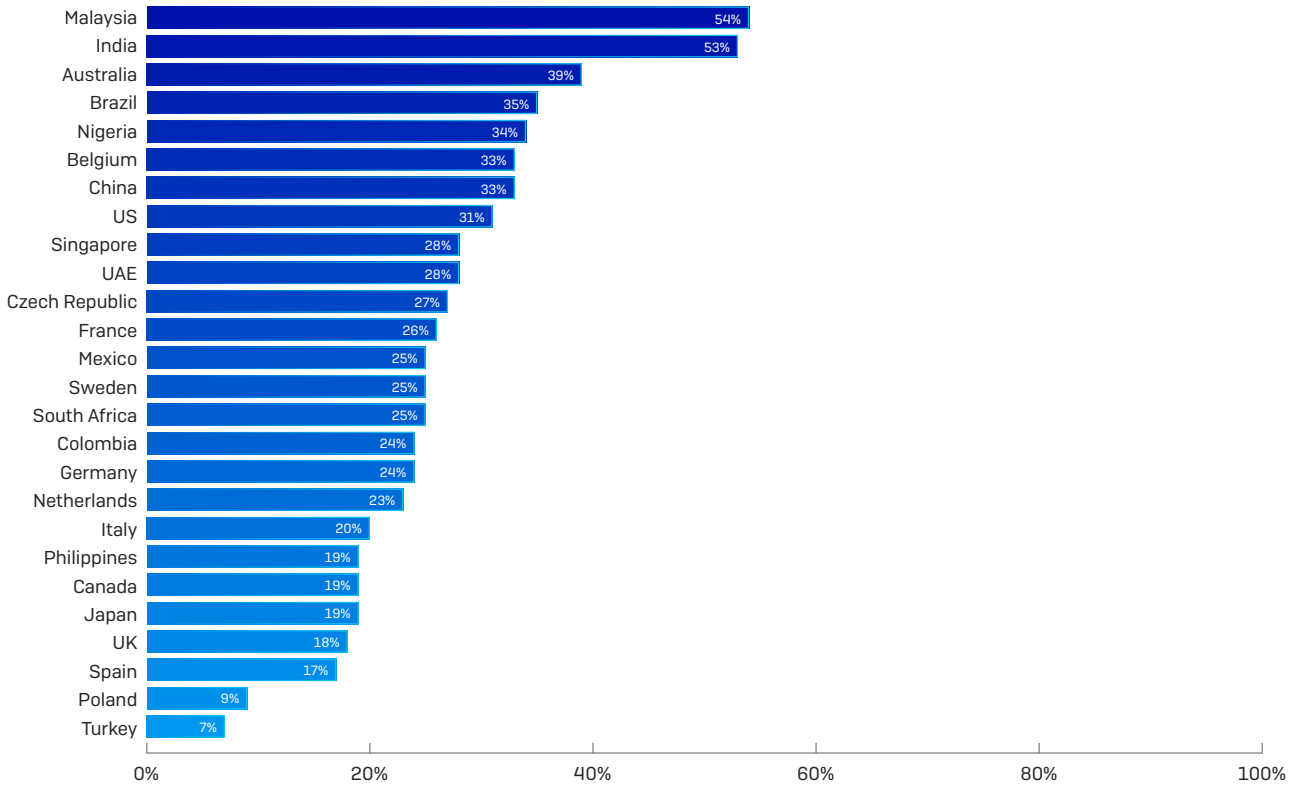
- **Middle East and Africa** (360 respondents) has some of the lowest attack rates outside of Europe, the result of geo-targeted attacks that go after the most lucrative opportunities. However, value is in the eye of the beholder. Here we see cryptojacking at its highest among all regions (22%) as criminals spin up hundreds of virtual servers to run illegal cryptomining and escape before being discovered.
- **United States** (413 respondents) reported surprisingly few incidents despite being the largest group of survey respondents. It was in the bottom 35% of countries suffering security incidents in the last year. As an advanced, Western country, it could be considered a lucrative target, yet only 30% of respondents report being hit by malware, 31% by ransomware, 28% suffering a data breach, and 21% having account credentials compromised. Contributing factors here point to clear ownership of security, with 90% of organizations understanding their responsibility for cloud security. With 85% of organizations being aware of all their cloud assets, the U.S. is a full 17 percentage points higher than the global awareness average.

Organizations hit by malware in the public cloud in the last year



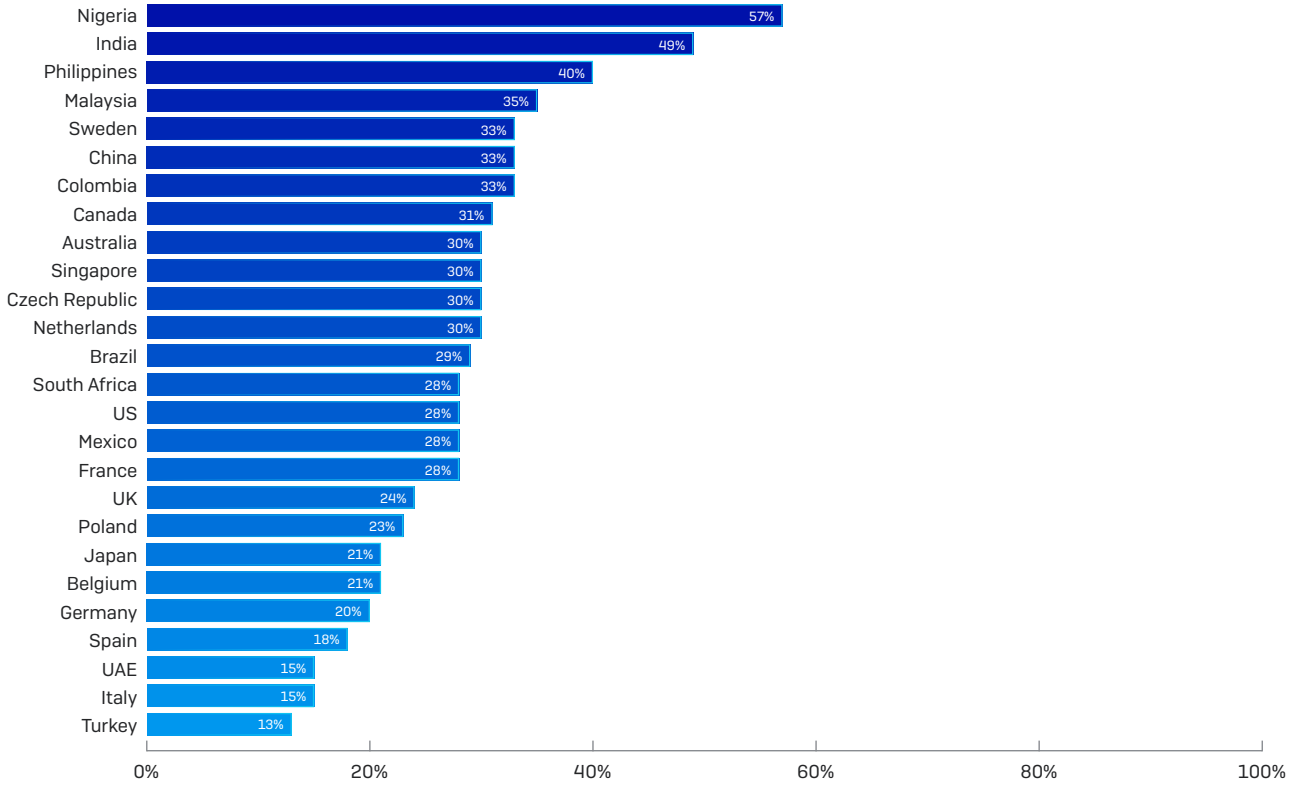
Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Malware". Base 3,521 respondents

Organizations hit by ransomware in the public cloud in the last year



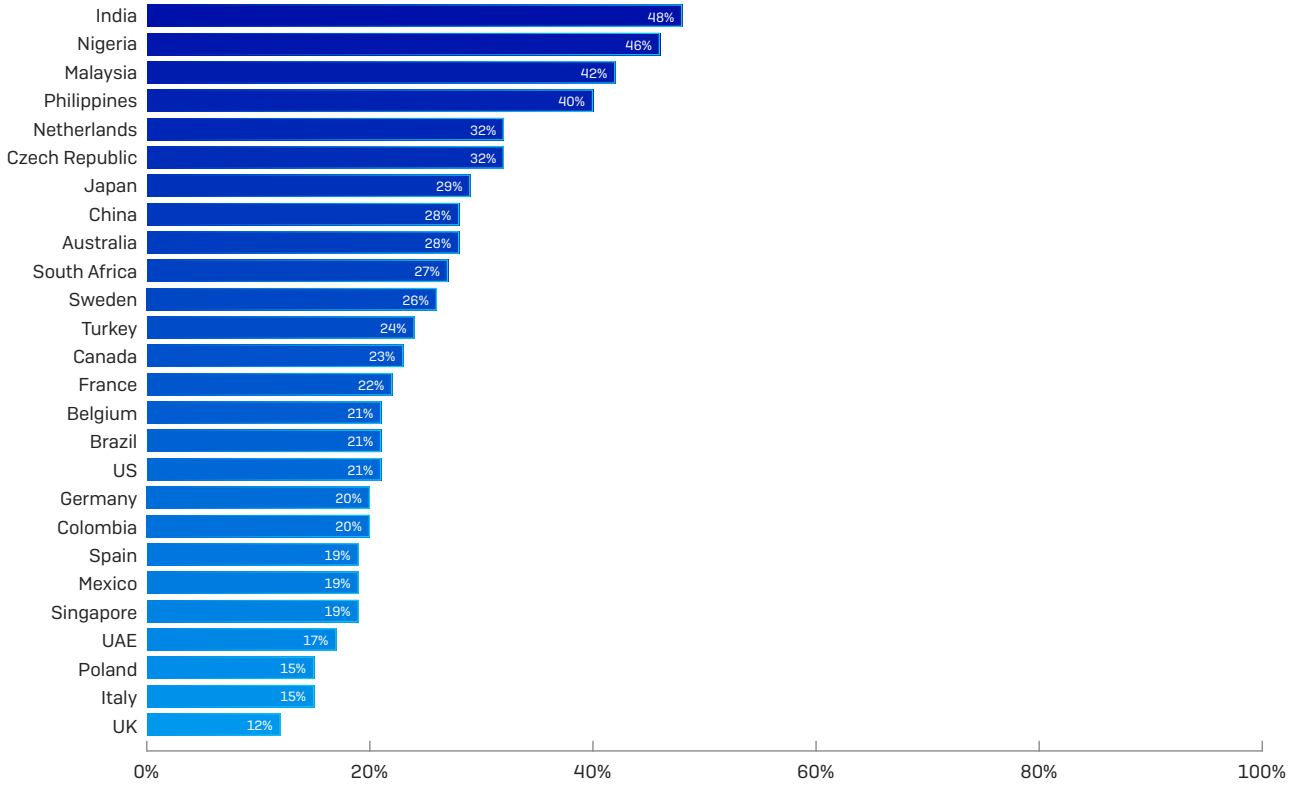
Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Ransomware". Base 3,521 respondents

Organizations with public cloud data exposed in the last year



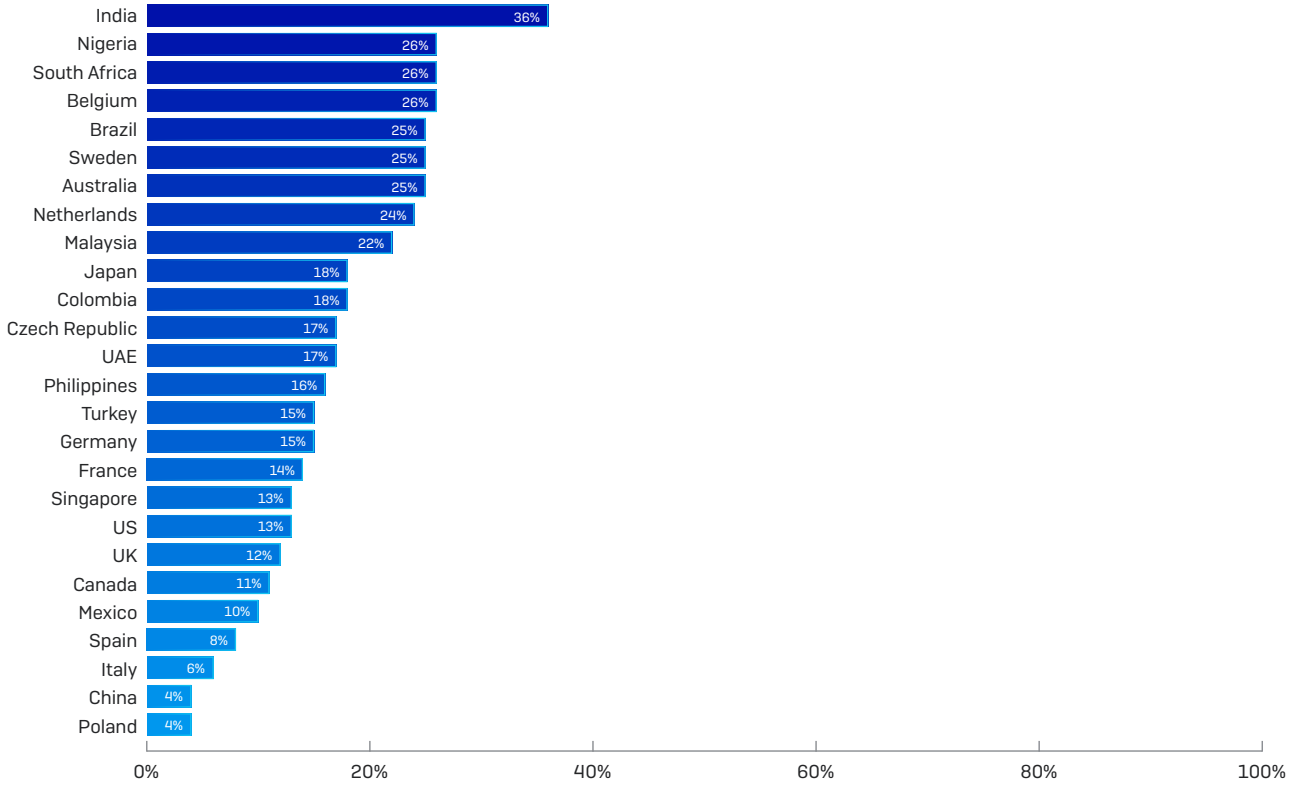
Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Exposed Data". Base 3,521 respondents

Organizations with cloud account credentials stolen in the last year



Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Stolen Credentials". Base 3,521 respondents

Organizations suffering a cryptojacking cyberattack in the public cloud in the last year



Has your organization suffered a public cloud security incident in the last 12 months? "Yes, Cryptojacking". Base 3,521 respondents

Part 2: How criminals are getting in

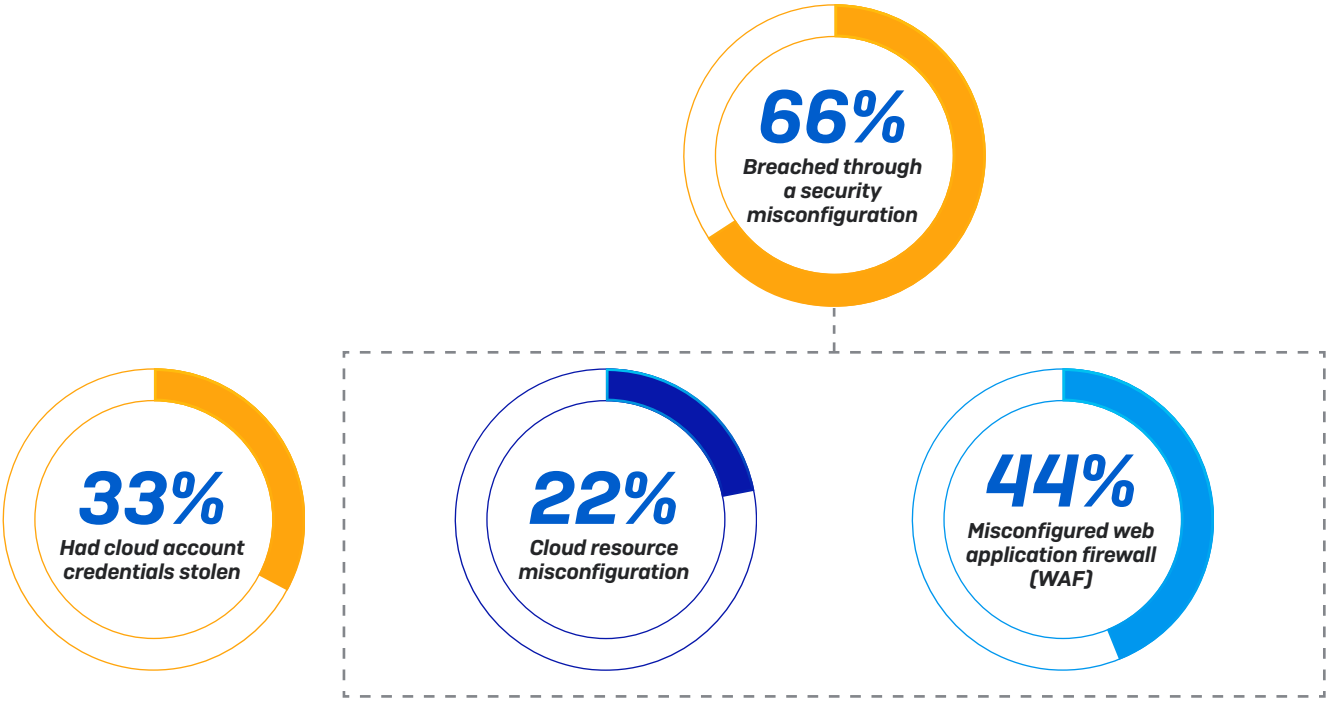
Two-thirds of organizations leave back doors open to criminals

When it comes to the cloud, it's best to think of a network like a building with multiple windows and multiple openings – they all add up to multiple potential access points for someone, or something, to get in and out.

For example, a misconfigured route table on an organization's firewall leaves the window open. Virtual machines running private server workloads or hosting sensitive data suddenly become accessible from the internet.

Accidental exposure continues to plague organizations, and this is reflected in our survey responses. Security gaps in misconfigurations were exploited in 66% of attacks, while 33% of attacks used stolen credentials to get into cloud provider accounts.

As organizations start to introduce new cloud services in order to provide shared storage, containers, database services, and serverless functions, the potential for misconfiguration only increases, which in turn expands an organization's attack surface.



How did the attacker get into your organization's environment? Base 3,521 respondents

Entry methods vary across the globe

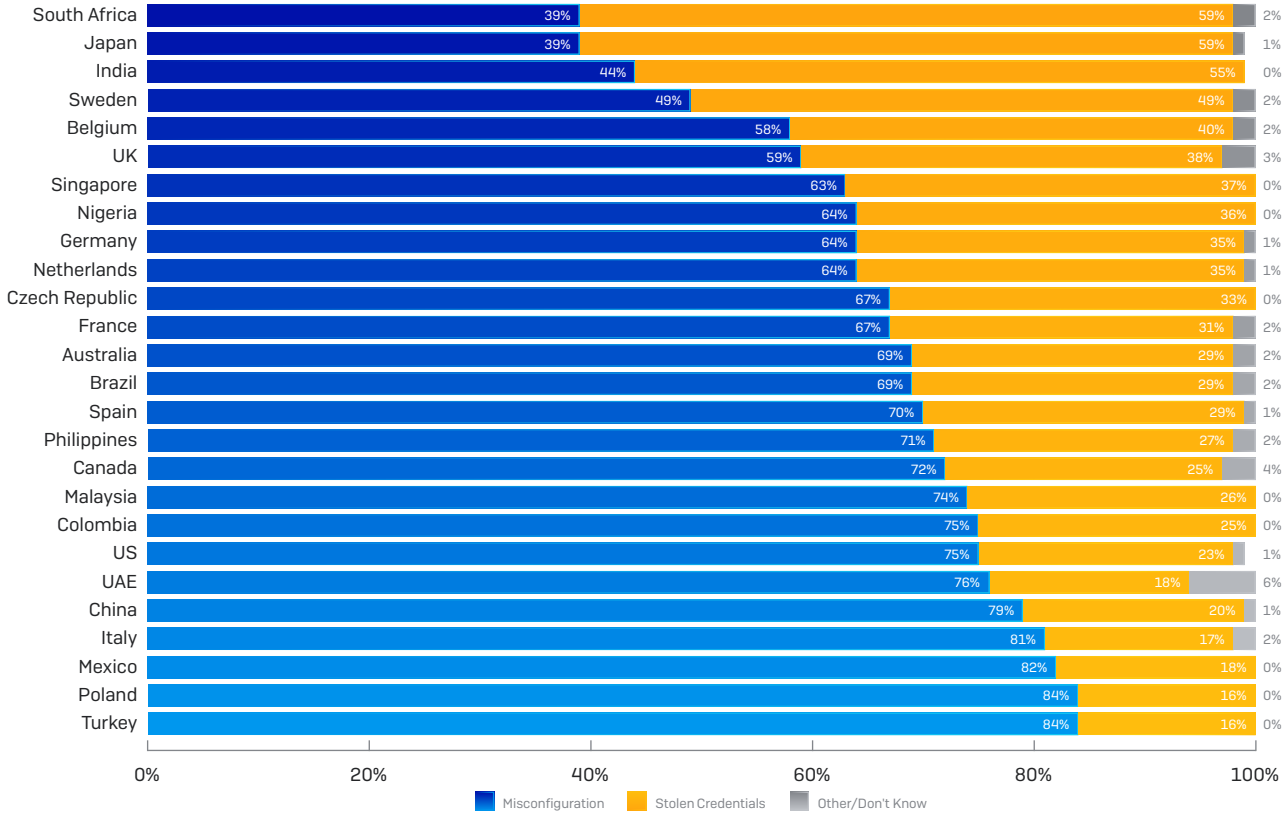
Every organization represents value to a cybercriminal. That value might be in the data that can be sold or held onto for ransom. It could also be the organization's wallet that's used to pay for cryptomining virtual machines. And while in the real world, targeting based on Gross Domestic Product (GDP) or industry sectors may be the norm, isn't as clear cut in the cloud.

An organization's security posture is often the deciding factor when it comes to choosing entry methods and weak points (misconfiguration 66%, or credentials 33%). But it's important to realize that though misconfigurations can still give cybercriminals access to cloud accounts, such access may last for less time: up to six hours or so when temporary credentials are obtained thanks to a resource misconfiguration, for instance.

Our survey also highlights the role that visibility of cloud assets plays when it comes to how an organization is targeted:

- **South Africa** and **Japan** showed the highest number of stolen cloud provider account credentials in our survey. These organizations also have amongst the highest levels of asset visibility across cloud environments, which suggests a stronger security posture overall with less chance of misconfigurations.
- **Turkey** and **Poland** show the reverse: with the lowest levels of visibility, these organizations were most likely to be attacked via misconfigured cloud assets.

How organizations were compromised



How did the attacker get into your organization's environment?" Base 2,456 respondents. Due to rounding, occasionally the totals do not add up to 100%

Identity security represents a huge challenge

A review of cloud accounts by the Sophos Cloud Optix cloud security posture management service discovered worrying trends in organizations' security posture as it relates to cloud account access.

Thirty-three percent of organizations reported that cybercriminals gained access by stealing cloud provider account credentials. Once inside, however, all attacks utilized Identity and Access Management (IAM) roles and permissions to navigate the compromised cloud accounts. Managing access to cloud accounts is an enormous challenge and yet only quarter of organizations in our survey saw it as a top area for concern.

The scale and interwoven nature of individual and group access to services means that organizations often simply can't accurately see how their services can be accessed, and this lack of visibility is exploited by attackers.

Why it Matters

Granting extensive access permissions to IAM users, groups and cloud services is a risky practice. If those credentials are compromised, the cybercriminals will have access to any services and data those permissions grant.

Why it Matters

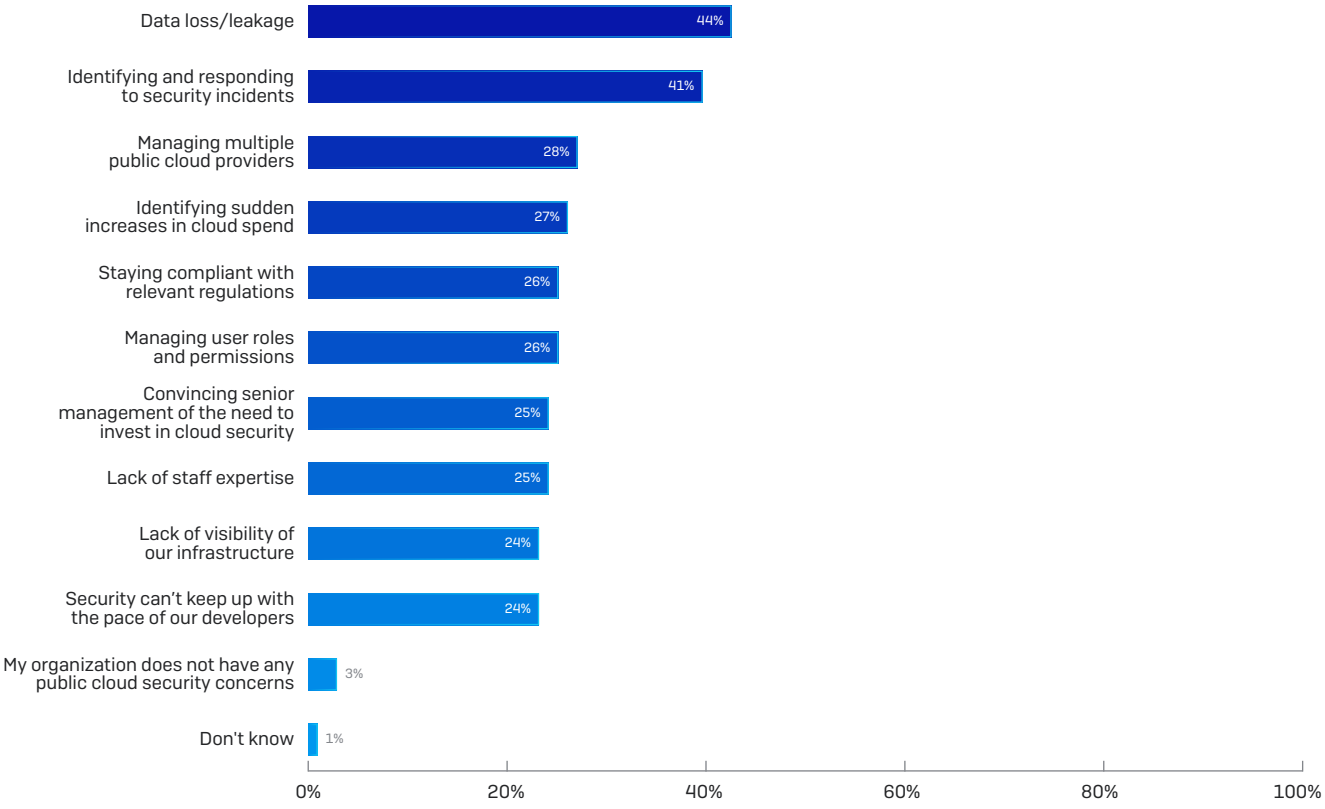
All user accounts should have MFA enabled to ensure protection against password compromises. MFA adds an extra layer of protection on top of a username and password.

Part 3: Organizations are not focusing on root causes

The most worrying outcome for organizations is data loss

Data security topped the list as the most likely concern, cited by 44% of respondents. The rapid growth of cloud usage has resulted in fractured distribution of data, with 73% of organizations now utilizing at least two public clouds platforms. This multi-platform approach compounds the visibility challenge for security teams, who often must switch between multiple platforms for a complete picture of cloud assets.

Top cloud security concerns among organizations



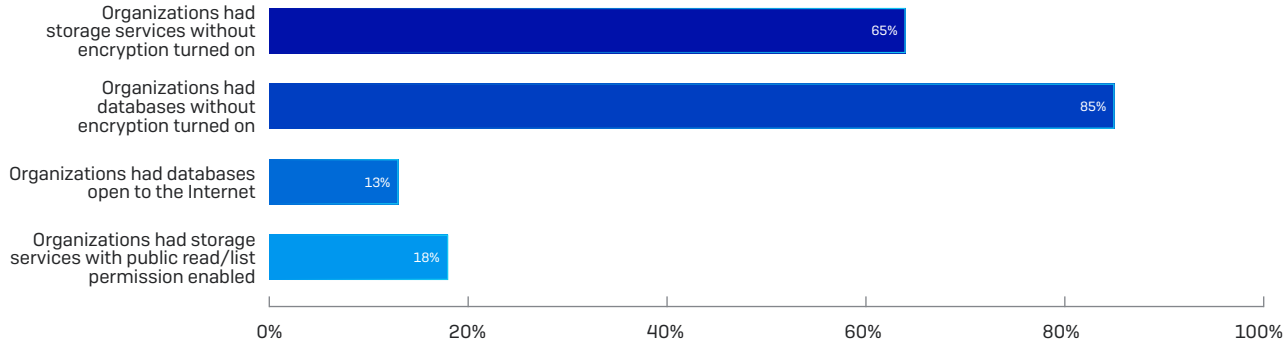
Combination of responses ranked first, second and third for the question "What are your organization's biggest public cloud security concerns?" Base 3,521 respondents

A significant root cause is a lack of cloud expertise

To properly secure a cloud environment, good design and clear use cases are necessary in order to leverage platform tools effectively and extend them with third-party services. This requires skilled experts, either employed directly by organizations or available through partners. Unfortunately, while 70% of organizations in our survey suffered a security breach in the last year, only a quarter see lack of staff expertise as a top concern.

The impact of configurations on data security

A review of cloud accounts by the Sophos Public Cloud Security team discovered that accidental data exposure through misconfigured storage services continues to plague organizations, with 60% leaving information unencrypted. Organizations are making it easy for attackers to search for and identify new targets.

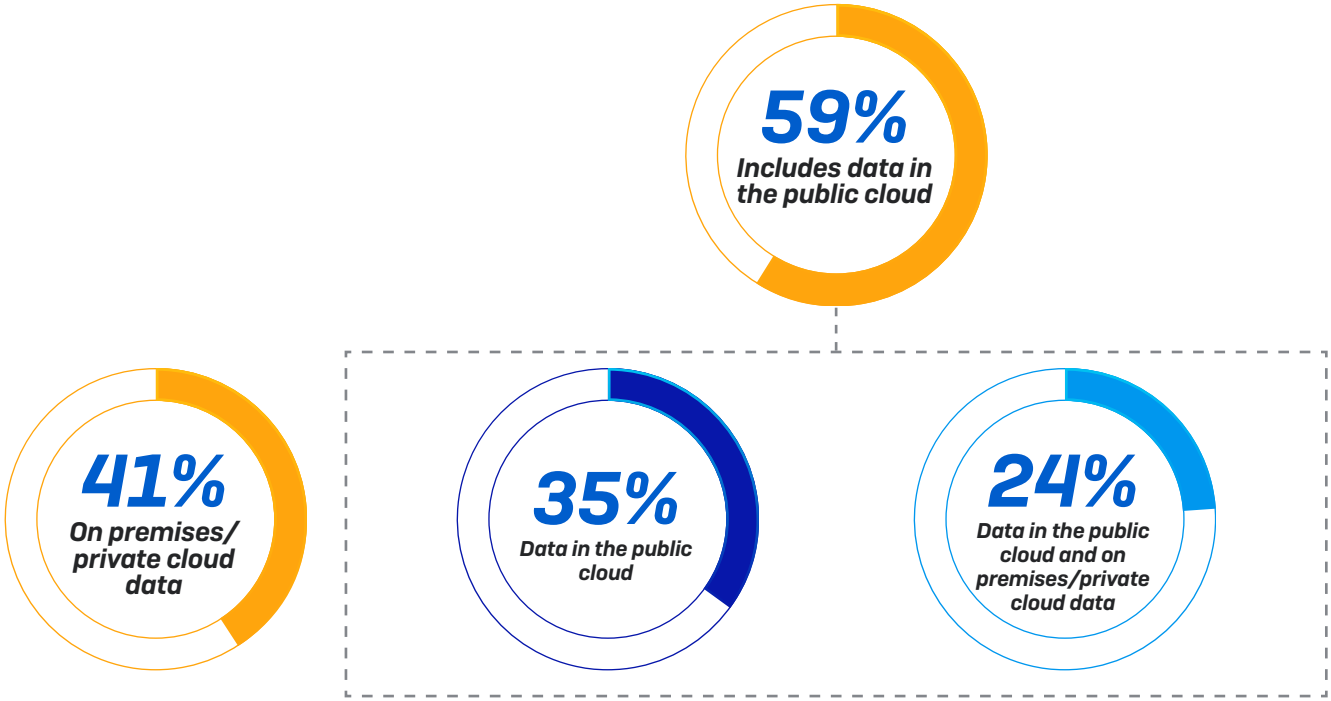


Why it matters

Encryption is critical in stopping cybercriminals from seeing and reading stored information, and is a requirement for many compliance and security best-practice standards. While "public mode", a setting that can be applied to databases, shared storage and other cloud provider services is a major course of data breaches. Misconfiguring cloud services in "public mode" allows cybercriminals to automate their searches for these weak points in security. Guardrails should be in place to prevent such misconfigurations.

Most successful ransomware attacks now hit the public cloud

In parallel to this cloud security survey, Sophos recently released a survey of 5,000, IT managers that explored their experiences with ransomware. Among those organizations, 59% of attacks where the data was encrypted involved data in the public cloud. While it's likely that respondents took a broad interpretation of public cloud – including cloud-based services such as Google Drive and Dropbox, and cloud backup such as Veeam – it's clear that cybercriminals are targeting data wherever it's stored.

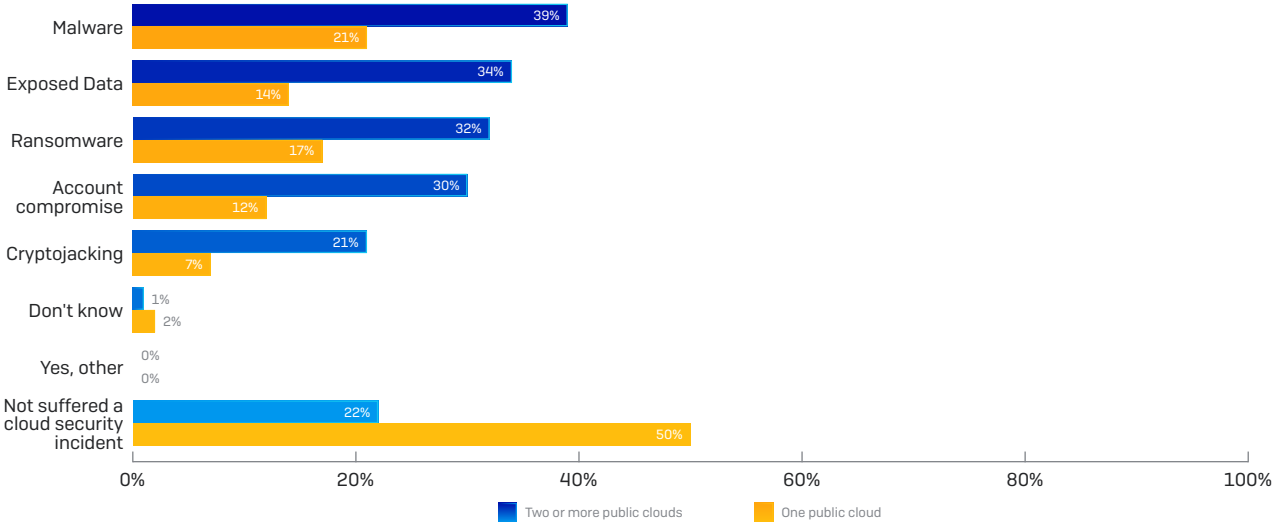


Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? Responses from respondents whose organization's data had been encrypted in the most recent ransomware attack. Base: 1,849 respondents.

Multi-cloud creates multiple challenges

Security risks inevitably multiply as organizations expand their number of cloud environments. Seventy-three percent of the organizations surveyed were using two or more public cloud providers and reported up to twice as many security incidents as those using one cloud platform.

Single and multi-cloud organizations hit by cyberattacks in the last year



Multi-cloud organizations include those respondents selecting one or more cloud providers for the question "Which of the following public clouds does your organization host data or workloads in?" Base 3,521 respondents

The secret to effective cybersecurity across dispersed environments in Amazon Web Services, Microsoft Azure, and Google Cloud Platform is to improve overall security posture and address the most important security aspects. Ensure architecture is secure and configured correctly, gain complete architecture visibility, regularly review who has access to cloud accounts and services (including permissions levels), and, importantly, ensure consistent security management across multiple cloud environments.

Recommendations

Moving from traditional to cloud-based workloads offers huge opportunities for organizations of all sizes, yet this survey has confirmed that securing the public cloud is imperative. It also provides insight into how to minimize the risk of a security incident:

1. **Start with the assumption that attackers will find cloud assets.** Cybercriminals are automating their searches for vulnerable cloud services. Whether an organization has used the cloud to host data and workloads for some time or has recently accelerated the use of public cloud provider services, accurate visibility of cloud services in use is the only guaranteed route to ensure they are configured securely and protected against threats.
2. **Invest in cloud workload protection with anti-malware technology.** Seventy percent of survey respondents suffered a security incident in the last year. Among that majority, 34% were hit by malware, 28% hit by ransomware (an advanced form of malware), and 17% were hit by cryptojacking (which can be malware). These results highlight that malware is the number one threat to organizations and the sensitive data they hold.
3. **Protect data wherever it's held.** Data protection is the highest concern for global organizations. Almost 60% of ransomware attacks in the last year that successfully encrypted data included data in the public cloud. Cloud strategies should include protecting data in the public cloud, private cloud, and on premises.
4. **Continually monitor cloud resource configurations.** Two-thirds of survey respondents were compromised through misconfigured cloud resources, allowing attackers to exploit these weaknesses to carry out malicious activity. Proactive monitoring of configurations by a security team can significantly reduce the likelihood of breaches.
5. **Proactively manage cloud access.** On average, IAM roles were compromised in 33% of cyberattacks reported by the survey respondents, rising to 59% in specific countries. Effective management of individual and group user permissions is key to ensuring over-privileged roles are not compromised.
6. **Provide secure remote access for workers.** Ensure the same level of protection is in place for virtual desktops as it is for other critical server workloads. Virtual desktops run on virtual machines, which are susceptible to the same threats. Likewise, as remote workers access private applications and sensitive data, they should be equipped with VPN access to ensure secure connections.
7. **Deploy a layered defense.** Cybercriminals use a wide range of techniques to get around defenses. When one is blocked, they move on to the next one until they find something a weakness that can be exploited. Make sure to defend against all possible vectors of attack.
8. **Learn responsibilities for securing public cloud provider services.** Public cloud providers offer a great deal of flexibility. And while they're responsible for physical protection at the datacenter and virtual separation of customer data and environments, whatever organizations store or run in the cloud is their responsibility to secure. Almost half of survey respondents didn't fully understand their responsibilities. To find out more, visit the Amazon Web Services or Microsoft Azure websites.

Secure the cloud with Sophos

Protection from the latest generation of public cloud cyberattacks requires a new level of visibility and security automation. Sophos gives you the advanced protection technologies you need to disrupt the entire attack chain.

- **Sophos Cloud Optix** extends detection and response in the public cloud. Continually monitor cloud infrastructure configurations to detect insecure deployments, suspicious access events, over-privileged IAM roles, unusual network traffic, and sudden spikes in cloud spend, with guided remediation to shrink incident response times. Guardrails lock down configurations to stop accidental or malicious changes that could impact security posture.
- **Sophos Intercept X for Server with EDR** secures cloud, on-premises, or hybrid workload environments. It protects Windows and Linux virtual machines and virtual desktops from the latest threats, including ransomware, file-less attacks, and server-specific malware. Automate detection and response with unparalleled visibility to hunt down evasive threats, see and control exactly which apps are running, and automatically respond to incidents.
- **Sophos XG Firewall** protects the network edge with the ultimate all-in-one firewall solution. Get deep packet inspection with VPN for remote workers, IPS, ATP, URL filtering, bidirectional antivirus for WAF with authentication offloading, path-based routing, and country-level blocking. Synchronized communication with cloud workloads automates isolation and malware clean-up.

Start an instant demo at

www.sophos.com/demo

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-06-18 WPEN (DD)

SOPHOS