2019

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

netskope

INTRODUCTION

Organizations continue to adopt cloud computing at a rapid pace to benefit from the promise of increased efficiency, better scalability, and improved agility.

While cloud service providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) continue to expand security services to protect their evolving cloud platforms, it is ultimately the customers' responsibility to secure their data within these cloud environments.

The 2019 Cloud Security Report highlights what is and what is not working for security operations teams in securing their cloud data, systems, and services in this shared responsibility model.The results are a continuation of past challenges:

- The top three cloud security challenges faced by cybersecurity professionals are data privacy (52%) and protecting against data loss and leakage (51%).
- Insecure interfaces and APIs take the number one spot in this year's survey as the single biggest perceived vulnerability to cloud security (57%). This is followed by misconfiguration of the cloud platform (48%),and unauthorized access through misuse of employee credentials and improper access controls (46%).
- The top two operational security headaches SOC teams are struggling with are compliance (45%) and lack of qualified security staff (44%).

Overall, the findings in this report emphasize that security teams must reassess their security posture and strategies, and address the shortcomings of legacy security tools to protect their evolving IT environments.

This 2019 Cloud Security Report has been produced by Cybersecurity Insiders, the 400,000 member information security community, to explore how organizations are responding to the evolving security threats in the cloud.

Many thanks to Netskope for supporting this important research project.

We hope you'll 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

CLOUD SECURITY CONCERNS

Although cloud providers offer increasingly robust security measures, customers are ultimately responsible for securing their workloads in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals in our survey are data privacy (52%) and protecting against data loss and leakage (51%). This is followed by fraud (32%), concerns about accidental exposure of credentials (30%), and performance issues (29%).

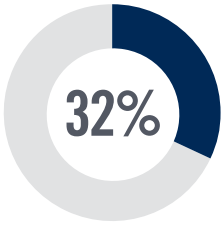
What are your biggest cloud security concerns?

52%

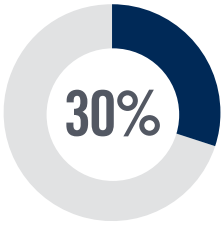
Data privacy/confidentiality

51%

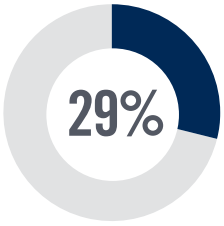
Data loss/leakage



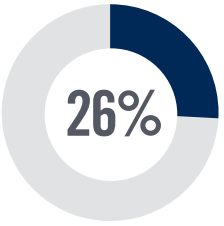
Fraud (e.g., theft of SSN records)



Accidental exposure of credentials



Performance



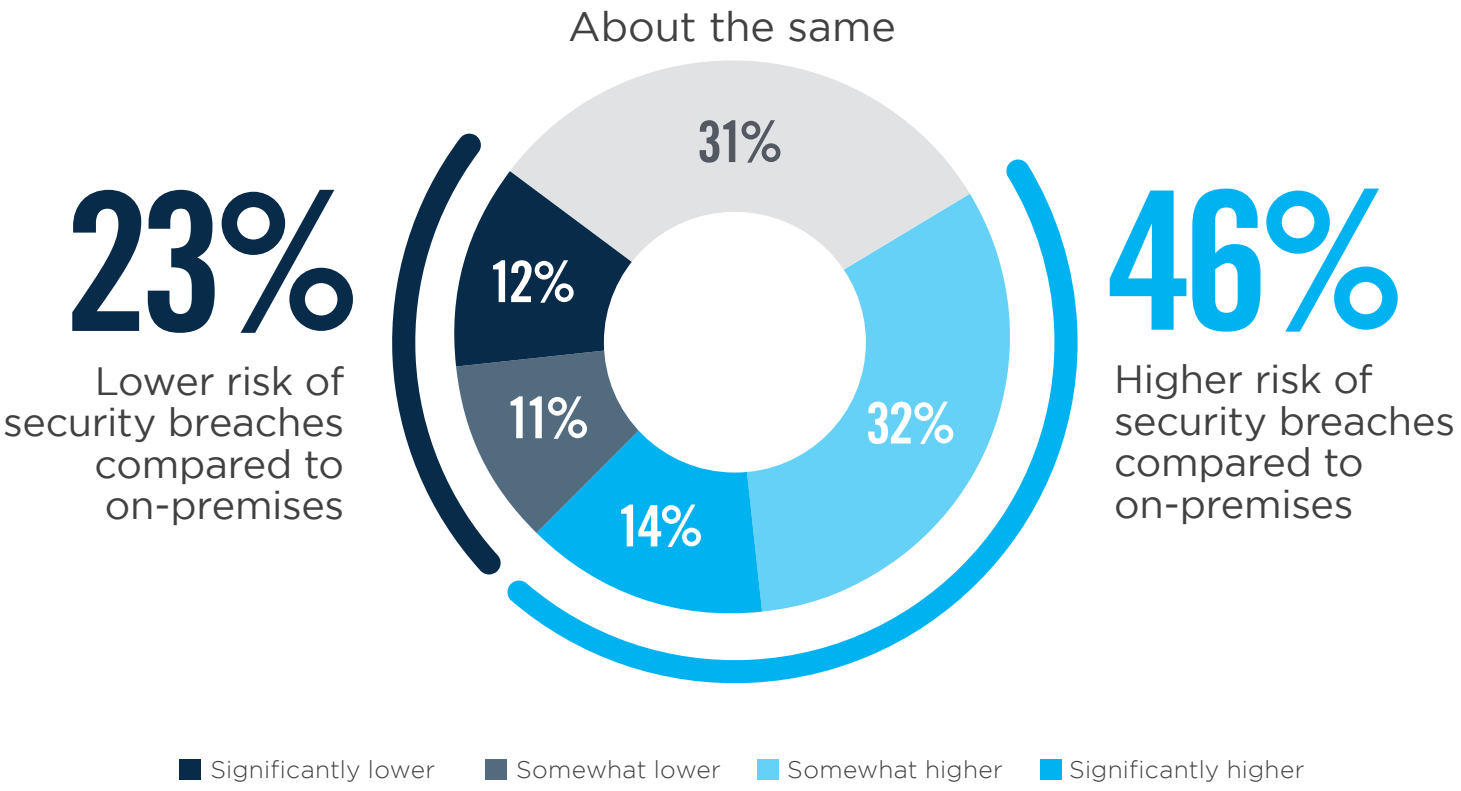
Disaster discovery

Legal and regulatory compliance 24% | Data sovereignty/residency/control 24% | Liability 23% | Incident response 22% | Availability of services, systems and data 22% | Visibility & transparency 20% | Business continuity 18% | Lack of forensic data 15% | Having to adopt new 14% | Not sure/other 6%

CLOUD VS ON-PREMISES SECURITY RISK

The perception persists that public clouds are at higher risk of security breaches compared to traditional on-premises environments (46%), a three percentage point decline relative to last year's survey. The respondents who believe that public clouds are less risky increased to 23%, up by six percentage points.

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



OPERATIONAL SECURITY HEADACHES

As workloads continue to move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top two security headaches SOCs are struggling with are compliance (45%) and lack of qualified security staff (44%) - a perennial challenge. Setting consistent security policies across cloud and on-premises environments (36%) is tied with lack of visibility into infrastructure security (36%).

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

45%

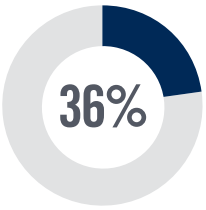
Compliance

44%

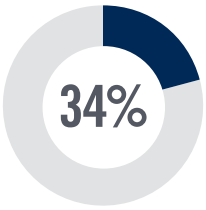
Lack of qualified staff

36%

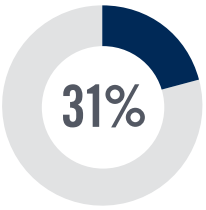
Setting consistent security policies



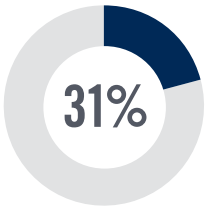
Visibility into infrastructure security



Lack of integration with on-prem security technologies



Reporting security threats



Securing access from personal and mobile devices

Complex cloud to cloud/cloud to on-prem security rule matching 28% | Securing traffic flows 27% | Security can't keep up with the pace of changes to new/existing applications 25% | Understanding network traffic patterns 25% | No automatic discovery/visibility /control to infrastructure security 22% | Remediating threats 22% | Can't identify misconfigurations quickly 22% | Justifying more security spend 16% | Automatically enforcing of security across multiple datacenters 13% | Lack of feature parity with on-prem security solution 11% | No flexibility 5% | Not sure/Other 7%

BIGGEST CLOUD SECURITY THREATS

Insecure interfaces and APIs take the number one spot in this year's survey as the single biggest vulnerability to cloud security (57%). This is followed by misconfiguration of the cloud platform (48%), and unauthorized access through misuse of employee credentials and improper access controls (46%).

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

57%

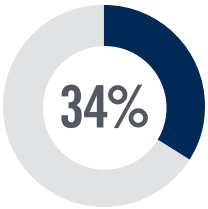
Insecure interfaces /APIs

48%

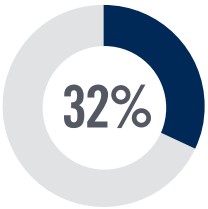
Misconfiguration of the cloud platform /wrong setup

46%

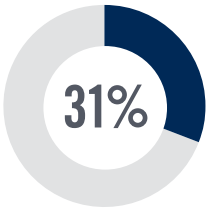
Unauthorized access



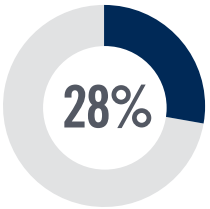
External sharing of data



Hijacking of accounts, services or traffic



Malicious insiders



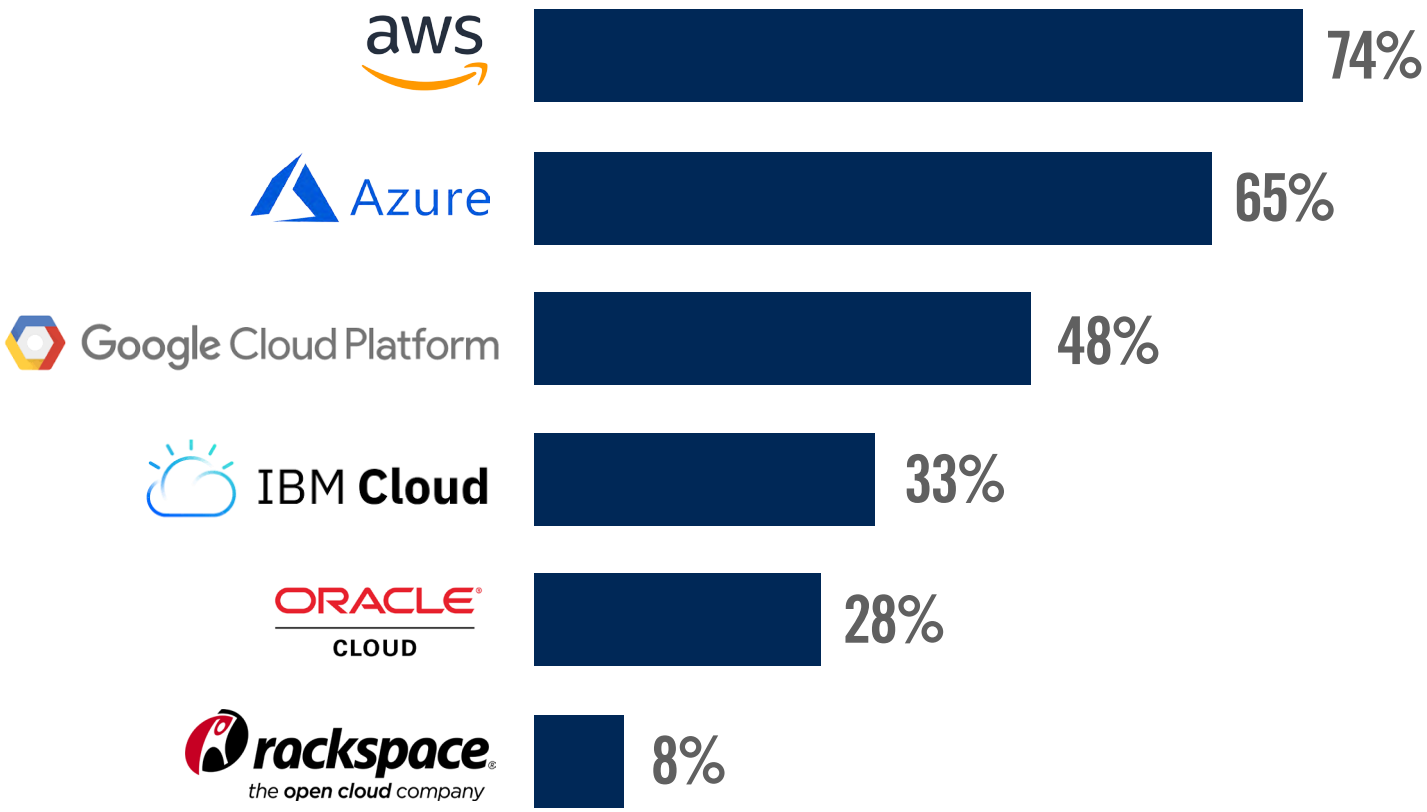
Denial of service attacks

Cloud cryptojacking 25% | Lost mobile devices 15% | Foreign state-sponsored cyber attacks 11% | Malware/Ransomware 11% | Theft of service 2%

TOP CLOUD PROVIDERS

Over the past few years, public cloud providers have continued to mature and expand their service offerings. The two biggest cloud providers continue to compete for the lead in our survey: Amazon Web Services (74%) and Microsoft Azure (65%). Google Cloud Platform remains a strong third place (48% percent) among our survey participants.

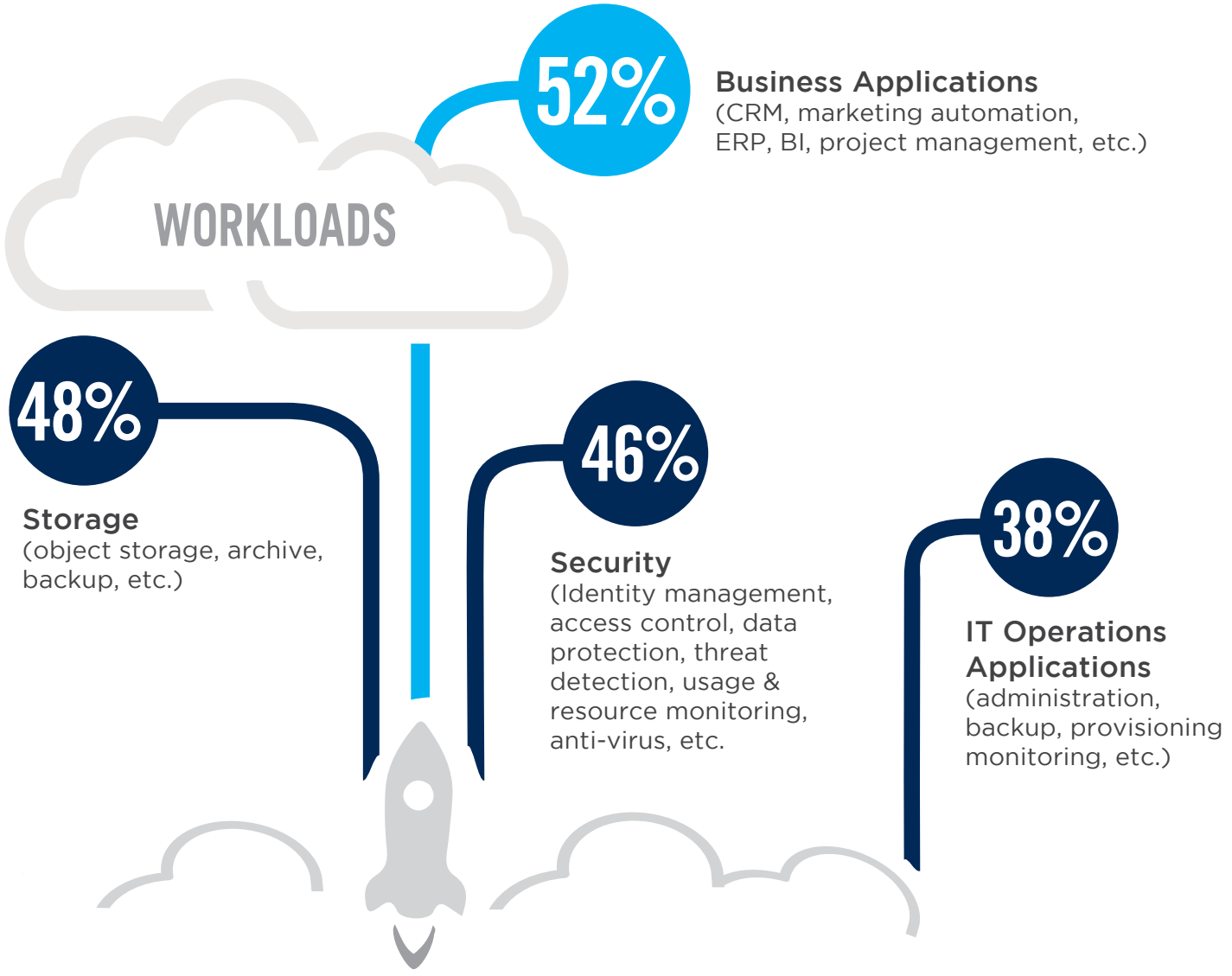
What cloud IaaS provider(s) do you currently use or plan to use in the future?



MOST COMMON WORKLOADS

As organizations embrace cloud services, more mission-critical and production-grade applications are moving to the cloud. The top three cloud services and workloads that organizations are deploying are business applications (such as CRM, ERP, marketing automation, etc.) (52%), storage (48%), security (46%), and IT ops (38%).

What services & workloads is your organization deploying in the cloud?



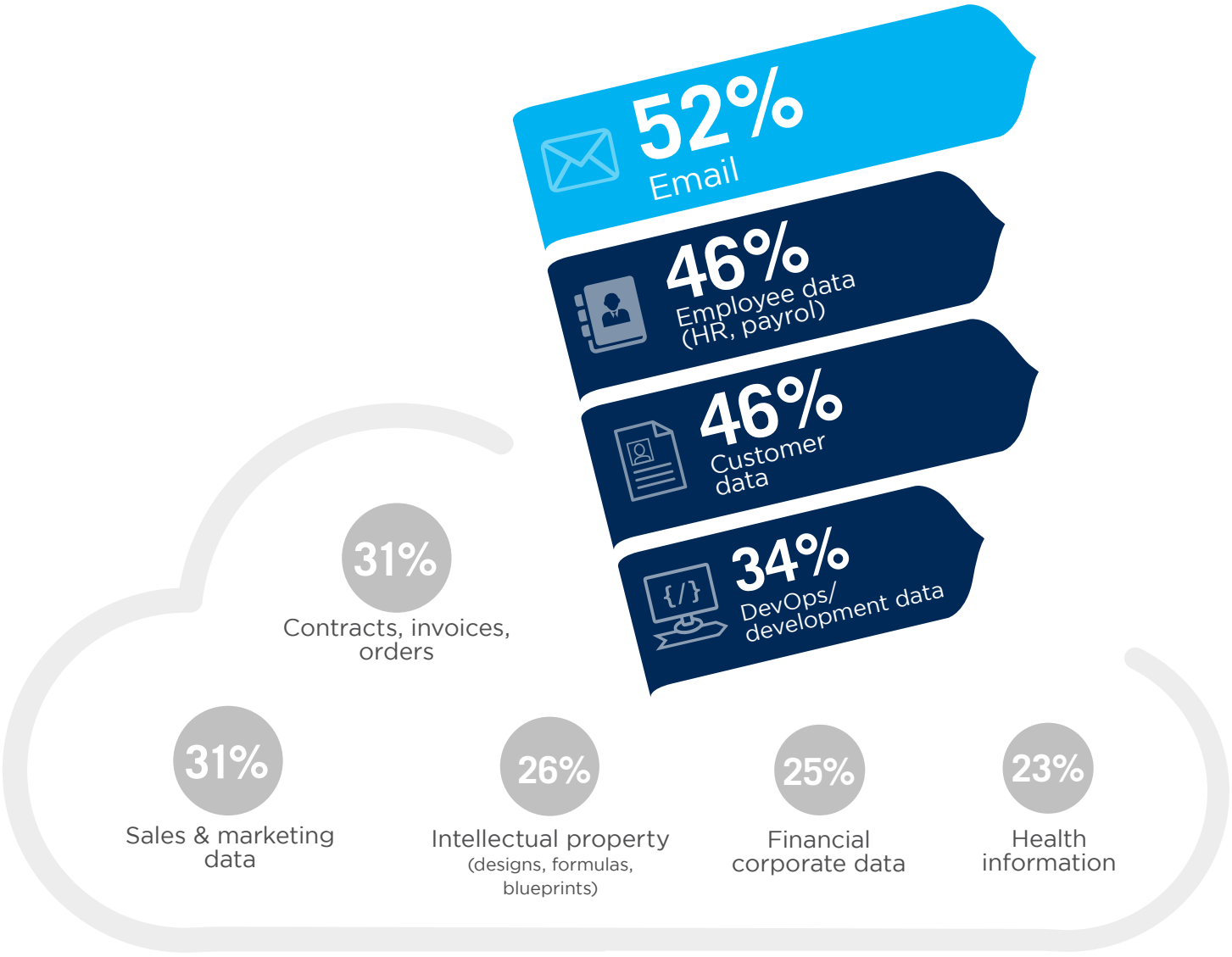
Virtualization 36% | Networking & Content Delivery (virtual private cloud, DNS, etc.) 36% | Productivity Applications (email, collaboration, instant messaging, etc.) 32% | Database (relational, NoSQL, caching, etc.) 30% | Operating System 30% | Developer/Testing Applications 26% | Compute (servers, containers, etc.) 22% | Desktop and Application Streaming 14% | Middleware 10% | Runtime 8% | Other 2%

DATA IN THE CLOUD

Email continues to be the most common type of information stored in the cloud (52%), followed by employee data (46%) - tied with customer data (46%) - and devops data (34%).

This continues a trend of organizations becoming more comfortable with moving their business-critical applications and data to the cloud.

What types of corporate information do you store in the cloud?



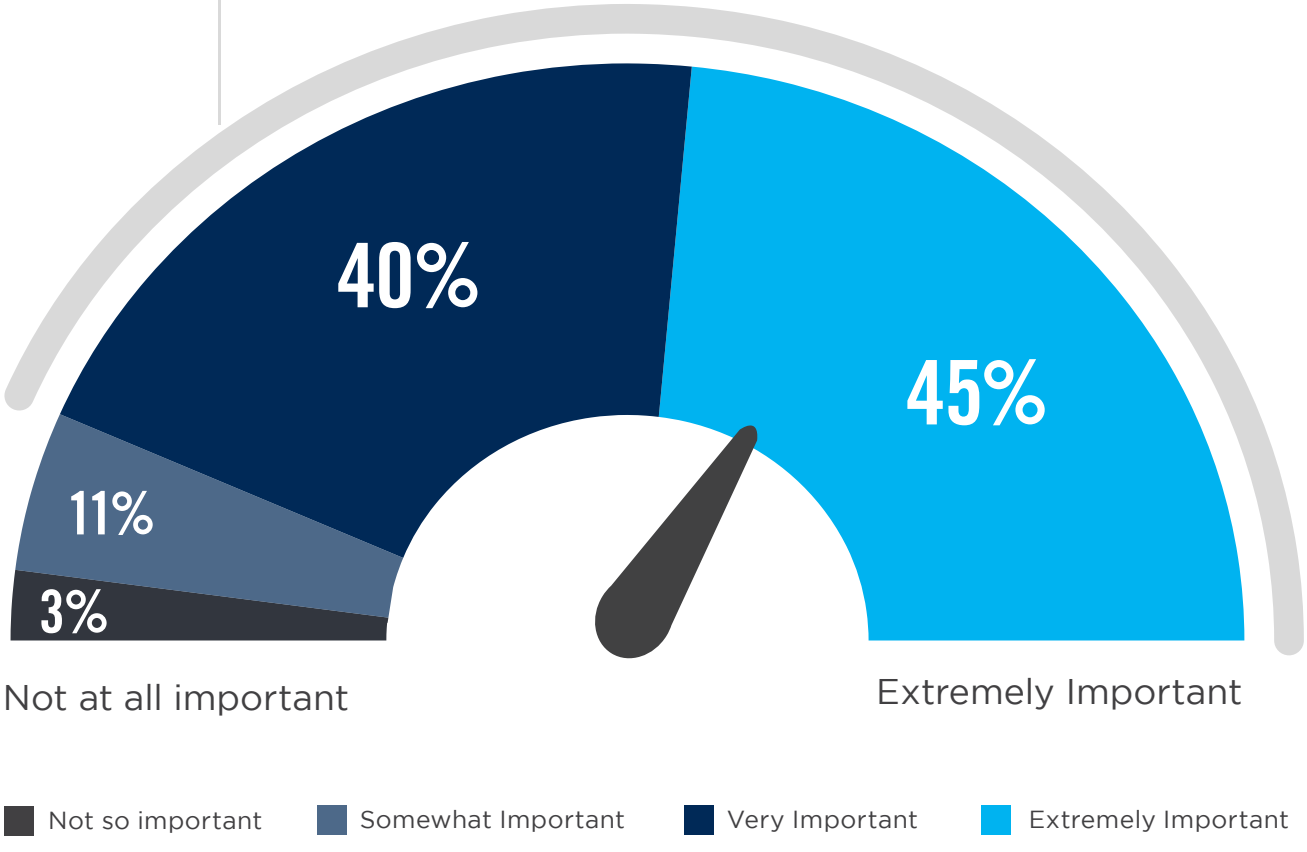
Other 6%

CONTINUOUS COMPLIANCE

Continuous compliance is very important to extremely important to a majority of organizations (85%) as they are securely migrating workloads to the cloud.

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

85% Find extremely to very important to use continuous compliance when migrating workloads to the cloud

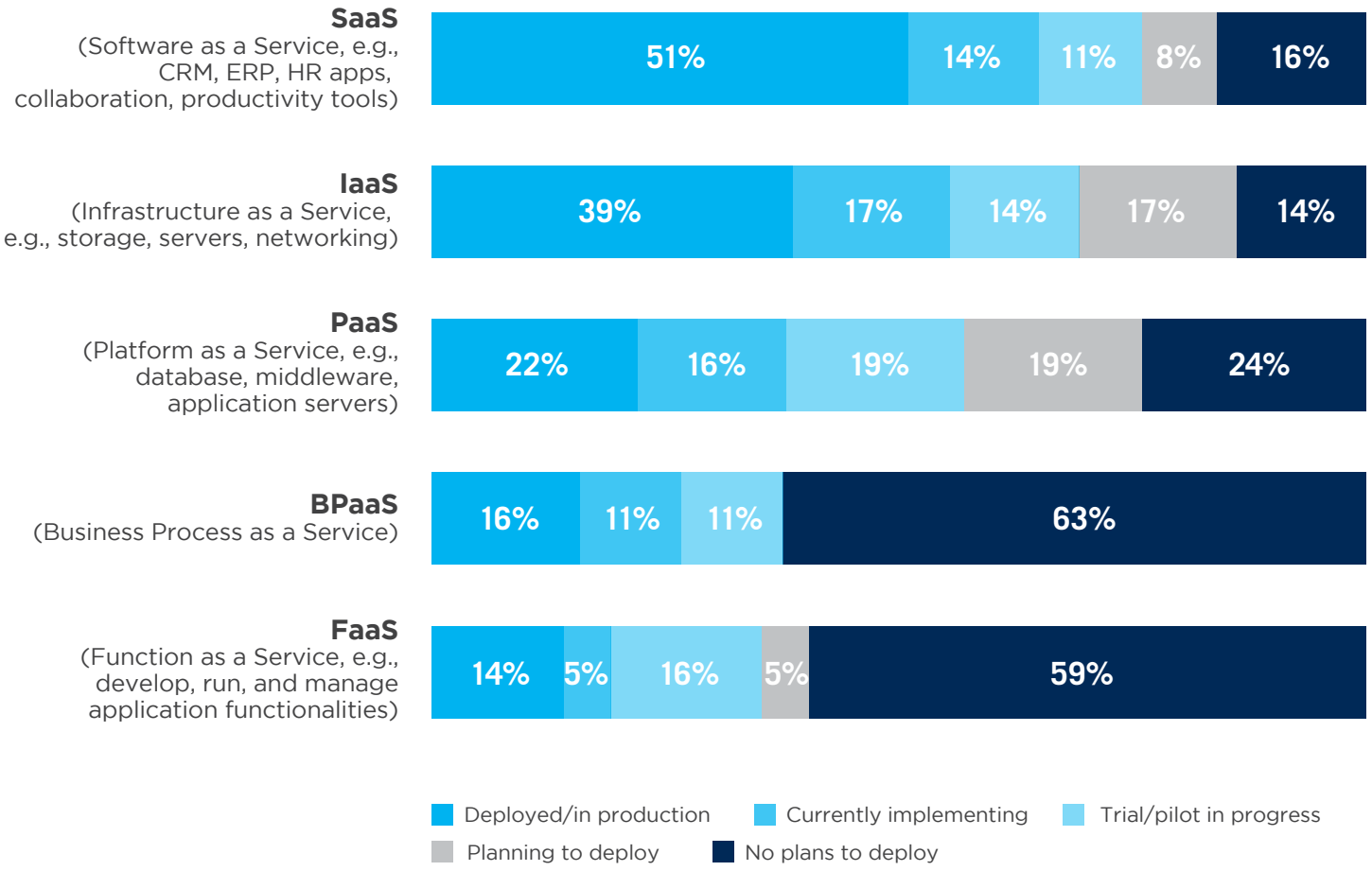


CLOUD ADOPTION TRENDS

SaaS remains the most deployed cloud model (51%), followed by IaaS (39%), and PaaS (22%), both showing continued strong adoption.

Newer deployment models such as BPaaS (16%) and FaaS (14%) have lower rates of production deployments but are gaining momentum.

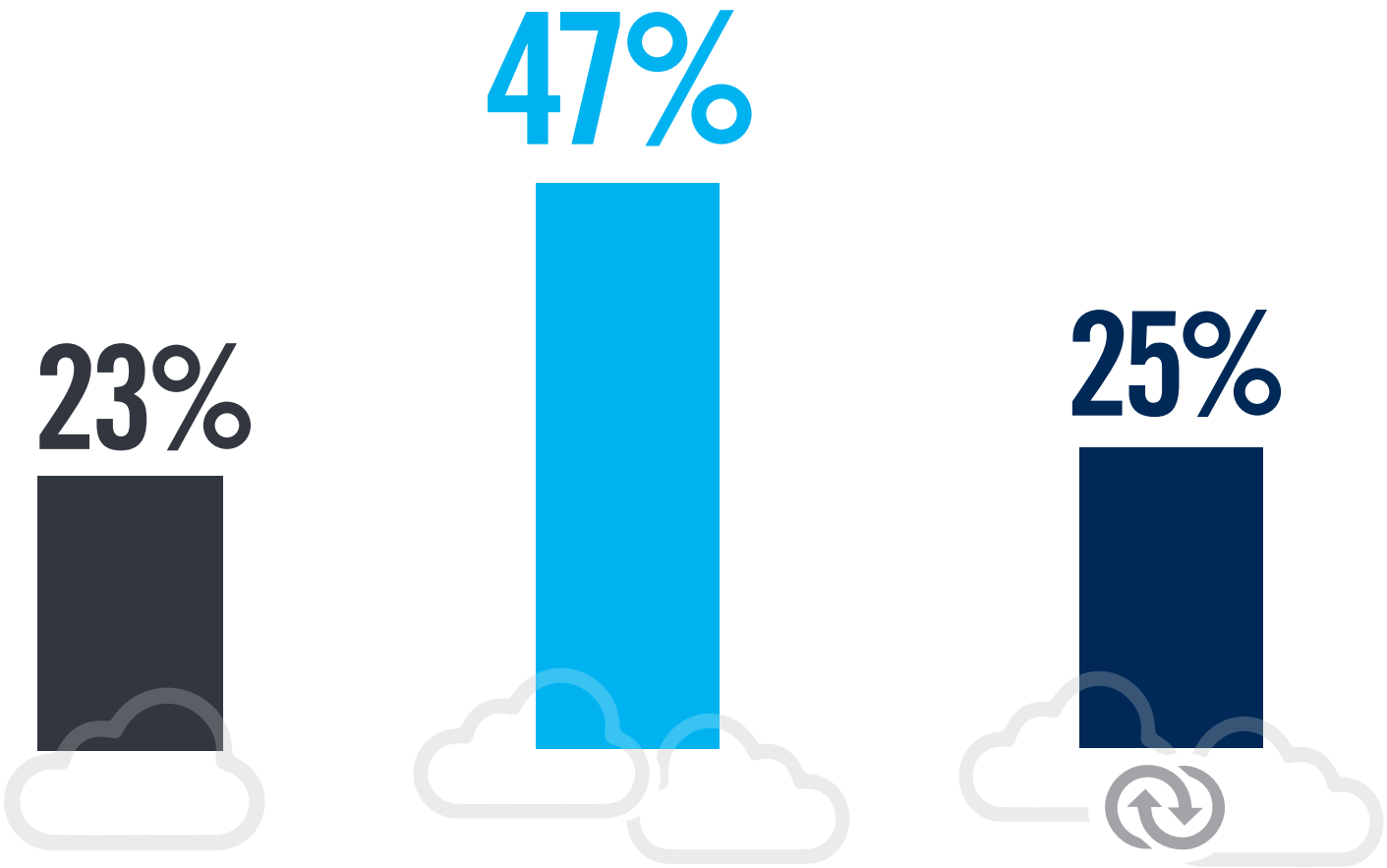
What is your organization's state of adoption of cloud computing?



CLOUD STRATEGY

Forty-seven percent of organizations in this survey say their primary cloud deployment strategy is a multi-cloud model, followed by hybrid cloud models (25%), and single cloud deployments (23%). Organizations are increasingly leveraging more than one cloud provider for a number of reasons, including high availability, disaster recovery, and multi-vendor sourcing efficiencies and risk mitigation.

What is your primary cloud deployment strategy?



SINGLE CLOUD

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

HYBRID
(e.g. integration between multiple providers, managed as a single cloud)

Other 5%

BARRIERS TO CLOUD ADOPTION

Despite all of its benefits, cloud computing is still not without its challenges. Lack of qualified staff continues to top the list of barriers to faster cloud adoption (38%), remaining at the top spot as last year. Legal and regulatory compliance barriers (30%) and integration with existing IT environments (27%) round out the top three barriers.

What are the biggest barriers holding back cloud adoption in your organization?

38%

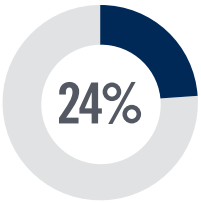
Lack of staff resources or expertise

30%

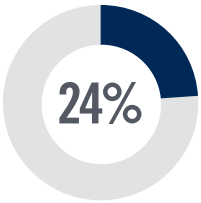
Legal & regulatory compliance

27%

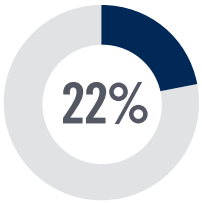
Integration with existing IT environment



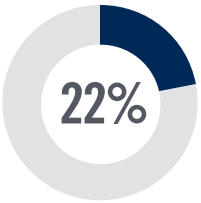
Data security, loss & leakage risks



Complexity managing cloud deployment



General security risks



Lack of maturity of cloud service models

Lack of budget 22% | Cost/Lack of ROI 19% | Lack of management buy-in 19% | Fear of vendor lock-in 16% | Internal resistance and inertia 16% | Billing & tracking issues 16% | Loss of control 14% | Lack of customizability 14% | Lack of transparency and visibility 11% | Dissatisfaction with cloud service offerings/performance/pricing 11% | Availability 11% | Performance of apps in the cloud 8% | Lack of support by cloud provider 5% | Other 3%

CLOUD SECURITY PRIORITIES

Organizations focus on malware defense (30%), reaching regulatory compliance (15%), and securing major cloud apps (14%) as their number one cloud security priorities this year.

What are your cloud security priorities for your company this year?

30%

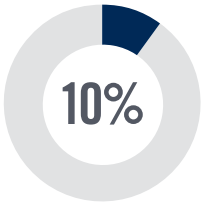
Defending against malware

15%

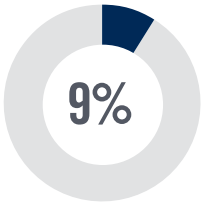
Reaching regulatory compliance

14%

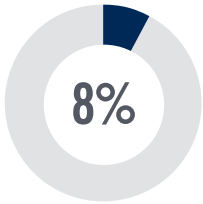
Securing major cloud apps already in use



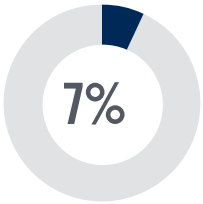
Discovering unsanctioned cloud apps in use



Securing mobile devices



Preventing cloud misconfigurations



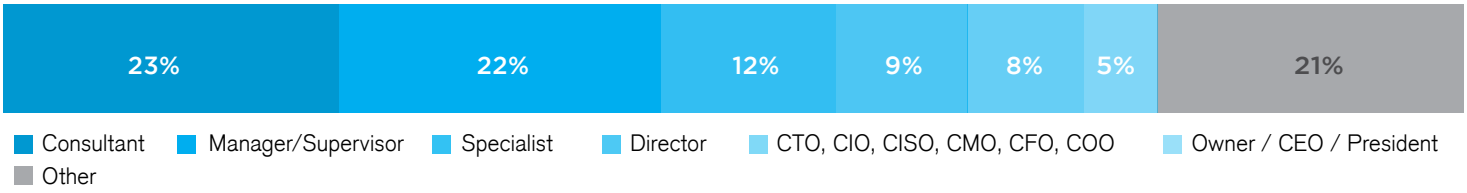
Securing BYOD (bring your own device)

Securing less popular cloud apps already in use 6%

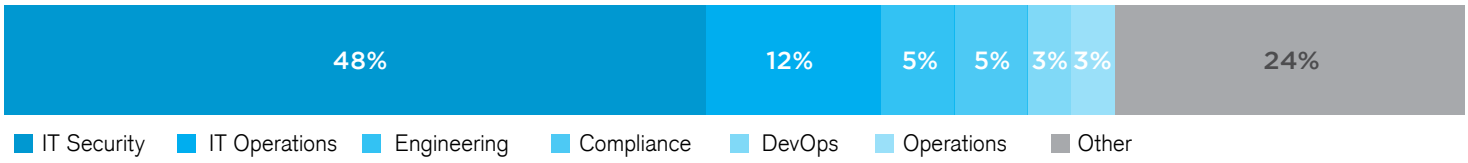
METHODOLOGY & DEMOGRAPHICS

This Cloud Security Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in March of 2019 to gain deep insight into the latest trends, key challenges and solutions for cloud security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

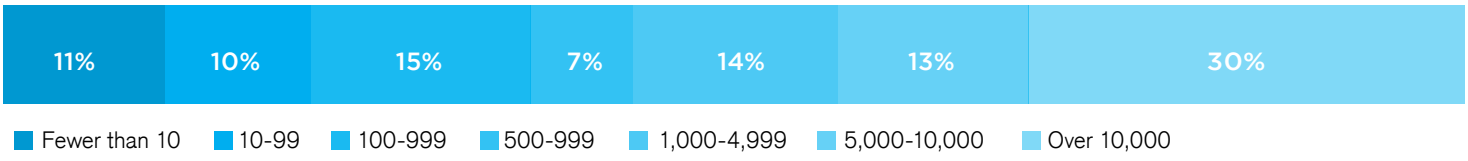
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Netskope is the leader in cloud security. We help the world's largest organizations take full advantage of the cloud and web without sacrificing security. Our patented Cloud XD technology eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud services and millions of websites. With full control through one cloud-native interface, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks. Netskope — smart cloud security.

www.netskope.com