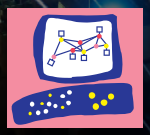
2019

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

Cloud Security Challenges, Solutions, and Trends



Check Point®
SOFTWARE TECHNOLOGIES LTD

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 public 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:

- **Despite all of its benefits, cloud computing still bears challenges. Data security and general security risks (a total of 57%) made it to the top of the list of barriers to faster cloud adoption, followed by lack of budget (26%), compliance challenges (26%), and lack of qualified staff (26%).**
- **Legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. 66% of respondents say traditional security solutions either don't work at all or provide limited functionality in cloud environments.**
- **The biggest operational cloud security headaches IT organizations are struggling with are compliance and lack of visibility into infrastructure security (67% in total). Setting consistent security policies across cloud and on-premises environments and the continuing lack of qualified security staff are tied for third place (31% each).**
- **Unauthorized access and insecure interfaces tie for the number one spot as the biggest vulnerabilities to cloud security (42% each).**
- **The three most concerning cloud data leakage vectors include malware and ransomware (27%), compromised accounts (21%), and misconfigurations (20%).**

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 was produced in June 2019 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 Check Point Software 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

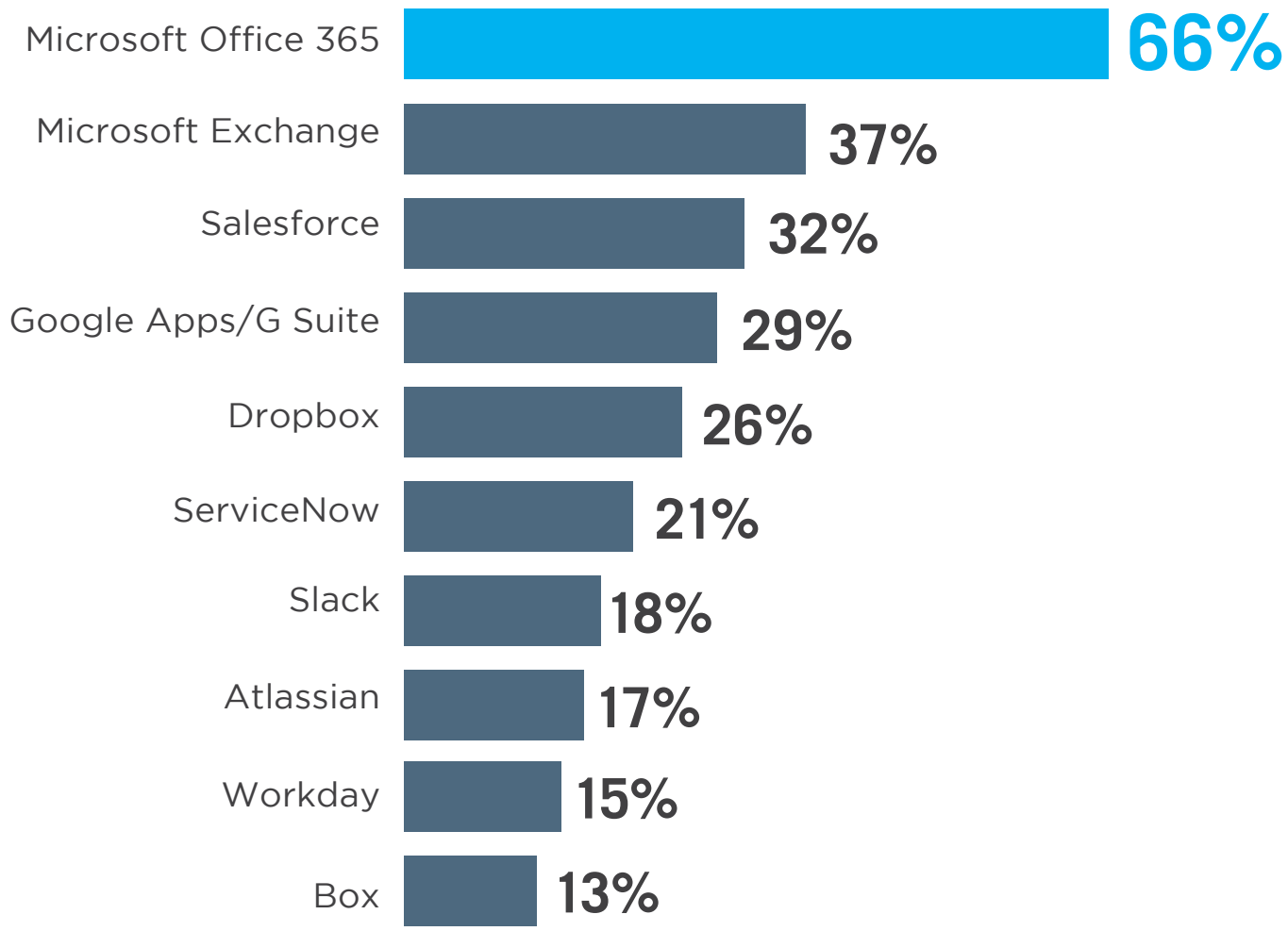
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

MOST POPULAR CLOUD APPS

Software as a Service (SaaS) has become the de facto delivery model for many organizations to utilize business applications, often replacing traditional on-premises applications. These business applications include email, collaboration, customer relationship management, human resources, marketing automation, business intelligence, storage and many more. In this year's survey, the most popular SaaS application is Microsoft Office 365 (66%), followed by Microsoft Exchange (37%). Rounding out the top five most popular SaaS apps are Salesforce (32%), Google G Suite (29%), and Dropbox (26%).

Which of the following cloud SaaS services are currently deployed in your organization?



DATA IN THE CLOUD

For the fourth year in a row, email is the most common information stored in the cloud (63%), followed by customer data (45%) and employee data (including HR and payroll at 42%), moving up from fifth place last year.

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

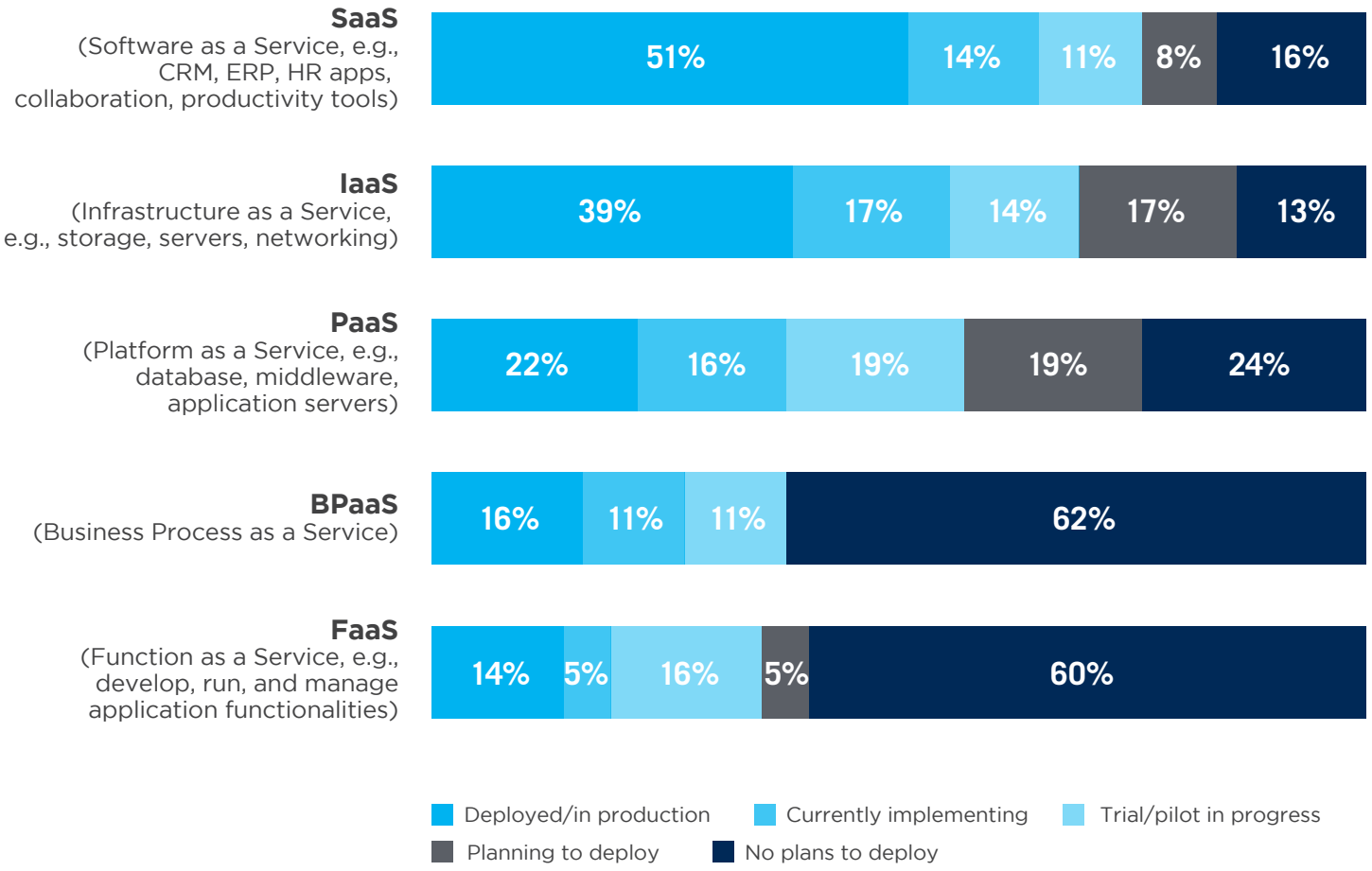
Other 5%

CLOUD ADOPTION TRENDS

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

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

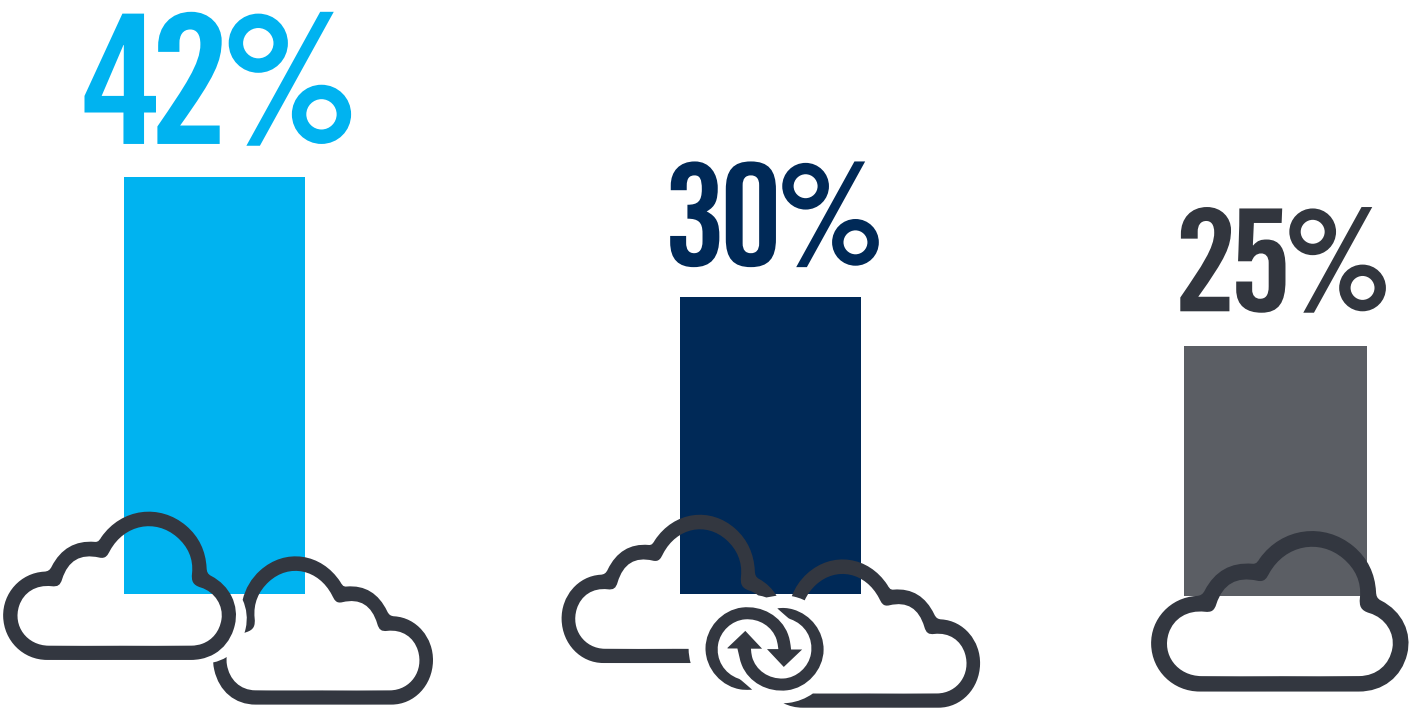
What is your organization's state of adoption of cloud computing?



CLOUD STRATEGY

Forty-two percent of organizations in this survey say their primary cloud deployment strategy is a multi-cloud model, followed by hybrid cloud models (30%), and single cloud deployments (25%). 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?



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

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

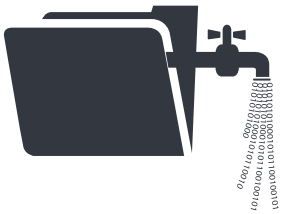
SINGLE CLOUD

Other 3%

BARRIERS TO CLOUD ADOPTION

Despite all of its benefits, cloud computing is still not without challenges. Data security (29%) and general security risks (28%) combined with lack of budget (26%), compliance challenges (26%) and lack of qualified staff (26%) top the list of barriers to faster cloud adoption.

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



29%

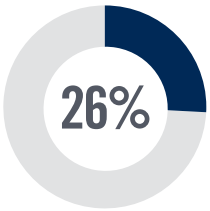
Data security, loss & leakage risks

28%

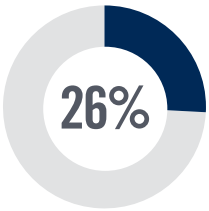
General security risks

26%

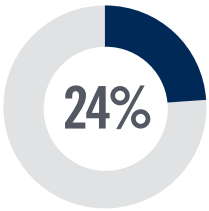
Lack of budget



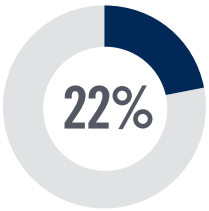
Legal & regulatory compliance



Lack of staff resources or expertise



Integration with existing IT environment



Loss of control

Complexity managing cloud deployment 20% | Fear of vendor lock-in 20% | Cost/lack of ROI 19% | Internal resistance and inertia 19% | Performance of apps in the cloud 16% | Lack of transparency and visibility 16% | Lack of customizability 16% | Billing & tracking issues 15% | Lack of management buy-in 13% | Availability 13% | Lack of maturity of cloud service models 13% | Dissatisfaction with cloud service offerings/performance/pricing 11% | Lack of support by cloud provider 10% | Other 4%

OPERATIONAL SECURITY CHALLENGES

As workloads continue to move to the cloud, cybersecurity professionals are increasingly realizing the complications with protecting these workloads. The top two security headaches SOCs (Security Operations Centers) are struggling with are compliance (34%) and lack of visibility into infrastructure security (33%). Setting consistent security policies across cloud and on-premises environments (31%) and the continuing lack of qualified security staff (31%) are tied for third place.

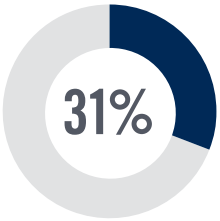
What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

34%

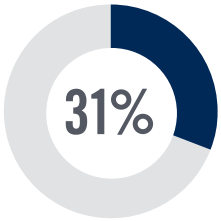
Compliance

33%

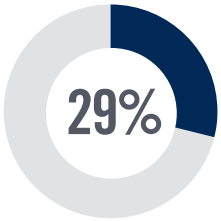
Visibility into infrastructure security



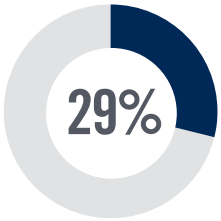
Setting consistent security policies



Lack of qualified staff



Lack of integration with on-premises security technologies



Security can't keep up with the pace of changes to new/existing applications

Securing traffic flows 24% | Can't identify misconfigurations quickly 24% | Complex cloud to cloud/cloud to on-premises security rule matching 24% | Securing access from personal and mobile devices 23% | Reporting security threats 23% | Remediating threats 22% | Understanding network traffic patterns 21% | Justifying more security expenditure 21% | No automatic discovery/visibility/control to infrastructure security 19% | Automatically enforcing security across multiple datacenters 17% | Lack of feature parity with on-premises security solution 14% | No flexibility 8% | Not sure/other 10%

BIGGEST CLOUD SECURITY THREATS

Unauthorized access (42%) and insecure interfaces (42%) tie for the number one spot in this year's survey as the biggest vulnerabilities to cloud security. This is followed by misconfiguration of the cloud platform (40%) and hijacking of accounts (39%).

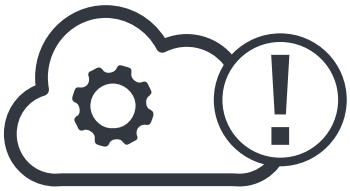
What do you see as the biggest security threats in public clouds?

42%

Unauthorized access

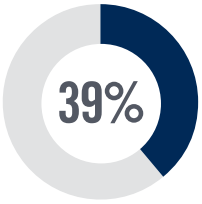
42%

Insecure interfaces/APIs

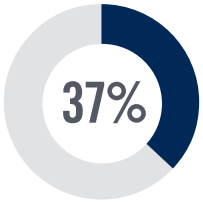


40%

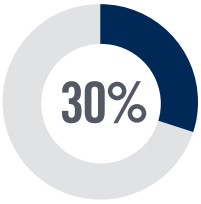
Misconfiguration of the cloud platform/ wrong setup



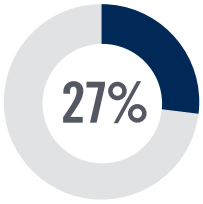
Hijacking of accounts, services or traffic



External sharing of data



Malicious insiders



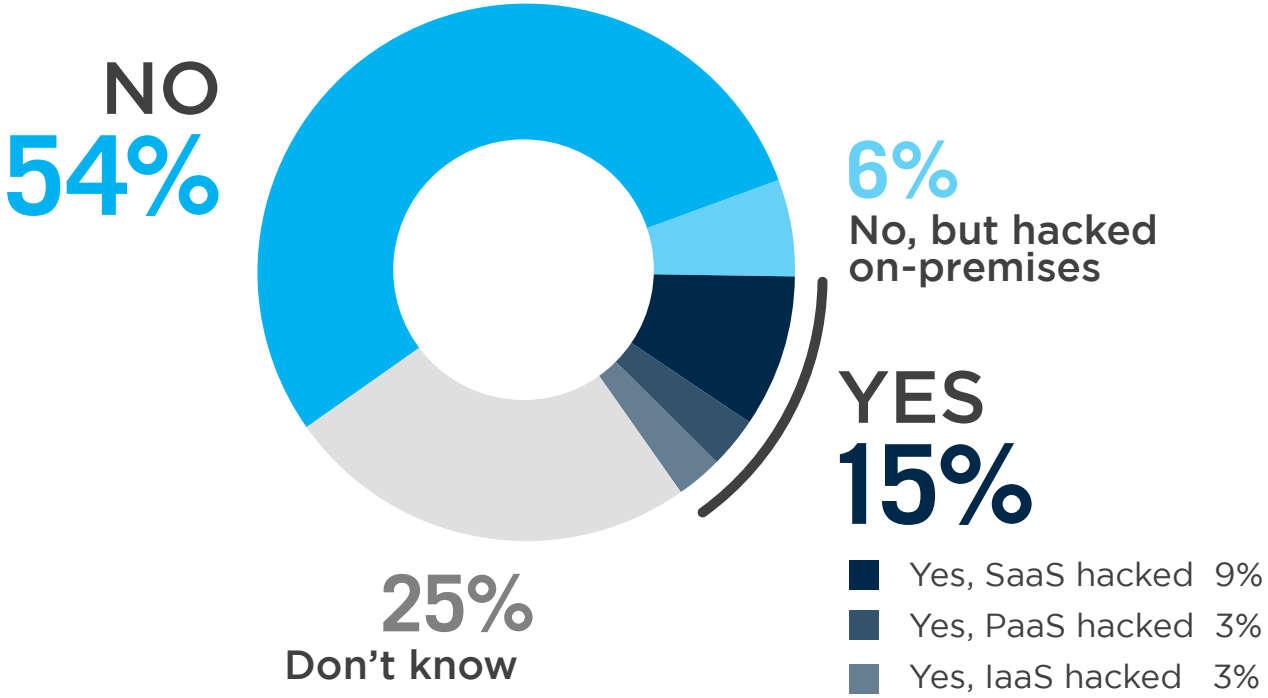
Malware/ransomware

Denial of service attacks 24% | Foreign state-sponsored cyber attacks 22% | Cloud cryptojacking 19% | Theft of service 16% | Lost mobile devices 13% | Other 1%

HACKED IN THE CLOUD

While a majority of organizations say their cloud instances have not been hacked (54%), an alarming 25% do not know whether they have been breached in the cloud. Fifteen percent of organizations confirmed a cloud security incident.

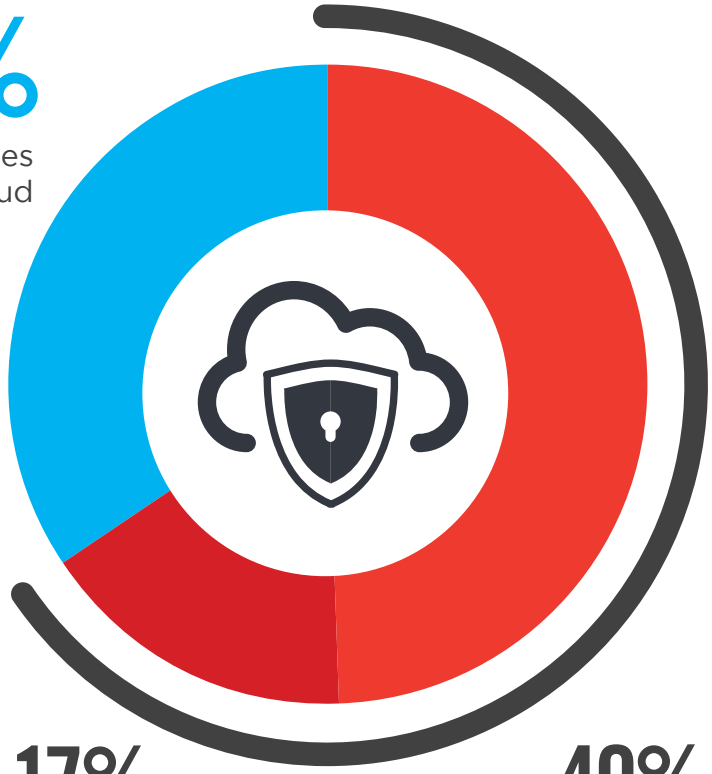
Has your organization ever been hacked in the cloud?



TRADITIONAL TOOLS IN THE CLOUD

As workloads continue to move to the cloud, organizations are faced with unique security challenges that cloud adoption presents. Many legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. Sixty-six 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?



34%
All capabilities work in the cloud

66%
Claim traditional security solutions either don't work at all or have limited functionality

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

49%
Limited functionality

BARRIERS TO ADOPTION OF CLOUD-BASED SECURITY SOLUTIONS

Despite the significant advantages offered by cloud-based security solutions, some barriers to adoption still exist. When it comes to business transformation and cloud adoption, three important aspects must be aligned: people, process and technology. Our survey reveals that the biggest challenge organizations are facing is not technology, but people and processes. Staff expertise and training (41%) continues to rank as the highest barrier, followed by budget challenges (40%), data privacy concerns (38%), and lack of integration with on-premises platforms (34%).

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

41%

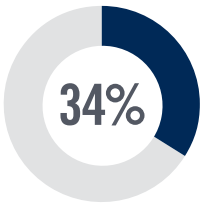
Staff expertise/ training

40%

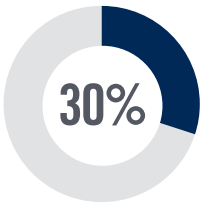
Budget

38%

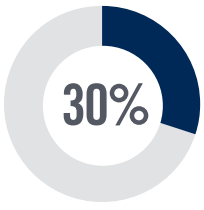
Data privacy



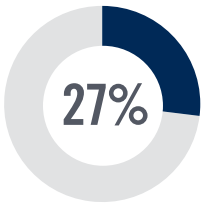
Lack of integration with on-premises security technologies



Regulatory compliance requirements



Solution maturity



Data residency

Limited control over encryption keys 21% | Scalability and performance 21% | Integrity of cloud security platform (DDoS attack, breach) 19% | Sunk cost into on-premises tools 17% | Not sure/other 8%

SECURITY CONTROLS

Encryption of data-at-rest (38%), automation of compliance (37%), and APIs for reporting, auditing and alerting on security events (34%) are the three most frequently mentioned security controls to increase organizations' confidence in adopting public clouds.

Which of the following security controls would most increase your confidence in adopting public clouds?

38%

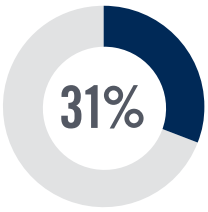
Encryption of data-at-rest

37%

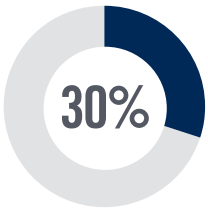
Automating compliance

34%

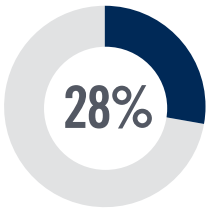
APIs for reporting, auditing and alerting on security events



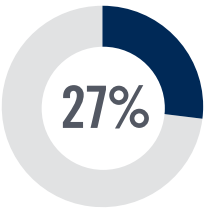
Isolation/ protection of virtual machines



Setting and enforcing security policies across clouds



Leveraging data leakage prevention tools



Creating data boundaries

Protecting workloads 26% | Limiting unmanaged device access 25% | Leveraging threat prevention tools 24% | Proxying traffic for real-time security at access 21% | Other 2%

KEY CLOUD SECURITY FEATURES

When selecting cloud security solutions, organizations prioritize the ability to write custom rules and remediation actions (44%), followed by integration with change management platforms, such as ServiceNow, Remedy, JIRA, etc. (41%), and integration with security scanner tools such as Rapid7, Qualys, Tenable, etc. (41%).

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

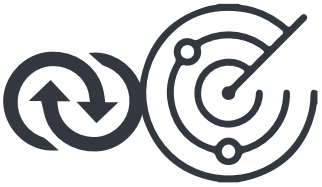
44%

Ability to write custom rules and remediation actions

41%

Integration with change management platforms

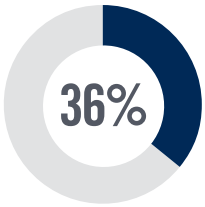
(ServiceNow, Remedy, JIRA, etc.)



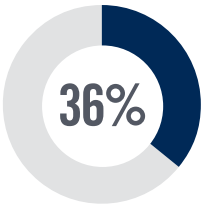
41%

Integration with security scanner tools

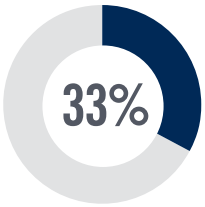
(Rapid7, Qualys, Tenable, etc.)



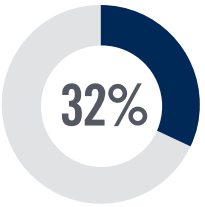
Integration with end-to-end vulnerability remediation tools (TrueSight Server Automation, IBM BigFix, TrueSight Vulnerability Manager, Chef, Puppet, etc.)



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



Billing model (monthly, yearly, flat)



User community support

Integration with alerting tools, such as OpsGenie that support integration with phone, messaging, Slack, email, etc. 29% | Billing by usage instead of number of accounts 26% | Research-based policies (i.e. content beyond the CIS best practices) 25% | Other 3%

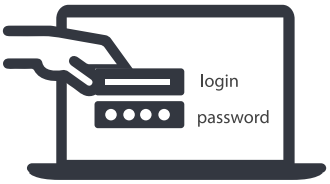
DATA LEAKAGE

The three most concerning data leakage vectors include malware and ransomware (27%), compromised accounts (21%), and misconfigurations (20%).

What is the data leakage vector that you find most concerning for your organization?

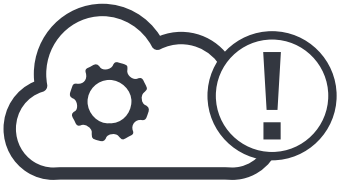
27%

Malware/ ransomware



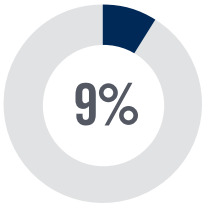
21%

Compromised accounts

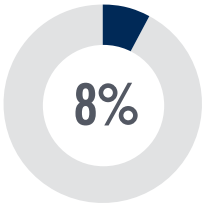


20%

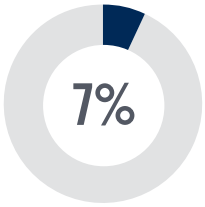
Misconfigurations



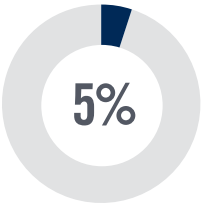
Vulnerabilities in underlying app infrastructure



Unmanaged devices



Unsecured WiFi



Unsanctioned cloud apps

Other 3%

CLOUD SECURITY PRIORITIES

Organizations focus on malware defense (25%), reaching regulatory compliance (20%), and securing major cloud apps (15%) as their top three cloud security priorities this year.

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

25%

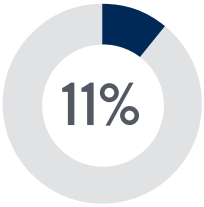
Defending against malware

20%

Reaching regulatory compliance

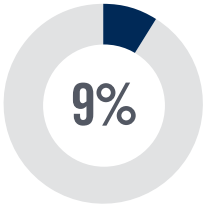
15%

Securing major cloud apps already in use

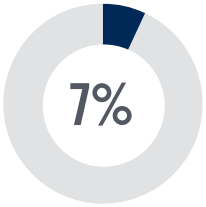


Preventing cloud misconfigurations

Securing mobile devices



Discovering unsanctioned cloud apps in use

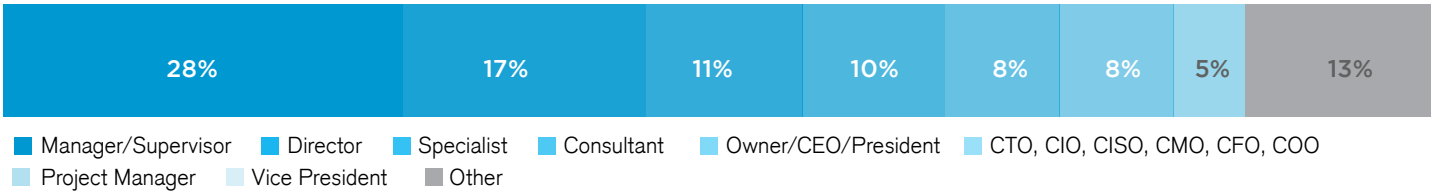


Securing less popular cloud apps already in use

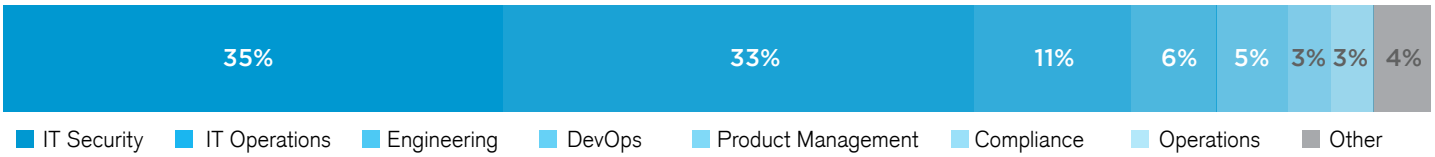
METHODOLOGY & DEMOGRAPHICS

This Cloud Security Report is based on the results of a comprehensive online survey of 674 cybersecurity and IT 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.

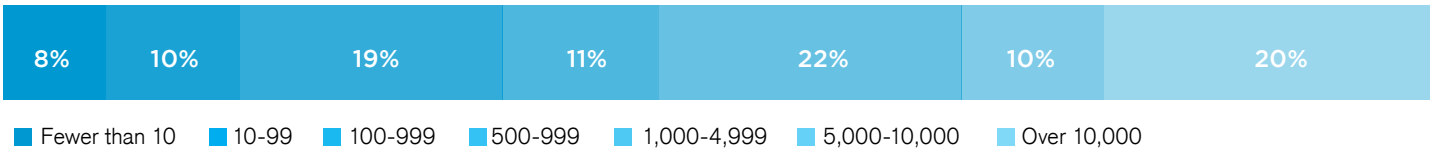
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Check Point®
SOFTWARE TECHNOLOGIES LTD

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

www.checkpoint.com

Process efficiencies and increased network agility are driving SaaS, PaaS and IaaS technology adoption at a rapid pace. This new infrastructure is also presenting businesses with a unique set of security challenges. Check Point cloud security protects assets in the cloud from the most sophisticated threats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks.

CHECK POINT
CloudGuard™