2019

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

edgile

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 cloud security concern of cybersecurity professionals is data loss and leakage (64%).
- Unauthorized access through misuse of employee credentials and improper access controls (42%) takes the number one spot in this year's survey as the single biggest perceived vulnerability to cloud security, tied with insecure interfaces and APIs (42%). This is followed by misconfiguration of the cloud platform (40%).
- The top two operational security headaches SOC teams are struggling with are compliance (34%) and lack of visibility into cloud security (33%).

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 Edgile 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

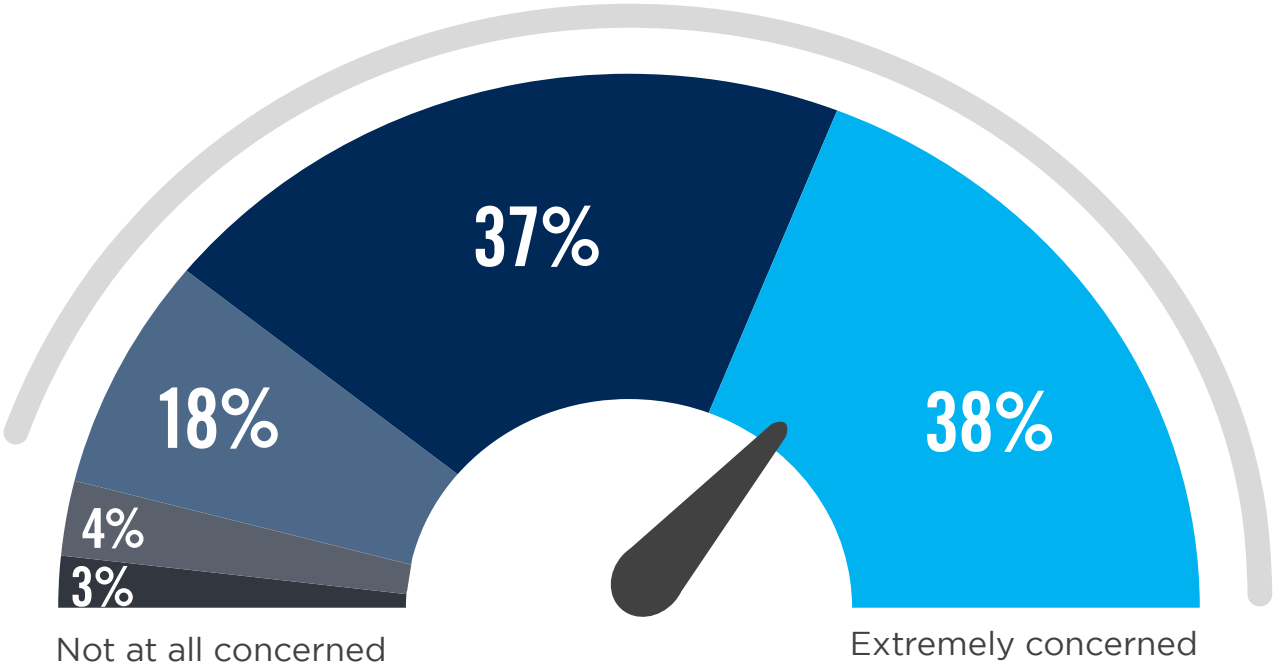
Cybersecurity
INSIDERS

SECURITY IN PUBLIC CLOUDS

While adoption of public clouds continues to surge, security concerns are showing no signs of abating. An overwhelming majority of cybersecurity professionals (93%) say they are at least moderately concerned about public cloud security, a small increase from last year.

How concerned are you about the security of public clouds?

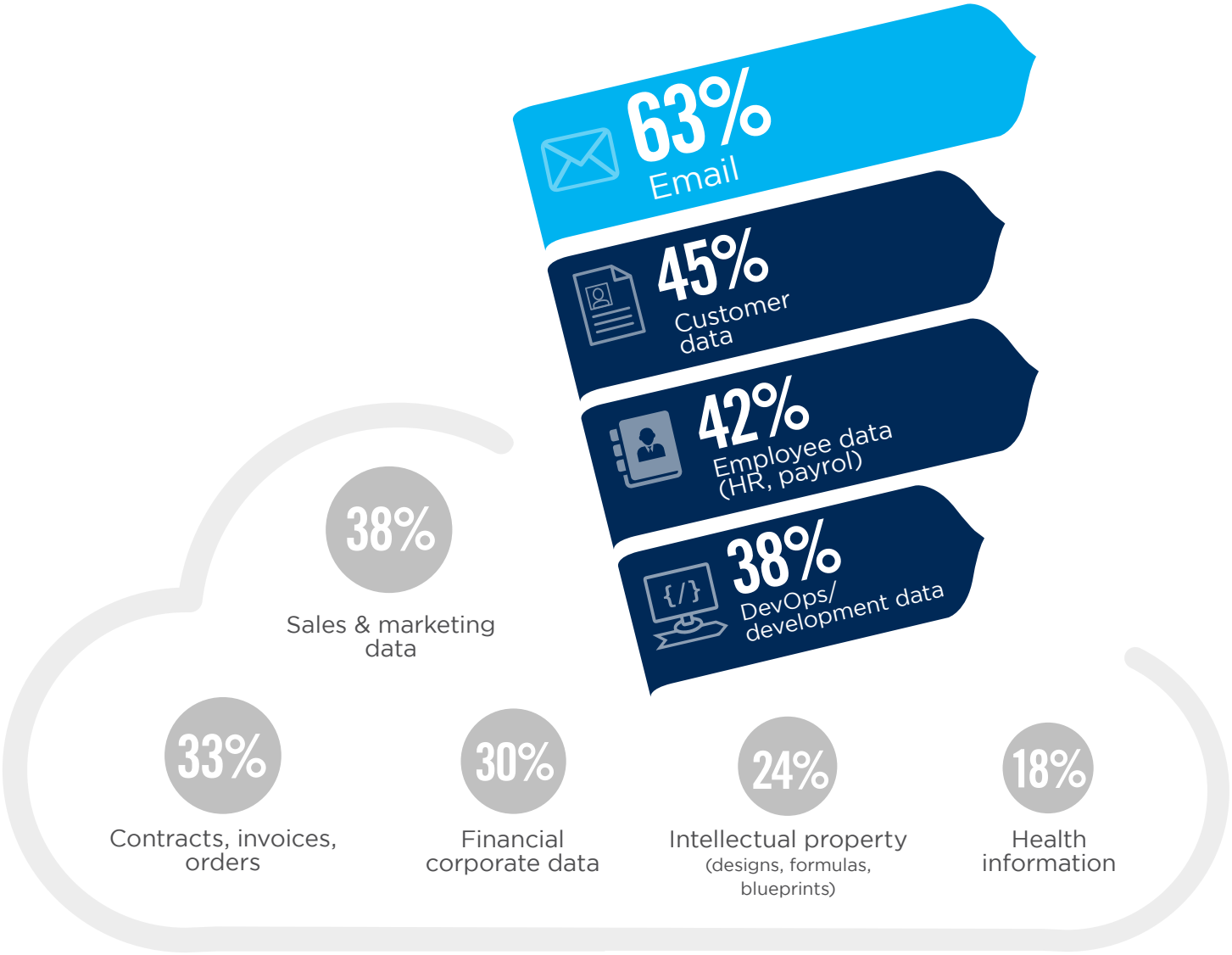
93% Organizations are moderately to extremely concerned about cloud security



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 (42%) moving up from fifth place last year.

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



Other 5%

COMPLIANCE CHALLENGES

When it comes to compliance challenges, monitoring cloud services for new vulnerabilities stands out with 43%, followed by going through audits and risk assessments (40%), and monitoring for compliance (39%). Continuous compliance of workloads migrating from on-premises to cloud is very important to extremely important to 84% of organizations.

Which part of the cloud compliance process is the most challenging?

43%

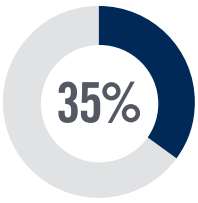
Monitoring for new vulnerabilities in cloud services that must be secured

40%

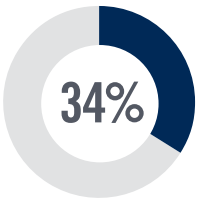
Going through audit/risk assessment within the cloud environment

39%

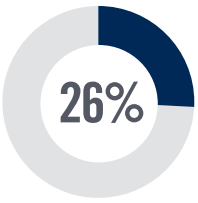
Monitoring for compliance with policies and procedures



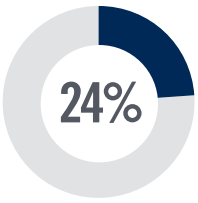
Staying up to date about new/changing compliance and regulatory requirements



Data quality and integrity in regulatory reporting



Scaling and automating compliance activities



Applying/following the shared responsibility model

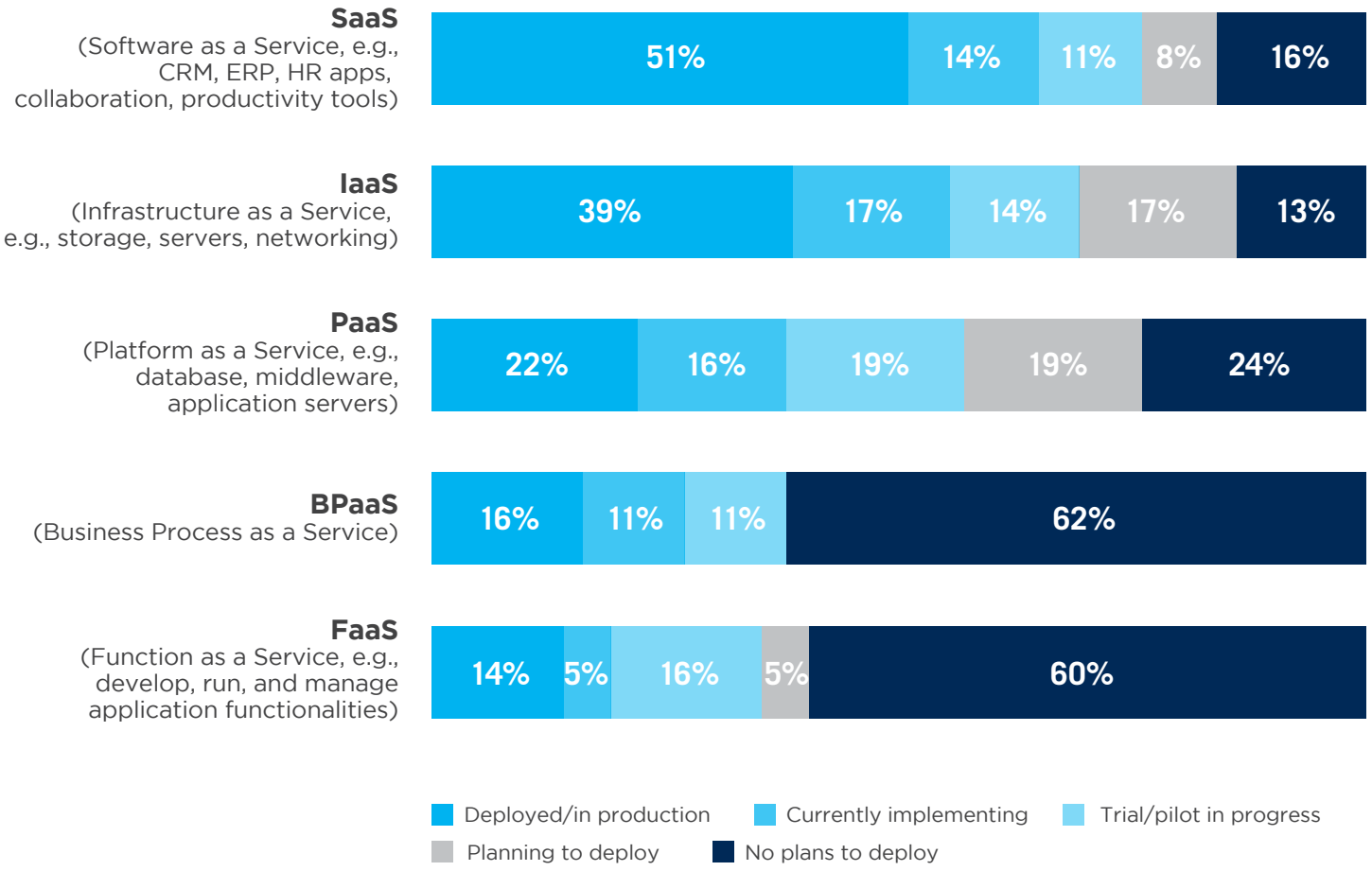
Other 12%

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.

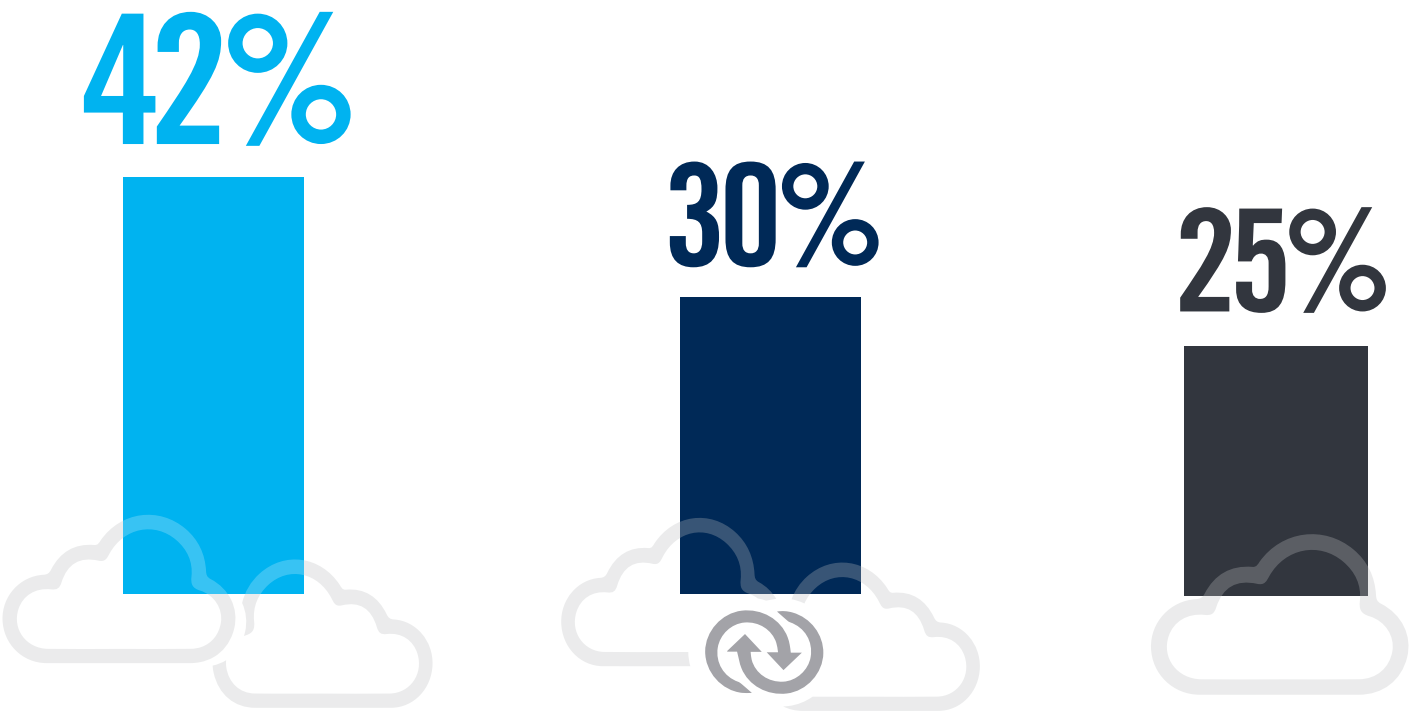
What is your organization's state of adoption of cloud computing?



CLOUD STRATEGY

Forty-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, managed as a single cloud)

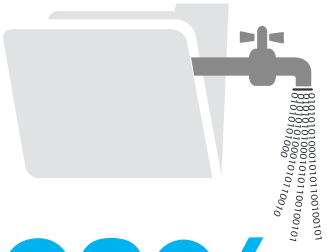
SINGLE CLOUD

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%

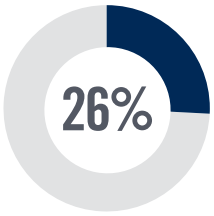
Data security, loss & leakage risks

28%

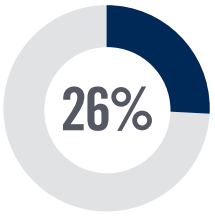
General security risks

26%

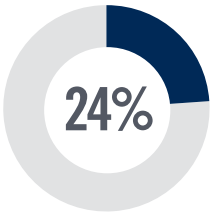
Lack of budget



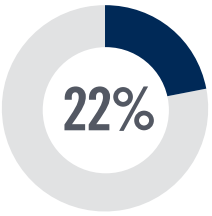
Legal & regulatory compliance



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%

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%

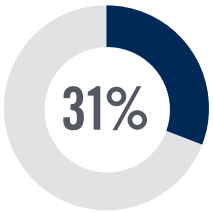
Encryption of data-at-rest

37%

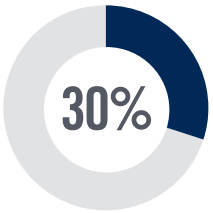
Automating compliance

34%

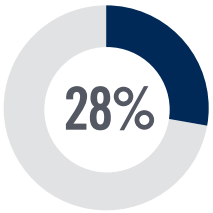
APIs for reporting, auditing and alerting on security events



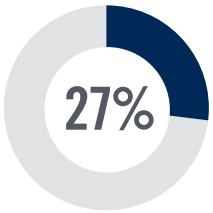
Isolation/ protection of virtual machines



Setting and enforcing security policies across clouds



Leveraging data leakage prevention tools



Creating data boundaries

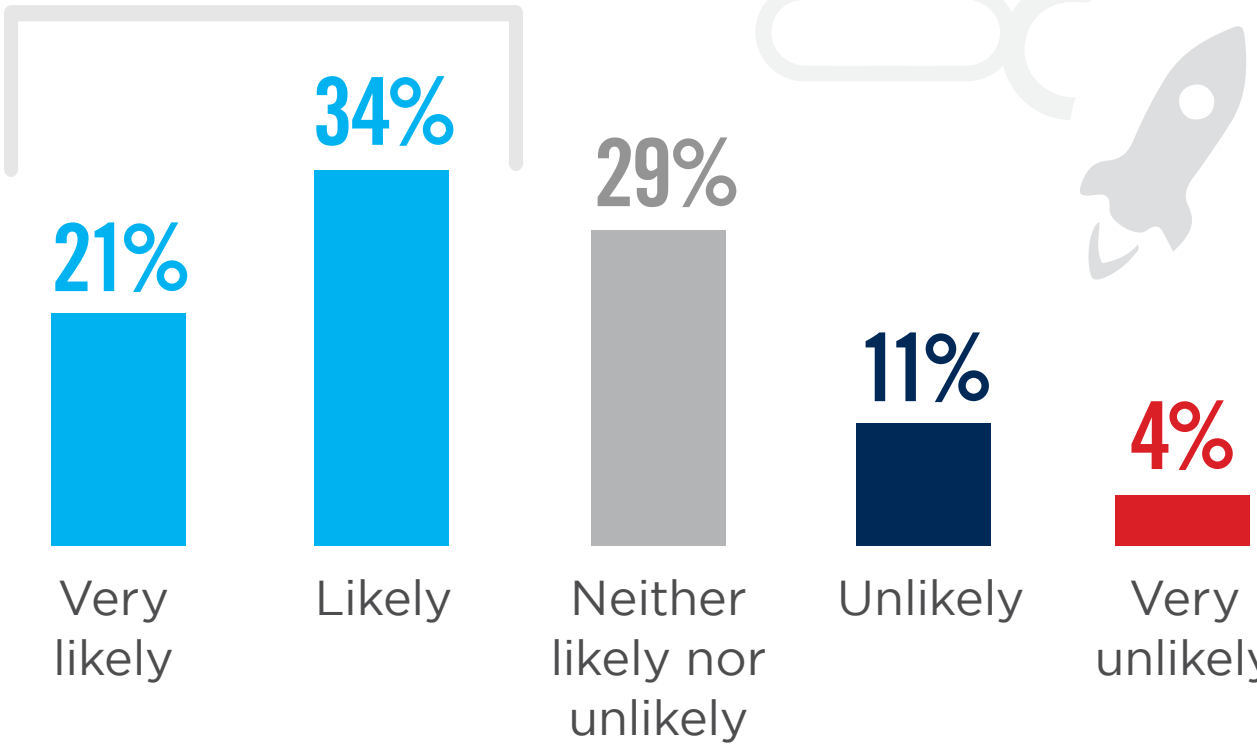
Protecting workloads 26% | Limiting unmanaged device access 25% | Leveraging threat prevention tools 24% | Proxying traffic for real-time security at access 21% | Other 2%

NEW CLOUD SECURITY SOLUTION

Despite the high levels of satisfaction with their cloud security solutions, a majority of 55% is looking to deploy a new cloud security solution within the next 12 months. Only 15% are unlikely to do so.

How likely is your organization to deploy a new cloud security solution within the next 12 months?

55% Is looking to deploy a new cloud security solution within the next 12 months



VENDOR CRITERIA

When looking for a new cloud security vendor, organizations prioritize cost effectiveness (55%), ease of deployment (46%) and whether security tools are cloud native (45%).

What do you look for in your cloud security provider?

46%

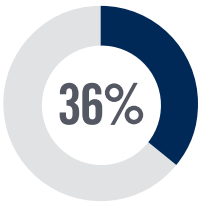
Ease of deployment

45%

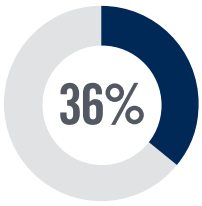
Security tools are cloud native

37%

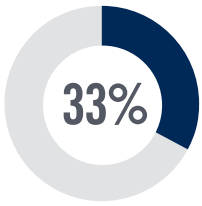
Tools can deploy with automation, support scalability, touchless deployments, etc.



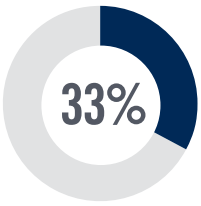
Integrates seamlessly with cloud platforms



Multi-cloud support



Demonstrates cloud knowledge



Interoperable with on-premises solutions

Extends on-premises policies to the cloud 33% | Policy customization 32% | Other 2%

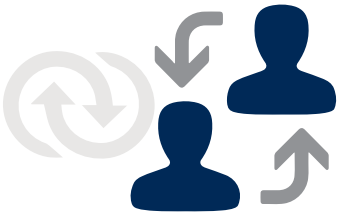
KEY CLOUD SECURITY FEATURES

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 like Rapid7, Qualys, Tenable (41%).

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

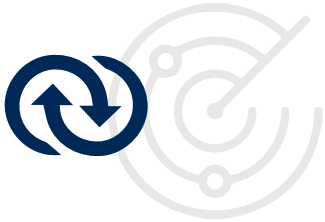
44%

Ability to write custom rules and remediation actions



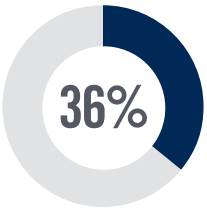
41%

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

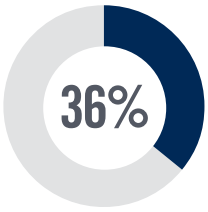


41%

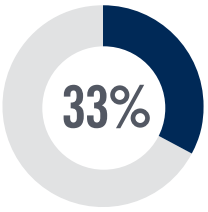
Integration with security scanner tools
(Rapid7, Qualys, Tenable)



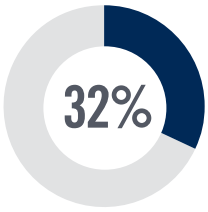
Integration with end-to-end vulnerability remediation tools (TrueSight Server Automation, IBM BigFix, TrueSight Vulnerability Manager, Chef, Puppet, etc.)



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



Billing model (monthly, yearly, flat)



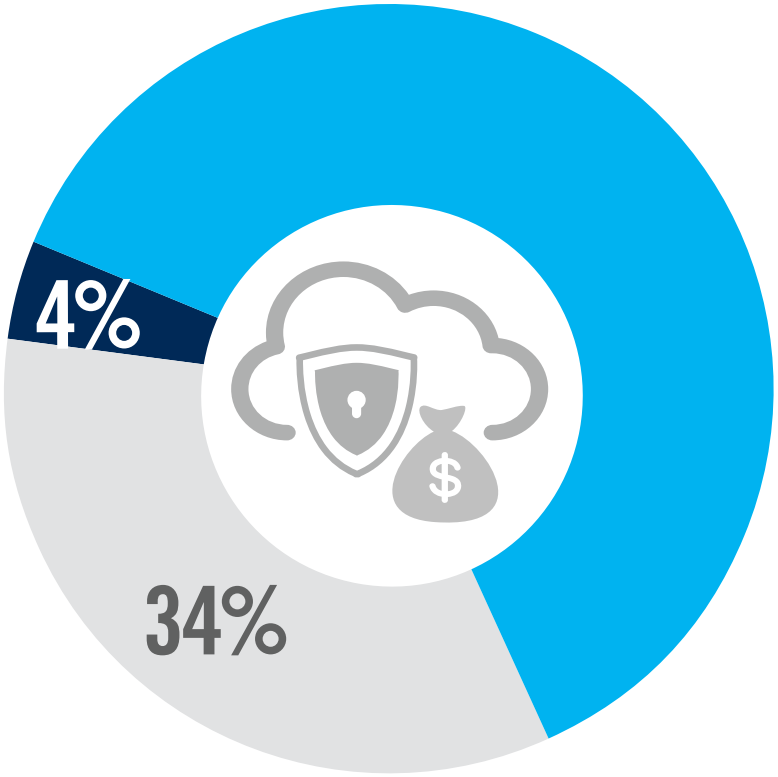
User community support

Integration with alerting tools like 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%

CLOUD SECURITY BUDGET

Cloud security remains a priority for most organizations which is why we see a significant share of respondents predicting an increase of 62% over the next 12 months.

How is your cloud security budget changing in the next 12 months?



Respondents predict an increase of

62%

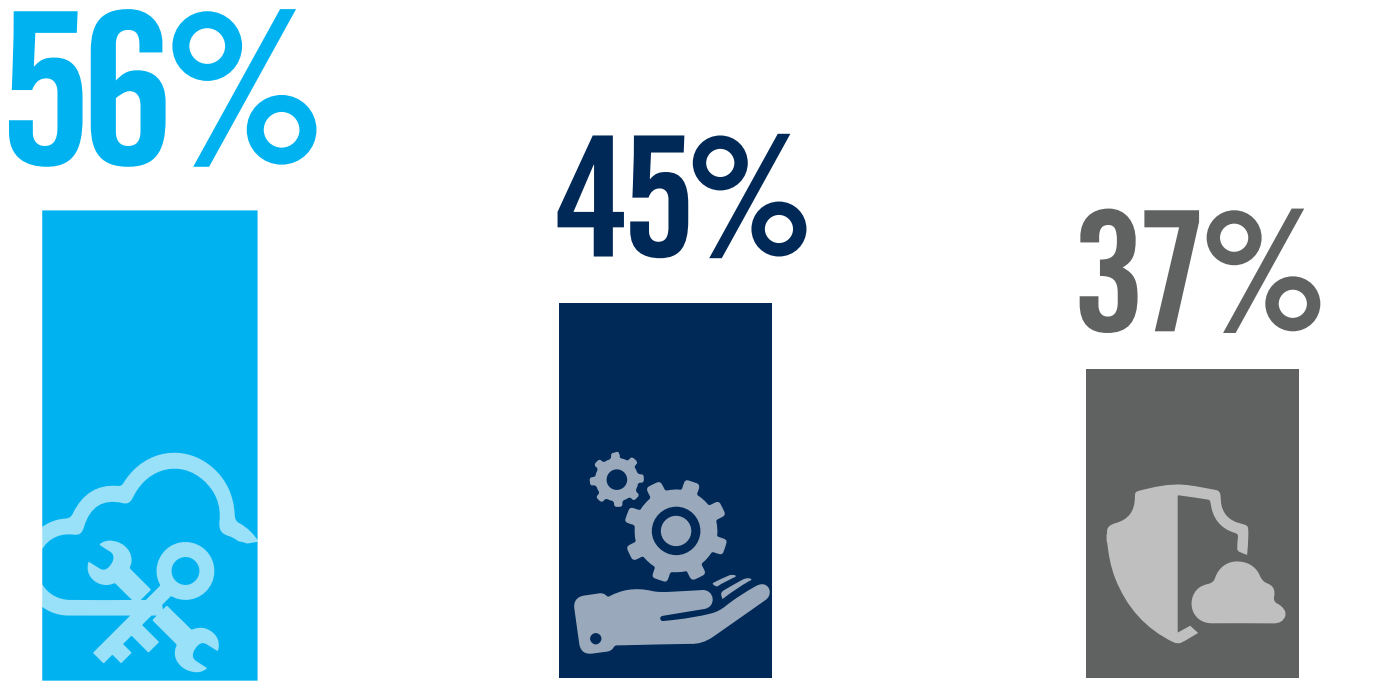
over the next 12 months

Increase Unchanged Decrease

CLOUD SECURITY SOURCING

A majority of organizations (56%) utilize cloud providers' native security tools for their security needs. This is followed by outsourcing security to managed services providers (45%) and the deployment of third-party cloud security solutions (37%).

How do you source cloud security?



Cloud provider native security tools

Managed services provider

Third-party cloud security vendor

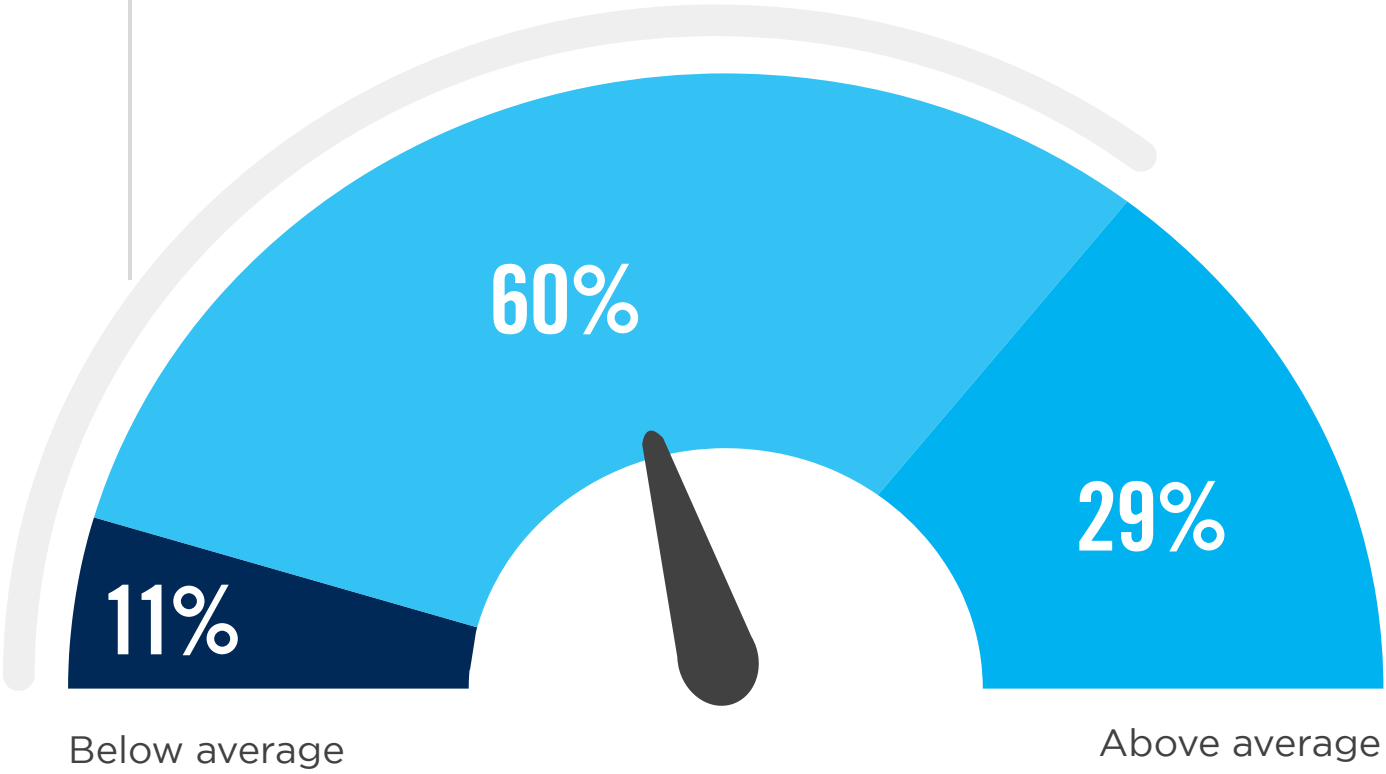
Other 3%

SECURITY READINESS

When asked about their overall security readiness, 71% consider themselves average to below average.

How would you rate your team's overall security readiness?

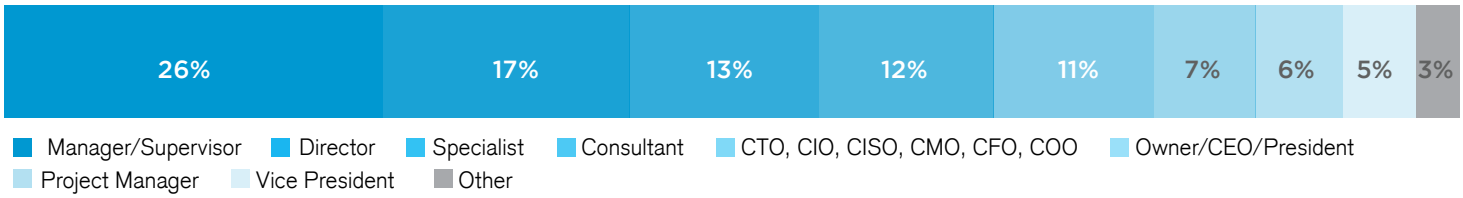
71% Consider their overall security readiness below average



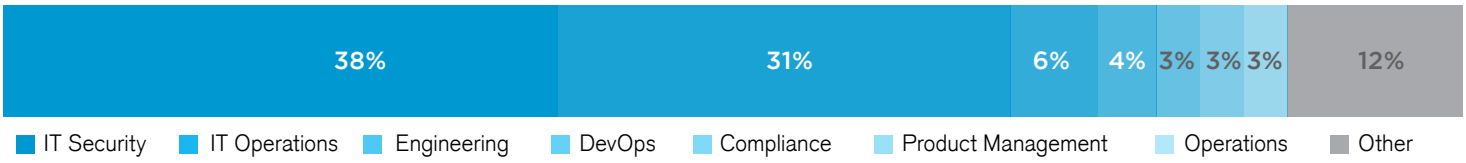
METHODOLOGY & DEMOGRAPHICS

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.

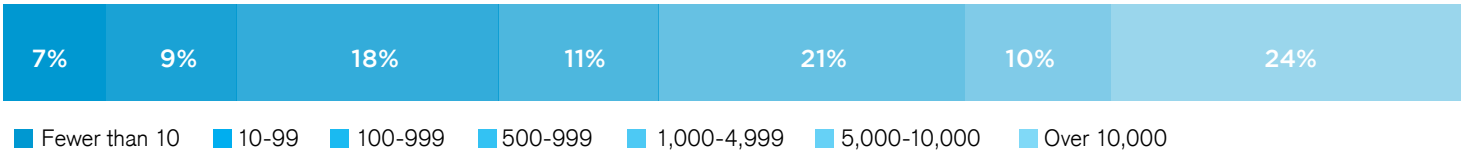
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Edgile is the trusted cyber risk and compliance partner to the world's leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

Edgile.com