COALFIRE

Cloud Security Intelligence Report

Cloud with Confidence

securities

Cybersecurity INSIDERS

2019 edition

Table of contents

Executive summary

The cloud has become such a dominant enterprise architectural paradigm that some industry pundits suggest dropping it from the IT lexicon altogether. Today, most analysts report that approximately 90% of enterprises are in the cloud, whether public, private, or hybrid deployments.

Despite the cloud's appeal for its promises of increased efficiency, better scalability, and improved agility, security concerns abound; 93% of enterprises are moderately to extremely concerned about cloud security, providing a barrier to a more aggressive embrace of cloud strategies. 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 Coalfire Cloud Security Intelligence Report, developed in partnership with Cybersecurity Insiders, highlights what is and is not working for security operations teams when securing their cloud data, systems, and services in this shared responsibility model. The results are a continuation of past challenges:

- The top cloud security concerns of cybersecurity professionals are data loss and leakage (64%) and data privacy/ confidentiality (62%).
- Unauthorized access through misuse of employee credentials and improper access controls (42%) and insecure interfaces and APIs (42%) are tied for the top spot in this year's survey as the single biggest perceived vulnerability to cloud security. They are followed by misconfiguration of the cloud platform (40%).
- The top two operational security headaches SOC teams struggle with are compliance (34%) and lack of visibility into infrastructure security (33%). Staffing issues continue to be a challenge: 31% cite a lack of qualified staff as a hurdle.
- Of special concern is the number of organizations (25%) that lack visibility into their own security status.

Overall, the findings in this report emphasize that organizations must regularly reassess their security postures, while also re-evaluating whether their cloud deployments are meeting their business objectives and the promised benefits of the technologies. They must address the shortcomings of legacy security tools to protect their evolving IT environments.

This report was conducted in cooperation with Cybersecurity Insiders, leveraging their 400,000-member information security community, to provide a detailed look at how organizations are responding to the evolving security threats in the cloud.

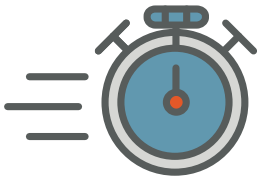
Drivers of cloud-based security solutions

Organizations recognize several key advantages of deploying cloud-based security solutions. Respondents selected cost savings (42%) along with faster time to deployment (39%) and better performance (34%) as the top three factors for selecting cloud-based security solutions.

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

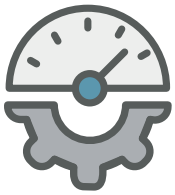
42%

Cost savings



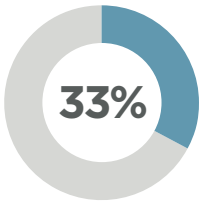
39%

Faster time to deployment

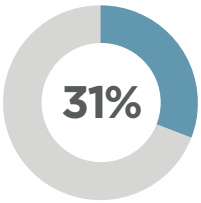


34%

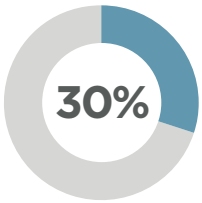
Better performance



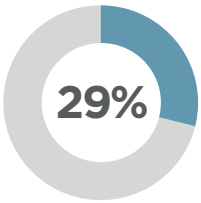
Our data/workloads reside in the cloud (or are moving to the cloud)



Reduced effort around patches and upgrades of software



Need for secure app access from any location



Meet cloud compliance expectations

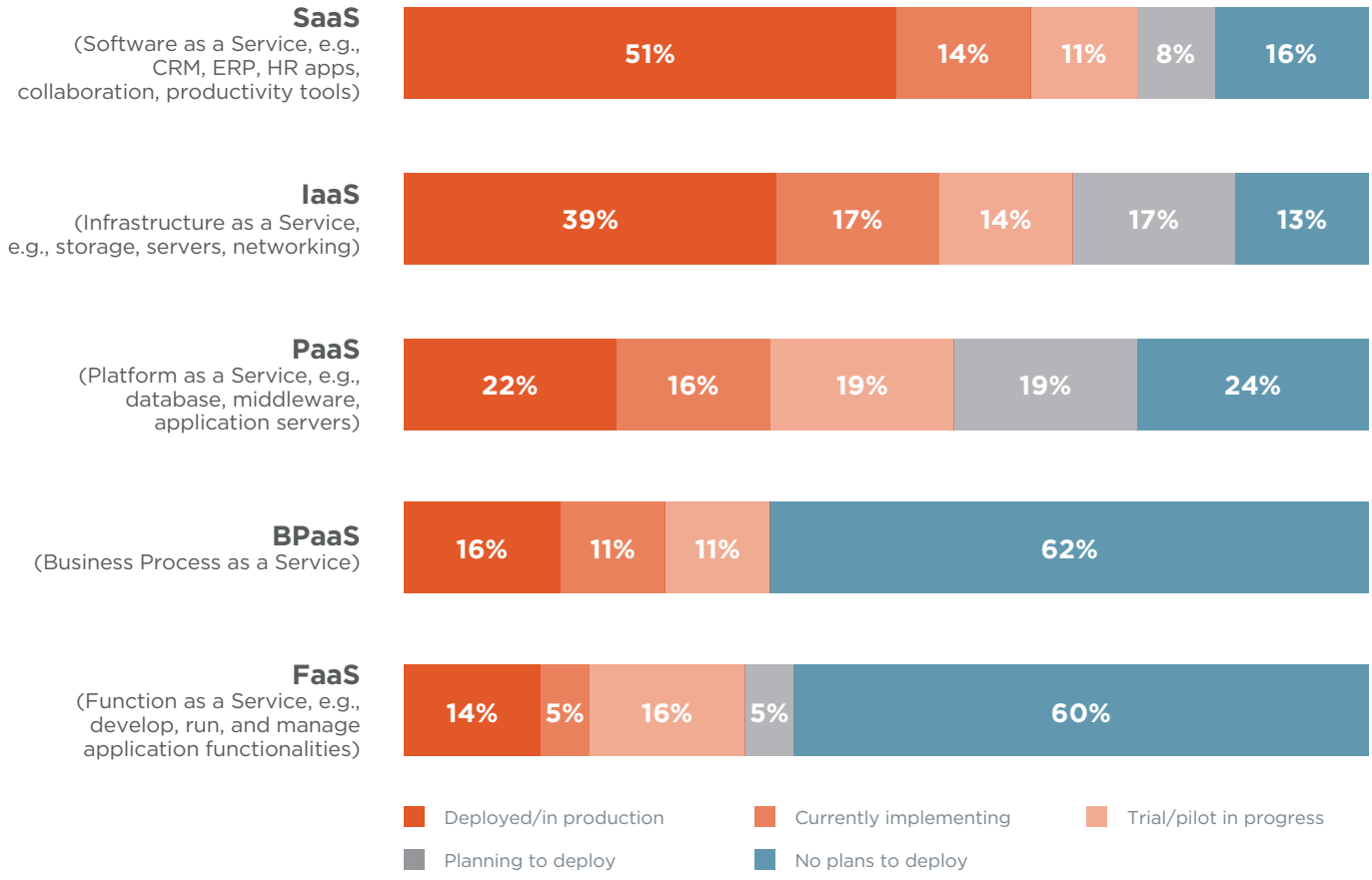
Better visibility into user activity and system behavior 25% | Reduction of appliance footprint in branch offices 23% | Easier policy management 22% | Other 2%

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.

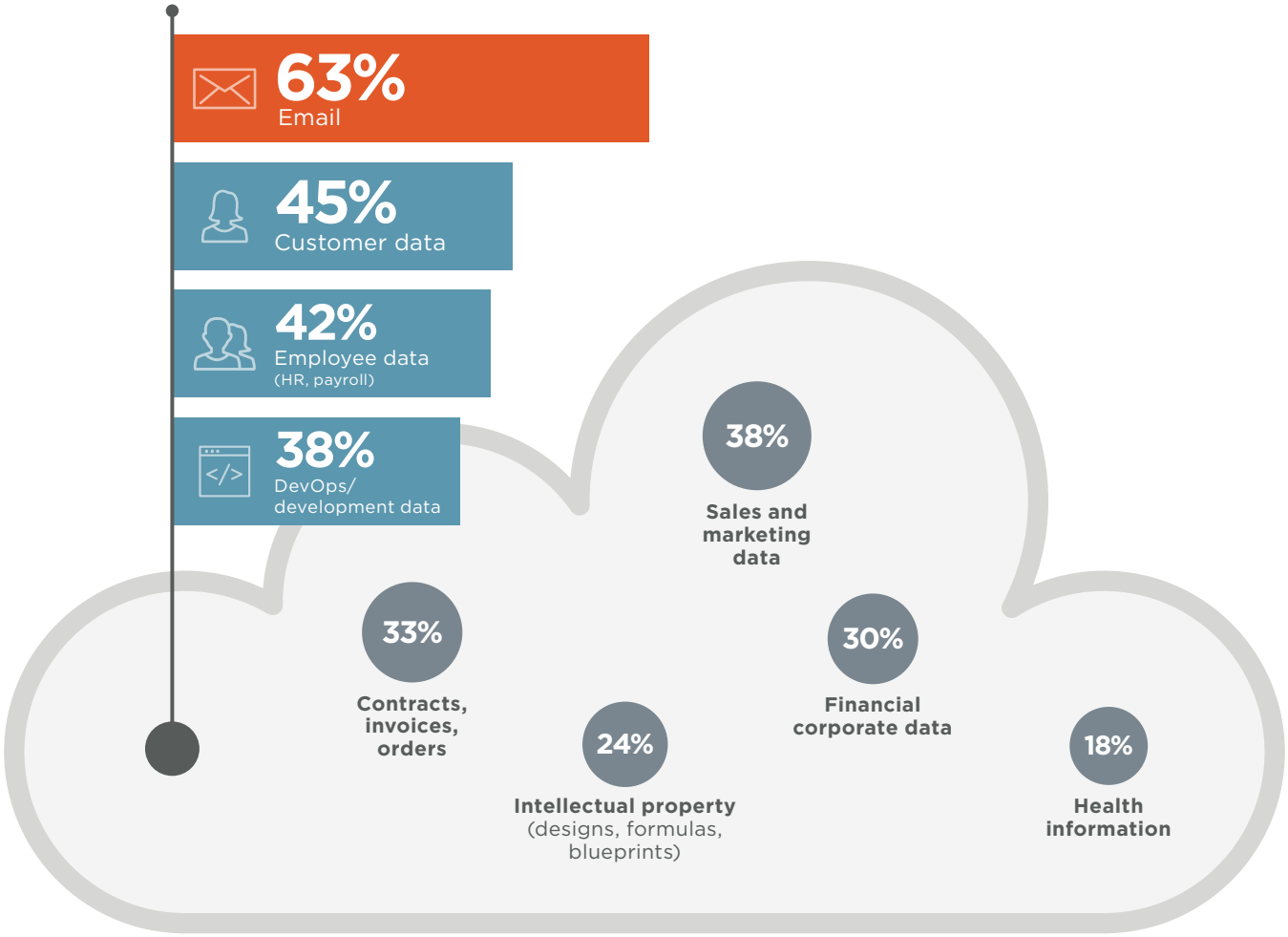
What is your organization's state of adoption of cloud computing?



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?

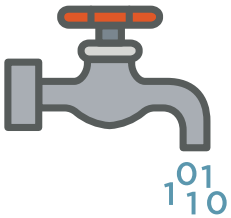


Other 5%

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%

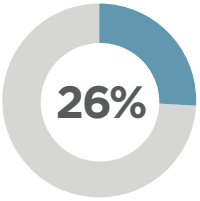
Data security, loss, and leakage risks

28%

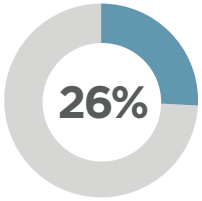
General security risks

26%

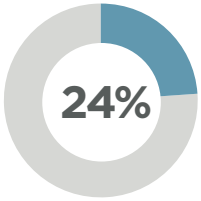
Lack of budget



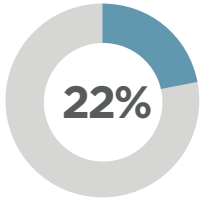
Legal and regulatory



Lack of staff



Integration with existing



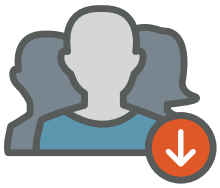
Loss

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%

Barriers to cloud-based security adoption

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%

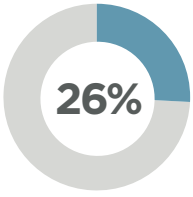
Staff expertise and training

40%

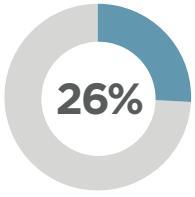
Budget challenges

38%

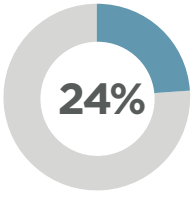
Data privacy concerns



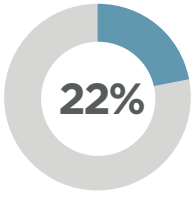
Legal and regulatory



Lack of budget



Integration with existing



Loss

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%

Cloud adoption hurdles

The most frequently mentioned hurdles to faster cloud adoption include lack of control (55%), followed by cost issues (36%), and security concerns (29%).

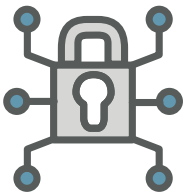
What surprises did you uncover that may slow/stop cloud adoption?

Other 10%

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%

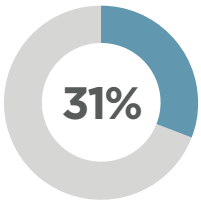
Encryption of data-at-rest

37%

Automating compliance

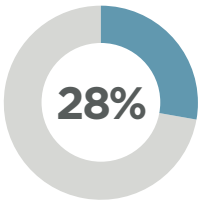
34%

APIs for reporting, auditing, and alerting on security events

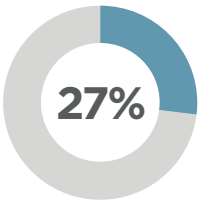


Isolation/protection of virtual machines

Setting and enforcing security policies



Leveraging data leakage prevention tools



Creating data boundaries

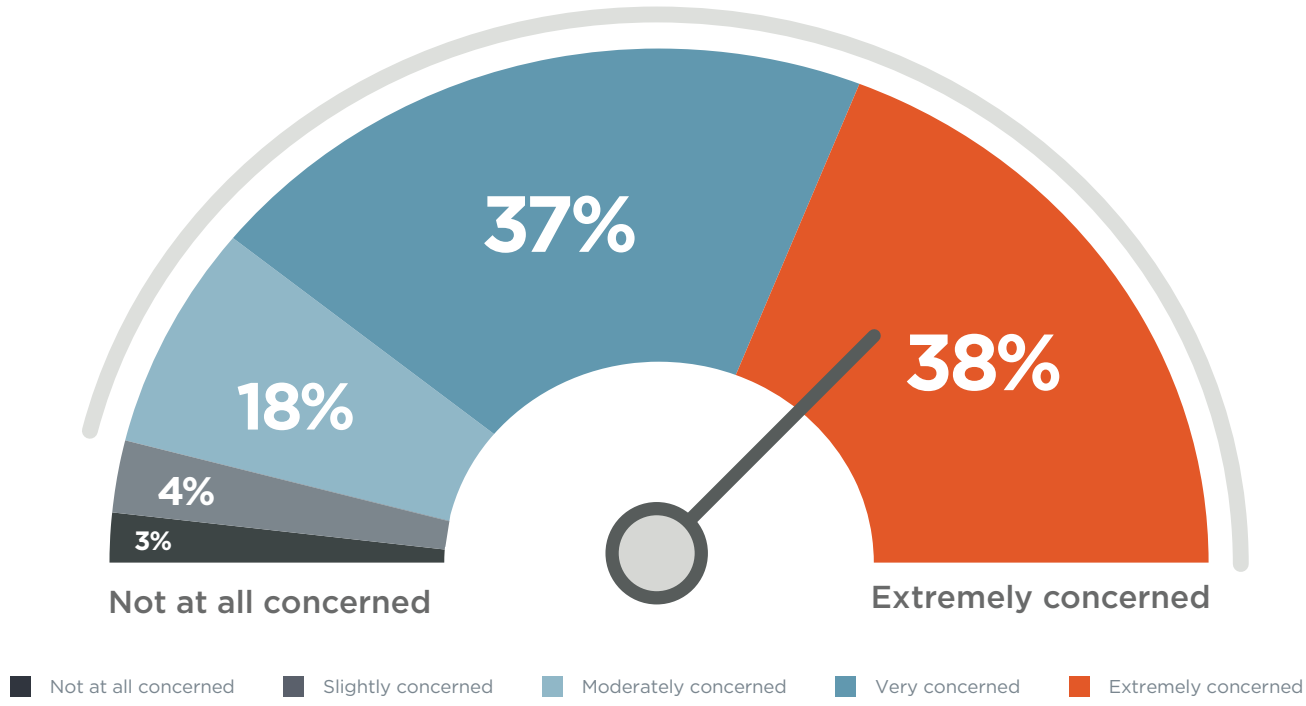
Protecting workloads 26% | Limiting unmanaged device access 25% | Leveraging threat prevention tools 24% | Proxying traffic for real-time security at access 21% | Other 2%

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?

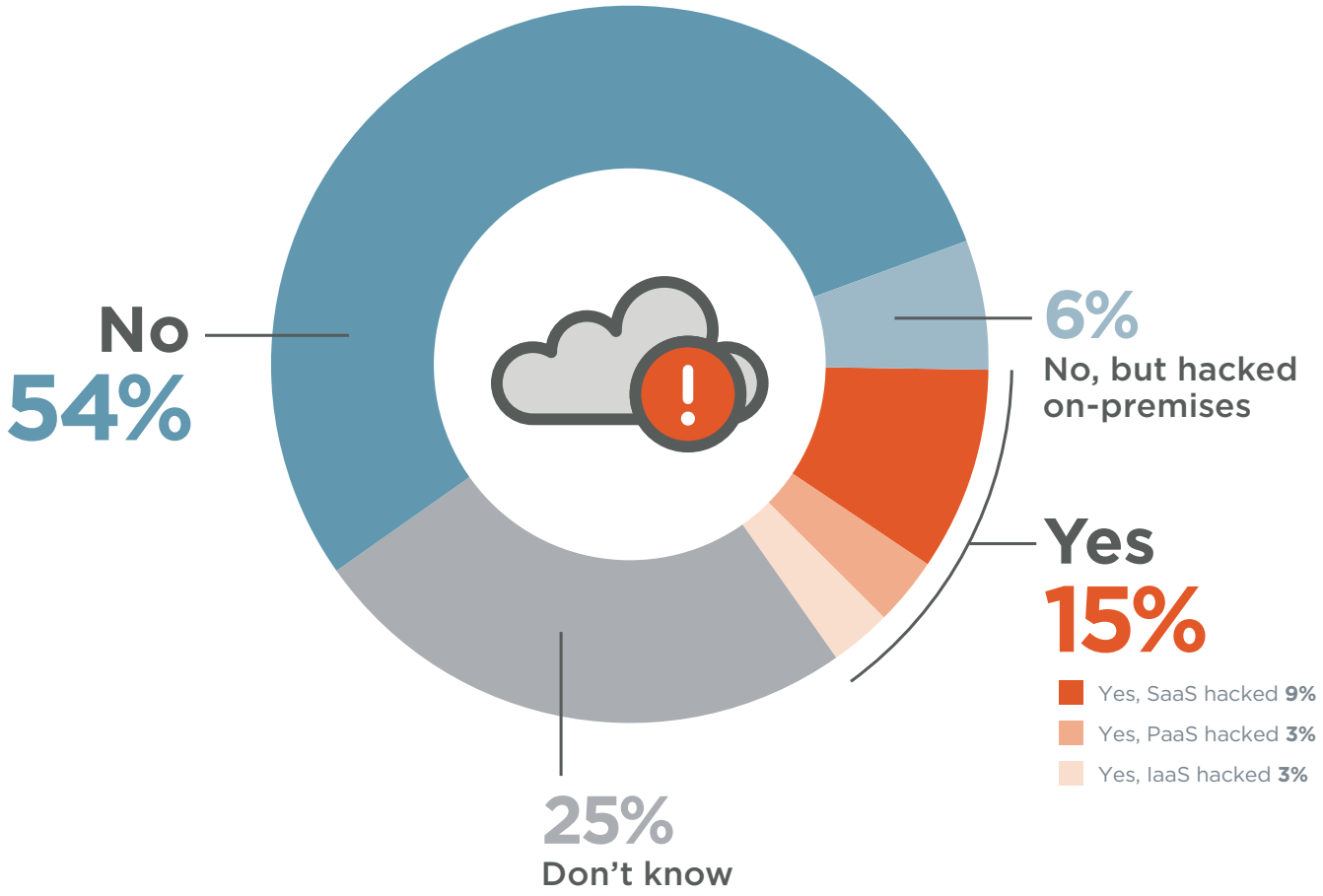
93% of organizations are moderately to extremely concerned about cloud security



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?



Operational security headaches

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 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.

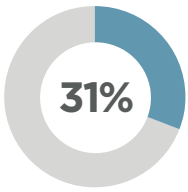
What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

34%

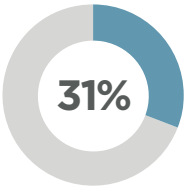
Compliance

33%

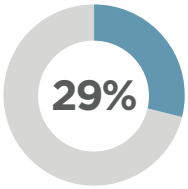
Visibility into infrastructure security



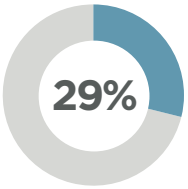
Lack of qualified staff



Setting consistent security policies



Lack of integration with on-premises security technologies



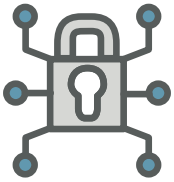
Security can't keep up with the pace of changes to

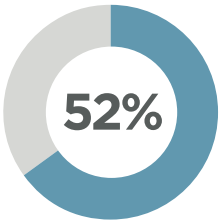
Can't identify misconfigurations quickly 24% | Complex cloud to cloud/cloud to on-premises security rule matching 24% | Securing access from personal and mobile devices 23% | Reporting security threats 23% | Remediating threats 22% | Understanding network traffic patterns 21% | Justifying more security 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%

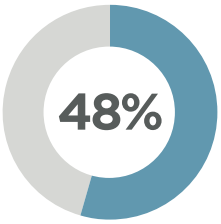
Data protection technologies

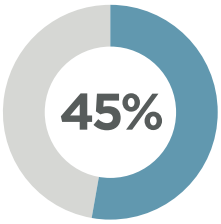
The most frequently deployed security technologies to protect data in the cloud include access controls (52%), encryption and tokenization (48%), and security features offered by the cloud services provider (45%).

How do you protect data in the cloud?







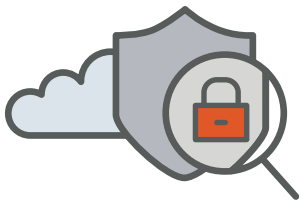


We deploy cloud security monitoring tools 36% | We connect to the cloud via protected networks 36% | We deploy additional security services offered by third-party vendors 25% | We don't protect data in the cloud 6% | Not sure/other 10%

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%

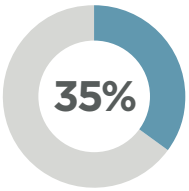
Monitoring for new vulnerabilities in cloud services that must be secured

40%

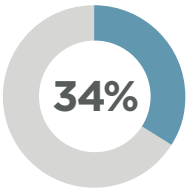
Going through audit/risk assessment within the cloud environment

39%

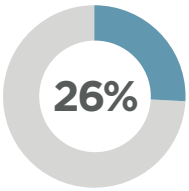
Monitoring for compliance with policies and procedures



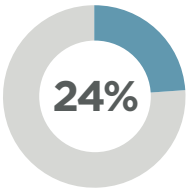
Staying up to date on new/changing compliance and



Data quality and integrity in regulatory reporting



Scaling and automating compliance activities



Applying/following the shared responsibility model

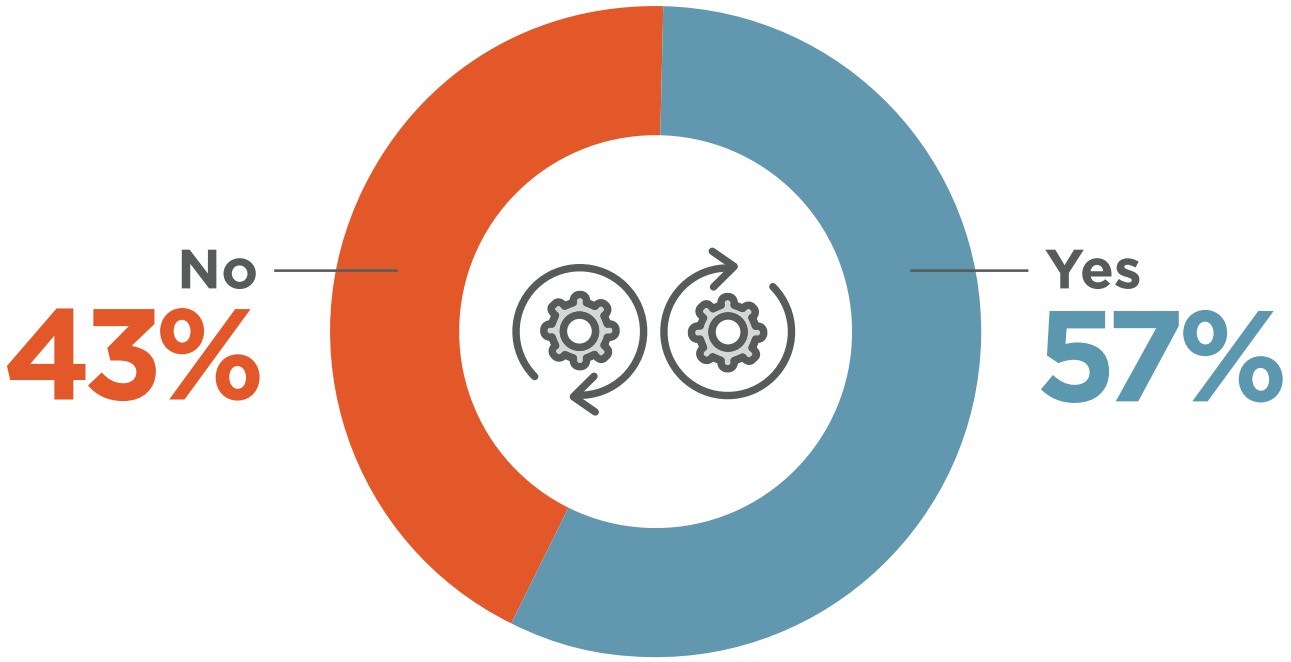
Other 12%

DevOps toolchain integration

More organizations are adopting DevOps for faster software development and delivery while improving application quality and security. A DevOps toolchain is the integration of a set of software development tools used to support development, operations, and delivery tasks.

We asked IT professionals whether they integrate their DevOps toolchain into their cloud deployments. We recorded 57% said yes and 43% said no.

Do you integrate your DevOps toolchain into your cloud deployments?



Biggest cloud security threats

Unauthorized access (42%) and insecure interfaces (42%) take the number-one spot in this year's survey as the single biggest vulnerability 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%

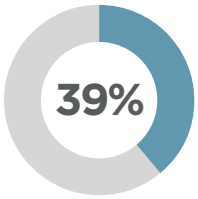
Unauthorized access

42%

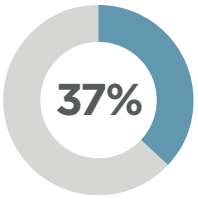
Insecure interfaces/APIs

40%

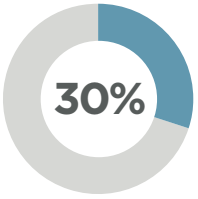
Misconfiguration of the cloud platform/ wrong setup



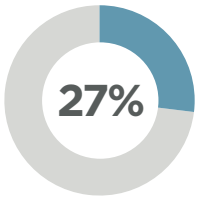
Hijacking of accounts



External sharing of data



Malicious insiders



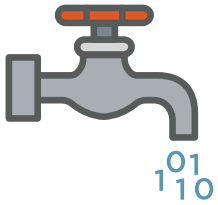
Malware/ ransomware

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

Cloud security concerns

Although cloud providers offer increasingly robust security measures, customers are ultimately responsible for securing their workloads in the cloud. The top cloud security challenges highlighted in our survey are about data loss (64%) and data privacy (62%). This is followed by compliance concerns (39%) tied with concerns about accidental exposure of credentials (39%).

What are your biggest cloud security concerns?

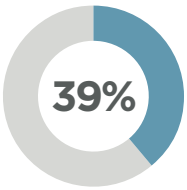


64%

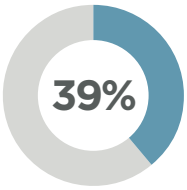
Data loss/leakage

33%

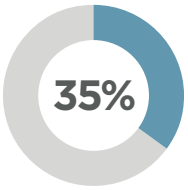
Data privacy/ confidentiality



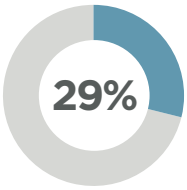
Legal and regulatory



Accidental exposure



Data sovereignty/



Incident

Fraud (e.g., theft of SSN records) 28% | Visibility & transparency 28% | Lack of forensic data 27% | Disaster recovery 25% | Availability of services, systems and data 25% | Liability 24% | Performance 23% | Business continuity 23% | Having to adopt new security tools 19% | Not sure/other 8%

Cloud security priorities

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

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

25%

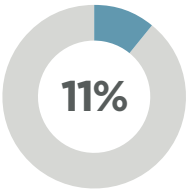
Defending against malware

20%

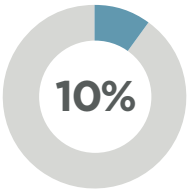
Reaching regulatory compliance

15%

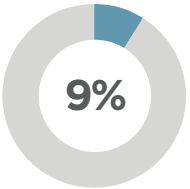
Securing major cloud apps already in use



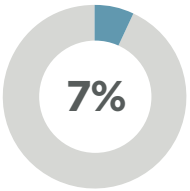
Preventing cloud misconfigurations



Securing mobile devices



Discovering unsanctioned cloud apps in use



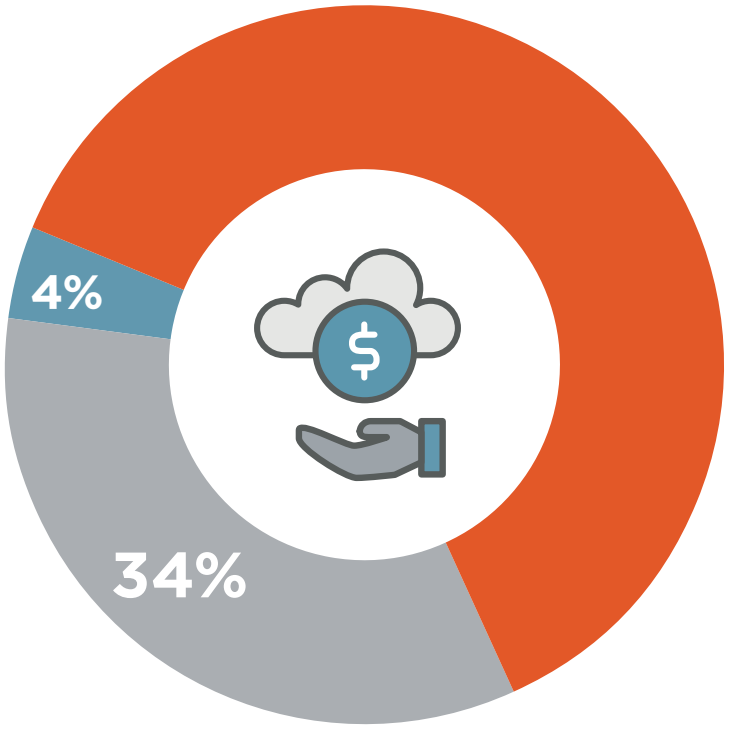
Securing less popular cloud apps already in use

Securing BYOD (Bring Your Own Device) 4%

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

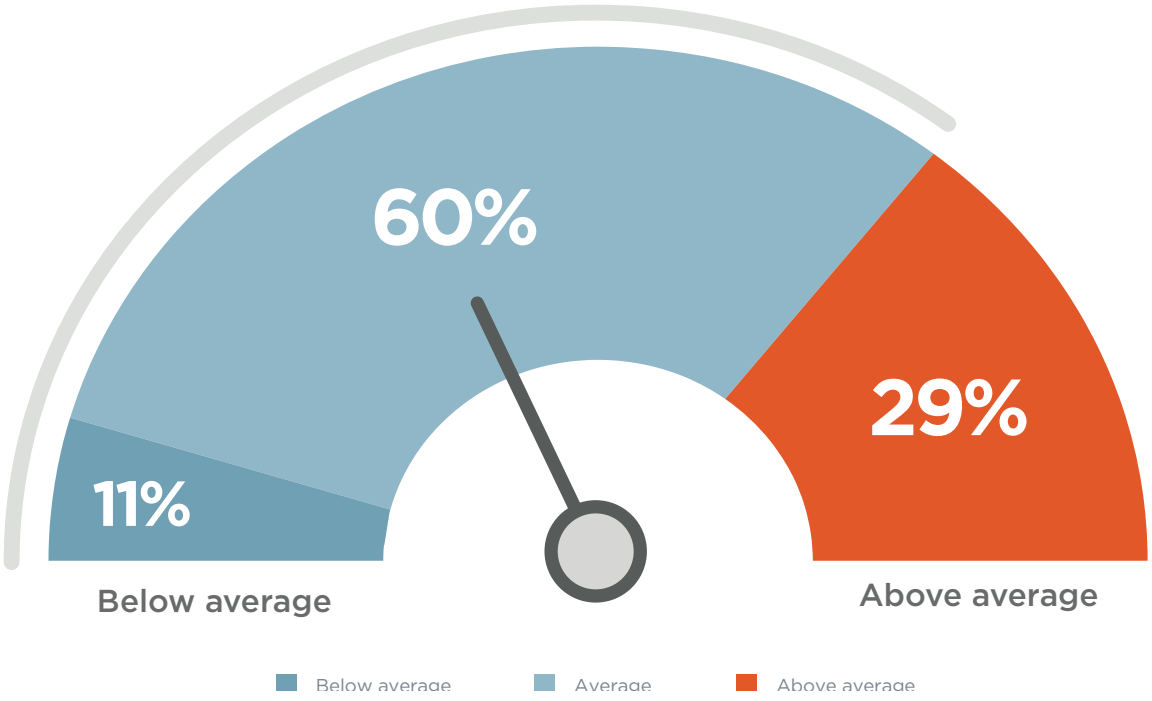
Increase Unchanged Decrease

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 average or less.

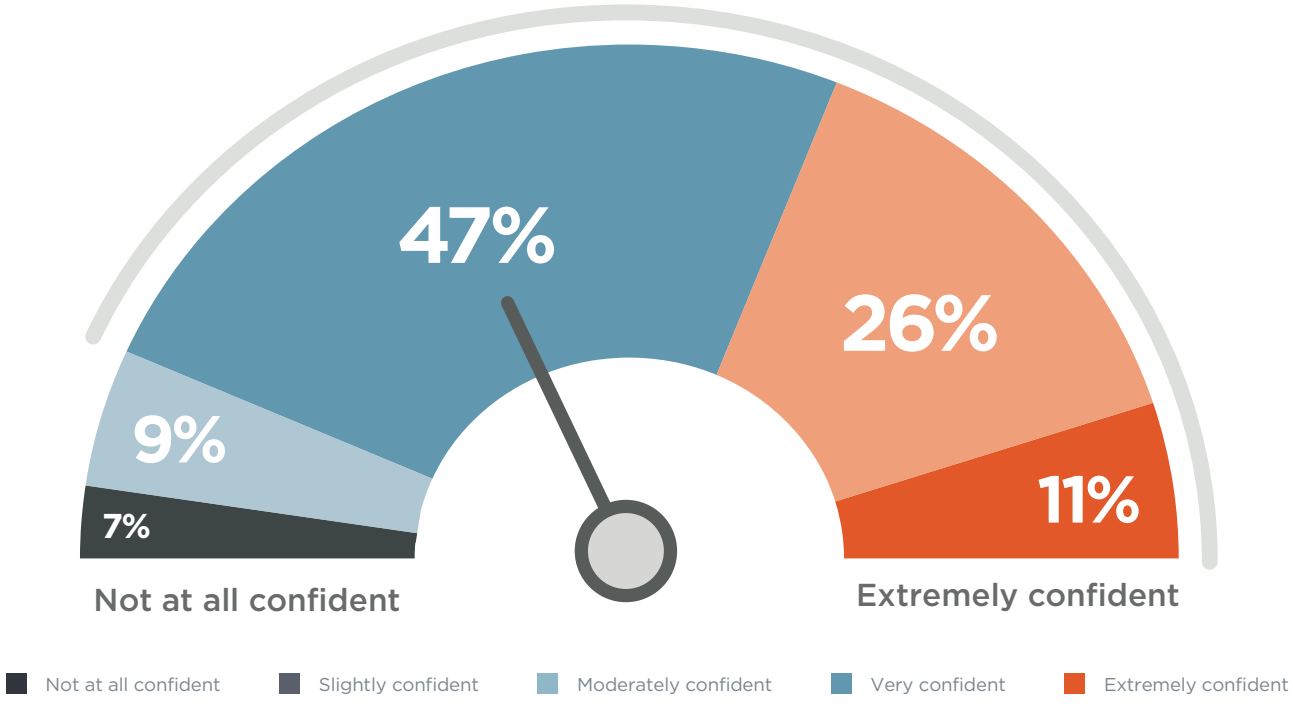


Cloud security confidence

Most organizations are at least moderately confident in their cloud security posture (84%) – perhaps reflecting a level of overconfidence not supported by the security incidents and challenges presented in this report.

How confident are you in your organization's cloud security posture?

84% Most organizations are at least moderately confident in their cloud security posture

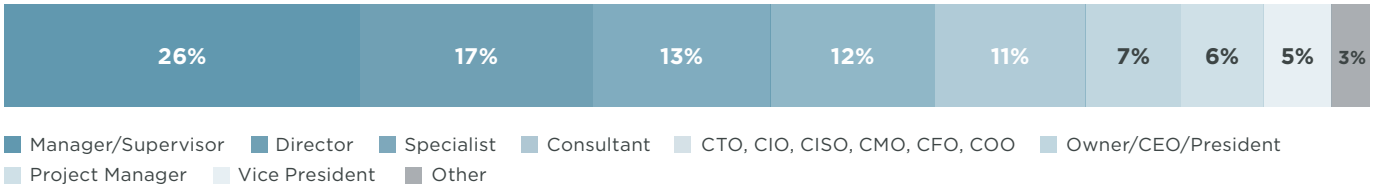


Methodology and demographics

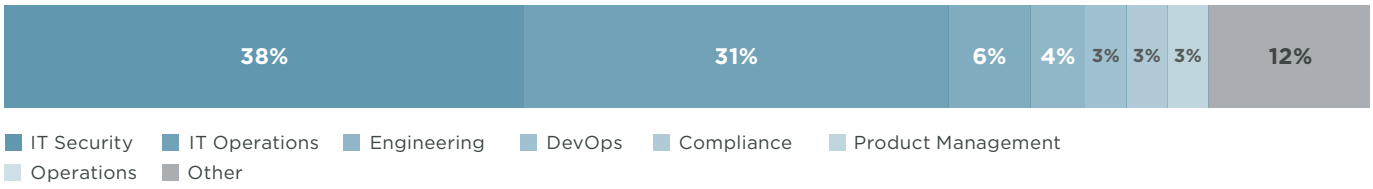
The 2019 Coalfire Cloud Security Intelligence Report was developed in partnership with Cybersecurity Insiders. The report is based on the results of a comprehensive online survey of cybersecurity professionals conducted in March of 2019 to gain deep insight into the latest trends, key challenges, and 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.

Cybersecurity Insiders conducted the survey, summarized the results, and reserves all right to the data.

Career level



Department



Company size