# Table of contents

**Executive summary** .......................................................... 3

**Cloud usage**
- What are the main drivers for considering cloud-based security solutions? ............... 4
- What is your organization’s state of adoption of cloud computing? ......................... 5
- What types of corporate information do you store in the cloud? ............................ 6
- What are the biggest barriers to cloud adoption in your organization? ................. 7
- What are the main barriers to migrating to cloud-based security solutions? ........... 8
- What surprises did you uncover that may slow/stop cloud adoption? ................... 9
- Which security controls would increase your confidence in adopting public clouds? ... 10

**Cloud breaches**
- How concerned are you about the security of public clouds? ............................... 11
- Has your organization ever been hacked in the cloud? ....................................... 12

**Protecting your cloud environment**
- What are the biggest operational, day-to-day headaches with protecting cloud workloads? ................................................................. 13
- How do you protect data in the cloud? ................................................................ 14
- Which part of the cloud compliance process is the most challenging? ................. 15
- Do you integrate your DevOps toolchain into your cloud deployments? ............ 16

**Cloud security threats and concerns**
- What do you see as the biggest security threats in public clouds? ....................... 17
- What are your biggest cloud security concerns? ............................................... 18

**Cloud security outlook**
- What are your company’s cloud security priorities this year? ............................ 19
- How is your cloud security budget changing in the next 12 months? .................. 20
- How would you rate your team’s overall security readiness? ............................ 21
- How confident are you in your organization’s cloud security posture? ............ 22

**Methodology and demographics** ............................................ 23
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?

- Cost savings: 42%
- Faster time to deployment: 39%
- Better performance: 34%

- Our data/workloads reside in the cloud (or are moving to the cloud): 33%
- Reduced effort around patches and upgrades of software: 31%
- Need for secure app access from any location: 30%
- Meet cloud compliance expectations: 29%

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?

**SaaS**
(Software as a Service, e.g., CRM, ERP, HR apps, collaboration, productivity tools)
- Deployed/in production: 51%
- Currently implementing: 14%
- Planning to deploy: 11%
- No plans to deploy: 8%
- No plans to deploy: 16%

**IaaS**
(Infrastructure as a Service, e.g., storage, servers, networking)
- Deployed/in production: 39%
- Currently implementing: 17%
- Planning to deploy: 14%
- No plans to deploy: 17%
- No plans to deploy: 13%

**PaaS**
(Platform as a Service, e.g., database, middleware, application servers)
- Deployed/in production: 22%
- Currently implementing: 16%
- Planning to deploy: 19%
- No plans to deploy: 19%
- No plans to deploy: 24%

**BPaaS**
(Business Process as a Service)
- Deployed/in production: 16%
- Currently implementing: 11%
- Planning to deploy: 11%
- No plans to deploy: 62%

**FaaS**
(Function as a Service, e.g., develop, run, and manage application functionalities)
- Deployed/in production: 14%
- Currently implementing: 5%
- Planning to deploy: 16%
- No plans to deploy: 5%
- No plans to deploy: 60%
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?

- **Email**: 63%
- **Customer data**: 45%
- **Employee data (HR, payroll)**: 42%
- **DevOps/development data**: 38%
- **Contracts, invoices, orders**: 33%
- **Sales and marketing data**: 38%
- **Intellectual property (designs, formulas, blueprints)**: 24%
- **Financial corporate data**: 30%
- **Health information**: 18%
- **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?

- Data security, loss, and leakage risks: 29%
- General security risks: 28%
- Lack of budget: 26%
- Legal and regulatory compliance: 26%
- Integration with existing IT environment: 24%
- Lack of staff resources or expertise: 22%
- Loss of control: 20%
- 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?

- Staff expertise and training: 41%
- Budget challenges: 40%
- Data privacy concerns: 38%
- Legal and regulatory: 26%
- Lack of budget: 26%
- Integration with existing: 24%
- Loss: 22%
- 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?

- Not enough control: 55%
- Too expensive: 36%
- Not secure: 29%

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?

- Encryption of data-at-rest: 38%
- Automating compliance: 37%
- APIs for reporting, auditing, and alerting on security events: 34%
- Isolation/protection of virtual machines: 31%
- Setting and enforcing security policies: 30%
- Leveraging data leakage prevention tools: 28%
- Creating data boundaries: 27%
- 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

- Not at all concerned: 38%
- Slightly concerned: 37%
- Moderately concerned: 18%
- Very concerned: 4%
- Extremely concerned: 3%

Emblem of cloud security concerns
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?

- No: 54%
- Yes, IaaS hacked: 3%
- Yes, PaaS hacked: 3%
- Yes, SaaS hacked: 9%
- No, but hacked on-premises: 6%
- Don’t know: 25%
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?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>34%</td>
<td>Compliance</td>
</tr>
<tr>
<td>33%</td>
<td>Visibility into infrastructure security</td>
</tr>
<tr>
<td>31%</td>
<td>Lack of qualified staff</td>
</tr>
<tr>
<td>31%</td>
<td>Setting consistent security policies</td>
</tr>
<tr>
<td>29%</td>
<td>Lack of integration with on-premises security technologies</td>
</tr>
<tr>
<td>29%</td>
<td>Security can’t keep up with the pace of changes to</td>
</tr>
</tbody>
</table>

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% | Remediation 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?

- 52% We use access controls
- 48% We use encryption
- 45% We use security services offered natively by the cloud provider
- 36% We deploy cloud security monitoring tools
- 36% We connect to the cloud via protected networks
- 25% We deploy additional security services offered by third-party vendors
- 6% We don’t protect data in the cloud
- 10% Not sure/other

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?

- Monitoring for new vulnerabilities in cloud services that must be secured: 43%
- Going through audit/risk assessment within the cloud environment: 40%
- Monitoring for compliance with policies and procedures: 39%

- Staying up to date on new/changing compliance and regulatory requirements: 35%
- Data quality and integrity in regulatory reporting: 34%
- Scaling and automating compliance activities: 26%
- Applying/following the shared responsibility model: 24%

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?

- **Yes** 57%
- **No** 43%
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?

- Unauthorized access: 42%
- Insecure interfaces/APIs: 42%
- Misconfiguration of the cloud platform/wrong setup: 40%
- Hijacking of accounts: 39%
- External sharing of data: 37%
- Malicious insiders: 30%
- Malware/ransomware: 27%
- 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

39% Legal and regulatory

39% Accidental exposure

35% Data sovereignty/

29% 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

- **11%** preventing cloud misconfigurations
- **10%** securing mobile devices
- **9%** discovering unsanctioned cloud apps in use
- **7%** 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.
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.

Below average: 11%
Average: 60%
Above average: 29%
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.

Not at all confident: 7%
Slightly confident: 9%
Moderately confident: 47%
Very confident: 26%
Extremely confident: 11%
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

<table>
<thead>
<tr>
<th>Career Level</th>
<th>26%</th>
<th>17%</th>
<th>13%</th>
<th>12%</th>
<th>11%</th>
<th>7%</th>
<th>6%</th>
<th>5%</th>
<th>3%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager/Supervisor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consultant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTO, CIO, CISO, CMO, CFO, COO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner/CEO/President</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice President</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Department

<table>
<thead>
<tr>
<th>Department</th>
<th>38%</th>
<th>31%</th>
<th>6%</th>
<th>4%</th>
<th>3%</th>
<th>3%</th>
<th>3%</th>
<th>12%</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DevOps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Company size

<table>
<thead>
<tr>
<th>Company Size</th>
<th>7%</th>
<th>9%</th>
<th>18%</th>
<th>11%</th>
<th>21%</th>
<th>10%</th>
<th>24%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10-99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100-499</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>500-999</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1,000-4,999</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5,000-10,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Over 10,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All right reserved. ©2019 Cybersecurity Insiders