State of Cloud Security Survey

New Fugue survey finds the split shift to 100% distributed teams is creating new cloud security risks for organizations and opportunities for malicious actors.

83% of companies are making the transition to 100% distributed teams.

84% of companies are concerned about cloud security during the transition.

About this survey
Fugue partnered with Propeller Insights to survey 300 IT, cloud, and security professionals, including DevOps engineers, cloud architects, security engineers, site reliability engineers (SREs), DevSecOps engineers, and application developers.

Professionals from companies representing a variety of industries that use Amazon Web Services, Microsoft Azure, and Google Cloud Platform for cloud computing were surveyed.


Cloud Security Concerns During the Covid-19 Crisis

New Fugue survey finds the rapid shift to 100% distributed teams is creating new cloud security risks for organizations and opportunities for malicious actors.

Are you concerned that you’ve been hacked and don’t know it?

84% of companies are concerned that they’ve been hacked and don’t know it.

Are you concerned that you’re vulnerable to a major cloud data breach?

92% of companies are concerned that they’re vulnerable to a major cloud data breach.

In the next year, do you think cloud misconfiguration risk will:

Increase or stay the same

45%

Increase

40%

Stay the same

76%

Are you concerned that you’ve been hacked and don’t know it?

84% of companies are concerned that they’ve been hacked and don’t know it.

Are you concerned that you’re vulnerable to a major cloud data breach?

92% of companies are concerned that they’re vulnerable to a major cloud data breach.

In the next year, do you think cloud misconfiguration risk will:

Increase or stay the same

45%

Increase

40%

Stay the same

76%

Challenges in Managing Cloud Misconfiguration

Lack of awareness of cloud security and policies

52%

Lack of adequate controls and oversight

49%

Too many APIs and interfaces to adequately govern

43%

Negligent insider behavior

32%

Human error

46%

in missing critical misconfigurations

Cloud Misconfiguration Remains the #1 Cause of Cloud-Based Data Breaches

76% of companies are concerned that they’ll experience a cloud misconfiguration incident in the next year.

44% of companies experienced a security event related to a misconfiguration or another cloud security incident in the past year.

39% of companies have more than 100 security events per month.

34% of companies have more than 100 cloud events per month.

32% of companies have more than 100 compliance violation events per month.

52% of companies have more than 100 object storage breaches per month.

40% of companies have more than 100 unauthorized access to instances or databases.

36% of companies have more than 100 system downtime events per week.

43% of companies have more than 100 compliance violation events per week.

39% of companies have more than 100 object storage breaches per week.

32% of companies have more than 100 unauthorized access to instances or databases per week.

28% of companies have more than 100 compliance violation events per day.

26% of companies have more than 100 object storage breaches per day.

25% of companies have more than 100 unauthorized access to instances or databases per day.

What’s Needed to Better Address Cloud Misconfiguration?

30% better visibility into cloud infrastructure

28% training and education

95% automated detection and remediation

The Cost of Managing Cloud Misconfiguration

46% more than 10 hours per week teams invest in managing the problem

43% more than a month per incident teams invest in managing the problem

47% more than 50 hours

37% 10-50 hours

14% less than 10 hours

Lack of awareness of cloud security and policies

52%

Lack of adequate controls and oversight

49%

Too many APIs and interfaces to adequately govern

43%

Negligent insider behavior

32%

Human error

46%

in missing critical misconfigurations

Cloud Misconfiguration Incidents

39% insider activity

52% unauthorized access to instances or databases

44% network or DDoS attacks

40% web app and application attacks

34% cloud service provider issues

32% compliance violations

36% encryption at rest disabled (or not enabled)

26% object storage breaches

25% unauthorized access to instances or databases

24% compliance violation events

23% system downtime events

22% object access events

20% compliance violation

15% object storage breaches

14% system downtime

12% unauthorized access to instances or databases

11% compliance violation

10% object access

9% system downtime

8% unauthorized access to instances or databases

7% compliance violation

6% object access

5% system downtime

4% unauthorized access to instances or databases

3% compliance violation

2% object access

1% system downtime

Fugue partners with Propeller Insights to survey 300 IT, cloud, and security professionals, including DevOps engineers, cloud architects, security engineers, site reliability engineers (SREs), DevSecOps engineers, and application developers.

Professionals from companies representing a variety of industries that use Amazon Web Services, Microsoft Azure, and Google Cloud Platform for cloud computing were surveyed.

www.fugue.com

Fugue is a cloud security company that helps organizations secure their cloud infrastructure and applications. Our mission is to make cloud computing safer, more secure, and more efficient.