2018
REPORT

Cloud Infrastructure Misconfiguration Report

Fugue

Executive Summary

Fugue is pleased to release the 2018 Cloud Infrastructure Misconfiguration Report. For this report, we surveyed IT, Cloud, and Security and Compliance professionals from more than 300 organizations across a broad number of industries about their cloud operations and how they view and manage misconfiguration risk.

As more organizations embrace the cloud, they are quickly realizing that managing security and compliance in the cloud is a big challenge. Part of that challenge lies in being able to identify and remediate misconfiguration.

In this report, we delve deeper into cloud misconfiguration: the causes, how teams address them, what percentages are deemed to be critical, and how automated remediation can help.

WHO WE SURVEYED

61%
IT/
DEVOPS

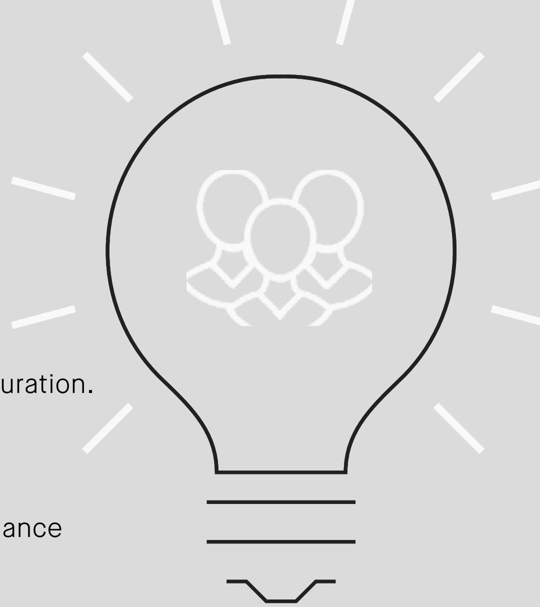
39%
SECURITY/
COMPLIANCE

64%
MANAGING 20 OR
MORE WORKLOADS

93%
CONCERNED ABOUT
COMPLIANCE

64%
USING CLOUD
AT SCALE

Key Findings



Common Misconfiguration Causes and Concerns:

- An overwhelming majority of cloud professionals (93%) say they are “somewhat concerned” or “highly concerned” that their organization is at risk of a major security breach due to misconfiguration.
- Based on the responses, 64% of organizations said that human error was the main cause for misconfiguration.
- The top two headaches for organizations struggling with misconfigurations are security/compliance incidents (89%) and system downtime (44%).

What Teams Are Doing Now:

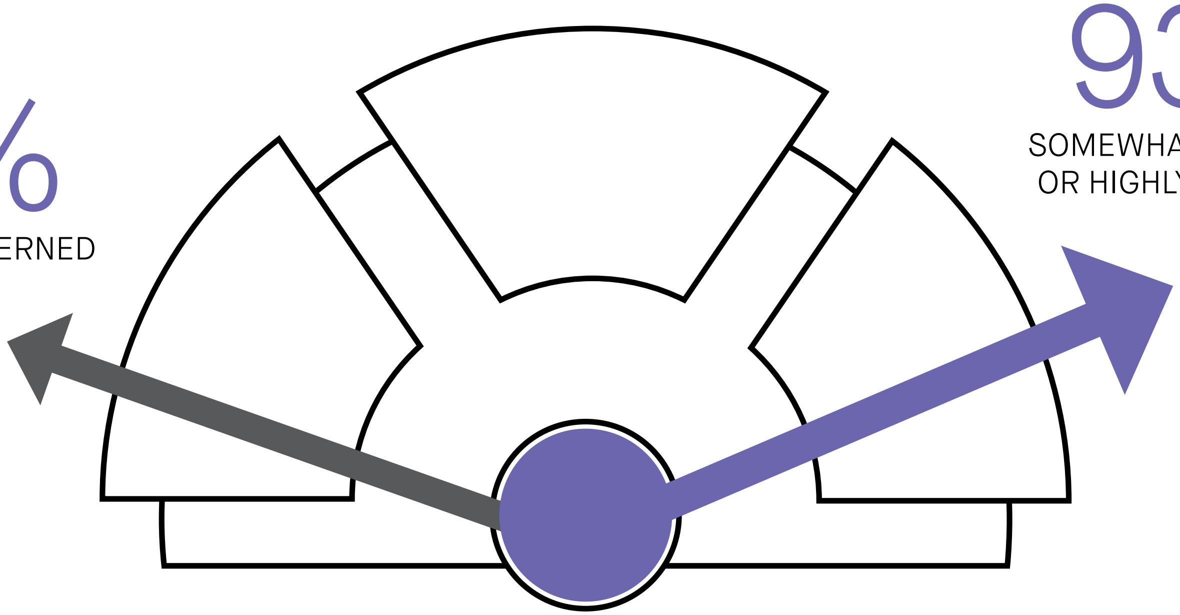
- Based on the survey, the two most common types of misconfiguration are permission control (66%) and security group rules (59%).
- With the ability to bring up thousands of resources within minutes, the risk of misconfiguration increases. 51% of organizations experience more than 50 misconfiguration events per day.

Seeing the Need for Automation:

- If organizations are not utilizing an automated remediation solution, they are most likely reviewing alerts to identify misconfiguration and prioritizing them for remediation. 49% dedicate at least one FTE to managing misconfigurations.
- Even with a dedicated FTE to monitor for misconfiguration, 79% of respondents indicated that critical misconfiguration events are still being missed.
- With so many resources to monitor, organizations can quickly become overwhelmed and frustrated. Based on the survey, 49% of organizations experienced human error in missing or miscategorizing critical misconfiguration events.
- An overwhelming majority of organizations (97%) find that an automated remediation solution would be very valuable for ensuring compliance and improving efficiency.

1. Cloud Security Concerns Due to Misconfiguration

As public cloud adoption continues to surge, security concerns due to misconfiguration are rising. An overwhelming majority of cloud professionals (93%) say they are “somewhat concerned” or “highly concerned” that their organization is at risk of a major security breach due to misconfiguration.



7%

NOT CONCERNED

93%

SOMEWHAT CONCERNED OR HIGHLY CONCERNED

2. Misconfiguration Causes

Misconfiguration can occur for a variety of reasons. Based on the responses, 64% of organizations said that human error was the main cause of misconfiguration.

64%
HUMAN ERROR

54%
LACK OF TEAM AWARENESS OF SECURITY & POLICIES

49%
LACK OF ADEQUATE CONTROLS & OVERSIGHT

47%
TOO MANY CLOUD APIS & INTERFACES TO ADEQUATELY GOVERN

3. Misconfiguration Headaches

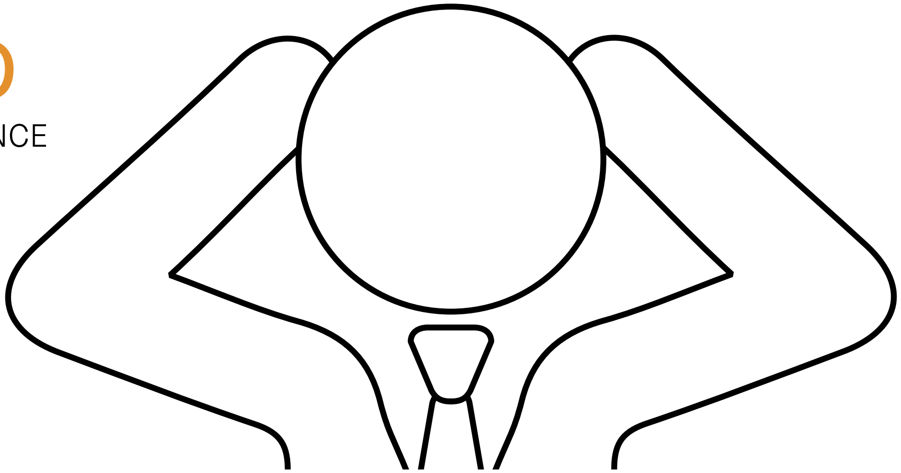
Cloud misconfiguration can cause headaches for organizations. The top 2 headaches for organizations struggling with misconfiguration are security/compliance incidents (89%) and system downtime (44%).

44%

SYSTEM DOWNTIME

89%

SECURITY/COMPLIANCE INCIDENTS

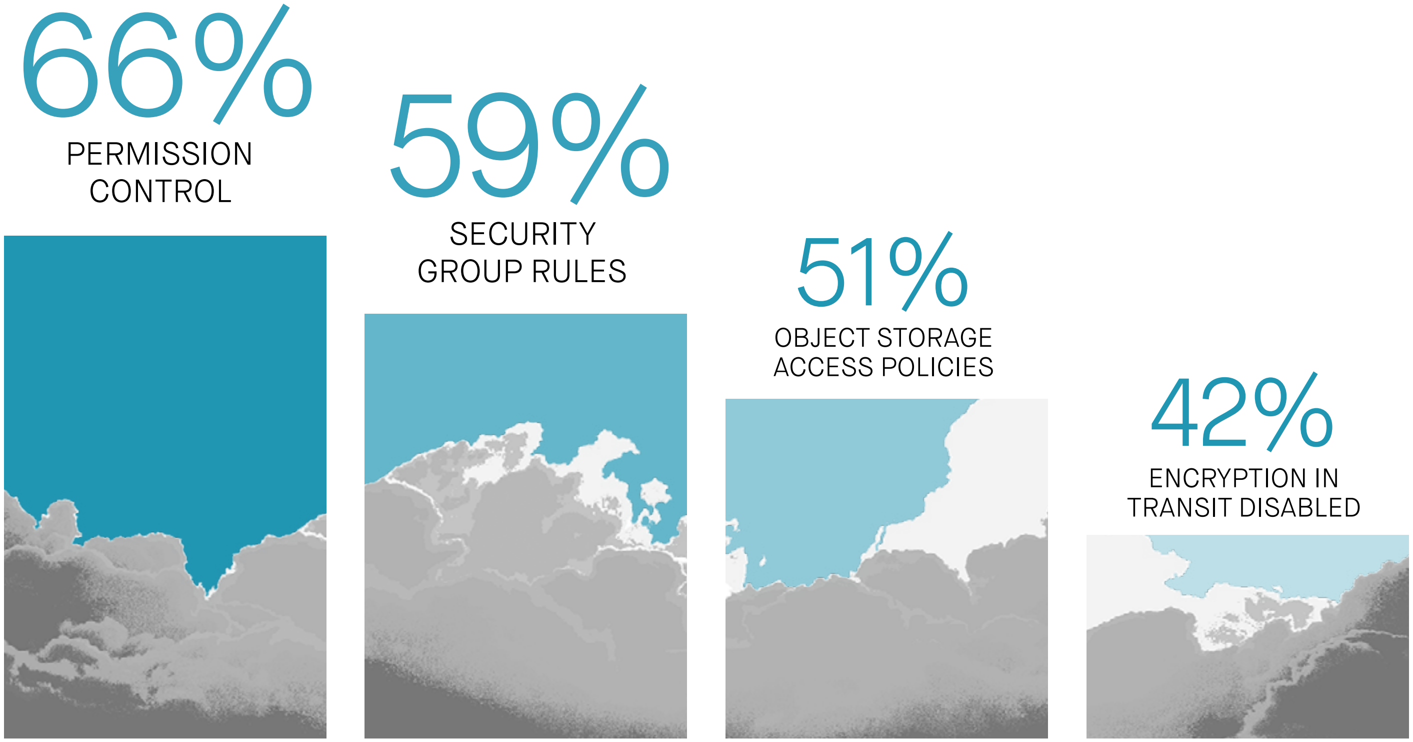


27%

REPORTED A CRITICAL SECURITY BREACH

4. Common Types of Misconfiguration

There are a number of different types of misconfiguration that organizations migrating to the cloud can encounter. Based on the survey, the two most common misconfiguration events are permission control (66%) and security group rules (59%).



5. Risk of Misconfiguration Increases

With the ability to bring up thousands of resources within minutes, the risk of misconfiguration increases. 51% of Ops teams experience more than 50 misconfiguration events daily.

51%

MORE THAN 50 PER DAY

1% MORE THAN 1000 PER DAY

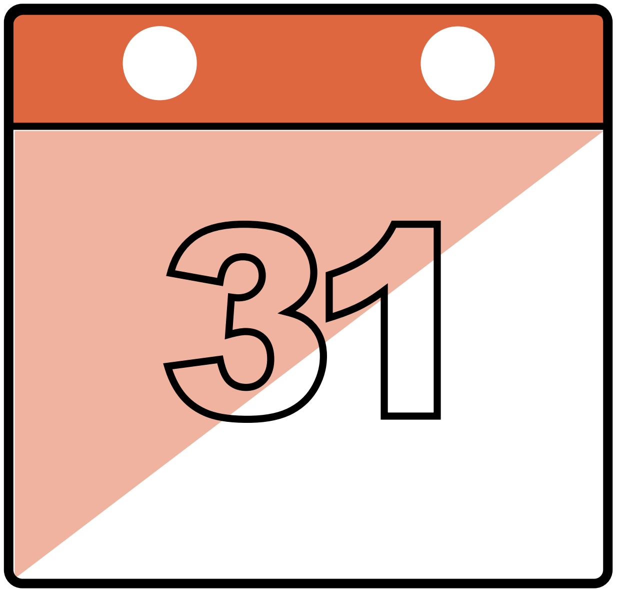
9% 1000-500 PER DAY

15% 500-250 PER DAY

14% 250-100 PER DAY

12% 100-50 PER DAY

2% NOT SURE



47%

1-50 PER DAY

6. Monitoring Alerts Can Be Time Consuming

If organizations are not utilizing a security solution with automated remediation, they are most likely manually reviewing alerts to identify and prioritize misconfiguration events for remediation.

49%

DEDICATE AT LEAST ONE FTE TO MANAGING MISCONFIGURATIONS

63%

IDENTIFY HALF OF ALERTS AS CRITICAL AND NEED REMEDIATION

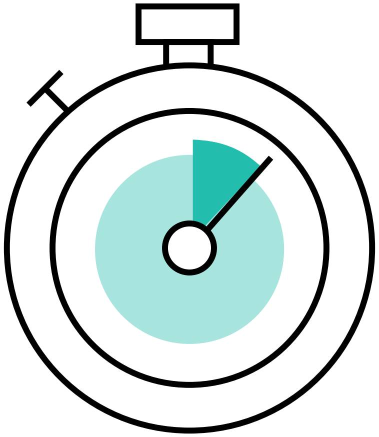
79%

TAKE MORE THAN FIVE MINUTES TO PRIORITIZE A SINGLE ALERT

7. Remediation Time is Longer Than Expected

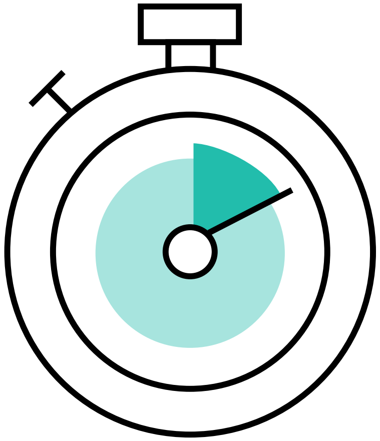
The process for remediating a misconfigured resource can be time consuming. The alert needs to be identified, reviewed, and prioritized as critical. This delay results in loss of critical time before the misconfiguration is fully remediated.

78%



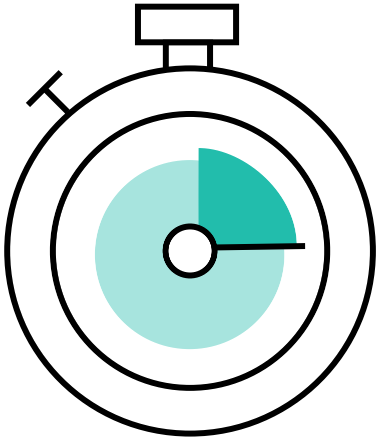
TAKE MORE THAN FIVE MINUTES TO EVALUATE A SINGLE MISCONFIGURATION

68%



WAIT 10 MINUTES TO MORE THAN ONE DAY BEFORE REMEDIATING

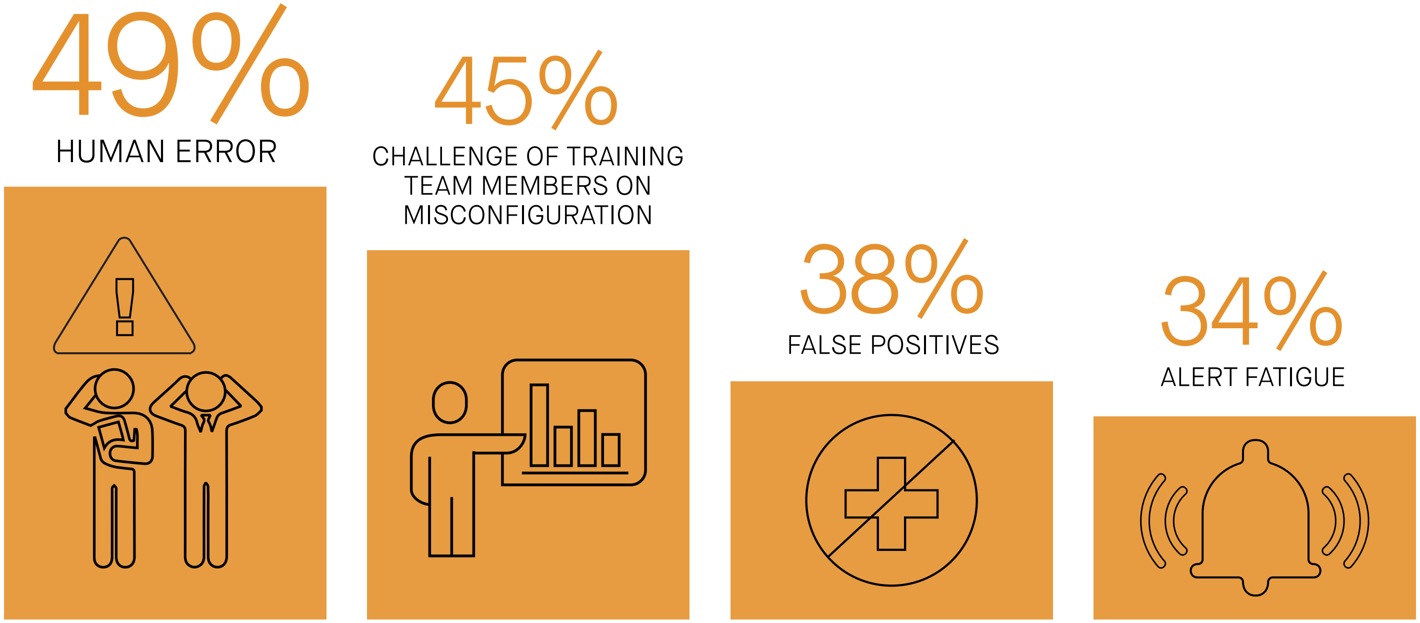
63%



TAKE 15 MINUTES OR LONGER TO REMEDIATE ONE MISCONFIGURATION

8. Human Error Tops Misconfiguration Frustrations

With so many resources to monitor, organizations can quickly be overwhelmed and make mistakes. Based on the survey, 49% of organizations cited human error as the main contributor for missing or miscategorizing critical misconfiguration events.



9. Mean Time to Remediation (MTTR) Actual vs. Ideal

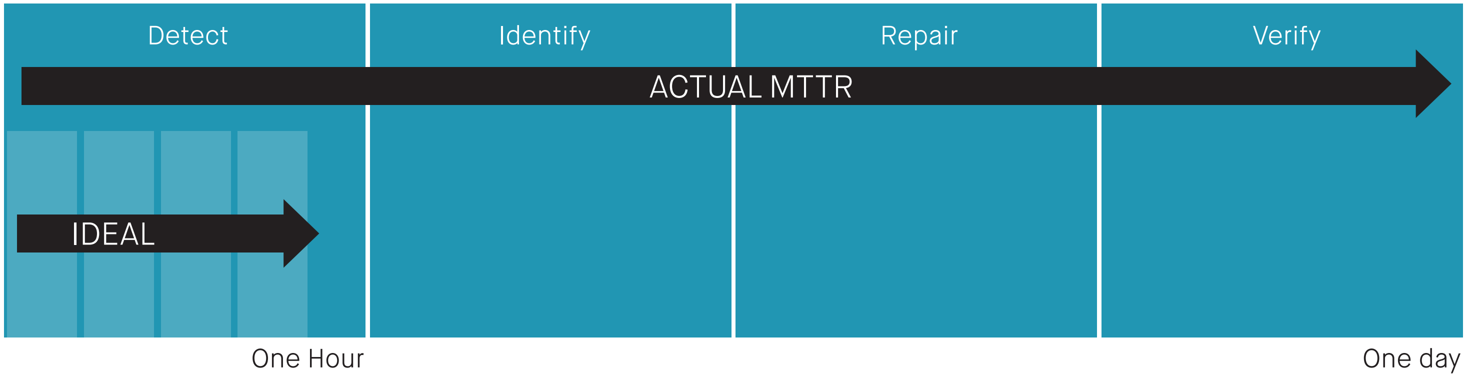
MTTR is the time that elapses between a misconfiguration first occurring until it's finally fixed. There is a big difference between what the actual MTTR is and what organizations feel the ideal MTTR should be.

58%

IDEAL MTTR WOULD BE LESS THAN ONE HOUR

86%

ACTUAL MTTR IS OFTEN ONE DAY



10. Automated Remediation Considered Very Valuable

Migrating to the cloud brings scalability, but manual identification and remediation of misconfiguration is impossible to scale. Yet most organizations still rely on manual processes to identify and remediate misconfiguration. When asked about the promise of automated remediation, respondents believe it can provide significant value for the following:

80%
KEEPING DATA SAFE

79%
ENSURING COMPLIANCE

75%
IMPROVING EFFICIENCY

Conclusion

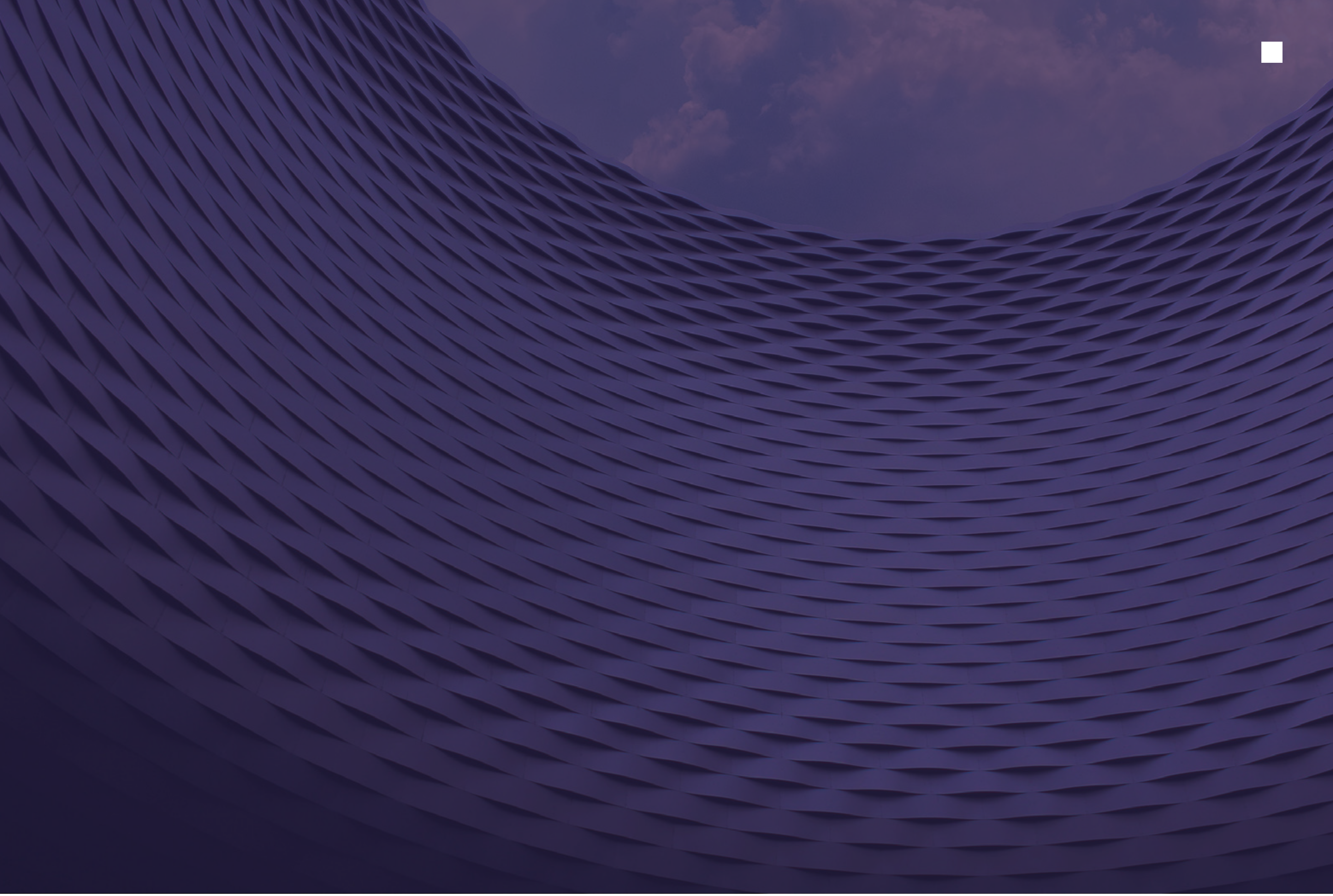
Organizations are rapidly embracing the cloud for its many benefits, including scalability and increased efficiency. While the cloud enables organizations to bring up thousands of resources within minutes, it also makes monitoring and manually correcting misconfigurations nearly impossible.

Cloud infrastructure misconfiguration has emerged as the number one cause of data breaches in the cloud. A majority (81%) of organizations indicated that they believe the frequency of misconfiguration will increase or remain constant in the next year, and a security solution that includes automated remediation is the only way forward.

TO LEARN MORE ABOUT HOW FUGUE CAN HELP ENTERPRISES IDENTIFY AND ELIMINATE CLOUD RISKS, VISIT WWW.FUGUE.CO.

Fugue

Fugue is a security and compliance solution that identifies and eliminates cloud risks. Our patented software automatically remediates misconfigurations and policy violations in near real time and ensures they are never repeated. With Fugue, cloud resources are always provisioned according to a single source of truth – and stay that way throughout the resources' lifetime.



www.fugue.co | hello@fugue.co | @FugueHQ