REPORT

The State of Cloud Security 2020

A report on the risks and challenges IT and cloud engineering teams are facing in 2020.

Fugue

Table of Contents

"Misconfiguration of cloud resources remains the most prevalent cloud vulnerability and can be exploited to access cloud data and services."

— The National Security Agency, *Mitigating Cloud Vulnerabilities*

Cloud Security Risks During the COVID-19 Crisis

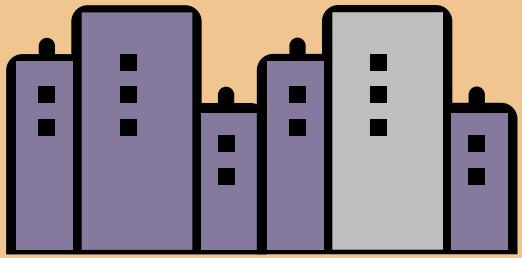
New devices and access patterns can create additional cloud vulnerabilities

As a vast majority of companies make the rapid shift to 100% work-from-home in order to stem the spread of COVID-19, a significant percentage of IT and cloud professionals are concerned about maintaining the security of their cloud environments during the transition.

96% of cloud engineering teams are now fully distributed and working from home in response to the crisis, with more than eight out of ten having made the rapid transition from either fully colocated or partially colocated.

Of those that are making the shift, a vast majority are concerned about new security vulnerabilities created during the swift adoption of new access policies, networks, and devices used for managing cloud infrastructure remotely.

IS YOUR TEAM TRANSITIONING TO 100% DISTRIBUTED?

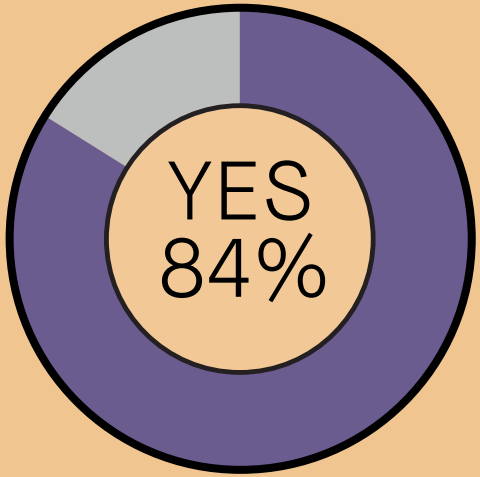


83%

OF COMPANIES

are making the transition to 100% distributed teams

ARE YOU CONCERNED ABOUT CLOUD SECURITY DURING THE TRANSITION?



"What our survey reveals is that cloud misconfiguration not only remains the number one cause of data breaches in the cloud, the rapid global shift to 100% distributed teams is creating new risks for organizations and opportunities for malicious actors."

— Phillip Merrick, CEO of Fugue

The Often Invisible Threat

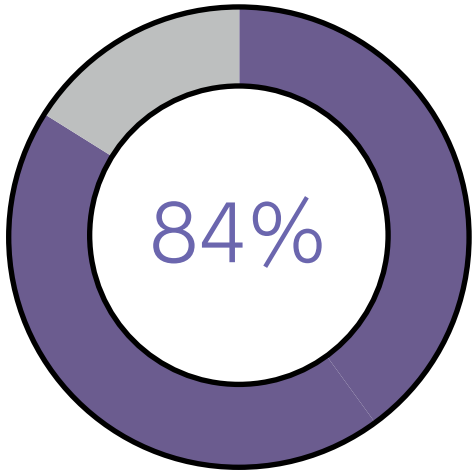
Cloud misconfiguration eludes traditional security and visibility tools

Cloud misconfiguration exploits can be extremely difficult to detect using traditional security analysis tools, even after the fact.

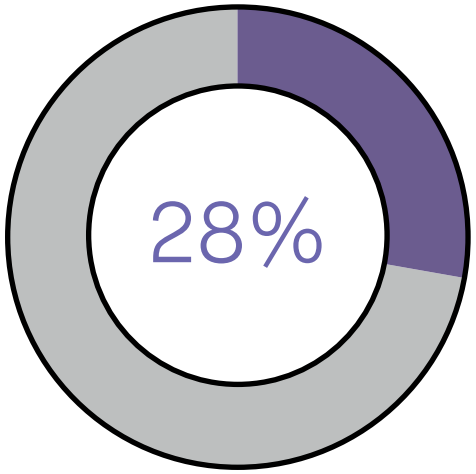
84% of IT professionals are concerned that their organization has already suffered a major cloud breach that they have yet to discover.

More than a quarter of professionals state that they've already suffered a critical cloud data breach that they are aware of.

ARE CONCERNED THEY'VE BEEN HACKED AND DON'T KNOW IT



HAVE ALREADY BEEN HACKED AND KNOW IT



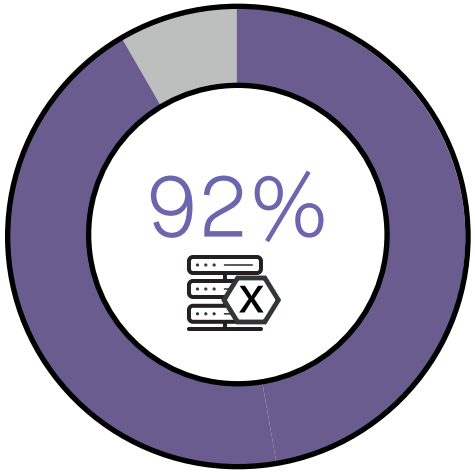
The Number One Cloud Risk

A vast majority of IT professionals are worried about cloud misconfiguration

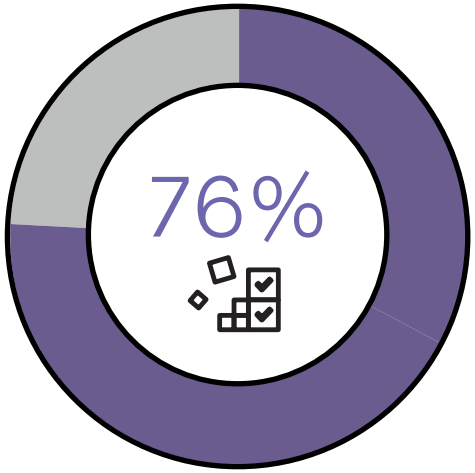
Cloud misconfiguration remains the number one cause of data breach for every organization using the cloud. More than 9 out of 10 professionals are worried that their organization is vulnerable to a major cloud misconfiguration-related data breach.

A third of respondents believe cloud misconfigurations will increase over the next year, and slightly more believe the rate of misconfiguration will stay the same. Only a quarter of respondents believe cloud misconfigurations will decrease at their organization.

WORRIED THEY'RE VULNERABLE TO A CLOUD BREACH



MISCONFIGURATION RISK WILL STAY THE SAME OR INCREASE



"Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes."

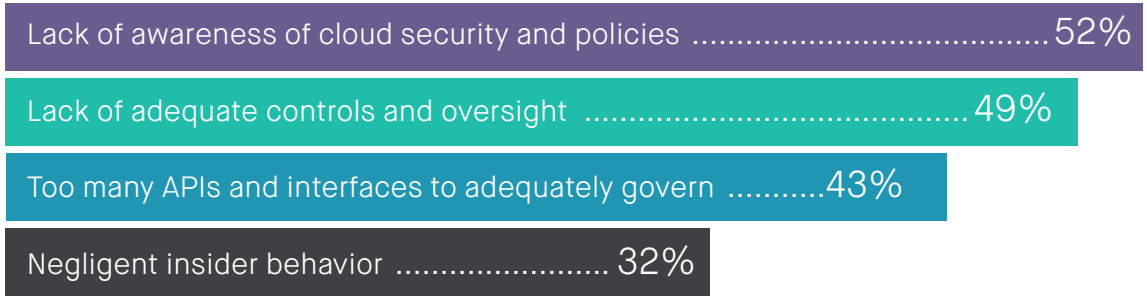
— Neil MacDonald, Gartner

The Most Dangerous Insider Threat

Cloud misconfiguration is entirely preventable, but rarely so

Cloud misconfiguration is a problem born of many causes—all of which are the result of user mistakes. The top causes of cloud misconfiguration cited are a lack of awareness, controls and oversight.

CAUSES OF CLOUD MISCONFIGURATION?



The Runaway Pace of Cloud Misconfiguration

Every team operating on cloud has a serious misconfiguration problem

CLOUD MISCONFIGURATION INCIDENTS PER DAY

1-10	24%
10-50	18%
50-100	19%
100-250	13%
250-500	13%
500-1,000	7%
More than 1,000	3%
Don't know	3%

"I'm seeing a lot of cloud configuration errors in the real world—and it's scaring the hell out of me."

— David Linthicum, InfoWorld

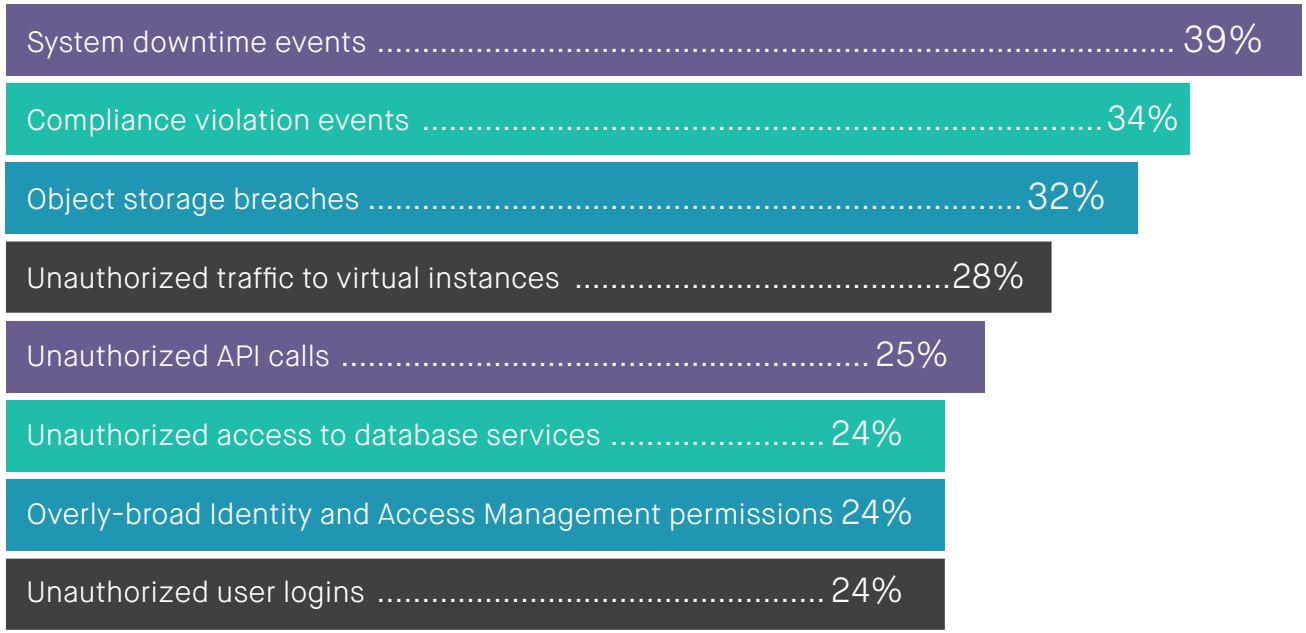
Critical Cloud Misconfiguration Incidents

Respondents cited a number of critical misconfiguration events they've suffered, including object storage breaches and unauthorized traffic to virtual server instances and database services.

Identity and Access Management resources remain one of the more complex cloud services to manage and configure securely, with overly-broad permissions giving malicious actors the ability to move laterally and access data.

Cloud misconfiguration was also cited as the cause of system downtime and compliance violation events, both of which can have severe financial impacts.

CRITICAL MISCONFIGURATION EVENTS



The Many Facets of Cloud Misconfiguration

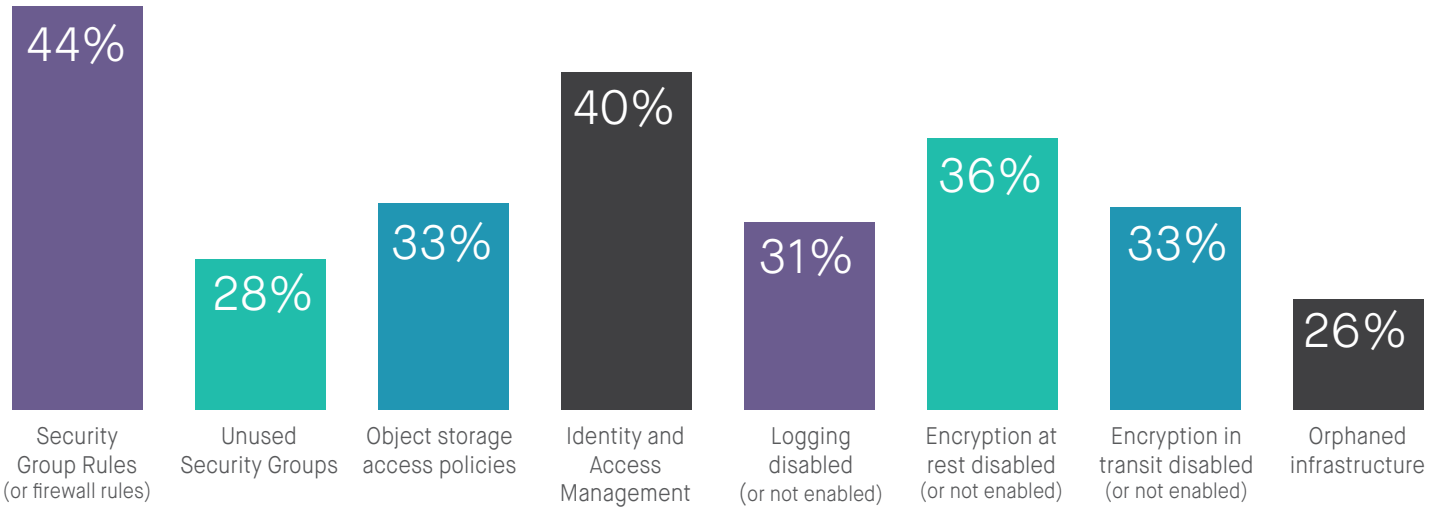
Cloud misconfiguration is not a singular problem

The explosion of new kinds of cloud services and the corresponding complexity of configuring them securely means teams are experiencing a wide variety of dangerous kinds of misconfiguration.

Services used to access cloud resources together represent the majority of critical misconfigurations teams are experiencing, with Security Groups, object storage access policies, and Identity and Access Management services most cited. Disabled (or not enabled) encryption is also quite common.

Orphaned infrastructure, which are unused cloud resources that are invisible to cloud engineering and security teams, typically go unpatched and unscanned for misconfiguration and can give malicious actors access to cloud environments and data.

CLOUD MISCONFIGURATIONS BY TYPE



"Cloud technology moves rapidly, making oversight a complex task."

— The National Security Agency, Mitigating Cloud Vulnerabilities

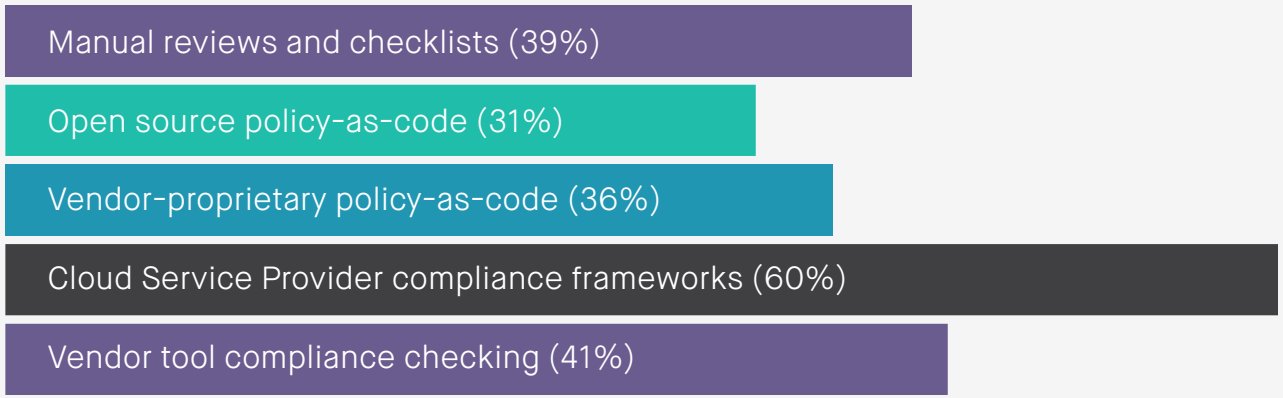
How Teams are Working to Prevent Cloud Misconfiguration

Respondents cite a variety of methods and tools for prevention

Cloud security is a software engineering problem, not a traditional security analysis one. Yet only 31% of teams are using open source policy-as-code to give engineers programmatic control over cloud security policies and employ version control and proper code reviews.

39% still rely on manual reviews before deployment.

TOOLS AND METHODS USED TO PREVENT MISCONFIGURATION



Challenges Teams Face in Eliminating Cloud Misconfiguration

An over-reliance on manual processes is creating new problems

While malicious actors use automation tools to scan the internet to find cloud misconfigurations within minutes of their inception, most cloud teams still rely on slow, manual processes to address the problem, creating new ones along the way.

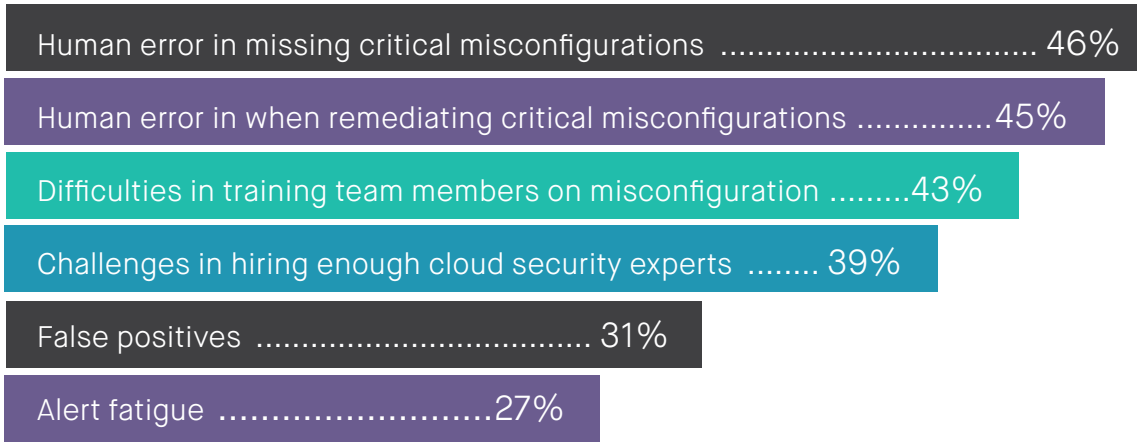
HOW TEAMS ARE MANAGING CLOUD MISCONFIGURATION

73%
Manual remediation

39%
Some automated remediation

40%
Manual audits of environments

CHALLENGES IN MANUALLY MANAGING CLOUD MISCONFIGURATION

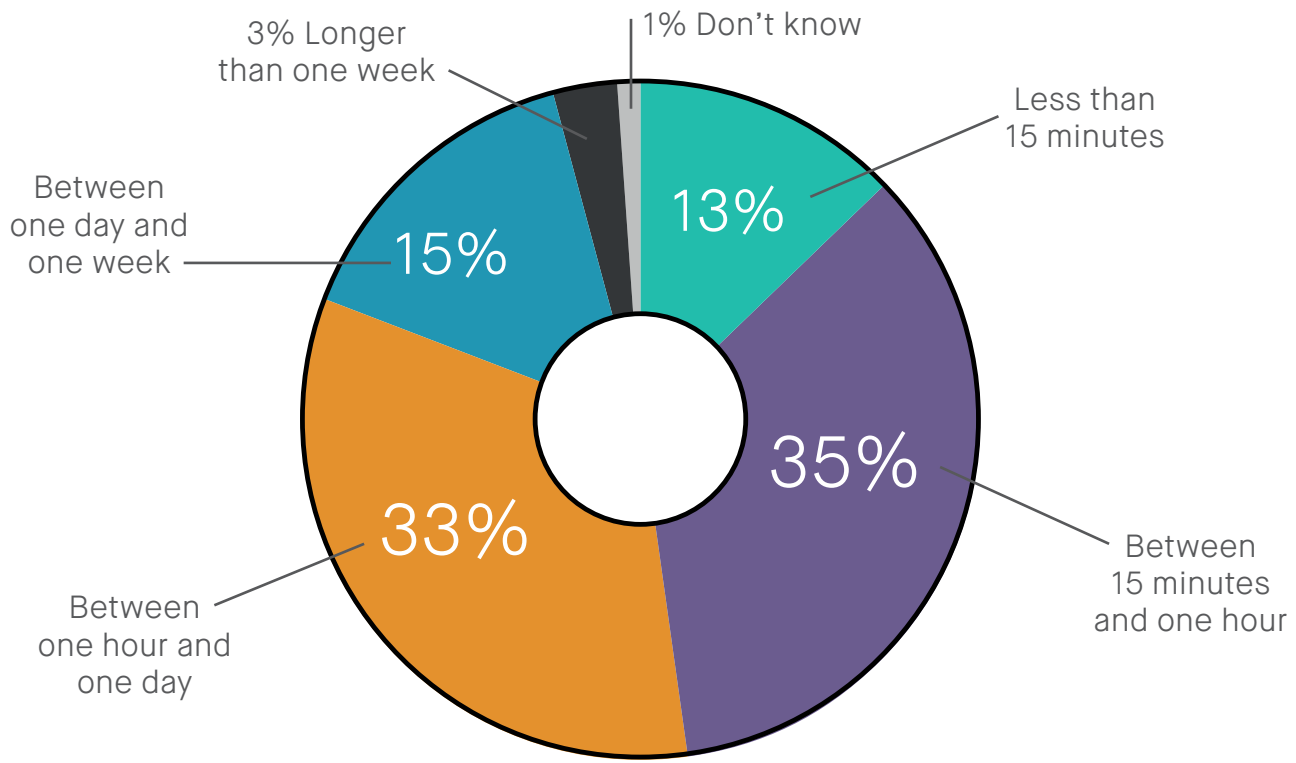


Measuring Cloud Misconfiguration Management

Mean Time to Remediation is lagging behind attackers

The effectiveness of an organization's response to cloud misconfiguration incidents is measured by the Mean Time to Remediation (MTTR). While 55% say their MTTR should be under one hour (and another 29% say it should be under one day), most are falling well short of that goal.

MEAN TIME TO REMEDIATION FOR CLOUD MISCONFIGURATION



"Skilled or well-funded hacker groups are employing automation to discover and exploit misconfigured cloud assets within hours of their deployment."

— John Breeden II, CSO Online

The Steep Cost of Managing Cloud Misconfiguration

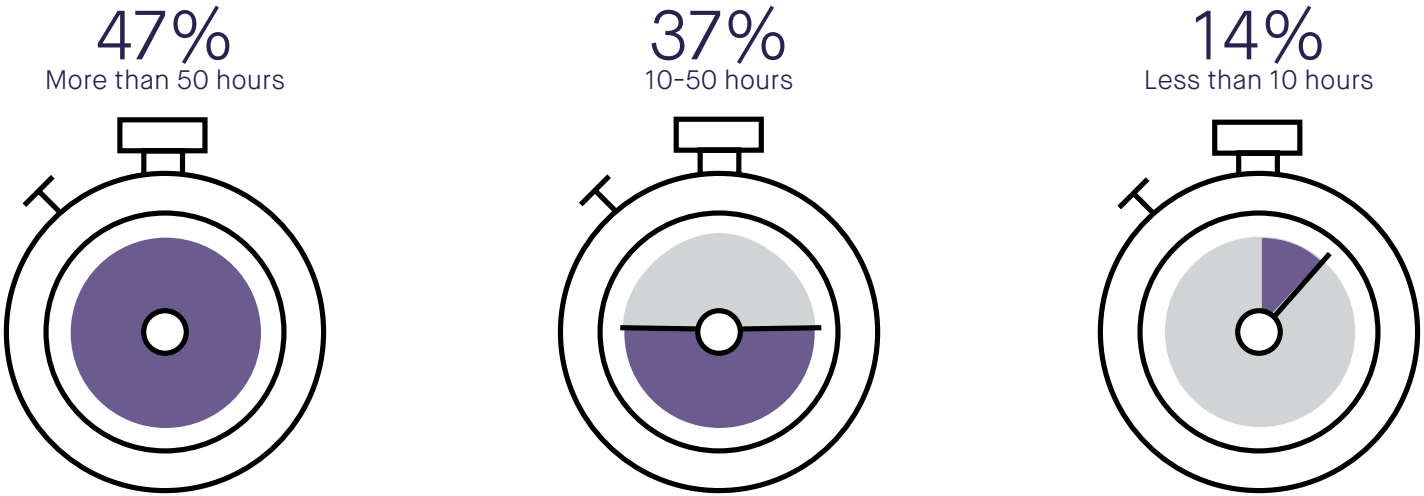
Relying on manual processes incurs a heavy burden on cloud teams

With cloud misconfiguration rates at such high levels and a widespread reliance on manual processes to manage it, the costs are predictably high for cloud customers.

Teams need to manually review alerts and tickets, identify critical misconfigurations that need remediation, perform manual remediation of incidents, and fill out reports about each incident.

Manual audits and compliance reports only adds to this burden, with 18% spending more than 100 hours on audits, remediation, and reporting. Only 1% of respondents don't have to comply with industry compliance standards or internal security policies.

HOURS PER WEEK INVESTED IN MANAGING CLOUD MISCONFIGURATION



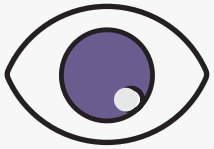
What Professionals Say They Need To Address The Problem

Automation, visibility, and reporting

More than 95% of respondents said that security automation (e.g. automated remediation) would help them be more efficient and cloud-based data security more effective. 44% cited challenges in gaining visibility into their cloud security posture and missing critical misconfigurations.

WHAT'S NEEDED TO BETTER ADDRESS CLOUD MISCONFIGURATION

95%
Automated detection and remediation



30%
Better visibility into cloud infrastructure

28%
Timely notifications on dangerous misconfiguration and drift

8%
Improved reporting to help prioritize remediation efforts

Recommendations

Knowing your cloud is secure at all times is a feeling few engineers or executives ever get to experience. Rather, cloud (in)security is an area full of frustrated engineers and sleepless executives—and unnecessary risk and wasteful spending for organizations.

Here are some steps organizations can take when traditional security tools are failing and throwing more people at the problem is no longer an option.

1: GET VISIBILITY INTO YOUR CLOUD

The cloud is 100% software-defined, and therefore everything running in your cloud is knowable at all times using your cloud provider's APIs. Even if your developers are constantly building and modifying cloud infrastructure, you can continuously monitor state to identify compliance issues and misconfiguration in near real time, and act swiftly to remediate issues.

2: EMPOWER YOUR ENGINEERS

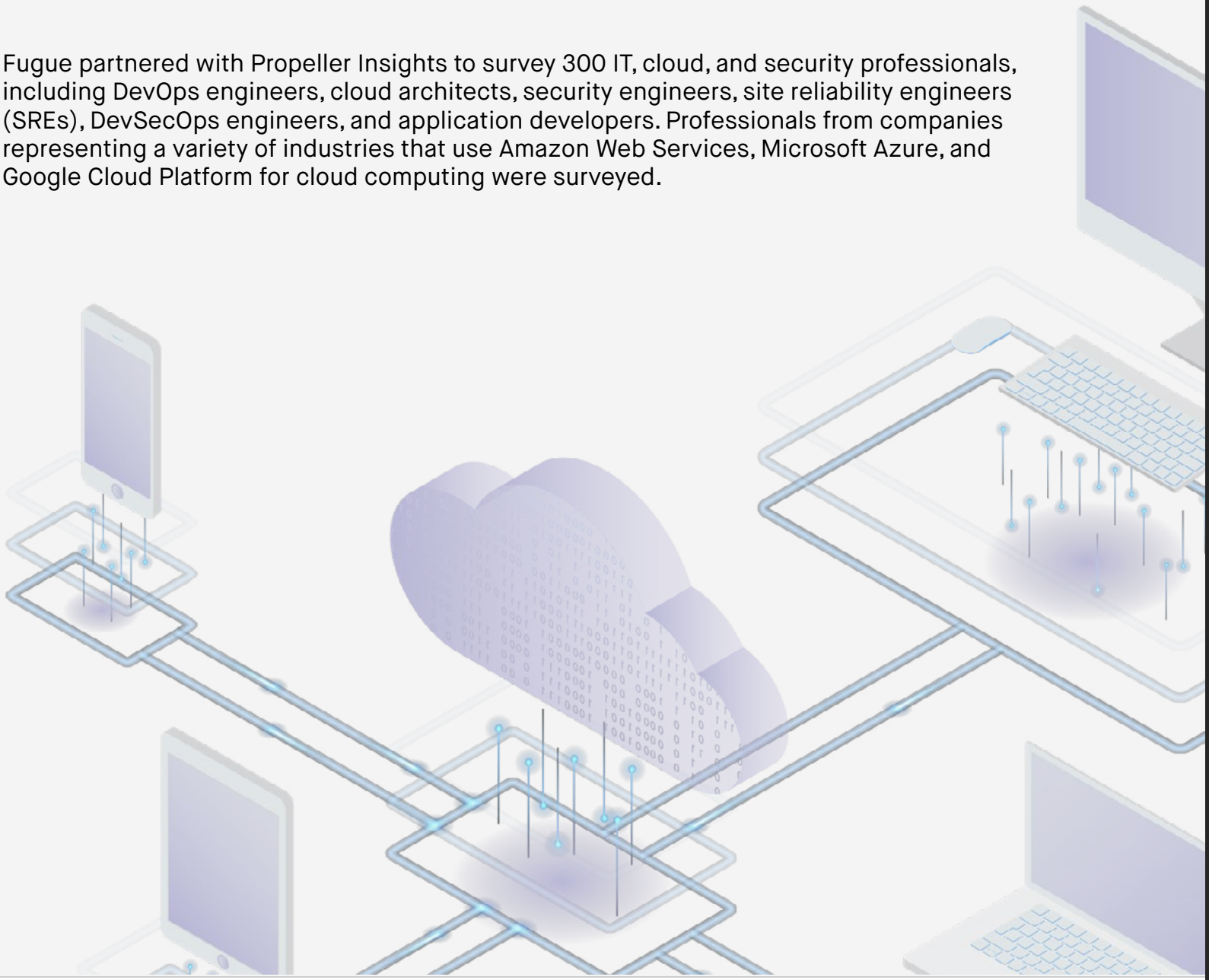
Because the cloud is 100% software-defined, it's also fully programmable, making cloud security the ideal domain for engineers. "Shift Left" and move cloud security earlier in the software development life cycle, when making corrective changes is faster and less costly. Adopt open source policy-as-code to help developers find and fix cloud security issues with the tools they use.

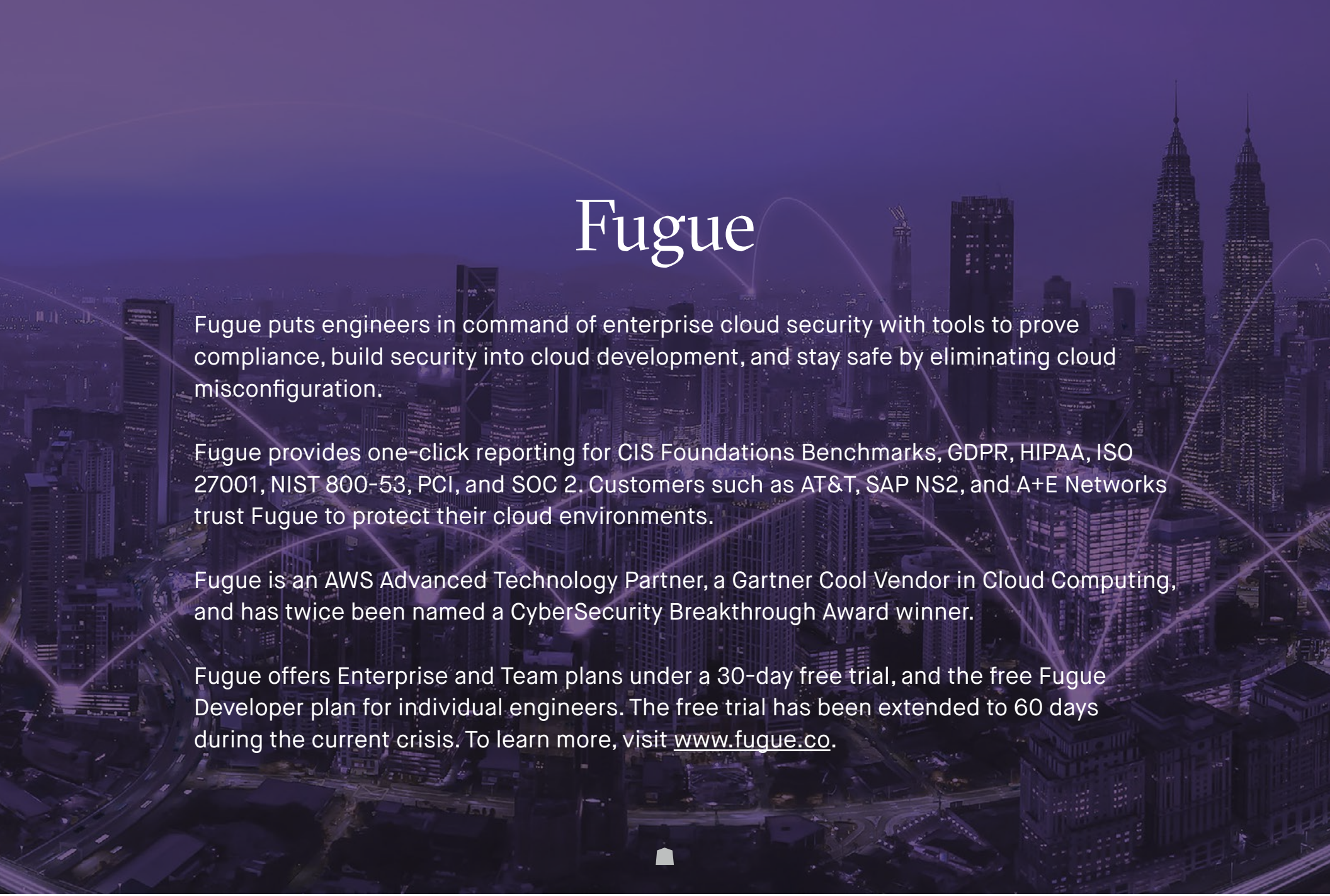
3: EMBRACE SECURITY AUTOMATION

Cloud security is a task too vast and complex for humans, but an ideal one for computers. Every manual process in your cloud security and compliance effort should be a candidate for automation, including deployment certifications, infrastructure audits, compliance reports, and remediations for security-critical resources. You'll move faster, stay safer, and save money.

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.





Fugue

Fugue puts engineers in command of enterprise cloud security with tools to prove compliance, build security into cloud development, and stay safe by eliminating cloud misconfiguration.

Fugue provides one-click reporting for CIS Foundations Benchmarks, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. Customers such as AT&T, SAP NS2, and A+E Networks trust Fugue to protect their cloud environments.

Fugue is an AWS Advanced Technology Partner, a Gartner Cool Vendor in Cloud Computing, and has twice been named a CyberSecurity Breakthrough Award winner.

Fugue offers Enterprise and Team plans under a 30-day free trial, and the free Fugue Developer plan for individual engineers. The free trial has been extended to 60 days during the current crisis. To learn more, visit www.fugue.co.