RESEARCH

Implementing Cloud Security Best Practices

August 2020

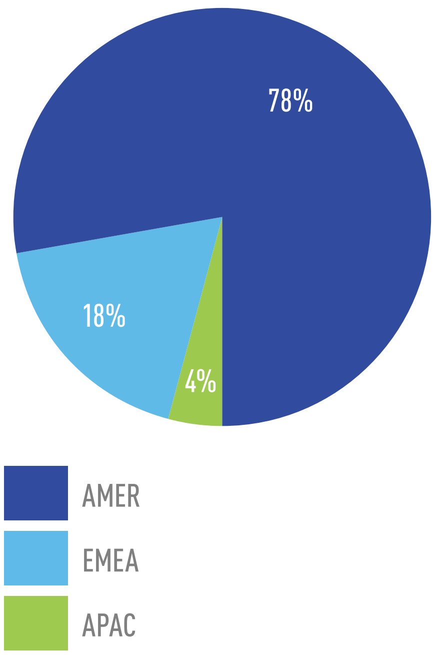
FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

As organizations expand further into the cloud, there continues to be an influx of simple mistakes, such as misconfigurations, that can expose organizations to significant security, privacy and regulatory risks. Tripwire partnered with Dimensional Research to understand what progress organizations are making towards securing their cloud environments and what areas of improvement exist for implementing industry best practices.

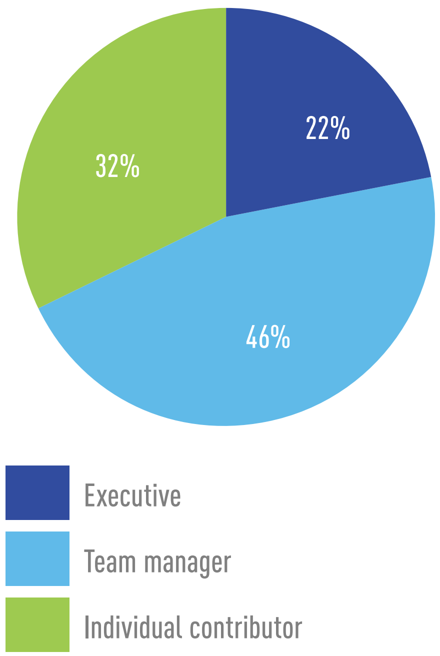
This report covers findings from a survey conducted by Dimensional Research in July 2020. A total of 310 qualified individuals completed the survey. All had responsibility for IT security of public cloud environments at a company with more than 100 employees.

INDIVIDUALS REPRESENTED

Region

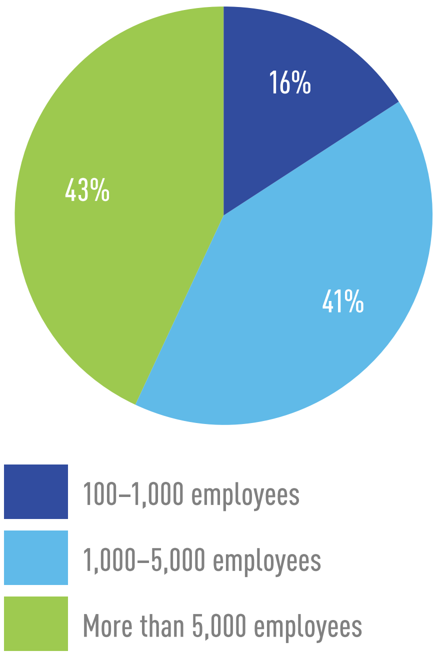


Job Level

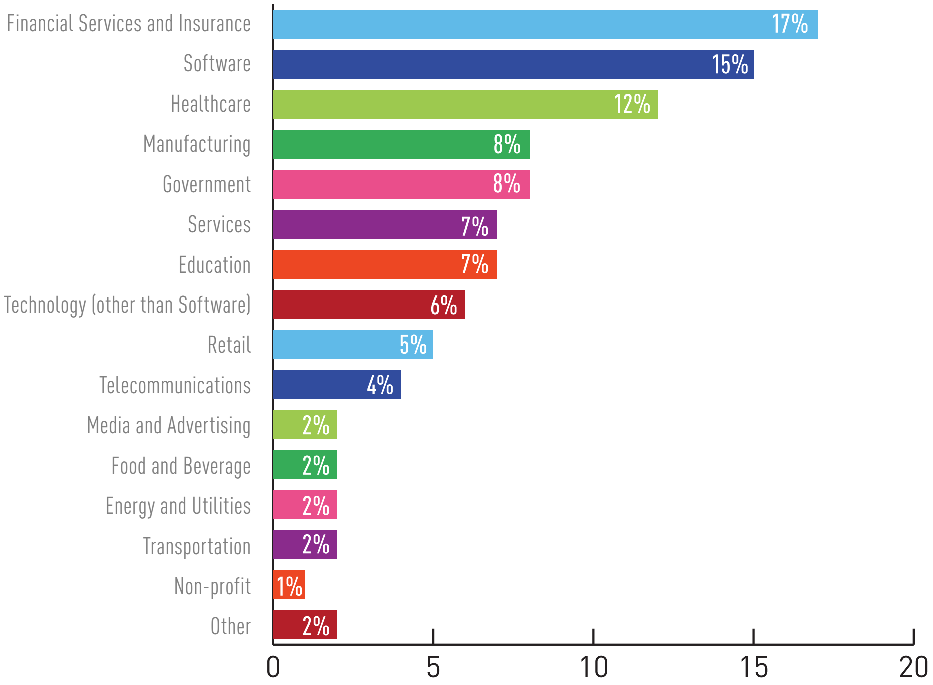


COMPANIES REPRESENTED

Company Size

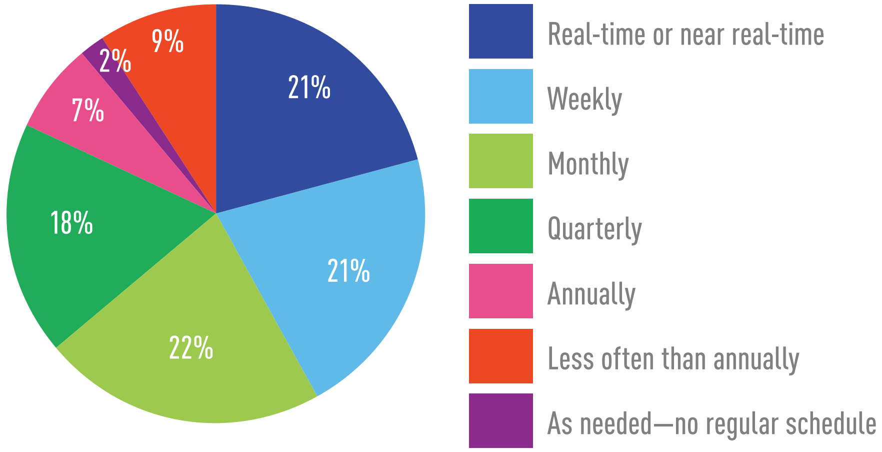


Industry

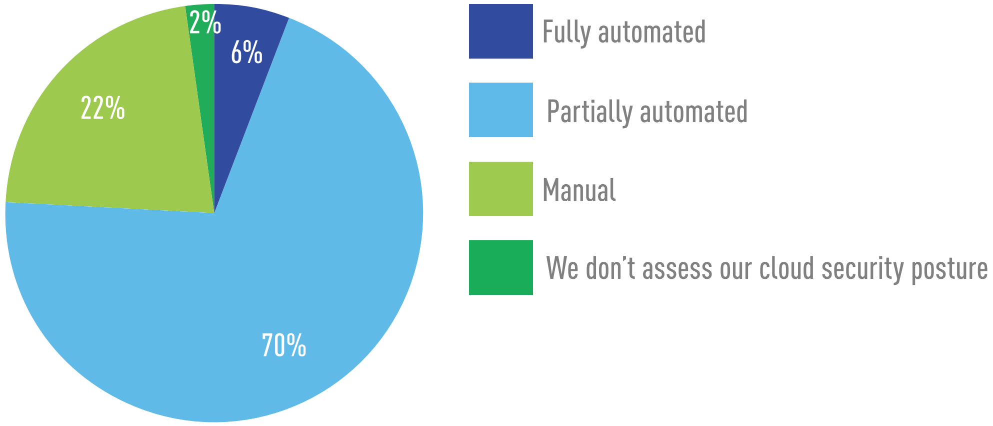


ONLY 21% ASSESS THEIR OVERALL CLOUD POSTURE IN REAL/ NEAR-REAL TIME, AND 22% STILL ASSESS THIS MANUALLY

How often does your company assess your overall cloud security posture?



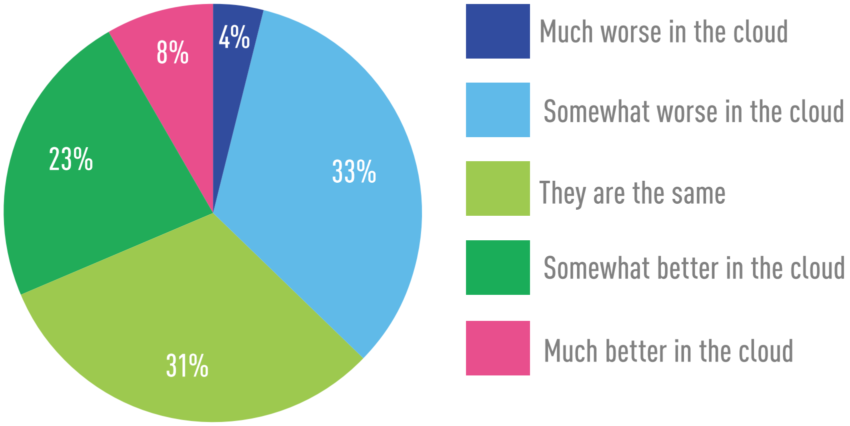
How does your company assess your overall cloud security posture?



Attackers are known to run automated searches to find sensitive data exposed in the cloud, making it critical for organizations to monitor their cloud security posture on a recurring basis and fix issues immediately.

37% ARE NOT AS CONFIDENT ABOUT RISK MANAGEMENT IN THE CLOUD AS THEY ARE IN OTHER AREAS

In your opinion, how does your organization's risk management capabilities in the cloud compare to other parts of the environment?

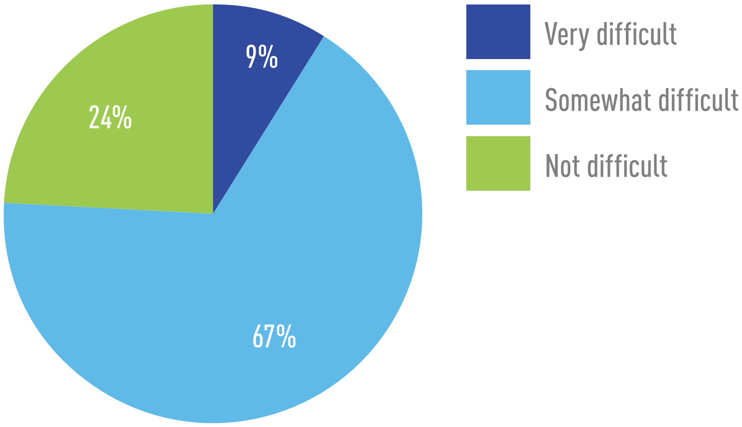


"Security teams are dealing with much more complex environments, and it can be extremely difficult to stay on top of the growing cloud footprint without having the right strategy and resources in place," said Tim Erlin, vice president of product management and strategy at Tripwire.

"Fortunately, there are well-established frameworks, such as CIS benchmarks, which provide prioritized recommendations for securing the cloud. However, the ongoing work of maintaining proper security controls often goes undone or puts too much strain on resources, leading to human error."

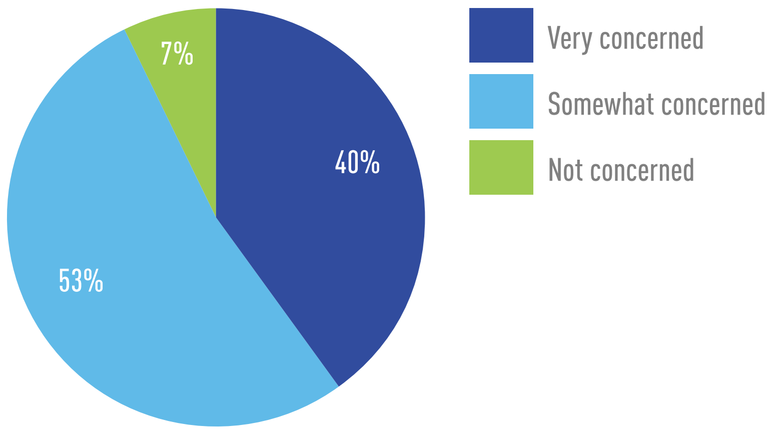
76% FACE CHALLENGES MAINTAINING SECURITY CONFIGURATIONS IN CLOUD ENVIRONMENTS

How difficult is it for your organization to maintain security configurations in cloud environments?



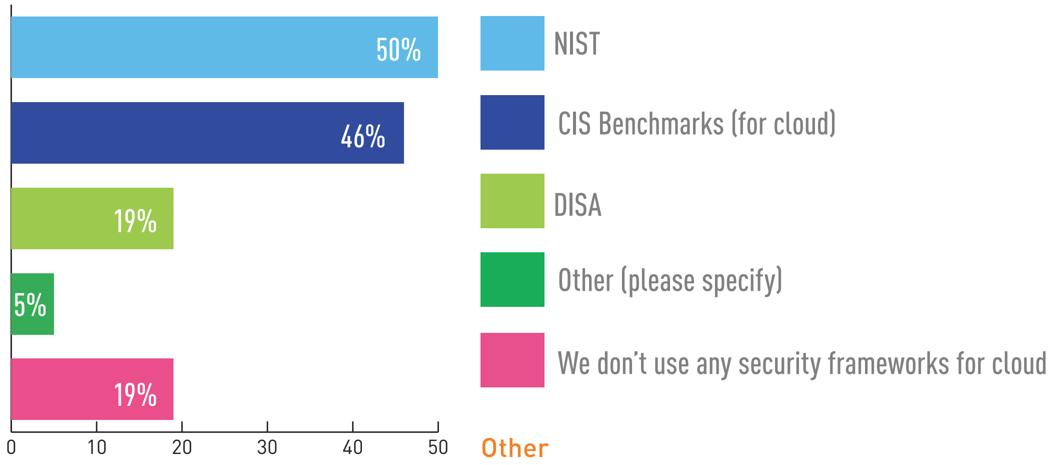
93% ARE CONCERNED ABOUT HUMAN ERROR CAUSING CLOUD DATA EXPOSURE

How concerned are you about human error causing accidental public exposure of data in your organization's cloud environments?



MOST FOLLOW A BEST PRACTICES FRAMEWORK, WITH NIST AND CIS AS THE TOP TWO

Which best practice security frameworks does your organization use for securing public cloud environments? Choose all that apply.

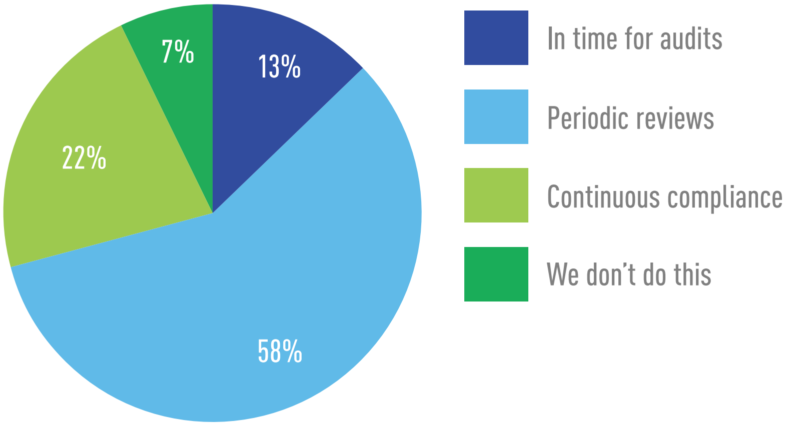


Other

Australian PSPF, Internal best practices, BSI, CCAF, CSA, Custom, HIPAA, ISO, ISO 27001; CSA STAR, MITRE, NCSC, NORMA/GEMMA/PETRA, SOC2 compliance

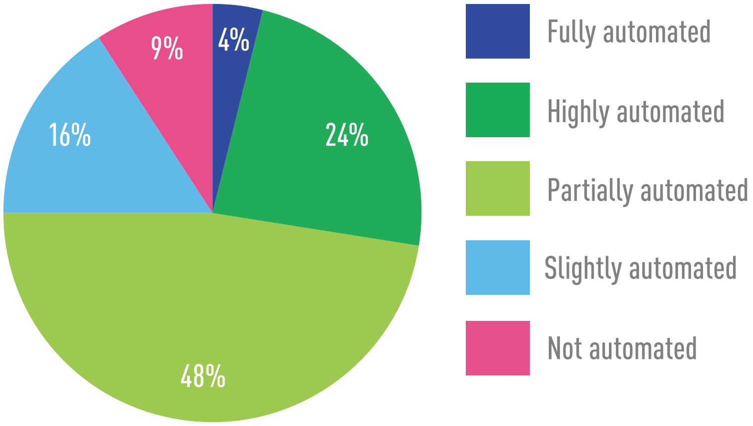
FEWER THAN ONE IN FOUR HAVE CONTINUOUS COMPLIANCE OF CLOUD SECURITY

How does your organization maintain cloud security compliance and regulations over time? Choose the one answer that most closely applies.



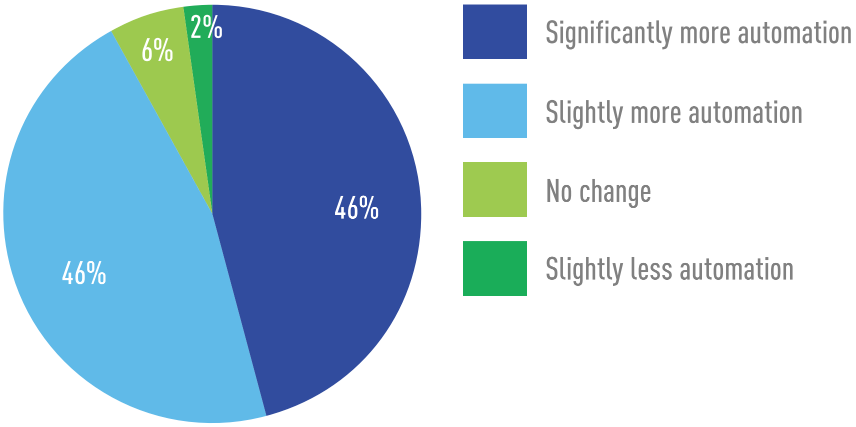
91% OF ORGANIZATIONS HAVE IMPLEMENTED SOME LEVEL OF AUTOMATED ENFORCEMENT IN THE CLOUD

How would you characterize the level of automated enforcement of your organization's security efforts for the cloud? Choose the one answer that most closely applies.



92% WOULD PREFER MORE AUTOMATION OF SECURITY ENFORCEMENT

In your ideal world, how would your organization change the level of enforcement automation?



Security teams are stretched thin. Hunting down every configuration issue across numerous cloud accounts is tedious work and prone to human error.

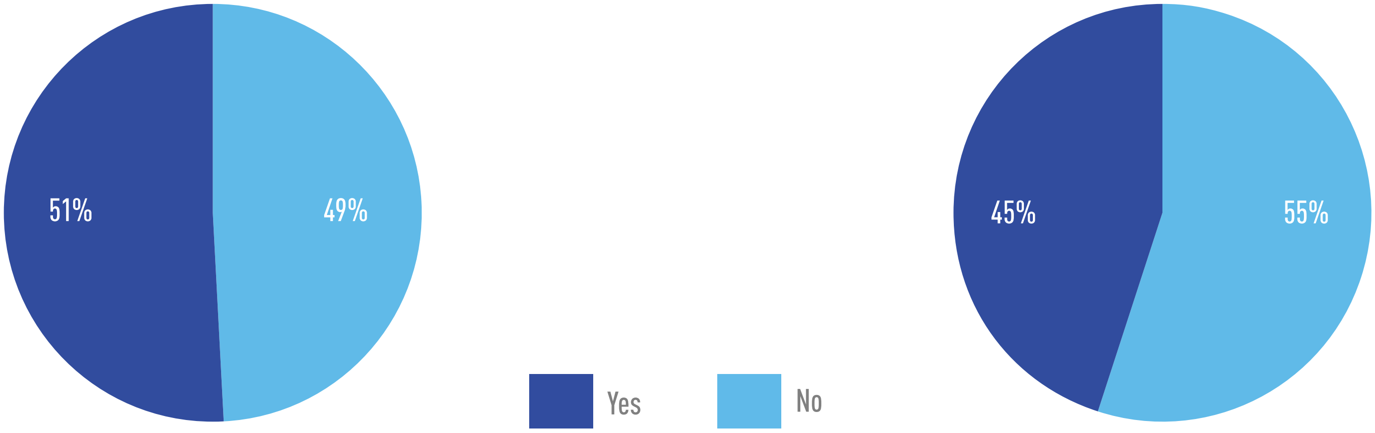
WHERE AUTOMATION IS HELPING TO MAINTAIN SPECIFIC SECURITY CONTROLS

Encryption settings

Does your organization have automated solutions for ensuring proper encryption settings are enabled for databases or storage buckets?

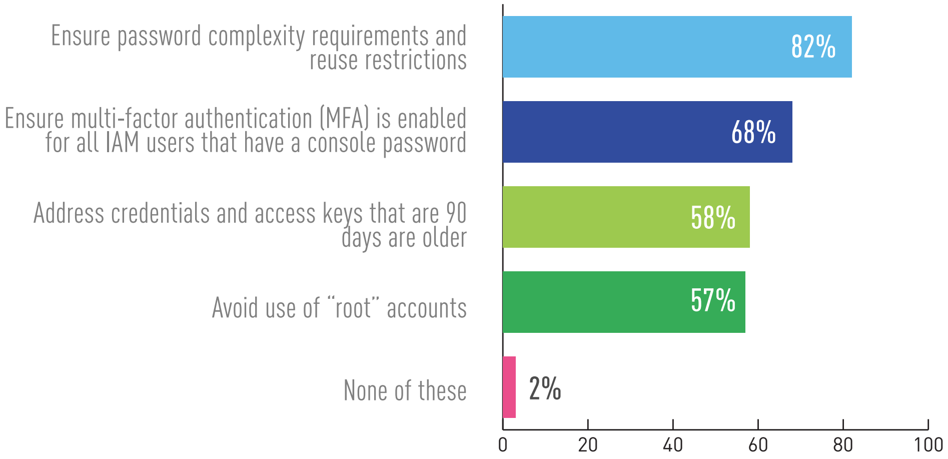
New cloud assets

Does your organization have an automated process for assessing new cloud assets as they are added to your environment?



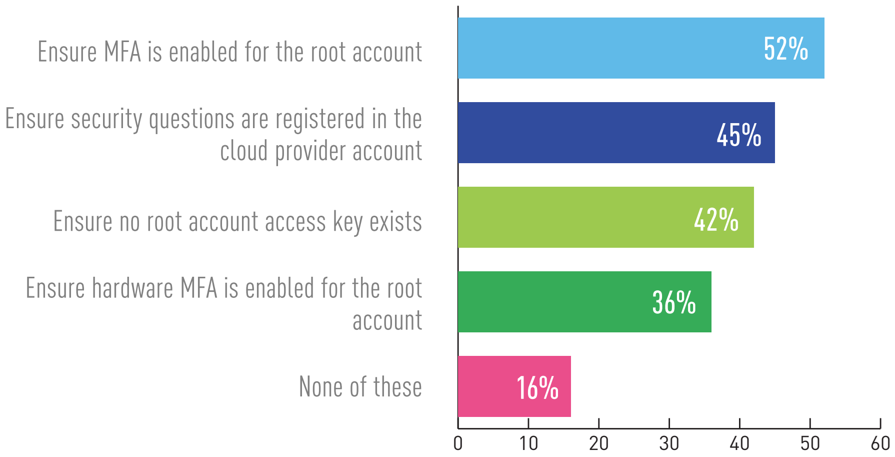
IDENTITY AND ACCESS MANAGEMENT

Does your organization have automated solutions for assessing the following Identity and Access Management controls? Choose all that apply.



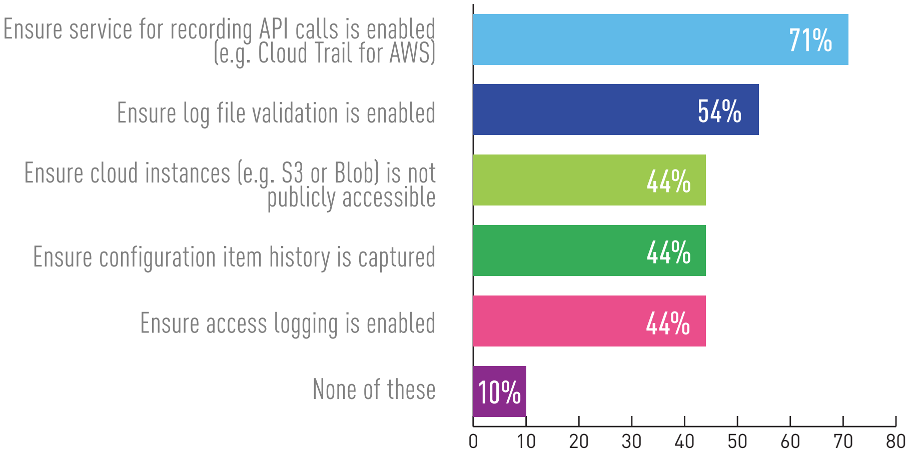
ROOT ACCOUNT ACCESS

What type of automated monitoring does your company have for root account access? Choose all that apply.



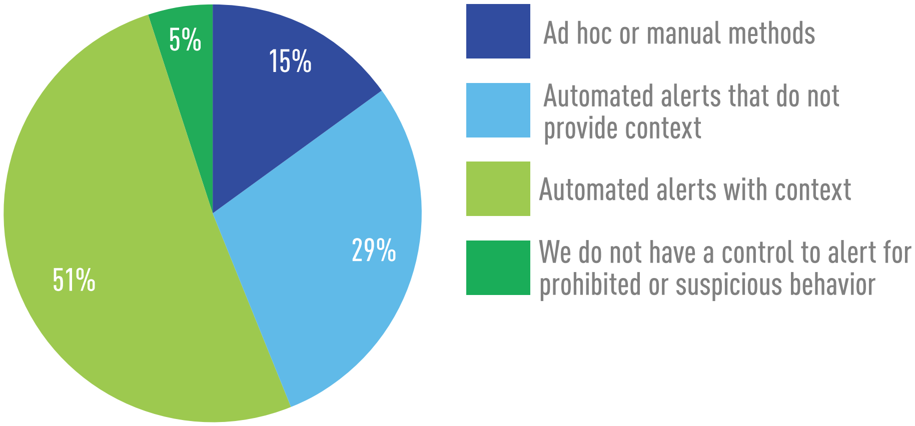
LOGGING

Does your organization have any of the following automatic assessments for logging controls? Choose all that apply.

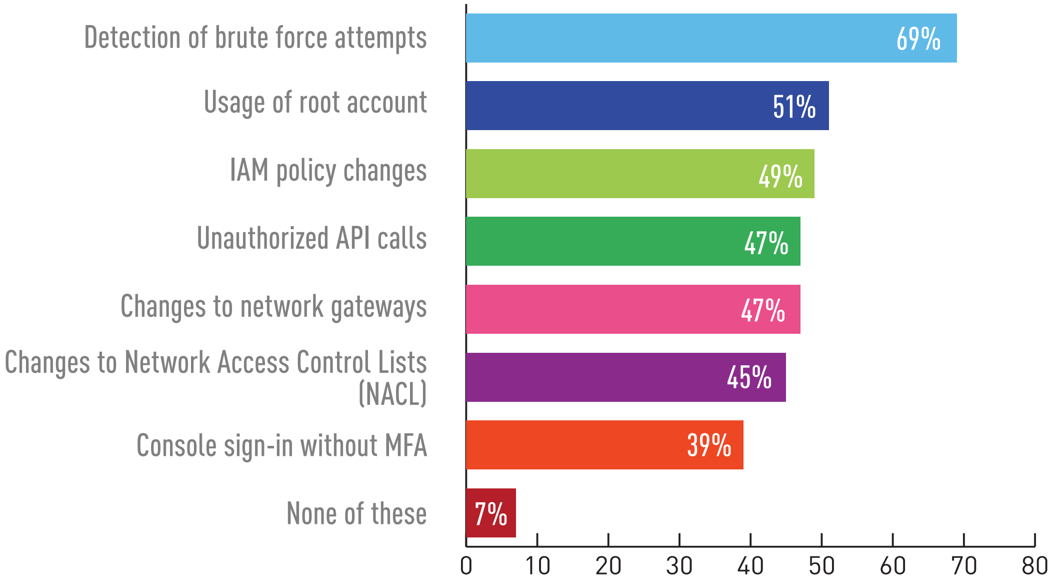


MONITORING

How is your organization alerted to automated alerts of prohibited or suspicious behavior? Choose the one answer that most closely applies.



Which of the following types of behaviors does your organization receive alarms for? Choose all that apply.



For information on cloud security solutions offered by Tripwire, please visit:
tripwire.com/solutions/cloud-cybersecurity

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook