INFOGRAPHIC

Five Best Practices for Preventing Cloud Misconfiguration

1

CHECK PERMISSION CONTROLS

Apply the principle of least privilege by only giving users and service accounts the minimum set of permissions to perform their needed tasks.

2

CONTINUOUSLY AUDIT FOR MISCONFIGURATION AND COMPLIANCE

Organizations should implement regular audits to check for signs of misconfiguration and to maintain security and compliance policy.

3

IMPLEMENT SECURITY MEASURES SUCH AS LOGGING AND ENCRYPTION

Turning on logging will allow you to track changes made to your resources and help identify the cause of misconfiguration.

4

CHECK FOR POLICY COMPLIANCE BEFORE PROVISIONING

Utilizing a security solution that offers a policy-as-code feature can help to ensure that configurations are compliant before deployment.

5

CHOOSE THE RIGHT SECURITY SOLUION

Organizations looking to bolster their cloud security should look at security solutions that include automated remediation.

To learn more, download the "Comprehensive Guide to Preventing Cloud Misconfiguration" ebook or visit www.fugue.co

Fugue

Learn more at www.fugue.co