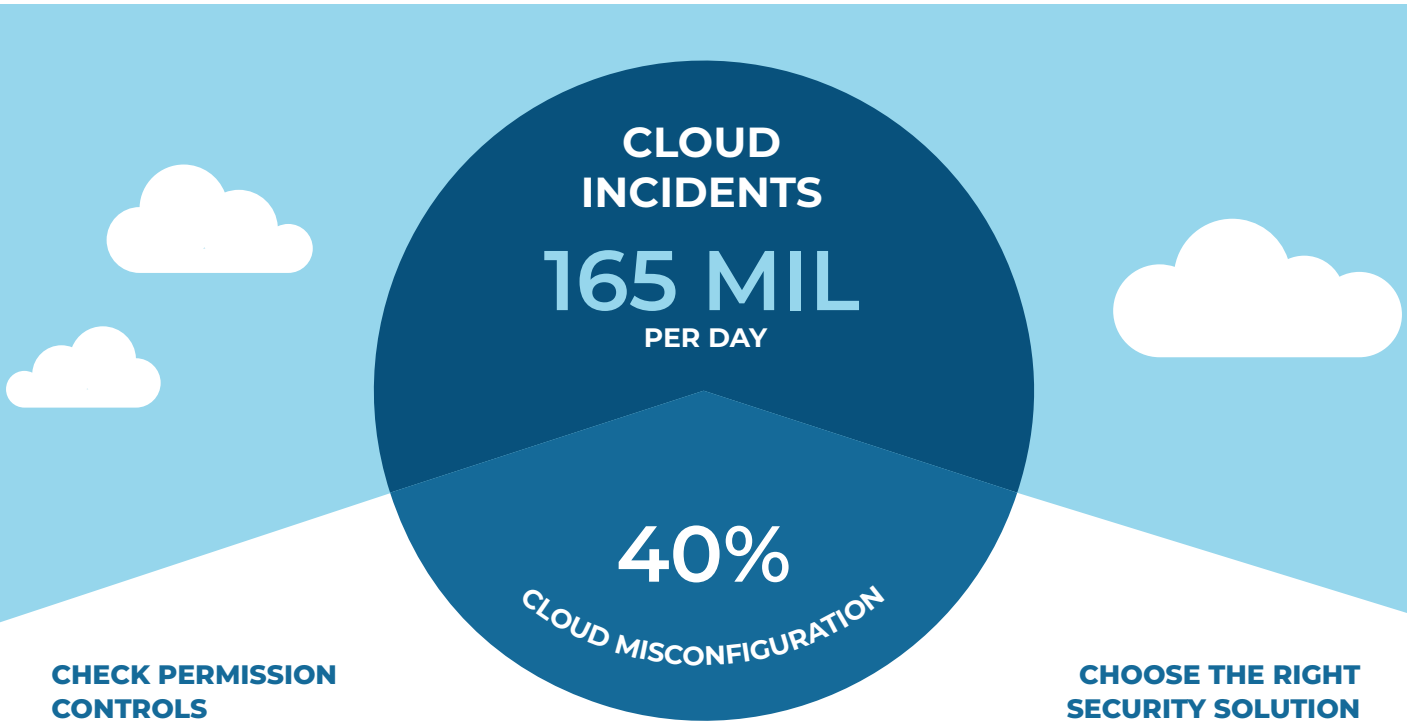
BEST PRACTICES FOR PREVENTING CLOUD MISCONFIGURATIONS

On average 165 million misconfigurations take place in the cloud every day and 40% of cloud related incidents can be traced back to misconfiguration in the cloud environment. That´s why you should take cloud misconfiguration seriously and implement these best practices to secure your cloud-based assets.



CHECK PERMISSION CONTROLS

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

CHOOSE THE RIGHT SECURITY SOLUTION

Look at security solutions that include automated remediation to bolster your cloud security.

AUDIT FOR MISCONFIGURATION & COMPLIANCE CONTINUOUSLY

Implement regular audits to check for signs of misconfiguration and to maintain security and compliance policies.

CHECK FOR POLICY COMPLIANCE BEFORE PROVISIONING

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

IMPLEMENT SECURITY MEASURES SUCH AS LOGGING & ENCRYPTION

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

Sources: Fugeo, TrendMicro

How can we help you?
Get in touch to find out more about our Cloud Workload Security!

SoftwareONE AG
Riedenmatt 4
CH-6370 Stans

T. +41 844 44 55 44
E. info@softwareone.com
www.softwareone.com/en/solutions/managed-security/cloud-workload-security