The Ultimate Guide to

CLOUD MISCONFIGURATIONS

WHAT ARE CLOUD MISCONFIGURATIONS?

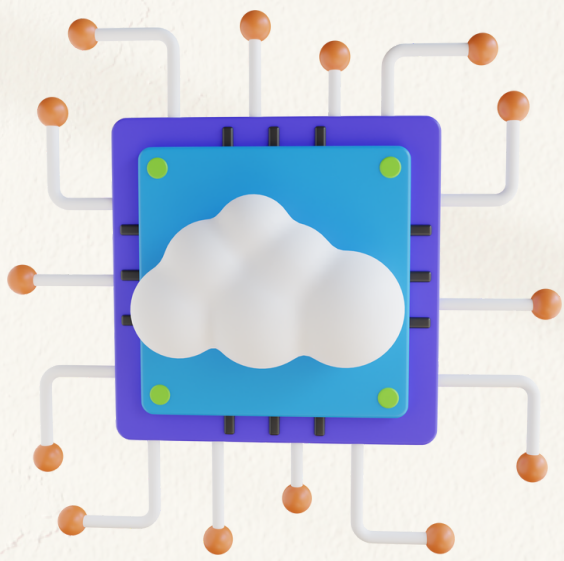
Cloud misconfigurations are errors in the configuration of cloud resources that can leave them exposed to attack.

Common Misconfigurations:

- Leaving default passwords unchanged
- Using weak passwords
- Granting excessive permissions
- Allowing public access to cloud resources
- Not encrypting data
- Not patching software
- Not monitoring the cloud environment for suspicious activity

WHY MISCONFIGURATIONS ARE A SECURITY RISK

Cloud misconfigurations can leave cloud resources exposed to attack, which can lead to data breaches, malware infections, and other security incidents.

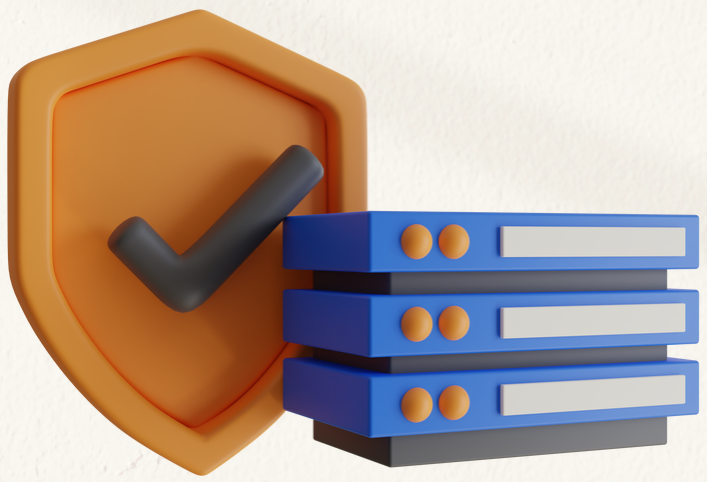


HOW TO IDENTIFY MISCONFIGURATIONS

Manually: Review the configuration of cloud resources and look for potential misconfigurations.

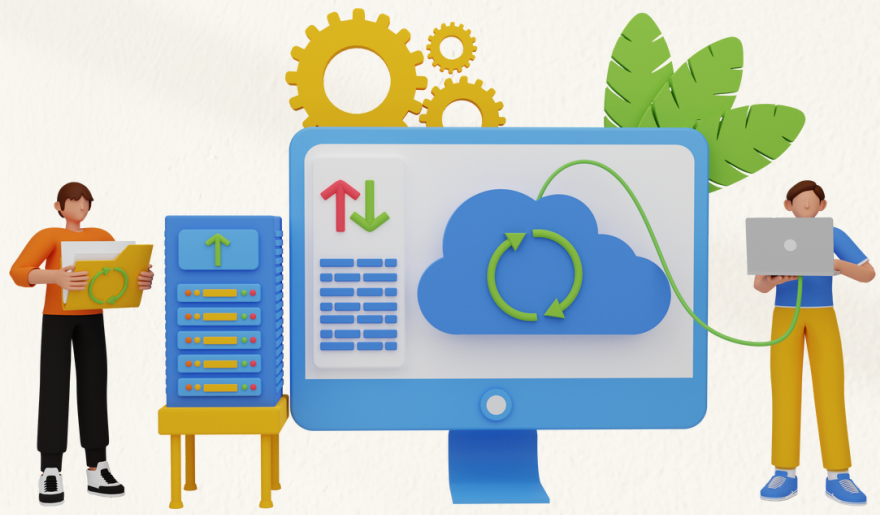
Automated: Use tools to scan cloud environments for misconfigurations.

Continuous: Use tools to continuously scan cloud environments for misconfigurations.



SELF-SERVICE AND OPEN-SOURCE TOOLS

- AWS Config
- GCP Cloud Audit Logging
- Azure Security Center
- CloudCheckr
- Qualys Cloud Scanning



BEST PRACTICES FOR CLOUD SECURITY

- Use strong passwords and multi-factor authentication.
- Keep your software up to date.
- Implement least privilege access.
- Encrypt your data.
- Monitor your cloud environment for suspicious activity.
- Use cloud security tools to identify and remediate misconfigurations

DON'T LET CLOUD MISCONFIGURATIONS PUT YOUR DATA AT RISK.

CONTACT OUR TEAM FOR CLOUD SECURITY AUDIT

+91 7305979769

contact@briskinfosec.com

BRISK INFOSEC

CYBER TRUST & ASSURANCE

YOUR PERFECT CYBERSECURITY PARTNER