



# Cloud

## Misconfigurations

One wrong checkbox , can leak Everything.



[sales@briskinfosec.com](mailto:sales@briskinfosec.com)

Swipe to explore



# Cloud Growth Misconfig Growth

As cloud adoption accelerates,  
security often lags behind.

- ☁️ More services bring added complexity
- ☁️ Speed-focused deployments often skip reviews
- ☁️ Multi-cloud setups lead to inconsistent controls
- ☁️ Fast-paced DevOps increases human error
- ☁️ Default settings cause unintended exposure



# What Attackers Are Exploiting

Attackers love cloud misconfigurations, they're easy to find and rarely monitored.



Publicly exposed S3 buckets



Default credentials in services



Over-permissive IAM roles



Disabled logging and alerts

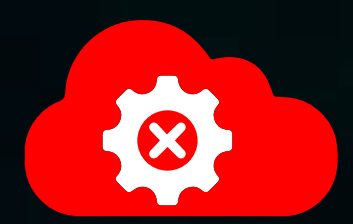


Unrestricted ports on VMs



# Misconfiguration Horror Stories

Small mistake,  
Massive consequence.



**Microsoft AI Research (2023)**  
38TB exposed via open blob



**Accenture (2021)**  
Storage misconfig leaked 4TB of data








**US Defense Firm (2024)**  
Open S3 bucket exposed files



# Must have Checklist for CSPM

Cloud Security Posture Management  
Essentials Checklist are

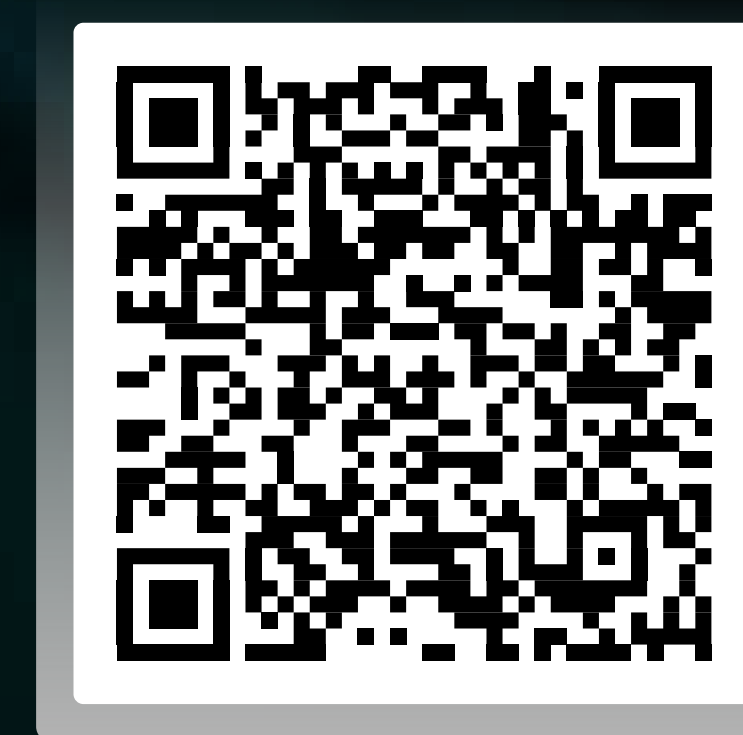
-  Automate config scans (Daily or real-time)
-  Enforce least privilege IAM roles
-  Audit storage permissions continuously
-  Enable visibility across multi-cloud
-  Set alerts for risky changes or exposures



# Fix It

Before They Find It

Talk to our Experts and secure your Cloud today.



Book a meeting