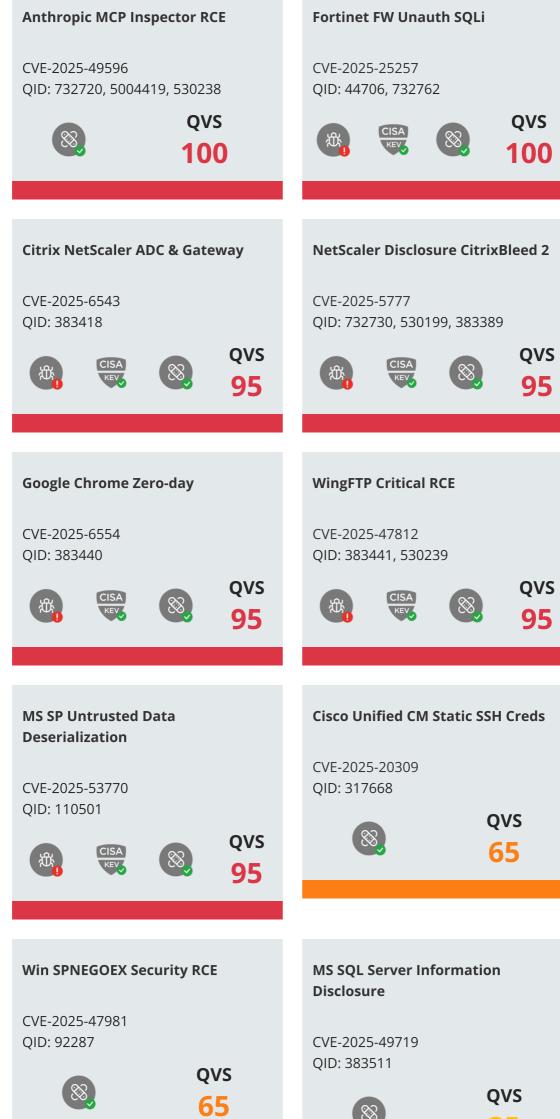


Measure, communicate, and eliminate your cyber risk—before it escalates into a crisis.





These vulnerabilities pose significant risks to your systems. To understand and address these critical threats, get your **personalized TruRisk Report**.

For more in-depth knowledge and details, visit **Qualys ThreatPROTECT** page and

subscribe to receive the latest updates on threats and vulnerabilities.

Cloud Security Snapshot: Key Misconfigurations

Contact your Technical Account Manager today to get yours.



Secrets should be auto rotated after not > 90

Public N/W Access is Disabled for storage

accounts

before it's too late.

Misconfiguration

The following percentages reflect how many resources across all customers have these misconfigurations. **Amazon Web Services (AWS)**

Resources Affected

(%)

93.00%

89.00%

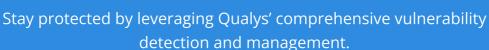
98.00%

Usage of root account is monitored	95.00%
Network ACLs allow ingress from 0.0.0.0/0 to port 3389	95.00%
Access keys unused for 90 or more days are disabled	74.00%
Encrypt the destination S3 bucket in the audit logging account	95.00%
Microsoft Azure	
Misconfiguration	Resources Affected (%)
App Service Authentication is set on Function Apps	97.00%
Function app has Client Certificates set to On	95.00%
VM disks for critical VMs are encrypted with	93.00%

Container Registry disallows unrestricted N/W Access	82.00%
Google Cloud Platform (GCP)	
Misconfiguration	Resources Affected (%)
API Keys are rotated every 90 days	84.00%
GCP Storage bucket is encrypted using CMK	79.00%
BigQuery Table is encrypted with CMK	87.00%
Enable Private Google Access for all subnetworks in the VPC	91.00%
Ensure that PostgreSQL instances are CMK-encrypted	88.00%
Oracle Cloud Infrastructure (OCI)	

Resources Affected (%)
99.00%
95.00%
87.00%
93.00%
94.00%

These misconfigurations pose significant risks to your cloud. To understand and address these critical issues, get your Cloud TruRisk **Insight Report**. This report identifies which misconfigurations are causing risks and provides actionable steps to remediate them. Contact your Technical Account Manager today to get your personalized report and secure your cloud.



detection and management.

fastest ways to remediate these critical risks and strengthen your security posture. Don't wait—proactive steps now can prevent costly breaches later.

Reach out to your Technical Account Manager today to discuss the

Thank you

for being part of our July newsletter! We hope these insights empower you to enhance your security posture. Get ready for next month's edition, filled with the latest updates and expert threat research tips.

We value your input—what topics would you like us to explore next? Drop us a line anytime at researchNewsletter@qualys.com. Until then, stay safe and secure!



Accessibility. Notice at Collection. Trust. Cookie Consent.