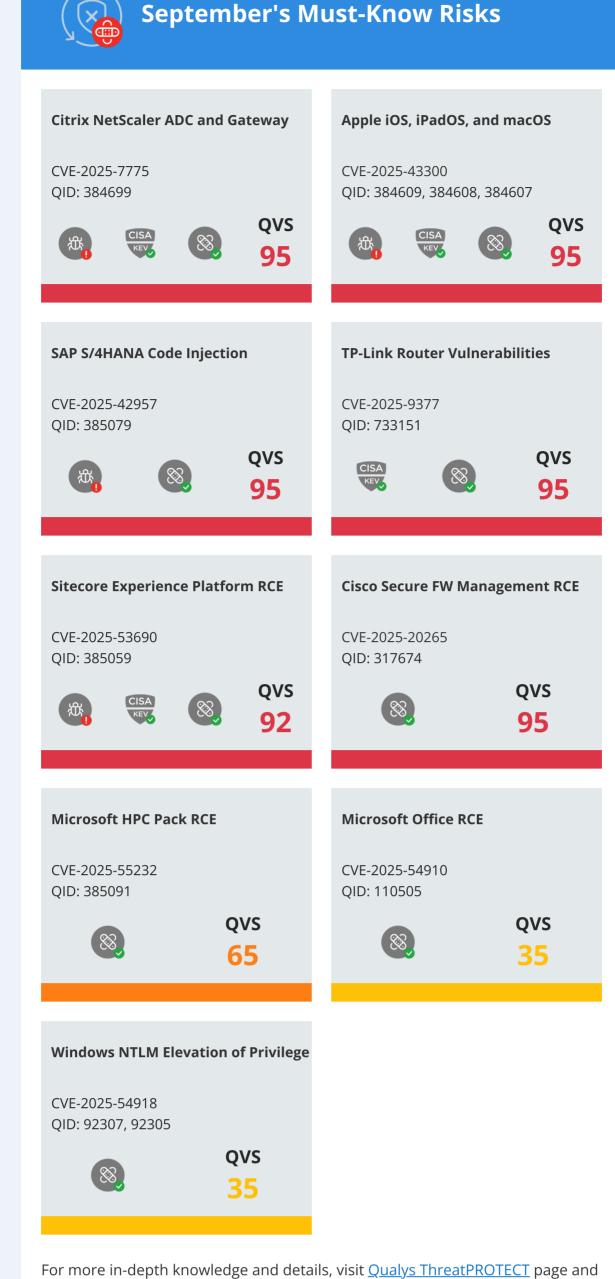


## cyber risk—before it escalates into a crisis.

Measure, communicate, and eliminate your

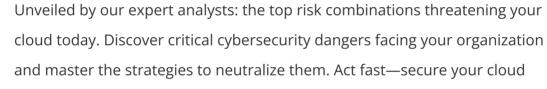


These vulnerabilities pose significant risks to your systems. To understand and address these critical threats, get your **personalized TruRisk Report**.

**Contact your Technical Account Manager today to get yours.** 

subscribe to receive the latest updates on threats and vulnerabilities.

**Cloud Security Snapshot: Key** Misconfigurations



before it's too late.

accessible

Apps

have these misconfigurations. **Amazon Web Services (AWS)** Resources Misconfiguration

Multi-factor authentication (MFA) is enabled for all

**Amazon OpenSearch Service domains are publicly** 

**App Service Authentication is not set on Function** 

Public network access is not disabled or restricted

in Cognitive Services accounts

**Google Cloud Platform (GCP)** 

Network security groups allow ingress from

User API keys rotate within 90 days or less

MFA is enabled for all users with a console

0.0.0.0/0 or ::/0 to port 22

password

IAM users that have a console password

Affected (%)

59.00%

26.00%

94.00%

69.00%

Resources

44.00%

90.00%

75.00%

The following percentages reflect how many resources across all customers

Access Keys unused for 90 days or greater are not disabled	72.00%
Security groups allow ingress from 0.0.0.0/0 to port 22	16.00%
Expired certificates are removed from Certificate Manager (ACM)	28.00%
Microsoft Azure	
Misconfiguration	Resources Affected (%)
Expiration Date is not set for all Secrets in RBAC Key Vaults	65.00%
Cognitive Services do not use private links	85.00%
Storage for Critical Data are Encrypted with Customer Managed Keys	88.00%

Misconfiguration	Affected (%)	
Project has Service Account with Admin Privileges	32.00%	
User-managed/external keys for service accounts are rotated every 90 days or less	92.00%	
GCP Storage bucket is encrypted not using customer-managed key	88.00%	
KMS encryption keys are not rotated within a period of 90 days	32.00%	
BigQuery Dataset is not encrypted with Customer- managed key	92.00%	
Oracle Cloud Infrastructure (OCI)		
Misconfiguration	Resources Affected (%)	
Object Storage buckets are publicly visible	38.00%	

**Boot volumes are encrypted with Customer** 96.00% Managed Key (CMK) 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.



cybersecurity community together to share insights and explore new solutions.

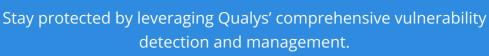
This year, we are proud to announce QSC's transformation from a user summit

into a premier industry event: the very first Risk Operations Conference

(ROCon). The Risk Operations Center (ROC) establishes a new frontier in risk management – aligning cybersecurity strategy with measurable business outcomes. ROCon will convene the global security community to embrace this

Join us as we usher in the new paradigm of cybersecurity Read the blog for the details.

vision and shape the future of cyber risk.



Reach out to your Technical Account Manager today to discuss the

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.

Thank you for being part of our September 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 <u>researchNewsletter@qualys.com</u>. Until then,

Accessibility. Notice at Collection. Trust. Cookie Consent.