Qualys TotalCloud v2.x

Release Notes

Version 2.6.0
October 04, 2023

What's New

Amazon Web Services

Introduced Widgets in Cloud Detection and Response

Enhanced Cloud Detection and Response Findings in Inventory

Introduced Support for TruRisk Insights in TotalCloud Inventory

New Tokens

Common Features

Introduced New Mandates

Control Changes

Qualys TotalCloud 2.6.0 brings you improvements and updates! Learn More

For updates to the TotalCloud APIs, refer to the TotalCloud API Release Note

For updates to the Connectors Application, refer to the Connector Release Note

Amazon Web Services

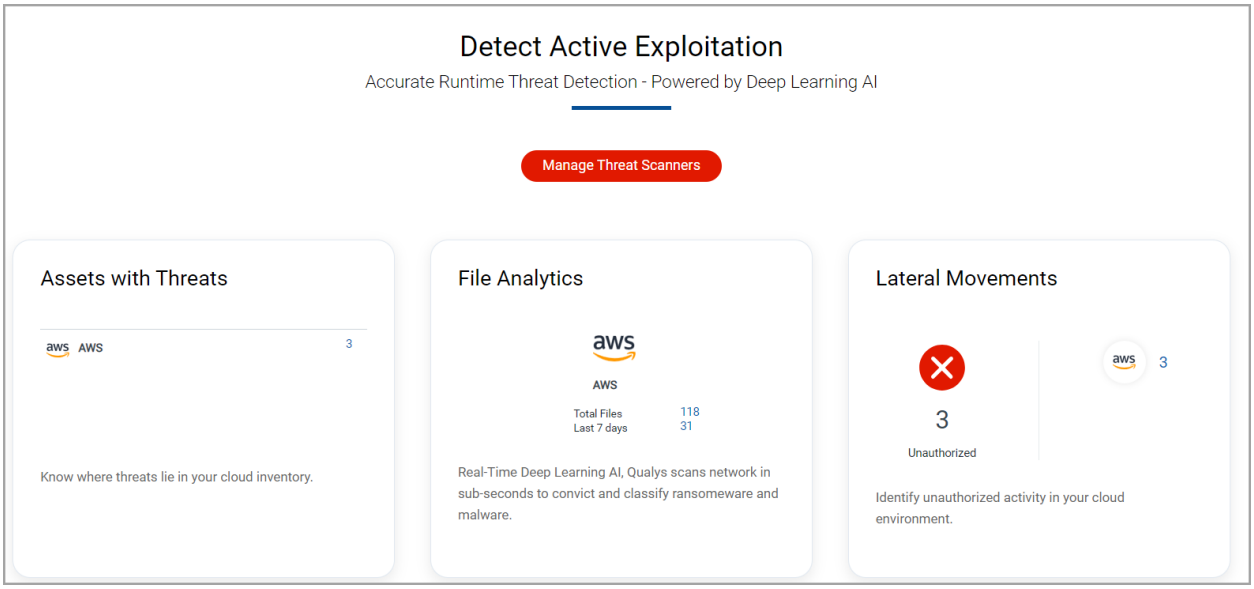
Features introduced to Amazon Web Services in this release.

Introduced Widgets in Cloud Detection and Response

We have introduced three new widgets for CDR on the TotalCloud homepage. The widgets highlight critical asset information, such as real-time count of assets with threats, analytics on malware/ransomware, and suspicious behavior in the network.

To access the new CDR widgets, navigate to the **TotalCloud Homepage** > **Detect Active Exploitation** tab.

The widgets should be visible once you have deployed threat scanners to set up CDR on your environment. If you haven't set up threat scanners yet, refer to the TotalCloud Online Help to learn more.



Assets with Threats – Identify how many assets in your cloud account are under threat. With CDR's real-time findings, you can always be one step ahead of your attacker with immediate updates.

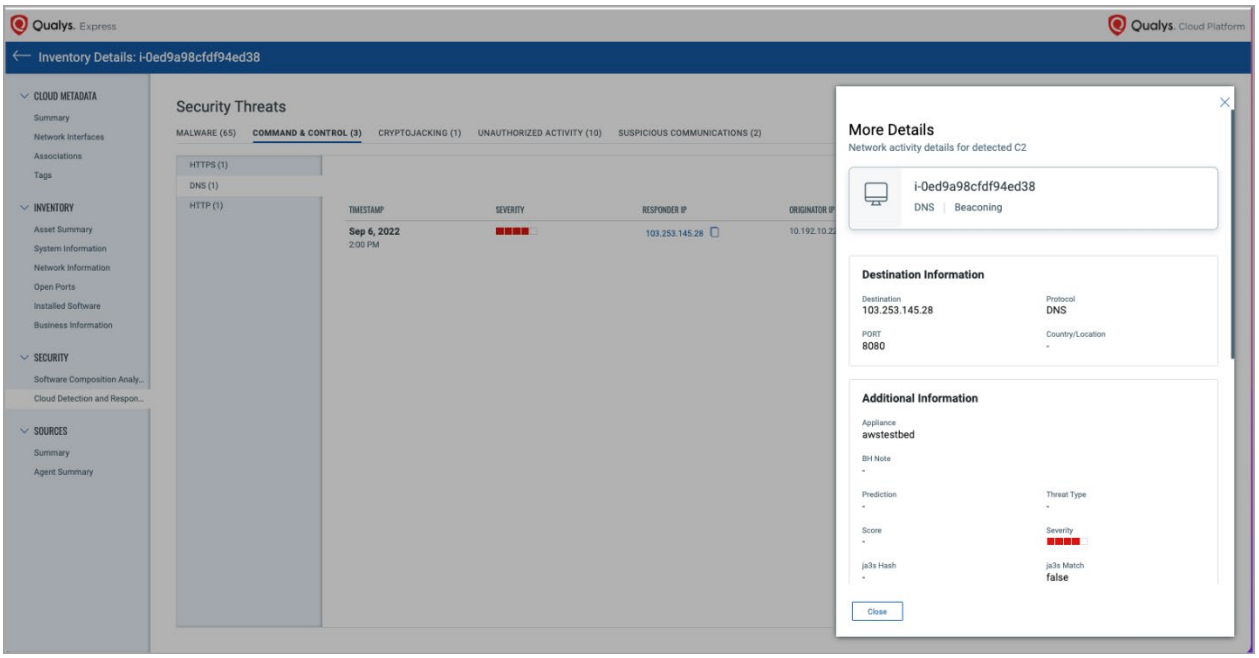
File Analytics – Qualys CDR scans your network to identify the files introduced and classify malicious entities. The widget shows you a count of the total malicious files in your network and the malicious files detected in the last seven days.

Lateral Movements- Keep track of suspicious activity in your account. Sniff out unauthorized movements, RDP brute-force attempts, and more. The widget shows you a count of unauthorized activities.

Learn more about leveraging the CDR widgets by referring to the Cloud Detection and Response section of the TotalCloud Online Help.

Enhanced Cloud Detection and Response Findings in Inventory

We have enhanced the CDR findings listed on the Asset summary in TotalCloud Inventory. The CDR findings highlight more details for all 5 forms of network attacks.



Malware – Learn more about potential malware attacks on your network. The detected threat is categorized into its type of malware, such as Backdoor attacks, Trojans, or Ransomware.

Command & Control – Learn more about occurrences of Command & Control attacks on your network protocols. Understand the source and destination of the encrypted communications and network probes.

Cryptojacking – Learn more about any crypto mining in your network by attackers. You receive direct information on which coin is mined and how it is done.

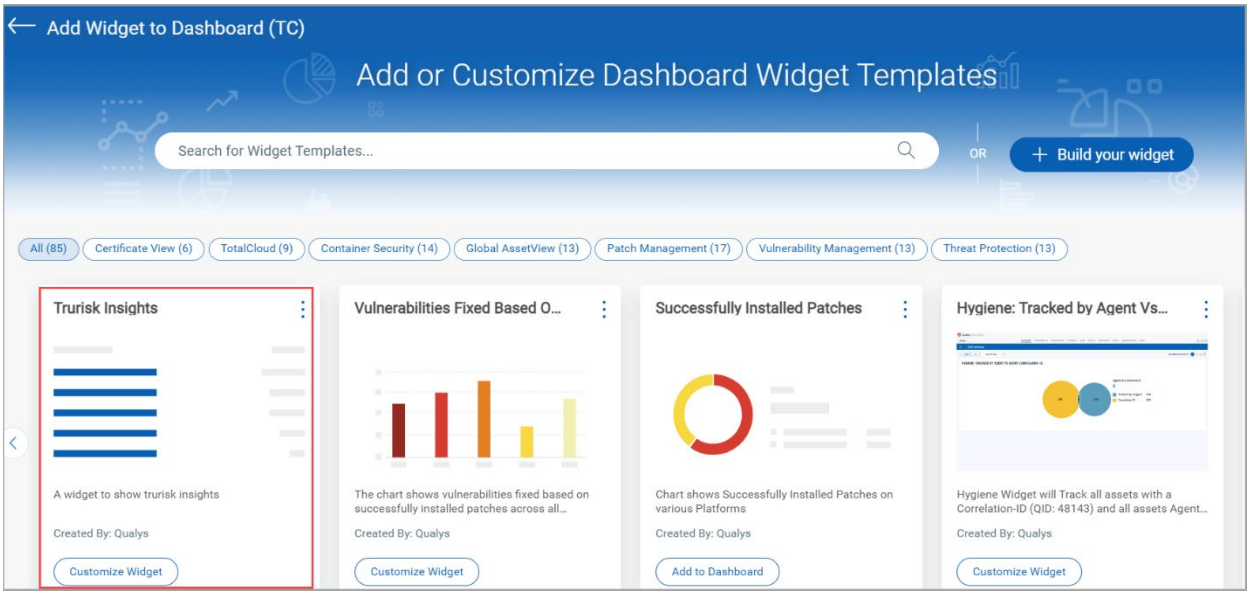
Unauthorized Activity – Learn more about all the unauthorized activity in your network. You receive information on the type of activity, whether a brute force attack, a port scan, etc.

Suspicious Communication – Learn more about suspicious network communication, whether internal or external.

Introduced Support for TruRisk Insights in TotalCloud Inventory

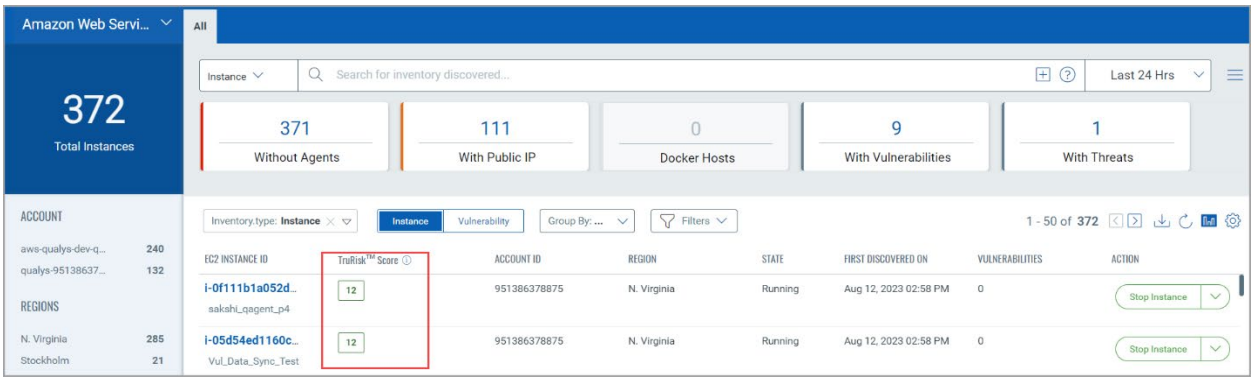
With this release, we have launched TruRisk insights on the TotalCloud dashboard. TruRisk Insights was introduced to help customers prioritize vulnerabilities based on TotalCloud findings. TruRisk Insights for TotalCloud leverages the findings of CSPM, FlexScan, CDR, and CWP to show a single widget with all your relevant resource data.

Navigate to **TotalCloud** > **Dashboard**. Click the **+** icon to add widgets.
You can find the TruRisk Insights widget listed.



We have also introduced the **TruRisk Score** column to the TotalCloud Inventory. This addition empowers customers by bringing external security, misconfiguration, and vulnerability scoring into the TotalCloud ecosystem.

You can find the **TruRisk Score** Column by navigating to the **Inventory tab**. A new column is visible next to the resource name. By default, the **TruRisk Score** listing is set to show the most critical scores on top of the list. You can further sort the findings as well.



The **TruRisk Score** only uses FlexScan findings to calculate your score.

New Tokens

With this release, we have introduced support for new tokens.

TruRisk Tokens

You can find this token for TruRisk Score introduced in the Inventory tab of TotalCloud. Use these tokens to find resources based on the TruRisk Score provided.

Navigate to **Inventory** > Any Resource type.

Name	Description
instance.riskScore	Use an integer value (0-1000) to search for all the EC2 instances with the specified risk score.

Report Tokens

We have introduced a new token in the reports tab of TotalCloud. Use the below token to find reports based on their report ID.

Name	Description
report.id	Use a text value ##### to show reports based on the report ID.

Common Features

Features introduced across the TotalCloud application in this release.

Introduced New Mandates

We have introduced support for new mandates in this release.

Doc ID	Document Name	Publisher	Version
6281	Payment Card Industry Data Security Standard (PCI-DSS) v4.0	PCI Security Standards Council	Ver. 4.0

Control Changes

Changes introduced to Controls and Policies in TotalCloud 2.6.0.

Amazon Web Services

Control changes for Amazon Web Services.

New Control in CIS Amazon Web Services Foundations Benchmark

We have introduced a new control for CIS Amazon Web Services Foundations Benchmark.

Platform	CID	Title
AWS	253	Ensure AWS Security Hub is enabled in all regions.

Migrated Control from CIS Amazon Web Services Foundations Benchmark to Amazon Web Services Best Practices Policy

We have migrated a new control in CIS Amazon Web Services Foundations Benchmark to Amazon Web Services Best Practices Policy.

Platform	CID	Title
AWS	67	Ensure all S3 buckets employ encryption-at-rest.

Title Changes for AWS CIS 2.0

We have changed the titles of the following controls for CIS Amazon Web Services Foundations Benchmark 2.0.

Platform	CID	Old Title	New Title
AWS	67	Ensure a log metric filter and alarm exist for unauthorized API calls	Ensure unauthorized API calls are monitored.
AWS	28	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	Ensure management console sign-in without MFA is monitored
AWS	29	Ensure a log metric filter and alarm exist for usage of the root account	Ensure usage of the 'root' account is monitored

Platform	CID	Old Title	New Title
AWS	30	Ensure a log metric filter and alarm exist for IAM policy changes	Ensure IAM policy changes are monitored
AWS	31	Ensure a log metric filter and alarm exist for CloudTrail configuration changes	Ensure CloudTrail configuration changes are monitored
AWS	32	Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	Ensure AWS Management Console authentication failures are monitored
AWS	33	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer-created CMKs	Ensure disabling or scheduled deletion of customer-created CMKs is monitored
AWS	34	Ensure a log metric filter and alarm exist for S3 bucket policy changes	Ensure S3 bucket policy changes are monitored
AWS	35	Ensure a log metric filter and alarm exist for AWS Config configuration changes	Ensure AWS Config configuration changes are monitored
AWS	36	Ensure a log metric filter and alarm exist for security group changes	Ensure security group changes are monitored
AWS	37	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	Ensure Network Access Control Lists (NACL) changes are monitored
AWS	38	Ensure a log metric filter and alarm exist for changes to network gateways	Ensure changes to network gateways are monitored
AWS	39	Ensure a log metric filter and alarm exist for route table changes	Ensure route table changes are monitored
AWS	40	Ensure a log metric filter and alarm exist for VPC changes	Ensure VPC changes are monitored
AWS	53	Ensure Encryption is enabled for the RDS database Instance	Ensure that encryption-at-rest is enabled for RDS Instances
AWS	172	Ensure a log metric filter and alarm exists for AWS Organizations changes	Ensure AWS Organizations changes are monitored

Microsoft Azure

Control changes for Microsoft Azure.

Deprecated Controls in Microsoft Azure Best Practices Policy

We have deprecated a control in Microsoft Azure Best Practices Policy.

Platform	CID	Title
Azure	50172	Ensure that public network access is disabled for Azure Key Vaults.

Issues Addressed

- We have fixed an issue where CID-52043 and CID 50070 generated false positive detections.

- We have enhanced our assessment report API to ensure reports based on report ID are generated as intended.

- We have fixed an issue where the customers reported their S3 buckets were not showing public access type despite having public access. We have introduced new parameters to ensure the access type is displayed correctly.
- We have added a note in the create report wizard. The note informs customers that control summary results only align with the selected resource evaluation filters when using the resource.result token in the search query.