tenable.cs™
cloud security

DATA SHEET

TENABLE'S CLOUD-NATIVE APPLICATION PROTECTION PLATFORM

SECURE EVERY STEP FROM **CODE TO CLOUD**

Tenable.cs provides complete and continuous visibility of exposures across all of your cloud resources and assets in a single platform. With Tenable.cs, you can detect and fix cloud infrastructure misconfigurations in the design, build and runtime phases of your software development lifecycle. Establish guardrails in DevOps pipelines to prevent exposures from reaching production. Continuously monitor AWS, Azure, and GCP environments to ensure any runtime changes adhere to policies, and create merge requests automatically to remediate configuration drifts.

Tenable.cs also provides continuous visibility into cloud host and container image vulnerabilities, without the need to manage scan schedules, credentials or agents. Cloud assets and container images are reassessed as new vulnerability detections are added and as new assets are deployed. This always-on approach allows you to spend more time focusing on the highest priority vulnerabilities and less time on managing scans and software.

KEY BENEFITS

Prevent Security Issues

Identify and remove cloud flaws during development before they ever reach production.

Accelerate Response

Automatically deliver remediations back to developers via merge requests.

Enforce Consistent Policies

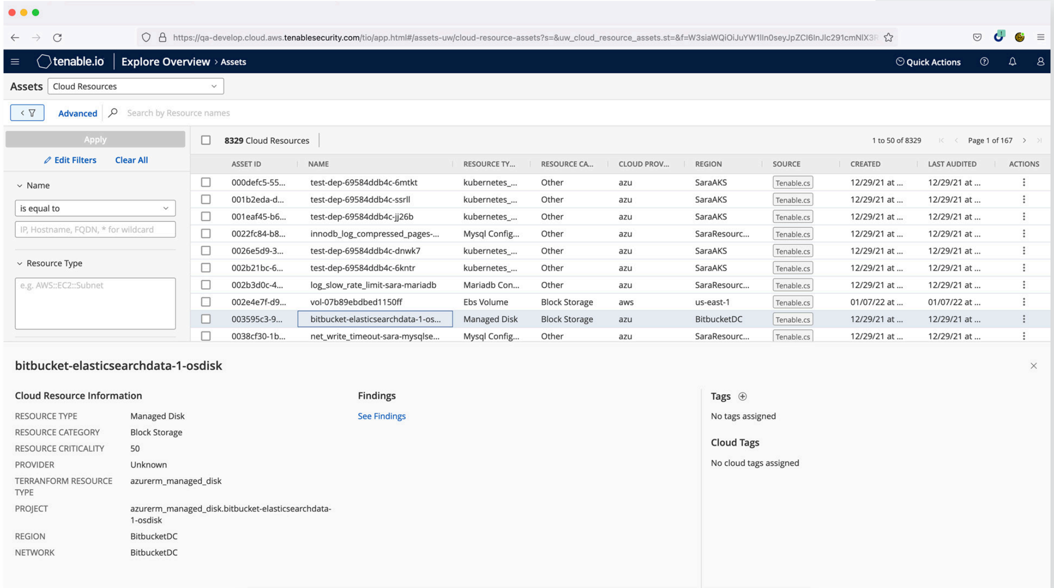
Take advantage of 1,800 policies across all leading standards, or create your own.

Improve Collaboration

Improve communication between security, cloud operations and DevOps for greater efficiency.

Gain Unified Visibility

Understand your security posture of cloud environments alongside your on-prem assets.


https://qa-develop.cloud.aws.tenablesecurity.com/tio/app.html#/assets-uw/cloud-resource-assets?s=&uw_cloud_resource_assets.st=&f=W3siaWQiOiJuYW1lIn0seyJpZCI6InJlc291cmNlX3R
tenable.io
Explore Overview › Assets
Quick Actions
Assets
Cloud Resources
Advanced
Search by Resource names
Apply
Edit Filters
Clear All
Name
is equal to
IP, Hostname, FQDN, * for wildcard
Resource Type
e.g. AWS::EC2::Subnet

□ **8329** Cloud Resources

1 to 50 of 8329 Page 1 of 167

	ASSET ID	NAME	RESOURCE TY...	RESOURCE CA...	CLOUD PROV...	REGION	SOURCE	CREATED	LAST AUDITED	ACTIONS
□	000defc5-55...	test-dep-69584ddb4c-6mtkt	kubernetes_...	Other	azu	SaraAKS	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	001b2eda-d...	test-dep-69584ddb4c-ssrll	kubernetes_...	Other	azu	SaraAKS	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	001eaf45-b6...	test-dep-69584ddb4c-jj26b	kubernetes_...	Other	azu	SaraAKS	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	0022fc84-b8...	innodb_log_compressed_pages-...	Mysql Config...	Other	azu	SaraResourc...	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	0026e5d9-3...	test-dep-69584ddb4c-dnwk7	kubernetes_...	Other	azu	SaraAKS	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	002b21bc-6...	test-dep-69584ddb4c-6kntr	kubernetes_...	Other	azu	SaraAKS	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	002b3d0c-4...	log_slow_rate_limit-sara-mariadb	Mariadb Con...	Other	azu	SaraResourc...	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	002e4e7f-d9...	vol-07b89ebdbed1150ff	Ebs Volume	Block Storage	aws	us-east-1	Tenable.cs	01/07/22 at ...	01/07/22 at ...	⋮
□	003595c3-9...	bitbucket-elasticsearchdata-1-os...	Managed Disk	Block Storage	azu	BitbucketDC	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮
□	0038cf30-1b...	net_write_timeout-sara-mysqlse...	Mysql Config...	Other	azu	SaraResourc...	Tenable.cs	12/29/21 at ...	12/29/21 at ...	⋮

bitbucket-elasticsearchdata-1-osdisk

Cloud Resource Information

RESOURCE TYPE	Managed Disk
RESOURCE CATEGORY	Block Storage
RESOURCE CRITICALITY	50
PROVIDER	Unknown
TERRANFORM RESOURCE TYPE	azurerm_managed_disk
PROJECT	azurerm_managed_disk.bitbucket-elasticsearchdata-1-osdisk
REGION	BitbucketDC
NETWORK	BitbucketDC

Findings

See Findings

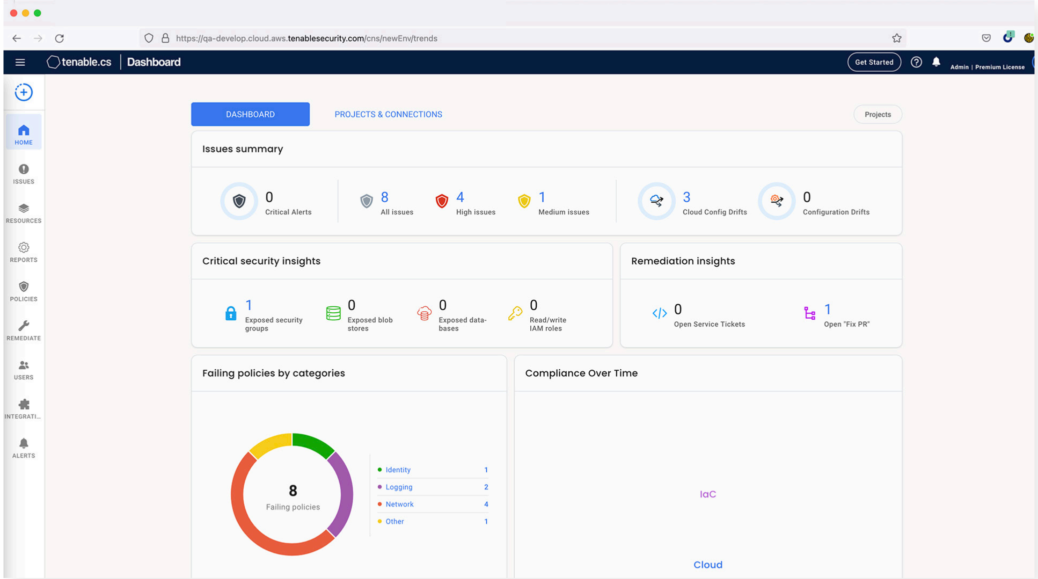
Tags

No tags assigned

Cloud Tags

No cloud tags assigned

Tenable.io within Tenable.cs enables organizations to programmatically detect and fix cloud infrastructure misconfigurations in design, build, and runtime.



Tenable.cs helps organizations establish guardrails in pipelines and automated workflows (CI/CD) to prevent unresolved misconfigurations or vulnerabilities from reaching the runtime environment. It monitors infrastructure deployed in AWS, Azure, and GCP to ensure compliant runtime changes, and drifts are propagated back to the IaC.

KEY CAPABILITIES

Secure Infrastructure as Code

Assess Infrastructure as Code (IaC) templates, including Terraform, AWS CloudFormation, Azure Resource Manager and Kubernetes, for policy violations. Integrate cloud infrastructure security into the DevOps pipeline to prevent security issues from reaching production. Quickly remediate IaC misconfigurations directly in development tools to enforce policies in both build-time and runtime.

Prevent Cloud Posture Drift

Identify discrepancies between IaC and your running cloud environment. Ensure your source of truth is always up to date, and enforce your security controls at runtime.

Auto Remediate Vulnerabilities

Automatically provide fix suggestions via pull or merge requests to reduce the burden on your development teams and meet developers in the tools they know. This ensures the quickest time to remediation to achieve compliance.

Visibility into Cloud Assets

Continuously discover and assess cloud assets without the need to install agents, configure a scan or manage credentials. Detect security issues quickly as new vulnerabilities are disclosed and as your cloud environment changes with instances spinning up and down.

Contextualize Risks

Understand application vulnerabilities in the context of their infrastructure configurations to gain a true picture of the risk they present. Understand the breach paths and prioritize their remediation.

Govern Compliance

Assess and document compliance to industry standards and established best practices such as CIS, PCI, GDPR. Take advantage of over 1,800 policies across 10 standards for comprehensive assessment. You can also create custom policies based on your individual needs.

Kubernetes & Container Security

Gain visibility into the secure posture of your container images and infrastructure. Integrate security testing of new container images and Kubernetes configurations into DevOps pipelines to ensure new builds and IaC are compliant with enterprise policies. View vulnerability data, package inventories and misconfigurations of all your container images and Kubernetes infrastructure. Sync container images from third-party registries to continuously assess them for newly discovered vulnerabilities. Keep Kubernetes deployments secure and prevent configuration drift.

Runtime Security for Cloud Infrastructure

Enforce your policies on your running cloud environment. Real-time alerting and remediation will ensure compliance. Policies are unified from IaC to cloud. Generate reports to demonstrate your security posture in the field over time.

For More Information: Please visit tenable.com/products/tenable-cs

Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

tenable