

UNIFIED CLOUD SECURITY POSTURE AND VULNERABILITY MANAGEMENT

SPEED CLOUD ADOPTION WHILE MEETING COMPLIANCE REQUIREMENTS WITH TENABLE CLOUD SECURITY

Rapid cloud development and migration have given way to highly complex, distributed environments – and a growing attack surface. At the same time, the number of siloed tools, rapid change, and a shortage of cloud security and compliance experts to secure the business are posing a seemingly insurmountable liability for enterprises.

Tenable Cloud Security addresses these challenges providing a single unified cloud security posture (CSPM) and vulnerability management (VM) solution that lets you see and secure all your cloud assets across multi-cloud environments. Enriched by the expertise and speed of Tenable Research, including the industry’s most comprehensive library of 71,000 known vulnerabilities, and nearly 1500 policies spanning 20 industry benchmarks and regulations, only Tenable Cloud Security provides a complete picture of cloud exposure spanning vulnerabilities and misconfigurations, across runtime, CI/CD pipelines, and developer code. With built-in compliance profiles, reporting and remediations, and risk-based scoring you can prioritize the risk that poses the greatest threat to your business.

KEY BENEFITS

Complete Visibility

Gain a 360° view of multi-cloud assets, repositories, configuration and drift

Reduced Exposure

Reduce the number of critical severity alerts with risk-based prioritization

Continuous Governance

Enforce the same consistent set of security policies from code to cloud

Improve Compliance

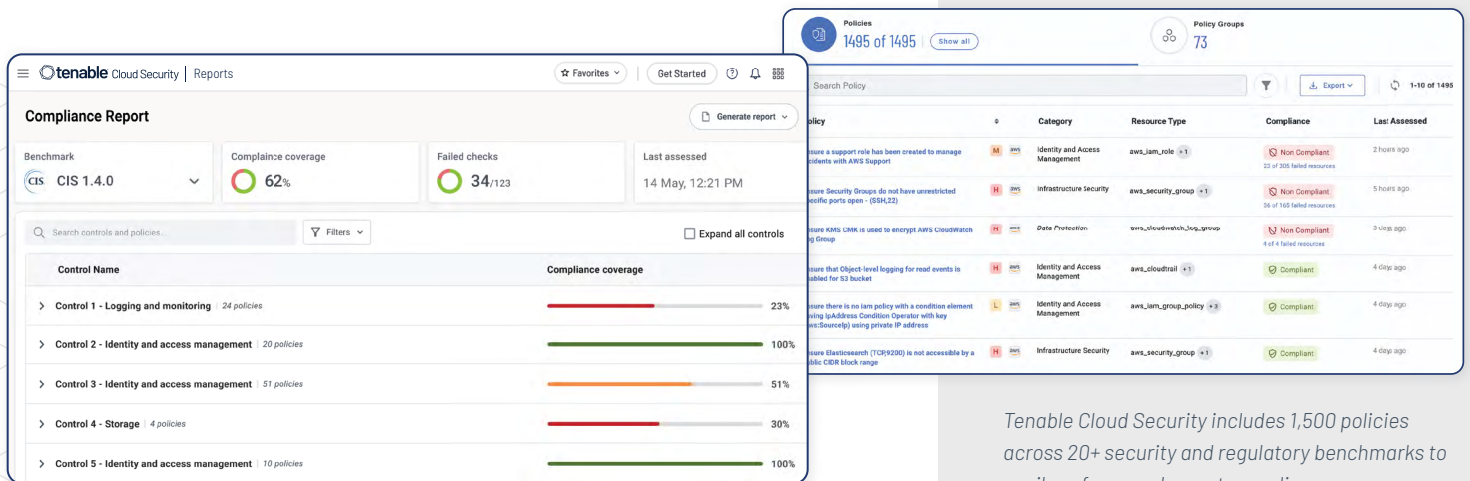
Minimize reporting time and effort with automated compliance reporting

Speed Remediation

Reduce MTTR for misconfigurations with remediation-as-code

Realize Rapid Time-to-value

Deploy and begin detecting CVEs and misconfigurations in under 5 minutes



The screenshot displays the Tenable Cloud Security interface. On the left, a 'Compliance Report' for CIS 1.4.0 shows a compliance coverage of 62% and 34 failed checks. The report lists five controls with their respective coverage: Control 1 (23%), Control 2 (100%), Control 3 (51%), Control 4 (30%), and Control 5 (100%). On the right, a 'Policies' table lists 1495 policies across various categories and resource types, with columns for Policy, Category, Resource Type, Compliance status, and Last Assessed.

Policy	Category	Resource Type	Compliance	Last Assessed
Ensure a support role has been created to manage tickets with AWS Support	Identity and Access Management	aws_iam_role	Non Compliant	2 hours ago
Ensure Security Groups do not have unrestricted egress ports open - (SSM,SS)	Infrastructure security	aws_security_group	Non Compliant	5 hours ago
Ensure AWS IAM LINK is used to encrypt AWS CloudWatch logs	Data Protection	aws_cloudwatch_logs_group	Non Compliant	3 days ago
Ensure that Object-level logging for read events is enabled for S3 bucket	Identity and Access Management	aws_cloudtrail	Compliant	4 days ago
Ensure there is no iam policy with a condition element using IpAddress Condition Operator with key aws:SourceIp using private IP address	Identity and Access Management	aws_iam_group_policy	Compliant	4 days ago
Ensure Elasticsearch (TCP9200) is not accessible by a public CIDR block range	Infrastructure Security	aws_security_group	Compliant	4 days ago

Tenable Cloud Security includes 1,500 policies across 20+ security and regulatory benchmarks to easily enforce and report compliance.

TENABLE HELPS UNIFY CLOUD SECURITY EFFORTS ACROSS YOUR TEAMS

New deployments to the cloud and published vulnerabilities never stop and neither can your organization's cloud security program. Tenable helps improve communication and reduce toil across security, operations and development teams by providing a cloud security framework that enables teams to easily scale security across all of their cloud environments and teams.

Vulnerability Management Teams

Runtime Agentless Scanning and Risk Prioritization

Gain complete visibility into cloud assets without deploying agents, prioritize and speed remediation with deep insight into asset criticality and CVE exploitability from Tenable Research, and stop risky deployments before they reach production.

Cloud Security Architects and Engineers

Multicloud Governance and Exposure Management

Implement a common policy framework across all of your cloud runtime environments, ensure systems are compliant, manage public exposure risks, and secure system access. Scale cloud security by automatically scanning code repositories for vulnerabilities and running tests as part of CI/CD pipelines.

Developers and DevOps Engineers

Codified Policies and Pre-Built Integrations

Limit rework with codified policies and remediation instructions that can be easily run as part of local development and automated CI/CD workflows.

Showing details for > Issues > Instance > AWS-instance-1

Resource Details Resource configurations **Vulnerabilities** Misconfigurations Drifts

4 vulnerabilities Severity ▾

Severity	Name	Last seen
Critical	CVE-2018-4828: Adobe Flash Player Vulnerability - Unauthenticated Attacker	08.10.2
High	CVE-2017-9450: AWS CloudFormation bootstrap allows root privileges	08.10.2
Medium	CVE-2022-25166: Amazon AWS VPN Client 2.0.0 leaks Net-NTLMv2 hash	08.10.2
Low	CVE-2020-8912: AWS S3 Crypto SDK for GoLang leaves key recoverable	08.10.2
Info	CVE-2022-41316: HashiCorp Vault certificate vulnerability	08.10.2

Showing details for > Issues > Instance > AWS-instance-1

Resource Details Resource configurations Vulnerabilities **Misconfigurations** Drifts

3 failing policies Severity ▾

Severity	Failing policy	Source	Last detected
High	Ensure versioning is enabled for AWS S3 Buckets Policy group: Accurics Security Best Practices for AWS v2	Cloud	08.10.21 @ 07:06 PM
High	Ensure MFA Delete is enable on S3 buckets Policy group: Accurics Security Best Practices for AWS v2	Cloud	08.10.21 @ 07:06 PM
High	Ensure bucket policy is enforced with least privileges for all AWS S3 buckets Policy group: Accurics Security Best Practices for AWS v2	Cloud	08.10.21 @ 07:06 PM

With Tenable Cloud Security, teams have 360° visibility of cloud assets, including configurations, vulnerabilities, misconfigurations, drifts, and remediations - in a single-pane-of-glass.

KEY CAPABILITIES

Complete Cloud Workload Visibility and Zero Day Threat Detection

Get Complete Visibility with Agentless Assessment with Live Results

Continuously discover, inventory 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.

Risk Centric Exposure Management

Contextualize and prioritize risks based on whether or not a resource is publicly exposed, what assets it is connected to, and other key variables. Accurately communicate risks with stakeholders to take actions that drive business value.

Continuously Enforce Policies Across Runtime Environments

Continuously enforce policies on your running cloud environment with real-time alerting and remediation to ensure compliance. Generate reports to demonstrate your security posture over time.

Cloud/Kubernetes Security Posture Management (CSPM/KSPM) and Governance

Single Policy Framework from Code to Cloud

Automated policies are a core component to any enterprise class CSPM solution. Tenable Cloud Security includes 1,500 policies across 20+ standards such as CIS Benchmarks, SOC 2, PCI DSS, HIPAA, NYDFS and GDPR so you can enable policy guardrails across your entire organization in minutes. Quickly and easily define custom policies based on your individual needs.

Automated Drift Detection and Remediation

Continuously monitor your cloud infrastructure for configuration changes from the secure baseline. Receive automated alerts when changes are detected, risk assessments and remediation recommendations.

Identity and Access Management (IAM)

Ensure unauthorized access and data leaks are minimized by locking down full admin privileges and enforcing least privilege, including enforcing no public file systems or repositories, no access keys for root user account, no root user for administrative tasks, compliance with standard password policy, and MFA for root user account and console access.

Shift-Left: Secure Code and Remediate as Part of Local Development and DevSecOps Workflows

Dev Friendly Tooling

Build on the foundation of Terrascan, one of the most popular open source Infrastructure as Code security testing tools, Tenable.cs deeply integrates into the developer workflows.

Full Cloud Native Stack Coverage

Leverage a single tool for securing Infrastructure as Code (IAC), Helm charts, Terraform, Kubernetes, container images and source code repositories across multiple development environments.

Comprehensive Ecosystem Support

Integrate with popular developer and DevOps workflows including automation frameworks and third-party tools such as GitHub, Bitbucket, GitLab, Jenkins, Azure DevOps, and others.

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

Contact Us: Please email us at sales@tenable.com

or visit tenable.com/contact



COPYRIGHT 2023 TENABLE, INC. ALL RIGHTS RESERVED.
TENABLE, NESSUS, LUMIN, ASSURE, AND THE TENABLE
LOGO ARE REGISTERED TRADEMARKS OF TENABLE, INC.
OR ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES
ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.