

Close Cloud Exposure with Actionable Cloud Security

Cloud Native Application Protection Platform (CNAPP)

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**®
supporting a broad portfolio of industry-leading technologies
and a wide range of contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects
government agencies, industry partners, and technology
providers to deliver innovative, mission-focused solutions.

In partnership with Tenable, we provide technology solutions
that drive modernization, strengthen operations, and ensure
compliance with evolving government standards.



To learn more about how Carahsoft can support
your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/tenableresources



Join Events & Webinars:
carah.io/tenableevents



Discover Technology Solutions:
carah.io/tenable



Learn About Procurement:
carah.io/tenablecontracts



Connect With Our Team:
Tenable@carahsoft.com
703-581-6600

Cloud Native Application Protection Platform (CNAPP)

Close cloud exposures with actionable cloud security



Rapid cloud adoption has given way to highly complex, distributed environments — and a growing attack surface. New cloud-based attack vectors have combined with known risks to create fast-moving threats to hybrid and multi-cloud infrastructure. To add complexity, many organizations are plagued by siloed security tools and a shortage of cloud expertise, which leads to fragmented visibility that buries security teams in alerts.

Tenable Cloud Security addresses these challenges by providing a unified Cloud Native Application Protection Platform (CNAPP) that empowers teams to close critical cloud exposures. It rapidly exposes multi-cloud security gaps and the toxic combinations of risks caused by misconfigurations, risky entitlements, vulnerabilities, and overly-permissive access to sensitive data. With Tenable Cloud Security, security teams can get a full picture of their cloud risk in one intuitive solution that simplifies security for even the most complex environments.

The solution analyzes all your cloud resources — infrastructure, workloads, data, and identities — to identify the most important exposures. Gain the context needed to recognize anomalous behavior, prioritize action based on the most likely attack paths, and achieve least-privilege access at scale. Demonstrate compliance with regulatory frameworks with intuitive reporting capabilities, and illustrate your cloud security progress over time.



Key benefits

- ➔ **Multi-cloud visibility for full-stack cloud security**
Gain a 360° view of all cloud resources including infrastructure, identities, workloads and data, and their exposures across all your clouds.
- ➔ **Reduced alert noise**
Find the toxic combination of issues and remediate priority risks immediately. Apply full-stack analysis to surface risk in context.
- ➔ **Continuous governance**
Secure cloud infrastructure across the complete lifecycle from development to deployment.
- ➔ **Simplified compliance reporting**
Minimize reporting time and effort with automated compliance reporting with built-in and custom policies.
- ➔ **Risk guidance and remediation**
Lower MTTR with detailed remediation guidance and automated response actions that close security gaps.
- ➔ **Scalable cloud expertise**
Democratize insights and accelerate organizational security efforts with an intuitive solution that empowers anyone to become an expert on their cloud environment.

Infrastructure as Code Security (IaC)

Scan IaC for exposures and feed Tenable findings into existing CI/CD workflows or auto-remediate directly with wizards. Assign alerts and auto-generated least-privilege IaC snippets via ticketing systems. Integrate with source-code repositories to initiate pull requests directly from the console.

Cloud Detection and Response (CDR)

Enrich cloud activity logs with resource-specific identity threat data and accelerate anomaly detection and response with contextualized and actionable insights into escalated privileges, changes to network configuration, and unauthorized use or theft of access keys.

Anomalous activity detected - data access		
Identity	Action	Service
 OpsScanner IAM Role Staging	ListAliases	 AWS Key Man... Service AWS
 JenkinsRole IAM Role Prod	GetObject	 Amazon S3 Service AWS
 JenkinsRole IAM Role Prod	RunInstances	 Amazon EC2 Service AWS
 prod-analytics IAM Role Prod	Decrypt	 AWS Key Man... Service AWS

FedRAMP Authorized

Tenable Cloud Security is FedRAMP authorized at the moderate impact level. This authorization streamlines the assessment and approval process for federal agencies' and delivers on our commitment to strengthen government cloud infrastructure through the use of safe and secure modern cloud technologies.

Data Security Posture Management (DSPM)

Know where and what types of sensitive data exist in your cloud, including PII, PHI, and company secrets. Understand data exposure risk from overly-permissive access, misconfigurations and vulnerabilities. Comply with data security regulations and industry standards.

Permissions Query				
Identity	Identity Type	Identity Account	Identity Labels	Origins
Resource Labels	Resource Scope	Usage	Permissions	Granted Through
Search	Select all	OS Unpatched	PI	Privileged
Public	Public Compute	Sensitive	Trusted Service	Vulnerable
Public Compute	Sensitive	Trusted Service	Vulnerable	Vulnerable Compute

Self-service Just-in-Time Access (JIT)

Grant speedy approval for time-bound, as-needed access to cloud resources—and, via IdP groups, to SaaS apps. Automatically revoke permissions and ensure that all access requests are logged for audit.

Access Requests					
Pending					
Created	Requestor	Account	Permission	Duration	
Jun 15 2021 08:23 am	Theo Wiggins	aws-prd-svc...	Power user	3 Hours	Deny Approve
Jun 22 2021 11:13 am	Mary Smith	prd-data...	BigQuery Reader	2 Days	Deny Approve
Active					
History					
Created	Requestor	Account	Permission	Duration	Status
Nov 6, 2021 10:34 am	Robert Garcia	aws-eu-stg-mks	Read-only	4 Weeks	Cancelled by me 10:34 am Nov 7, 2022
Nov 20, 2021 04:23 pm	Ahmed Haddad	PRD_BKD	Contributor	1 Week	Denied by admin 09:25 am Nov 21, 2022
Oct 24, 2021 04:23 pm	Ben Calinescu	PRD_BKD	Contributor	1 Week	Expired 07:00 am Nov 16, 2022

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us

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