**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 overlypermissive 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.

2 organizations	2 organizations	C 1 organizations	1 organizations	1 Cn-Premises	9,257 IAM Resources	14,360 Kubernetes Resources	7,244 Network Resources	5,340 Compute Resources	
12 Accounts	3 Subscriptions	86 Projects @ 789 • 5	86 Compartments	Account © 789	1,676 Data Resources	1,290 Container Resources	1,074 Management Resour	1,008 Security Resources	
pen Findings ③				Severity is all 💌	Trends ©			Lest 30 days	
2032 <sup>Critical</sup> TX Categories ©	234 High		<sup>dum</sup> 985	Low 50%	1,377 Coented findings     54 hove high/stitical avec     34 due to new feature	3 Resolve	3 14 d Findings	ය 3 Stared Findings	
Konneles - 217     St Logging - 327     On model hitsectors - 1175     On model hitsectors - 1175     Computer -     Xy Interver - 69     On the packing - 227		CO 15 Ender	nd Protection 35	9 Snoozed Findings	10	D5 Created	O 35 Excluded resources		
Compliance O Overall status O AWS Well Architected			89% Co e Pu -35% Co e Pu 70% Into e	inations (0) blic workloads with critical vale stemal principals with access t		Root user	If you cety have 5 minutes_O for user ML is not evaluate for user (C) implement () formation () MLR CC) instance () MLR CC) instance () Control () () () () () () () () () () () () ()		
CIS COPR COPR				vileges	O duster 25     Public KM	Image has critical vulnerabilities Crightcount2 (10052999200) Skey Crightcount2 (10052999200)			
soc2			05 0 400	vest users with high privileges		AKS cluster	AKS cluster allows anonymous requests to Kubelet servers     duster-2 Im Org/Subscription1		



#### **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.

## **Key capabilities**

## Cloud Security Posture Management (CSPM)

Simplify cloud compliance with a single solution that continuously scans configurations and resources across clouds, identifies violations, and automates reporting. Use built-in and custom policies and dynamically assess risk to achieve compliance with standards like NIST, CIS, PCI, SOC 2, and GDPR.



## **Cloud Workload Protection (CWP)**

Identify vulnerabilities, exposed secrets, sensitive data, malware, and misconfigurations across virtual machines, containers, and serverless functions. Get industry-leading vulnerability intelligence from Tenable Research to isolate a vulnerability and drill down into its code exploit maturity, known exploitations, tagged research, and historical CVSS, VPR, and EPSS scores.



## Cloud Infrastructure Entitlement Management (CIEM)

Discover all cloud identities, analyze risky permissions and enforce least-privilege access to critical workloads for all users, including humans, services, and machines. Get best-of-breed entitlements management that integrates with leading identity providers (IDPs). Layer identity context with workload-related exposures like misconfigurations, vulnerabilities and sensitive data access for better prioritization of security issues and reduced alerts.



## Kubernetes Security Posture Management (KSPM)

Protect Kubernetes clusters running in cloud-managed services, on-premises, and in self-managed K8s and OpenShift clusters. Analyze all container components of a Kubernetes cluster for risky permissions, malware, account usage, and configuration. Get a complete inventory of what's running and its severity level, and route remediation to the resource owner by initiating pull requests in the console.



## 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.



# 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.

Identity × Identity Typ	identity Act	count is CTF	Development (2000 × Iden	tity Labels × Originators × Perm	tissions × Permission Scope ×	15 items Group by Identities
Permission Category ×	Granted Through	× Conditio	ns × Resources × Resource Type	e × Resource Account is CTF Produ	ction (570 ×	
Resource Labels is PII ×	Resource Scope	× Usage	× +			
Q, Search			Originators	Permissions	Granted Through	Resources
<ul> <li>Select all</li> </ul>		:156b911d2	AD User   Ermetic Training	s3:AbortMultipartUpload +81	AdministratorAccess     AdministratorAccess     AdministratorAccess     AdministratorAccess     *1	DevAccountRole
OS Unpatched			AWS IAM Access Analyzer Service   AWS	s3:GetBucketAcl +4	AccessAnalyzerServiceRolePolicy +1     IAM Managed Policy AWS	Bi-wielding-bucket-a
🛃 Pil			AWS Support     Service   AWS	s3:GetAccelerateConfiguration +26	AWSSupportServiceRolePolicy +1     IAM Managed Policy   AWS	pi-wielding-bucket-a S3 Bucket   CTF Proc
Privileged			AWS Trusted Advisor Service   AWS	s3:GetBucketAcl +8	AWSTrustedAdvisorServiceRolePolicy     IAM Managed Policy   AWS	+1 pi-wielding-bucket- S3 Bucket   CTF Proc
Public				s3:AbortMultipartUpload +80	AmazonS3FulAccess +1     IAM Managed Policy   AWS	pli-wielding-bucket- S3 Bucket   CTF Proc
Public Compute				s3:AbortMultipartUpload +81	AdministratorAccess     AdministratorAccess     AMManaged Policy   AWS     AWS	A DevAccountRole
Sensitive				s3:GetAccelerateConfiguration +38	ReadOnlyAccess     MAM Managed Policy   AWS     +1	pli-wielding-bucket-a S3 Bucket   CTF Proc
Trusted Service				s3:AbortMultipartUpload +81	AdministratorAccess     A	A DevAccountRole
Vulnerable				s3:GetAccelerateConfiguration +38	ReadOnlyAccess +1     IAM Managed Policy   AWS	pii-wielding-bucket-

## 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 Requ	iests	+ Request Permission			
🗸 😶 Pending					2
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	よ Mary Smith	合 prd-data	BigQuery Reader	2 Days	× Deny × Approve
> 🕑 Active					0
- C History					2
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	🎝 Ahmud Haddad	🙏 PRD_BKD	Contributor	1 Week	Denied by admin 09:25 am Nov 21, 2022
Oct 24, 2021 04:23 pm	🌡 Ben Calinescu	A PRD_BKD	Contributor	1 Week	Expired 07:00 am Nov 16, 2022

#### About Tenable

Tenable<sup>®</sup> is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's Al-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 more than 44,000 customers around the globe.