



# HOLISTIC SECURITY FOR AWS, AZURE AND GCP

COMPREHENSIVE CLOUD-NATIVE APPLICATION  
PROTECTION FOR MULTI-CLOUD ENVIRONMENTS



# Table of Contents

<b>Executive Summary</b>	03
--------------------------	----

<b>What Is CNAPP?</b>	03
-----------------------	----

<b>Tenable Cloud Security: Streamline Your Cloud Security Strategy with Comprehensive CNAPP</b>	04
---	----

Visualize and manage all your cloud assets

Assess and prioritize risk across the cloud stack

Secure identities and entitlements, and enforce least privilege: CIEM

Protect workloads and manage vulnerabilities: CWP

Monitor Kubernetes clusters for risk and compliance: KSPM

Auto-remediate with simplicity and accuracy

Accelerate cloud detection and response: CDR

Enforce compliance: CSPM

Shift left with infrastructure as code (IaC) security

Self service, just-in-time (JIT) access management

<b>Why Organizations Choose Tenable</b>	12
---	----

<b>Take Action to Improve Your Cloud</b>	13
--	----

## EXECUTIVE SUMMARY

Cloud infrastructure is the new datacenter for many organizations, making it a key target for malicious actors. The order of the day for any organization deploying a cloud application is to reduce your attack surface, and to detect and remediate potential threats as quickly as possible.

Efforts to secure cloud infrastructure are hampered by myriad issues: fast cloud adoption, multiple cloud providers, a shortage of cloud and security expertise, a new perimeter that replaces the network with identities and the cloud's dynamic nature.

Many organizations reach first for cloud provider security tools or try to piece together familiar security technologies. But cloud risk is elusive. Cloud security needs a holistic, automated approach to be able to detect and remediate risk at scale. Enter CNAPP.

Tenable Cloud Security is a comprehensive Cloud-Native Application Protection Platform (CNAPP) for AWS, Azure and GCP. The solution empowers organizations to efficiently detect and minimize cloud infrastructure risk, and secure the new perimeter.

## WHAT IS CNAPP?

CNAPP solutions offer an integrated set of technologies that protect cloud applications and data from development to runtime. CNAPP replaces siloed cloud security solutions, which provide only partial coverage, and often create overhead and friction. A CNAPP solution encompasses many capabilities, with the essentials being cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), cloud workload protection (CWP), Kubernetes security posture management (KSPM) and infrastructure as code (IaC) scanning.

CNAPP simplifies cloud security for all involved, including the Security, DevOps, DevSecOps, IAM and IT teams. By using CNAPP, these disciplines can work collaboratively to continuously improve cloud security posture and govern access effectively without adverse impact to application continuity or time to market.

### CNAPP enables organizations to:

- See more clearly into risk and **improve the accuracy of remediation**
- Reduce the tools and effort in **securing cloud environments**
- Keep up with frequent **release cycles**

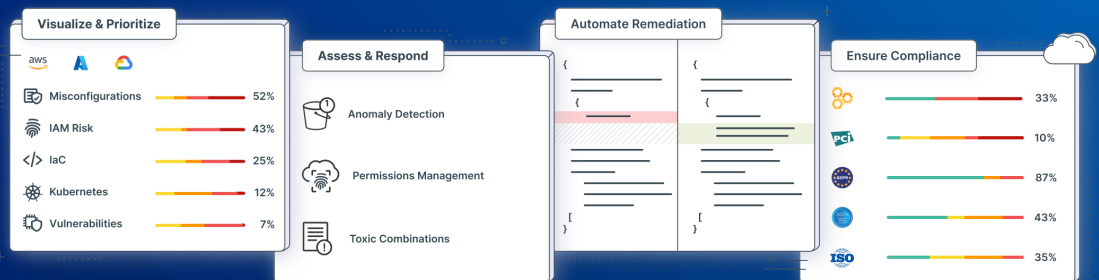
# TENABLE CLOUD SECURITY: STREAMLINE YOUR CLOUD SECURITY STRATEGY WITH COMPREHENSIVE CNAPP

Tenable Cloud Security is a complete CNAPP solution that automates complex cloud infrastructure security for AWS, Azure and GCP environments. An agentless SaaS solution, Tenable Cloud Security unifies full asset discovery, deep risk analysis, runtime threat detection and compliance reporting, combined with pinpoint visualization and guided remediation.

Tenable's unique comprehensive approach provides actionable visibility into risky access and toxic scenarios that put data at risk, reducing your cloud's attack surface and blast radius. Using Tenable, you can ramp up your security from development to production, driving a zero-trust strategy across your environment and democratizing security efforts throughout your organization.

Best of all, the Tenable solution deploys in minutes and delivers actionable insights within hours.

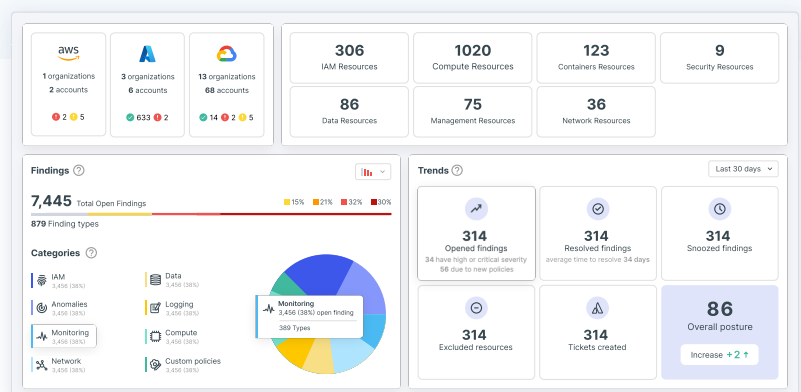
*Tenable Cloud Security provides holistic cloud security spanning the application lifecycle*



## VISUALIZE AND MANAGE ALL YOUR CLOUD ASSETS

Tenable Cloud Security provides a complete asset inventory for AWS, Azure and GCP, so you can manage all cloud resources, including workloads, identities, data, network and more, in one place. The platform provides deep visibility, enabling you to investigate configurations, permissions, and relationships to understand all cloud risks. Tenable continuously monitors your single- or multi-cloud environment, discovering and categorizing all resources and visualizing them in a meaningful, multi-dimensional context. Smart search and query tools let you drill down easily to understand more.

- ✓ Leverage a centralized dashboard for instant insights about any resource in your cloud
- ✓ Asset classification - granular resource labeling for pinpointing greatest risks



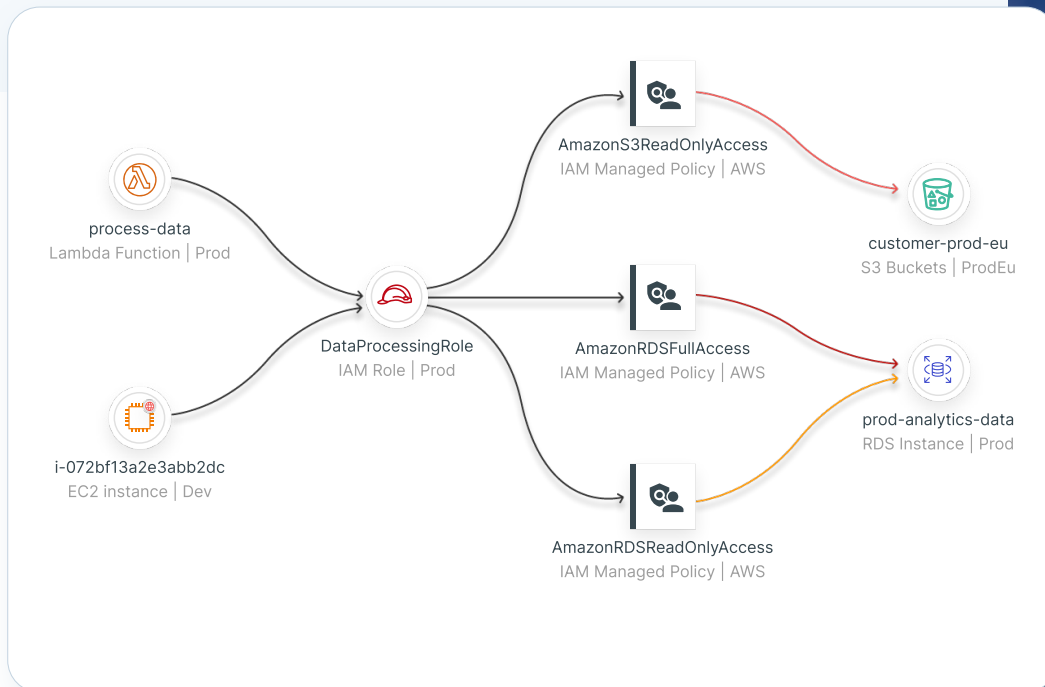
*Centralize visibility into all resources – including infrastructure, workloads, identities and data – in your single- or multi-cloud environment*



# ASSESS AND PRIORITIZE RISK ACROSS THE CLOUD STACK

Tenable Cloud Security applies full stack analysis to surface, contextualize and prioritize risk, including the toxic scenarios that can expose sensitive workloads and data. By continuously monitoring all cloud resources - workloads, identities, vulnerabilities, network and data - Tenable identifies risks, including misconfigurations, workload vulnerabilities, over-privileged permissions, public exposure of resources, flaws in IaC, and Kubernetes misconfigurations. Detailed, actionable insights point teams precisely toward what to address first, and save time on manual analysis and sifting through false positives.

- ✔ Simplify risk assessment with contextualized visualization and findings
- ✔ Focus first on what matters most

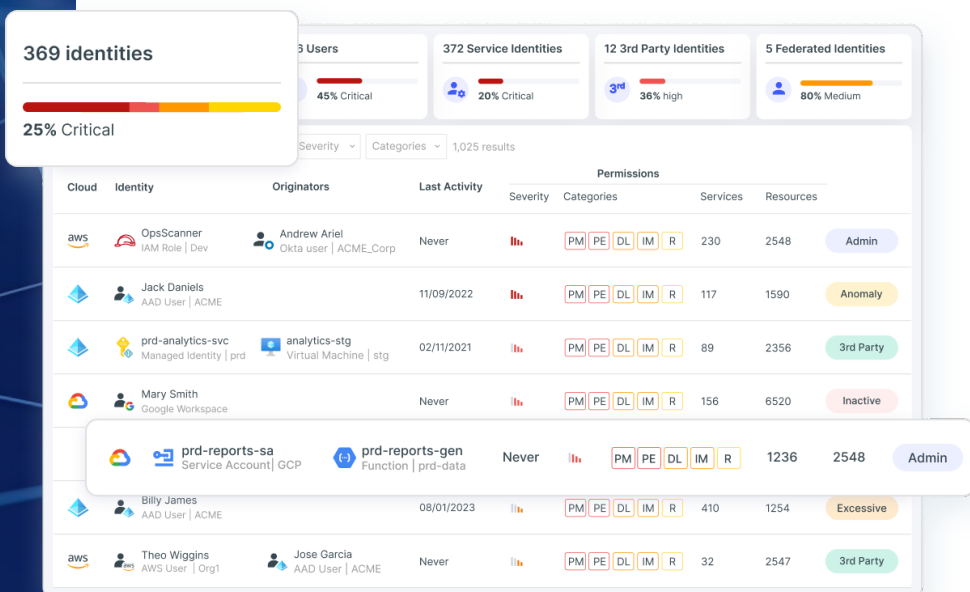


*Assess vulnerabilities, toxic scenarios and other security gaps prioritized by severity and with risk context revealed*

- ✓ Apply optimized policies, reducing permissions without disrupting productivity
- ✓ Enforce a zero-trust strategy across your cloud, minimizing your attack surface

## SECURE IDENTITIES AND ENTITLEMENTS, AND ENFORCE LEAST PRIVILEGE: CIEM

Tenable Cloud Security is the market leader in securing cloud identities and entitlements – the category known as cloud infrastructure entitlement management (CIEM). The platform discovers all identities (i.e. human, service, native/IAM, federated and third party) and their complex permissions, as well as all resources and activities in your cloud environment, giving deep, contextualized visibility into the state of entitlements. Applying full-stack analysis derived from a deep understanding of cloud infrastructures and permissions models, Tenable reveals and prioritizes precise risk findings such as excessive and inactive permissions, risky privileges, network exposure, leaked secrets and misconfigurations, as well as hidden toxic scenarios that put data at risk. The identity-first platform leverages its risk intelligence to generate right-sized, resource-level policies based on actual need to enforce least privilege. It offers guided automated remediation through one-click wizards, integration with existing workflows and easy-to-use code snippets for CI/CD pipelines. Tenable integrates with native and external identity providers and provides powerful access investigation tools.

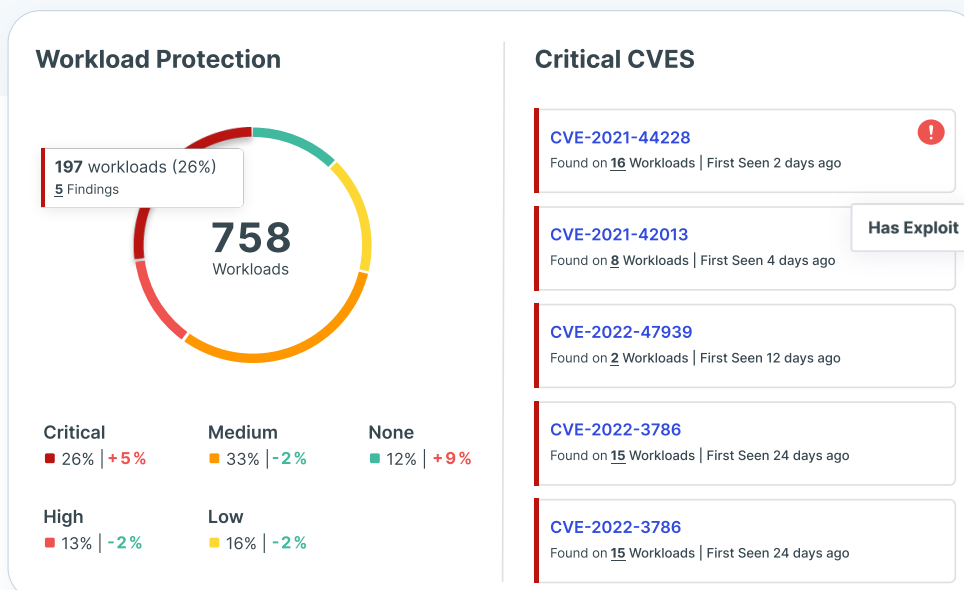


*Gain high-resolution visibility into each identity, the resources it can access, the actions it can perform and the permissions it actually needs*

# PROTECT WORKLOADS AND MANAGE VULNERABILITIES: CWPP

Tenable Cloud Security continuously scans virtual machines, containers and serverless functions, detecting and visualizing workload vulnerabilities, misconfigurations, malware and exposed secrets. As an integrated solution, the platform provides contextual prioritization of workload risk that takes into account everything from cloud configuration and network exposure to IAM and Kubernetes risk. Using an agentless approach, the platform helps Security, DevOps and DevSecOps teams prioritize mitigation by understanding which resources are the most vulnerable and/or have the largest blast radius. Tenable also monitors workload compliance, scanning for violations across standards such as AWS Well Architected, NIST, ISO 27001, SOC II, and implementing mitigating security controls.

- ✓ Gain visibility into the security posture of all your cloud workloads
- ✓ Detect and prioritize vulnerabilities in the context of infrastructure configuration, network exposure, permissions and other risks



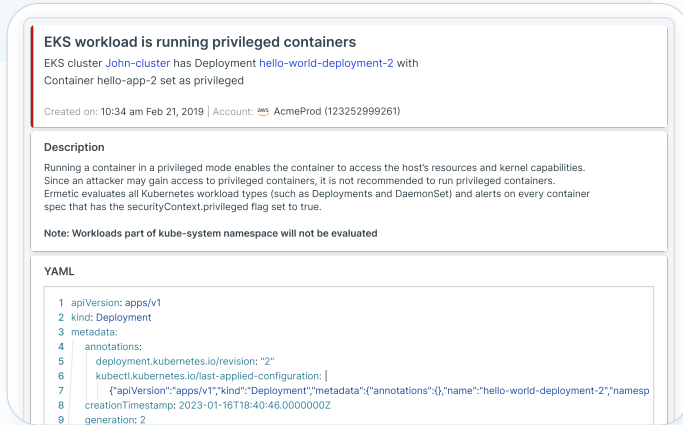
*Protect cloud workloads and focus remediation efforts on the vulnerabilities that matter most*



Detect and prioritize risk including toxic scenarios in context



Ensure compliance with standards such as CISA and CIS benchmarks for Kubernetes



*Enforce security best practices, compliance standards and organizational policies within Kubernetes clusters*

## MONITOR KUBERNETES CLUSTERS FOR RISK AND COMPLIANCE: KSPM

Tenable Cloud Security automates security and compliance for Kubernetes environments. The platform creates an inventory of all Kubernetes resources, including nodes, namespaces, deployments, servers and service accounts, and monitors them for configuration flaws, risky privileges, toxic scenarios, non-compliance and other issues. Tenable brings deep multi-cloud visibility, full-stack risk analysis and guided remediation to the management of Kubernetes security posture, reducing the cloud attack surface.

## AUTO-REMEDiate WITH SIMPLICITY AND ACCURACY

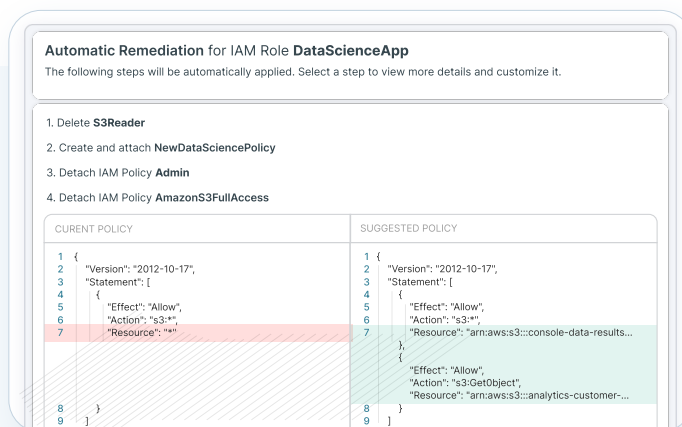
Tenable Cloud Security empowers organizations to simplify and accelerate risk remediation by ticketing detailed remediation instructions and, when possible, executing automated responses. The platform provides flexible remediation options including one-click remediation, optimized policies and configuration fixes fed into service tickets and IaC snippets provided directly in Terraform and CloudFormation. Tenable integrates with many platforms including Splunk, Datadog, Slack, ServiceNow and Jira, fitting seamlessly into existing IT and DevOps workflows.



Use step-by-step guidance and automatically generated policies to remediate accurately



Deliver developer-friendly findings to improve collaboration on remediation at scale



*Fix misconfigurations, policy violations and risky permissions with guided and automated remediation including seamless workflow integration*



# ACCELERATE CLOUD DETECTION AND RESPONSE: CDR

Tenable Cloud Security finds the signal in the noise to spot suspicious and unusual activity, quickly identifying cloud threats and making investigations easier. The platform applies continuous behavioral analysis against baselines based on built-in and custom policies, detecting and prioritizing anomalies such as unusual data access or suspicious activity like reconnaissance. Tenable correlates detected threats with the underlying cloud architecture to identify the root cause and make it easy for teams to understand the context of each risk. Intuitive visualization and smart querying of enriched, contextual activity logs simplifies investigation. The solution auto-alerts with accuracy and integrates with SIEM solutions, accelerating response.



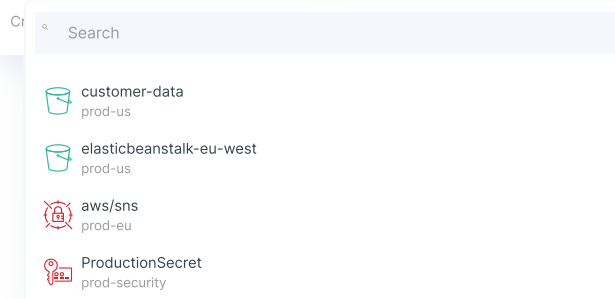
Monitor threats that pose potential malicious intent to your most critical assets



Drive rapid triage, forensics and response, reducing the potential impact of a breach

## Unusual Data Access

Role **AnalyticsApp** was observed accessing 4 data resources that were not accessed before



*Accelerate threat investigation and response with automated anomaly detection, enriched data sources and intuitive query tools*



Automatically assess compliance posture against tens of industry frameworks



Ensure consistency across your multi-cloud environment

Standard	Summary	
>  PCI DSS v4.0	<div><div></div></div> 10%	↓
>  AWS Well-Architected Framework	<div><div></div></div> 31%	↓
>  CIS Benchmark for AWS v1.5.0	<div><div></div></div> 61%	↓
>  GDPR	<div><div></div></div> 57%	↓
>  HIPAA	<div><div></div></div> 70%	↓
>  ISO 27001	<div><div></div></div> 55%	↓
>  NIST SP 800-53 Rev5	<div><div></div></div> 38%	↓
>  SOC2 Type II	<div><div></div></div> 49%	↓
>  CIS Benchmark for GKE 1.3.0	<div><div></div></div> 68%	↓

*Simplify cloud compliance with continuous assessment, and guided and automated remediation*

# ENFORCE COMPLIANCE: CSPM

Tenable Cloud Security continuously scans configurations and resources across clouds, identifies violations and automates remediation. The platform maps risks against industry standards and best practices, enabling you to manage compliance with regulations, frameworks and benchmarks, including GDPR, HIPAA, ISO, NIST, PCI, SOC2, CIS, AWS Well Architected and Kubernetes standards. Custom templates let you define organizational policies and the actions to be taken when a violation is detected. Using Tenable's reporting capabilities, you can generate scheduled or on-demand reports to provide high-level posture assessment for auditors, reviewers and other stakeholders.

# SHIFT LEFT WITH INFRASTRUCTURE AS CODE (IaC) SECURITY

Tenable Cloud Security enables organizations to implement shift-left security by scanning, detecting and fixing misconfigurations, compliance violations, high privileges and other risks in infrastructure as code. It helps developers and DevOps teams detect and resolve issues early – hardening cloud infrastructure environments as part of the CI/CD pipeline. The platform also enables teams to automatically remediate security findings in their native IaC environments. Tenable integrates with source code repositories, improving communication by enabling teams to comment and suggest fixes.

- ✓ Embed comprehensive cloud security checks in native development tools including Jenkins, BitBucket, CircleCI, GitHub and GitLab
- ✓ Automate remediation in existing workflows via guided remediation-as-code

**cody-smith** Develop - new service (ticket #4331) Latest commit 3fgh75 7 days ago Blame

1 resource "aws_db_instance" "mysql-app" {	1 resource "aws_db_instance" "mysql-app" {
2 allocated_storage = 10	2 allocated_storage = 10
3 db_name = "mydb"	3 db_name = "mydb"
4 engine = "mysql"	4 engine = "mysql"
5 instance_class = "db.t3.micro"	5 instance_class = "db.t3.micro"
6 storage_encrypted = false	6 storage_encrypted = true
7 username = "foo"	7 username = "foo"
8 password = "foobar"	8 password = "foobar"
9 }	9 }

*Shift left with IaC scanning and CI/CD integration, and guided remediation-as-code*

# SELF SERVICE, JUST-IN-TIME (JIT) ACCESS MANAGEMENT





Highly-privileged access to sensitive cloud environments is a significant challenge for organizations. Engineering teams are often granted “always on” elevated access when only brief, intermittent access is needed. Tenable Cloud Security helps you achieve zero standing privileges through a just-in-time (JIT) access portal that grants authorized, fine-grained, least-privilege access for a predefined period of time and revokes the temporary permissions right after. Developers quickly submit a request, automatically notify approvers and gain temporary access, saving time in getting the access they need. Tenable lets you continuously audit user activity during JIT approved elevated sessions and generate reports for all JIT access requests and authorizations.

- ✓ Save developers time with easy, automated access request and consent
- ✓ Secure privileged access with fine-grained entitlement management

Access Requests







+ Request Permission

⌵ Pending

Created	Requestor	Account	Permission	Duration	
Jun 15 2021 08:23 am	 Theo Wiggins	 prd-svc-...	Power user	3 Hours	<div><div>✗ Deny</div><div>✓ Approve</div></div>
Jun 22 2021 11:13 am	 Mary Smith	 prd-data-...	BigQuery Reader	2 Days	<div><div>✗ Deny</div><div>✓ Approve</div></div>

> Active

⌵ History

Created	Requestor	Account	Permission	Duration	Status
Nov 6, 2021 10:34 am	 Robert Garcia	 eu-stg-mks	Read-only	4 Weeks	<div><div>Cancelled by me 10:34 am Nov 7, 2022</div></div>
Nov 20, 2021 04:23 pm	 Ahmud Haddad	 PRD_BKD	Contributor	1 Week	<div><div>✗ Denied by admin 09:25 am Nov 21, 2022</div></div>
Oct 24, 2021 04:23 pm	 Ben Calinescu	 PRD_BKD	Contributor	1 Week	<div><div>⌚ Expired 07:00 am Nov 16, 2022</div></div>

*Facilitate privileged access for developers with quick requests and approvals while ensuring least privilege and avoiding long-standing privileges*



## WHY ORGANIZATIONS CHOOSE TENABLE

The Tenable CNAPP solution cuts through cloud complexity to secure the complete cloud infrastructure lifecycle from development to deployment. The platform empowers stakeholders with pinpoint accuracy in prioritizing and remediating risk, and simplifying and speeding up cloud security efforts.



Overcome gaps in security expertise with **powerful visualization** and **ease of use**



Move quickly from **insight to action** with **accurate risk prioritization**, and **guided and automated remediation**.



**Secure the new perimeter – cloud identities** – enforcing least privilege and zero trust



Accelerate cloud security efforts among **DevOps, IAM, IT, and security and risk teams**



## About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at [www.tenable.com](http://www.tenable.com).

# TAKE ACTION TO IMPROVE YOUR CLOUD SECURITY TODAY

Tenable offers organizations of all sizes a better way to ensure cloud security. It simplifies even the most complex issues and can deliver ROI to the tune of saving tens of thousands of person-hours.

Most importantly, Tenable moves the security needle forward as you adopt cloud and scale, providing accurate findings that foster trust and collaboration in staying on top of risks and threats, and pre-empting risk from the earliest development stage.

## About Tenable Cloud Security

Tenable Cloud Security reveals, prioritizes and remediates security gaps in cloud infrastructure. It unifies and automates full asset discovery, deep risk analysis, runtime threat detection and compliance, and empowers stakeholders with pinpoint visualization, guided recommendations and collaboration. Tenable Cloud Security is a comprehensive cloud-native application protection platform (CNAPP) spanning cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), cloud workload protection (CWPP), Kubernetes security posture management (KSPM) and infrastructure as code (IaC) security.

---

## Contact Us:

Please email us at [sales@tenable.com](mailto:sales@tenable.com) or visit [tenable.com/contact](https://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.