tenable | Data Sheet

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.

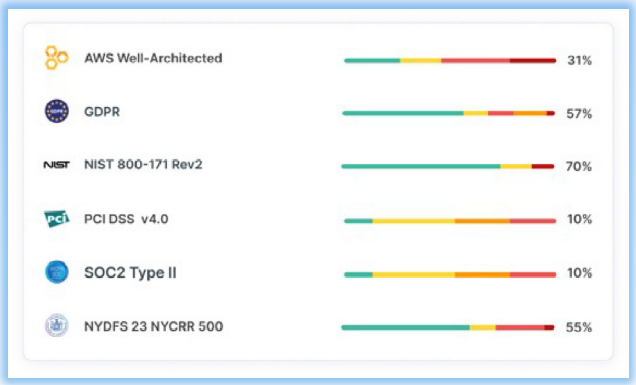
- **Scalable cloud expertise**

  Democratize insights and accelerate organizational security efforts with an intuitive solution that empowers anyone to become an expert on their cloud environment.

Key capabilities

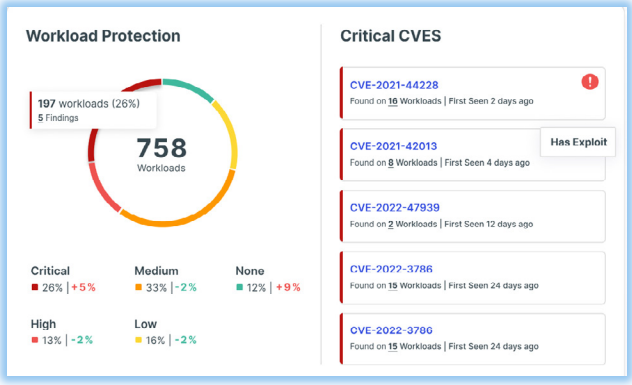
Cloud Security Posture Management (CSPM)

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.



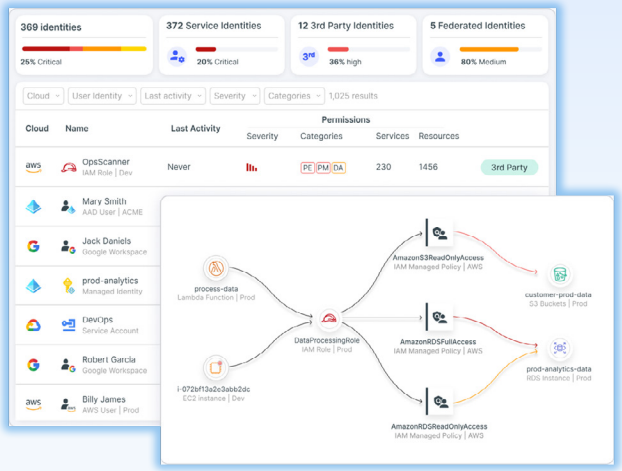
Cloud Workload Protection (CWP)

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.



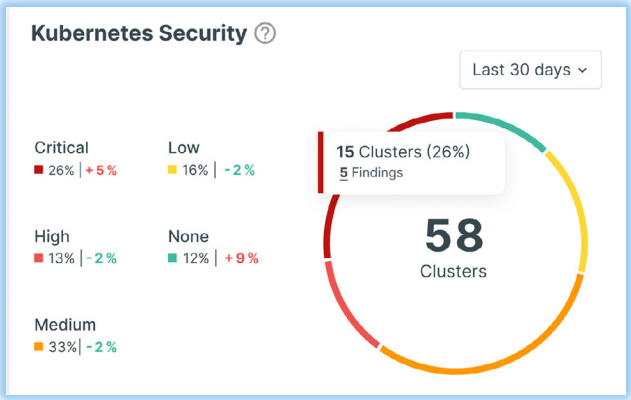
Cloud Infrastructure Entitlement Management (CIEM)

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.

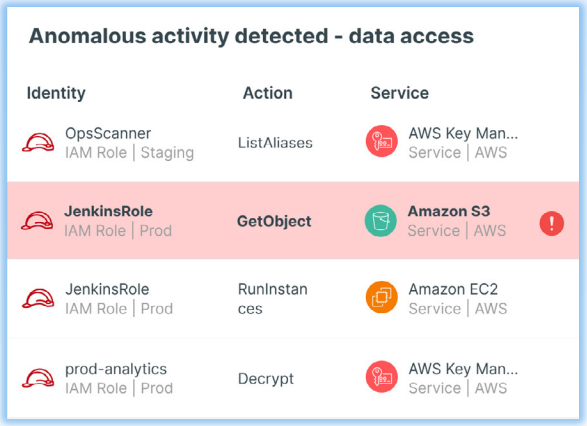


Infrastructure as Code Security (IaC)

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.

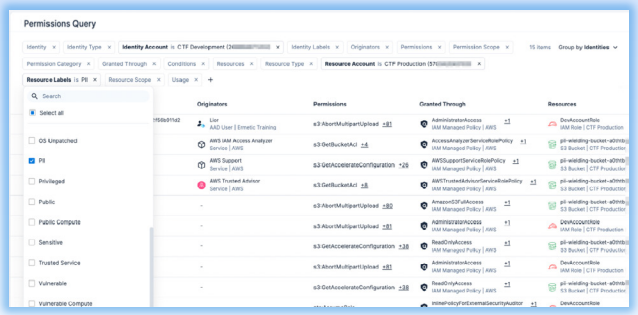
Cloud Detection and Response (CDR)

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.



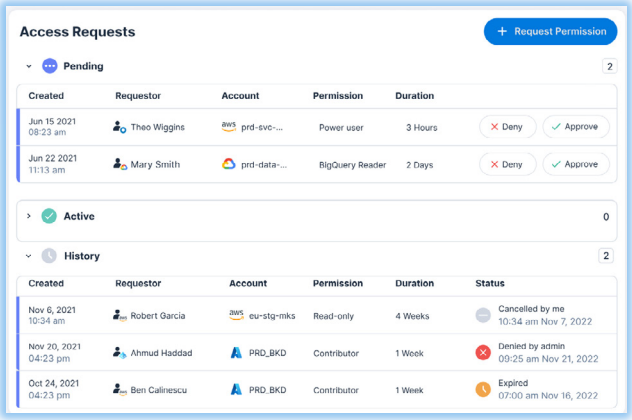
Data Security Posture Management (DSPM)

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.



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.



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.

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.

040325