tenable | Data Sheet

Data Security Posture Management (DSPM)

Data security in a unified cloud security solution

Improve cloud data security with discovery, classification and prioritization of data exposure risk

Data fuels innovation in the cloud, but the volume and complexity in hybrid and multi-cloud environments makes it difficult to secure. Siloed data security solutions produce many critical alerts, but how do security teams know if those risks should take priority over other exposures like an over privileged virtual machine or a workload with a severe CVE? If everything is "critical," nothing is, and security teams are left guessing where they should direct their remediation efforts.

While there are many cloud exposures to manage, data risks aren't something to ignore. Whether it's a breach of customer information, financial records, or intellectual property, unauthorized access to data can have severe regulatory and reputational consequences.

Tenable Cloud Security integrates Data Security Posture Management (DSPM) into its Cloud-Native Application Protection Platform (CNAPP). This unifies cloud security processes and enables teams to take action on the most threatening exposures without adding new tools or workflows.

Tenable Cloud Security surfaces risk from across the attack surface, including vulnerabilities, misconfigurations, excess privileges, and data. It uses this risk context to provide prioritized and actionable remediation guidance.

Key benefits

Gain complete visibility of your cloud data

- See all new data and new data resources as soon as they are created or modified and define your own data labels
- Get real-time data analysis to understand sensitivity and context within the attack surface

Proactively identify cloud data exposure

- Monitor data resource usage and identify anomalous access to data
- Reduce data exposure with identity and access insights

Reduce the likelihood of a data breach

- Enforce data protection and access best practices
- Remediate misconfigurations of sensitive resources

Get answers to tough cloud data security questions and close exposures faster

Protecting data in public cloud environments starts with answering three seemingly simple security questions.

- **What type of data do I have in the cloud? How is it classified? Is it sensitive?**
- **Where is my sensitive data in the cloud? Who has access?**
- **What are the risks to my cloud data?**

Tenable Cloud Security answers these tough cloud data security questions in an intuitive user interface. Agentless scanning continuously monitors your hybrid and multi-cloud environments to discover and classify data types, assign sensitivity levels, and reduce the likelihood of a data breach. Using built-in and customizable policies to identify risks, Tenable improves data controls by evaluating configuration and automatically provides remediation recommendations to close exposures and meet privacy and compliance requirements.

Find and classify data across hybrid and multi-cloud environments

Tenable Cloud Security uses APIs to perform agentless data store scans, allowing users to find shadow or unknown data and improve data hygiene across environments. Objects in cloud storage buckets are scanned to classify data into categories. They are then assigned a sensitivity level based on type and the findings are reflected in the Tenable Cloud Security dashboard.

If sensitive data is detected, users can explore what makes it sensitive and where it resides. Users can create custom Rego expressions to identify country or industry-specific data types, so sensitivity analysis and classification can be tailored to organizational security goals.

Prioritize data exposure with personalized precision

Exposing and closing data exposure isn't just about inventorying risk, it's about investigating why it's risky in the first place and its potential blast radius. Data risk context enriches other Tenable Cloud Security findings such as misconfigurations or IAM risks. Users can also create custom data labels or import them in from cloud environments to prioritize the exposures specific to organizational security goals.

Reduce risk by eliminating unnecessary access to data

Understand who has access to sensitive data and what they can do with that access. Tenable Cloud Security Permissions Query allows users to perform flexible and granular searches to expose cloud resources with identity risks and include sensitive data. This identity-intelligent risk correlation finds the pathways attackers could exploit to cause a breach. Block these attack pathways by remediating excessive permissions and use the Just-in-Time access provisioning add-on to preventatively reduce static or longstanding permissions.

Improve data compliance posture

With one-click compliance reporting, users can communicate the exposure of their multi-cloud environment and report on the risks to PII, PHI, PCI and other sensitive data. View compliance posture in the moment and over time with trend dashboards that demonstrate improvement to leadership.

Scale cloud adoption without leaving data security behind

With Tenable, security teams get a comprehensive view of their cloud data and the risks associated with it—even as their cloud footprint grows. Data classification takes place in-region and never leaves the environment so there's no impact on production workloads or compliance with regulatory standards. Tenable Cloud Security also reduces the risk of false positives by using a mix of context and content. The solution looks for indicators of sensitive information and then analyzes the content based on context from logic patterns. This filters out irrelevant content like synthetic or test data which many other solutions commonly report as false critical alerts.

With DSPM functionality integrated as part of a unified CNAPP, teams can focus on the risks that matter most—regardless of where those risks are in their cloud environments.

Tenable Cloud Security

Tenable Cloud Security is the actionable cloud security platform, rapidly exposing and closing priority security gaps caused by misconfigurations, risky entitlements and vulnerabilities. These weaknesses are the epicenter of cloud risk. Tenable is a world leader at isolating and eradicating these exposures at scale across infrastructure, workloads, identities and data.

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 more than 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.