tamnoon | sentra

Using Data Sensitivity in Cloud Asset Criticality

Enriching CNAPP / CSPM alerts with DSPM context

The Challenge

Cloud-native application protection platforms (CNAPPs) were not designed to provide visibility into the underlying data classification of resources.

For example, it's common for similar misconfigurations to be flagged with the same criticality ratings, even if the data within one misconfigured asset is far more sensitive than the data within another.

Without this data-awareness context, security teams have a hard time evaluating the actual priority of these alerts, and focus on what matters most.

Data Security Posture Management (DSPM) solutions like Sentra excel in classifying and assessing data sensitivity, offering critical insights into the actual importance of the underlying data.

Adding this layer of additional information coming from the DSPM into CNAPP alerts can prove to be very useful when deciding which alerts to tackle first.

Our Integrated Solution

Tamnoon integrates with CNAPPs and CSPMs to deliver human-verified, actionable remediation plans. By incorporating Sentra's DSPM insights, Tamnoon prioritizes cloud misconfigurations based on whether an asset contains sensitive data, such as PII, customer data, or credentials.

This hybrid approach—combining insights about the data an asset holds with its associated security issues—ensures that highly sensitive assets are prioritized, enabling the rapid remediation of critical cloud vulnerabilities.

Business Impact and Key Benefits

Enrich CNAPP Alerts With Data Context

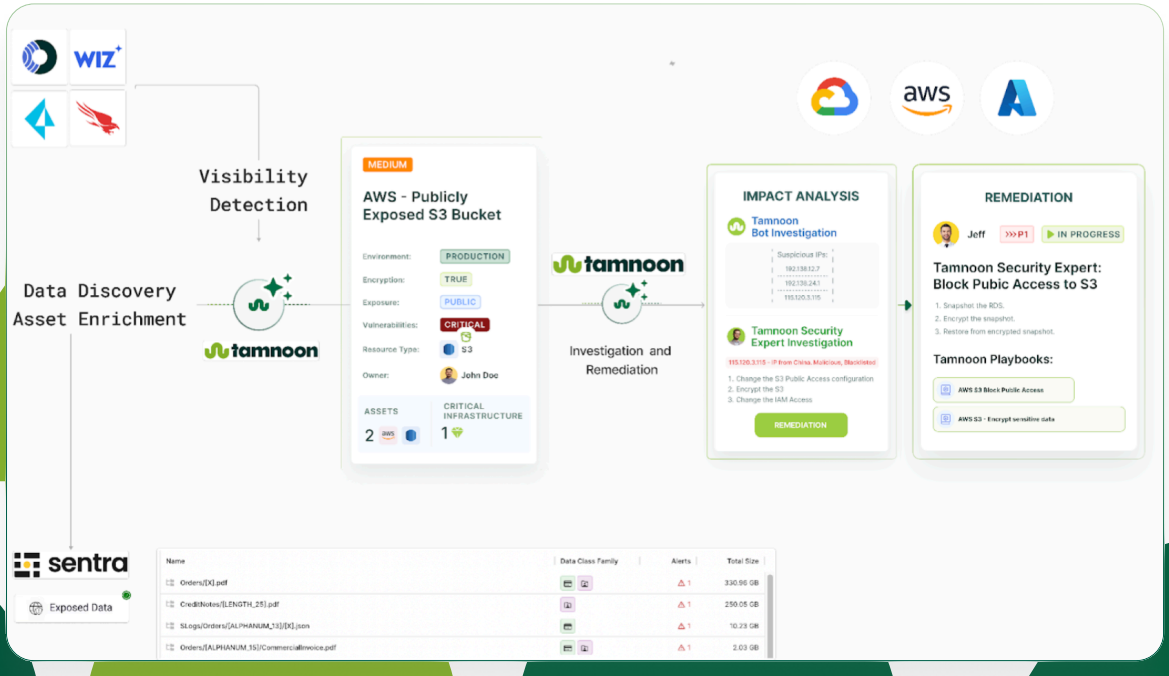
- Understand which assets contain which sensitive data and automatically tag them as “critical infrastructure”
- Automatically prioritize alerts using data context directly inside Tamnoon’s remediation platform
- Calculate the business impact of a vulnerability by identifying if any sensitive or regulated data is at risk

Remediate Issues Effectively

- Align security, engineering, and data teams on the issue’s importance by tying it directly to the risk of data exposure.
- Avoid wasting time on assets that don’t hold valuable or sensitive information, and focus on the ones that do.
- Use Tamnoon’s developer-friendly handoff process and playbooks to save your engineers time and effort

Actively Protect Your Organization

- Enjoy ongoing, automated monitoring continuously from Sentra as new sensitive information is added
- Defend assets holding valuable data from cloud threats using Tamnoon’s prevention mechanisms
- Stay compliant with leading standards such as PCI-DSS, HIPAA and GDPR by actively working on issues that could lead to data exfiltration



Use Cases in Action

The Tamnoon x Sentra collaboration at work:

Prioritizing Sensitive Exposed Resources

CNAPP

Generates five critical alerts for publicly exposed S3 buckets

sentra

Identifies three buckets containing PII and customer data

tamnoon

Prioritizes these three alerts, boosting their criticality and creating high-priority remediation tasks

Highlighting High-Risk IAM Roles

CNAPP

Flags ten IAM roles with over-permissive access

sentra

Highlights one role with access to sensitive data

tamnoon

Prioritizes this role, boosting its severity and creating a task for immediate remediation

Focusing on Critical Data in Publicly Exposed Databases

CNAPP

Generates critical alerts for three RDS instances with public IPs

sentra

Identifies one RDS containing customer SSNs and loan information

tamnoon

Prioritizes this alert, enhances its criticality, and generates a remediation task