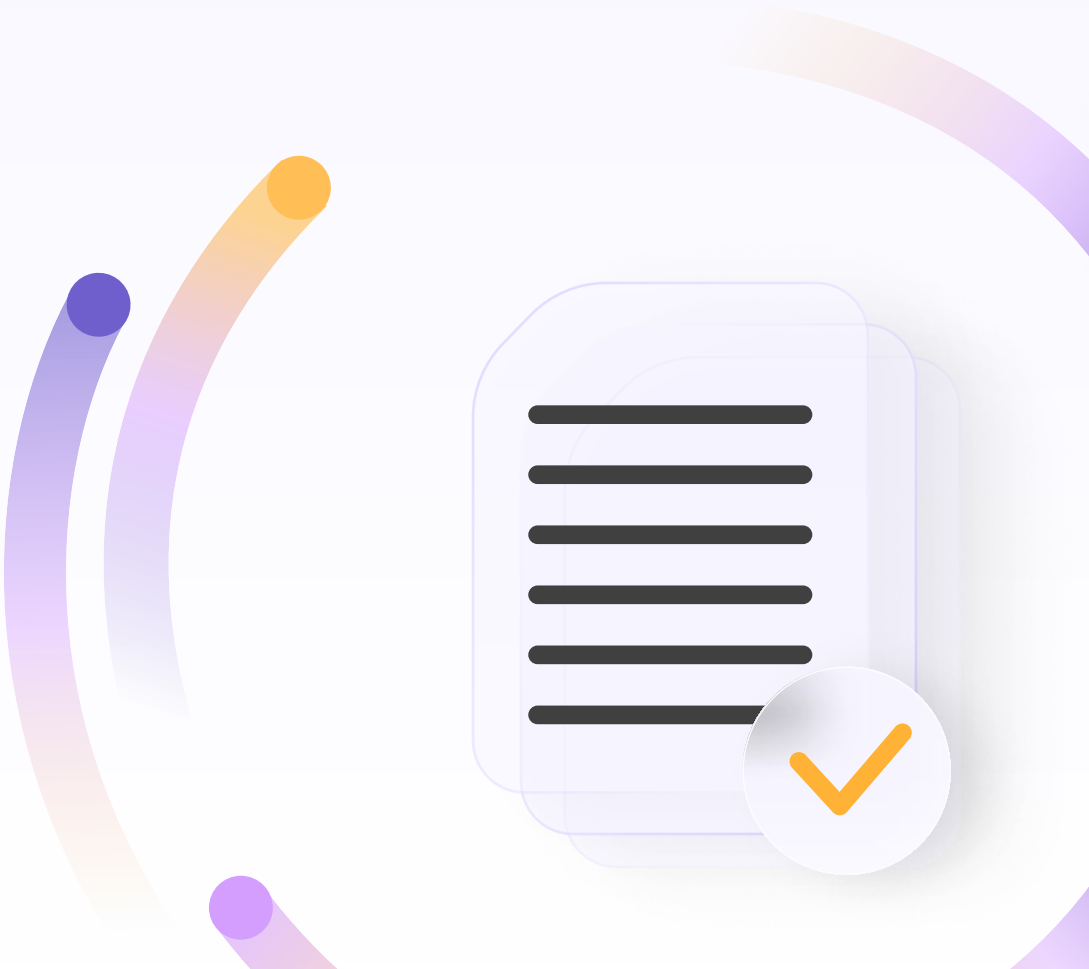
sentra

Request for Proposal (RFP) Guide

Data Security Platform (DSP) & Data Security Posture Management (DSPM)



Introduction

This RFP Guide is designed to help organizations create their own RFP for selection of Cloud-native Data Security Platform (DSP) & Data Security Posture Management (DSPM) solutions. The purpose is to identify essential requirements that will help you choose a solution to enable effective discovery, classification, and protection of sensitive data.

Instructions for Vendors

Each section provides essential and recommended requirements to achieve a best practice capability. These have been accumulated over dozens of customer implementations. Customers may also wish to include their own unique requirements specific to their industry or data environment.

1. Data Discovery & Classification

Requirement	Details
Shadow Data Detection	Can the solution discover and identify shadow data across any data environment (IaaS, PaaS, SaaS, On-Premises)?
Sensitive Data Classification	Does the solution support smart sampling of large file shares and data lakes to reduce and optimize the cost of scanning and provide full scan coverage in less time?
AI-based Classification	Does the solution leverage AI/ML to classify data in unstructured documents and stores (Google Drive, OneDrive, SharePoint, etc) and achieve more than 95% accuracy?
Data Context	Can the solution discern and 'learn' the business purpose (employee data, customer data, identifiable data subjects, legal data, synthetic data, etc.) of data elements and tag them accordingly?
Data Store Compatibility	Which data stores (e.g., AWS S3, Google Cloud Storage, Azure SQL, Snowflake data warehouse, On-Premises file shares, etc.) does the solution support for discovery?
Data Perimeters Monitoring	Can the solution track data movement between storage solutions and detect risky and non-compliant data transfers and data sprawl?

2. Data Access Governance

Requirement	Details
Access Controls	Does the solution map access of users and non-human identities to data based on sensitivity and sensitive information types?
Location Independent Control	Does the solution help organizations apply least privilege access regardless of data location or movement?
Identity Activity Monitoring	Does the solution identify over-provisioned, unused or abandoned identities (users, keys, secrets) that create unnecessary exposures?
Data Access Catalog	Does the solution provide an intuitive map of identities, their access entitlements (read/write permissions), and the sensitive data they can access?
Integration with IAM Providers	Does the solution integrate with existing Identity and Access Management (IAM) systems?

3. Posure, Risk Assessment & Threat Monitoring

Requirement	Details
Risk Assessment	Can the solution assess data security risks and assign risk scores based on data exposure and data sensitivity?
Compliance Frameworks	Does the solution support compliance with regulatory requirements such as GDPR, CCPA, and HIPAA?
Similar Data Detection	Does the solution identify data that has been copied, moved, transformed or otherwise modified that may disguise its sensitivity or lessen its security posture?
Automated Alerts	Does the solution provide automated alerts for policy violations and potential data breaches?
Data Loss Prevention (DLP)	Does the solution include DLP features to prevent unauthorized data exfiltration?
3rd Party Data Loss Prevention (DLP)	Does the solution integrate with 3rd party DLP solutions?
User Behavior Monitoring	Does the solution track and analyze user behaviors to identify potential insider threats or malicious activity?
Anomaly Detection	Does the solution establish a baseline and use machine learning or AI to detect anomalies in data access or movement?

4. Incident Response & Remediation

Requirement	Details
Incident Management	Can the solution provide detailed reports, alert details, and activity/change history logs for incident investigation?
Automated Response	Does the solution support automated incident response, such as blocking malicious users or stopping unauthorized data flows (via API integration to native cloud tools or other workflow solutions)?
Forensic Capabilities	Can the solution facilitate forensic investigation, such as data access trails and root cause analysis?
Integration with SIEM	Can the solution integrate with existing Security Information and Event Management (SIEM) or other analysis systems?

5. Infrastructure & Deployment

Requirement	Details
Deployment Models	Does the solution support flexible deployment models (on-premises, cloud, hybrid)? Is the solution agentless?
Cloud Native	Does the solution keep all data in the customer's environment, performing classification via serverless functions? (ie. no data is ever removed from customer environment - only metadata)
Scalability	Can the solution scale to meet the demands of large enterprises with multi-petabyte data volumes?
Performance Impact	Does the solution work asynchronously without performance impact on the data production environment?
Multi-Cloud Support	Does the solution provide unified visibility and management across multiple cloud providers and hybrid environments?

6. Operations & Support

Requirement	Details
Onboarding	Does the solution vendor assist customers with onboarding? Does this include assistance with customization of policies, classifiers, or other settings?
24/7 Support	Does the vendor provide 24/7 support for addressing urgent security issues?
Training & Documentation	Does the vendor provide training and detailed documentation for implementation and operation?
Managed Services	Does the vendor (or its partners) offer managed services for organizations without dedicated security teams?
Integration with Security Tools	Can the solution integrate with existing security tools, such as firewalls, DLP systems, and endpoint protection systems?

7. Pricing & Licensing

Requirement	Details
Pricing Model	What is the pricing structure (e.g., per user, per GB, per endpoint)?
Licensing	What licensing options are available (e.g., subscription, perpetual)?
Additional Costs	Are there additional costs for support, maintenance, or feature upgrades?

Conclusion

This RFP template is designed to facilitate a structured and efficient evaluation of DSP and DSPM solutions. Vendors are encouraged to provide comprehensive and transparent responses to ensure an accurate assessment of their solution's capabilities.

Sentra's cloud-native design combines powerful Data Discovery and Classification, DSPM, DAG, and DDR capabilities into a complete Data Security Platform (DSP). With this, Sentra customers achieve enterprise-scale data protection and do so very efficiently - without creating undue burdens on the personnel who must manage it.

To learn more about Sentra's DSP, request a demo here and choose a time for a meeting with our data security experts.

sentra