Cloud Security Capability options

This document outlines an options paper one per function (CSPM, SSPM, DSPM), covering core functions, stakeholders, rationale, implications, peer review, technical references, and a structured requirement fulfillment and evaluation model with ratings across compliance, business value, cost effectiveness, delivery, and operability.

CSPM, SSPM and DSPM directly map to strategic security capabilities, namely,

* CSPM > Cloud Configuration & Compliance Assurance
* SSPM > SaaS Application Security & Governance
* DSPM > Cloud Data Security & Risk Visibility

**CLOUD SECURITY POSTURE MANAGEMENT (CSPM)**

## Background

<Enterprise>’s cloud-first strategy and migration to Microsoft Azure introduces new risks associated with cloud infrastructure misconfigurations. To maintain compliance with regulatory requirements and reduce cloud security risk, CSPM is critical in providing visibility, continuous monitoring, and remediation across cloud environments.

## Functions the Security Capability Must Perform

Based on Gartner and industry standards:

* Continuous assessment of cloud resource configurations
* Identification and remediation of misconfigurations
* Visibility across multi-cloud environments
* Policy enforcement based on compliance frameworks (e.g., ISO 27001, APRA CPS 234)
* Automated remediation and alerting
* Integration with CI/CD pipelines
* Risk scoring and prioritization

## Stakeholders

* CISO and Security Operations Team
* Cloud Platform Engineering Team
* Compliance and Risk Management
* Application Owners

## Rationale

Cloud misconfigurations are a leading cause of security breaches. CSPM tools reduce this risk and support a proactive security posture by providing automation, visibility, and real-time remediation.

## Implications

* Potential overlap with CNAPP and SIEM tools
* Need for skilled resources to tune policies and remediations
* Tool integration with Azure and third-party platforms

## Peer Review

Insights from financial sector peers show strong adoption of integrated CNAPP tools for enterprise-wide cloud security management.

## Options Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Option** | **Description** | **Pros** | **Cons** | **Vendors** |
| 1. Native Cloud Tools | Azure Security Center | Cost-effective, easy integration | Limited multi-cloud support | Microsoft Defender for Cloud |
| 2. Standalone CSPM | Purpose-built tools | Best-of-breed, multi-cloud, agentless | Tool sprawl, learning curve | Wiz, Prisma Cloud, Orca |
| 3. CNAPP | CSPM + CWPP + CIEM | Broadest coverage, scalable | High complexity | Prisma Cloud, Wiz, Microsoft CNAPP |

## Technical Reference

* NIST SP 800-190
* Gartner Market Guide for CSPM
* CSA Cloud Controls Matrix

## Requirement Fulfilment

|  |  |  |
| --- | --- | --- |
| Requirement | Fulfilled (Y/N) | Notes |
| Monitoring and Analysis | Y | Real-time monitoring via APIs |
| Security Assessment | Y | Policy-based audits and misconfig checks |
| Security Controls | Y | Integrates with IAM, policies, tags |
| Risk Management | Y | Risk-based prioritization and scoring |
| Compliance | Y | Mappings to CIS, ISO, APRA CPS234 |

## Rating Categories

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vendor | Compliance | Business Value | Cost Effectiveness | Delivery | Operability |
| Prisma Cloud | High | High | Medium | High | Medium |
| Wiz | High | High | Medium | High | High |
| Microsoft Defender | Medium | Medium | High | High | High |

**SAAS SECURITY POSTURE MANAGEMENT (SSPM)**

## Background

<Enterprise> uses a wide range of SaaS applications like Microsoft 365, Salesforce, and Workday. These platforms are outside traditional perimeter controls, making configuration drift and third-party app risk a major concern.

## Functions the Security Capability Must Perform

* Centralized visibility across SaaS platforms
* Misconfiguration detection
* OAuth and third-party app access review
* User permissions and anomaly detection
* Data exposure monitoring
* Compliance reporting

## Stakeholders

* Security Operations
* IT Application Owners
* Compliance and Audit Teams
* Identity and Access Management Team

## Rationale

As SaaS adoption grows, centralized security control becomes critical. SSPM ensures that best practices and regulatory policies are enforced consistently.

## Implications

* Requires integrations across many SaaS APIs
* May require new onboarding processes for SaaS apps
* Needs strong collaboration with IT teams

## Peer Review

Organizations with similar SaaS usage (e.g., financial services) are increasingly adopting dedicated SSPM tools to ensure least privilege and configuration hygiene.

## Options Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Option | Description | Pros | Cons | Vendors |
| 1. Manual Auditing | Manual reviews | Low cost | High risk, not scalable | N/A |
| 2. SaaS-Native Security | Use built-in features | Integrated, low effort | Fragmented view | Microsoft, Salesforce |
| 3. Dedicated SSPM | Specialized SaaS visibility | Deep integrations, alerts | Subscription/licensing | AppOmni, Obsidian, DoControl |
| 4. CASB-integrated SSPM | SSPM via CASB | Broader control, analytics | Less deep config visibility | Netskope, Zscaler |

## Technical Reference

* Gartner Market Guide for SSPM
* CSA SaaS Security Guidelines

## Requirement Fulfilment

|  |  |  |
| --- | --- | --- |
| Requirement | Fulfilled (Y/N) | Notes |
| Monitoring and Analysis | Y | SaaS activity and user behavior |
| Security Assessment | Y | Configuration baselines |
| Security Controls | Y | Enforce via API integrations |
| Risk Management | Y | Detect privilege abuse, OAuth risk |
| Compliance | Y | Maps to ISO, APRA policies |

## Rating Categories

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vendor | Compliance | Business Value | Cost Effectiveness | Delivery | Operability |
| AppOmni | High | High | Medium | Medium | High |
| Obsidian | Medium | Medium | High | Medium | High |
| Netskope SSPM | High | High | Medium | High | Medium |

**DATA SECURITY POSTURE MANAGEMENT (DSPM)**

## Background

<Enterprise> handles sensitive financial, customer, and regulatory data across cloud and SaaS environments. DSPM provides visibility, governance, and protection for that data, addressing modern threats and regulatory pressure.

## Functions the Security Capability Must Perform

* Data discovery and classification (structured/unstructured)
* Access permissions and entitlements review
* Anomalous data access detection
* Shadow data detection
* Data lineage and context
* Compliance mapping (e.g., ISO 27001, CPS 234)

## Stakeholders

* Data Governance Office
* Cybersecurity Team
* Compliance and Risk Management
* Cloud Platform and SaaS Owners

## Rationale

Without visibility into data stores, <Enterprise> cannot effectively protect or govern data. DSPM enables proactive data-centric risk management.

## Implications

* High upfront integration effort
* May require data catalog consolidation
* Must integrate with DLP, IAM, and SIEM solutions

## Peer Review

DSPM is gaining traction in financial services as a more granular extension to DLP and cloud security practices.

## Options Evaluation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Option | Description | Pros | Cons | Vendors |
| 1. Legacy DLP | Extend DLP to cloud | Familiar tools | Lacks cloud-native support | Symantec, Forcepoint |
| 2. CNAPP-integrated DSPM | Bundled into existing platform | Lower cost, easier adoption | May lack deep data visibility | Wiz, Prisma |
| 3. Dedicated DSPM | Standalone data visibility | Deep classification, AI-powered | Emerging category, tool sprawl | Cyera, Laminar, Sentra |

## Technical Reference

* Gartner Hype Cycle for Data Security
* CSA Data Security Lifecycle
* NIST SP 800-53 Rev 5

## Requirement Fulfilment

|  |  |  |
| --- | --- | --- |
| Requirement | Fulfilled (Y/N) | Notes |
| Monitoring and Analysis | Y | Detect sensitive data use/access |
| Security Assessment | Y | Discover data location and flow |
| Security Controls | Y | Role-based access, tagging |
| Risk Management | Y | Context-aware risk scoring |
| Compliance | Y | Maps to APRA, ISO, NIST |

## Rating Categories

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vendor | Compliance | Business Value | Cost Effectiveness | Delivery | Operability |
| Cyera | High | High | Medium | Medium | High |
| Laminar | Medium | Medium | Medium | Medium | Medium |
| Wiz DSPM | Medium | High | High | High | High |