Prisma Cloud DSPM

Limited GA
PCS 24.2.2

Table of Contents

Overview **3**
Key Features and Benefits of Prisma Cloud DSPM 3

Pre-configuration **4**

Configuration **4**
Logging in to DSPM Console 4
Onboarding Cloud Accounts 5
Licensing 6
Offboarding 7

Overview

Prisma Cloud Data Security Posture Management (DSPM), previously known as the Dig Security platform, helps organizations to discover, classify, protect, and govern data across multi-cloud environments.

With Prisma Cloud DSPM, organizations can reduce data misuse, achieve compliance, and prevent ransomware attacks and data breaches. It recently became the first DSPM solution to support Optical Character Recognition (OCR) for image classification, and a pioneer to provide data security for generative AI deployments.

Note: DSPM (Dig Security) has a Limited General Availability (LGA) on the Prisma Cloud platform starting with the 24.2.2 release.

Key Features and Benefits of Prisma Cloud DSPM

- **Automated discovery and classification of data assets** in public clouds including AWS, Azure, GCP, and cloud-based data warehousing solutions, such as Snowflake. Discovery is followed by Data classification with 100+ automated classifiers (e.g. PCI, PII, PHI, FTC, GDPR, and CCPA) and the ability to add custom tailored classifiers. This allows users to locate where sensitive data resides and ensure continuous compliance with latest security and privacy regulations.

- **Data Security Posture Management (DSPM)** identifies data risks that are associated with sensitive data exposure, compliance violations, and data residency issues. It incorporates both content and context of data (e.g. people accessing the data, location, destination, and encryption), which allows security teams to prioritize remediation efforts and efficiently reduce data exposure.

- **Data Detection and Response (DDR)** detects and responds to data breaches through continuous monitoring of all data interactions in real time including admin events, data events, and connections. Prisma Cloud DSPM evaluates data activity against an evolving threat model of cloud data stores and includes hundreds of detections, developed by Prisma Cloud data researchers, in order to detect data exfiltration attempts, compliance breaches, and data misuse.

Follow the steps listed below to enable DSPM in Prisma Cloud and utilize Prisma Cloud credits to secure your data assets.

- Login to Prisma Cloud via single sign-on (SSO) and switch the persona to Data Security.
- Consolidated reporting of Dig Security credits via Prisma Cloud
- Review features offered by DSPM.

Pre-configuration

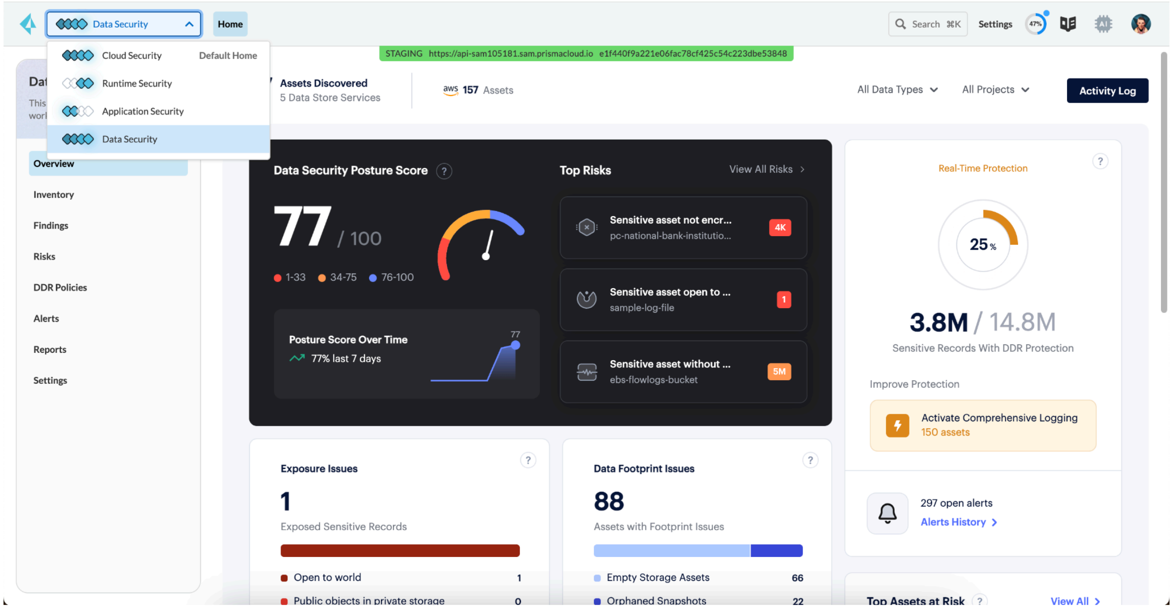
To activate DSPM on your Prisma Cloud tenant, contact your Customer Success (CS) or Solutions Architect (SA) and provide the following information:

- Account Name
- Prisma Cloud Tenant ID
- Prisma Cloud App URL

Configuration

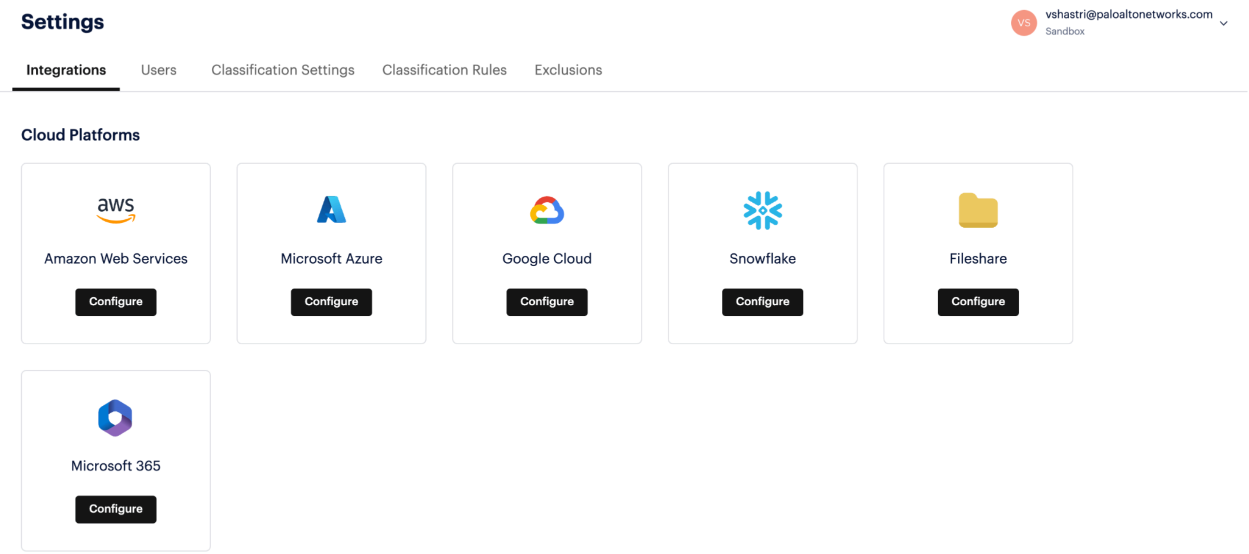
Logging in to DSPM Console

After completing pre-configuration, use the Prisma Cloud SSO and switch the persona to **Data Security**, to log in to your DSPM (Dig Security) console.



Onboarding Cloud Accounts

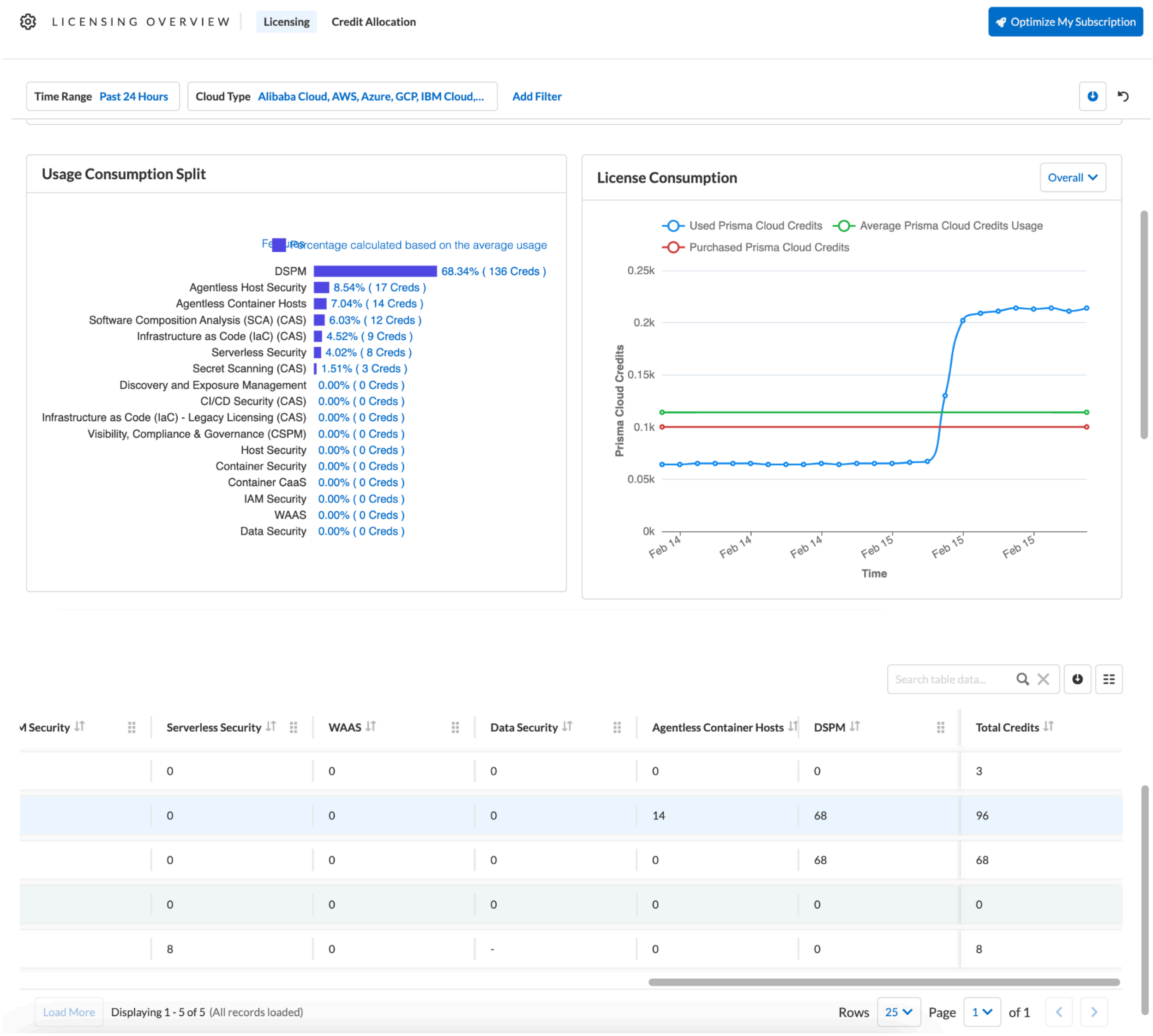
During the ongoing integration of DSPM (Dig Security) with Prisma Cloud, the initial release requires you to onboard DSPM on the Dig console. Follow the steps in Dig Documentation to onboard your cloud accounts.



Licensing

DSPM is a new module where all the Dig Security licensing will be reported and aggregated. The DSPM module ensures automatic discovery and security for data stores.

The consumption of DSPM credits is determined by the category of protected data assets. A charge of 1 credit per data asset applies to all protected IaaS and PaaS data assets. For DbaaS such as Snowflake, the billing is set at 1 credit per Terabyte of stored data.



Time Range: Past 24 Hours

Cloud Type: Alibaba Cloud, AWS, Azure, GCP, IBM Cloud,...

Usage Consumption Split

Fe■ures Percentage calculated based on the average usage

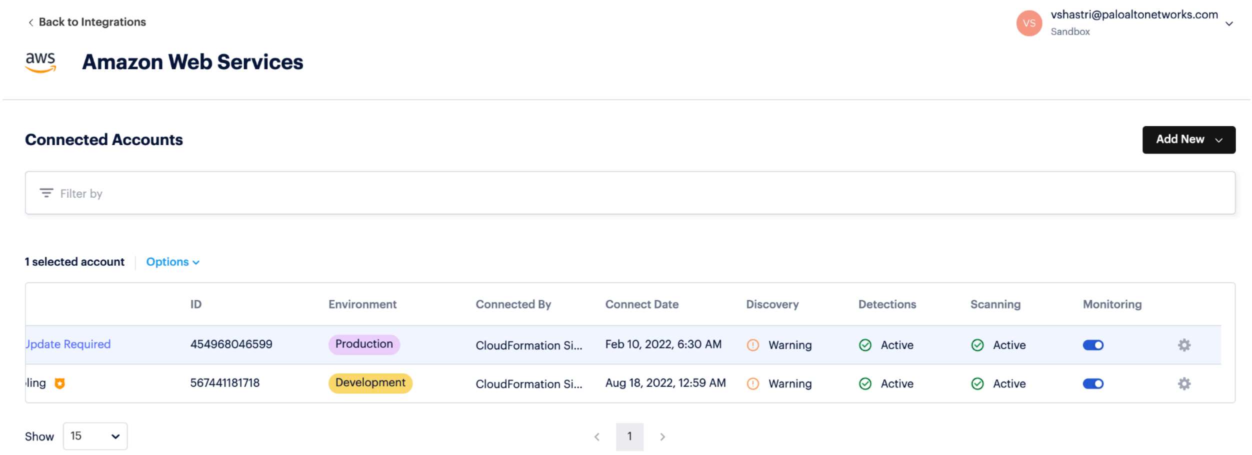
DSPM	68.34% (136 Creds)
Agentless Host Security	8.54% (17 Creds)
Agentless Container Hosts	7.04% (14 Creds)
Software Composition Analysis (SCA) (CAS)	6.03% (12 Creds)
Infrastructure as Code (IaC) (CAS)	4.52% (9 Creds)
Serverless Security	4.02% (8 Creds)
Secret Scanning (CAS)	1.51% (3 Creds)
Discovery and Exposure Management	0.00% (0 Creds)
CI/CD Security (CAS)	0.00% (0 Creds)
Infrastructure as Code (IaC) - Legacy Licensing (CAS)	0.00% (0 Creds)
Visibility, Compliance & Governance (CSPM)	0.00% (0 Creds)
Host Security	0.00% (0 Creds)
Container Security	0.00% (0 Creds)
Container CaaS	0.00% (0 Creds)
IAM Security	0.00% (0 Creds)
WAAS	0.00% (0 Creds)
Data Security	0.00% (0 Creds)

M Security	Serverless Security	WAAS	Data Security	Agentless Container Hosts	DSPM	Total Credits
	0	0	0	0	0	3
	0	0	0	14	68	96
	0	0	0	0	68	68
	0	0	0	0	0	0
	8	0	-	0	0	8

Displaying 1 - 5 of 5 (All records loaded)

Offboarding

If you decide to discontinue using DSPM, offboard your accounts by disabling monitoring on those specific accounts.



‹ Back to Integrations

aws **Amazon Web Services**

VS vshastri@paloaltonetworks.com
Sandbox

Connected Accounts

Add New

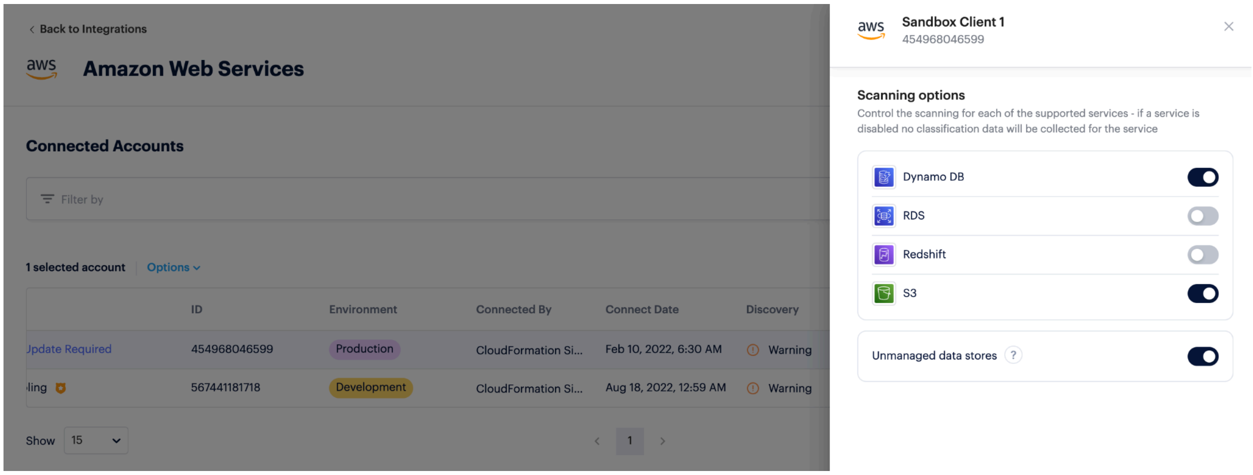
Filter by

1 selected account | Options

	ID	Environment	Connected By	Connect Date	Discovery	Detections	Scanning	Monitoring	
Jpdate Required	454968046599	Production	CloudFormation Si...	Feb 10, 2022, 6:30 AM	Warning	✓ Active	✓ Active	●	⚙
ling	567441181718	Development	CloudFormation Si...	Aug 18, 2022, 12:59 AM	Warning	✓ Active	✓ Active	●	⚙

Show 15 ‹ 1 ›

Alternatively, if you prefer only to exclude certain data assets from discovery and scanning, click on the settings icon and disable monitoring for specific data stores within that account.



‹ Back to Integrations

aws **Amazon Web Services**

Connected Accounts

Filter by

1 selected account | Options

	ID	Environment	Connected By	Connect Date	Discovery
Jpdate Required	454968046599	Production	CloudFormation Si...	Feb 10, 2022, 6:30 AM	Warning
ling	567441181718	Development	CloudFormation Si...	Aug 18, 2022, 12:59 AM	Warning

Show 15 ‹ 1 ›

aws **Sandbox Client 1**
454968046599

Scanning options
Control the scanning for each of the supported services - if a service is disabled no classification data will be collected for the service

Dynamo DB	●
RDS	○
Redshift	○
S3	●

Unmanaged data stores ? ●