Why DSPM?

Prisma® Cloud believes that cybersecurity teams, data security teams, and privacy and compliance professionals shouldn’t struggle to protect their data from cyberthreats. Our ultimate goal is to make data security easy. And our leading data security posture management (DSPM) platform with built-in data detection and response (DDR) capabilities was purpose-built to make that happen.

Prisma Cloud DSPM facilitates the building of robust data security programs by helping security teams:

- Know what data exists across their cloud environments
- Understand how their data is used by colleagues, applications, vendors, and machines
- Protect their data at rest and in motion across cloud data stores

Data Security Approaches

In the rapidly evolving world of data security, organizations must stay ahead of the evolving threat landscape and protect their mission-critical data. As more companies shift their operations to the cloud, the need for robust data security solutions has become far more essential. Without the right technologies, workflows, and processes, securing data in cloud environments is an uphill battle.

To date, there are five approaches that organizations can implement to secure their data. Only one of them, though, is tailored to secure data in cloud environments.

On-Premises Data Security

The first approach involves deployment of traditional data security technologies. They're great solutions for protecting data on-premises, but their risk models have yet to be adapted to public cloud environments. Protecting data on-premises is entirely different than protecting data in the cloud. On-premises technologies lack cloud-native capabilities and require agents or connection strings that prevent them from performing automated discovery of data stores. On-premises solutions can neither scale as quickly and efficiently as cloud solutions nor handle the variety and volatility of cloud assets. Only a cloud-native solution can support cloud-native data stores, identify native risks, understand data flows and lineage, and conduct real-time data detection and response (DDR).

Due to the continuous rise in digital transformation and the migration of organizational data to cloud platforms, the on-premises approach can't support modern customer use cases aligned with cloud data security. While vendors in this space may attempt to acquire companies with expertise in cloud security, their technologies weren't built with a cloud-first methodology.

Privacy-Driven Data Security

Another approach is building a data security program based on compliance with data privacy laws and regulations. These solutions are primarily aimed at addressing privacy concerns rather than focusing on overall data security: regulation compliance doesn't translate to secure data.

Compliance and privacy technologies typically cater to legal professionals and lack a comprehensive cybersecurity risk model or security mindset. They weren't built from the ground up to detect and classify data, to meet security use cases, and to integrate into the workflows that security operation centers (SOCs) follow when triaging, investigating, and responding to cybersecurity incidents. Some vendors may try to expand their offerings to appeal to chief information security officers (CISOs). But their products aren't as suited for data security as those of specialized security vendors. These technologies can't find data, monitor it, and show how it flows through the environment in real time. In other words, they can't see when data is under attack.

Cloud Service Provider Add-on Data Security

Cloud service providers (CSPs) have developed data security add-ons and secondary solutions to their main product offerings. They're great solutions to get started with, but since they're CSP-specific, they work only in that provider's single cloud service environment. They're limited in scope and don't offer data discovery, posture management, or detection and response capabilities.

While these solutions provide native integration with their own cloud platforms, they can be costly and narrowly focused. They also don't secure DBaaS or IaaS environments. This approach to data security has significant advantages, but will not provide the comprehensive coverage and risk modeling capabilities that organizations require to meet their data security needs.

Cloud Security Posture Management (CSPM) Data Security

CSPM-driven data security is also a great place to start, but it focuses on detecting resources and vulnerabilities within a cloud environment. Once resources are detected, CSPM solutions help security teams respond to cloud infrastructure misconfigurations and patch vulnerabilities. CSPM isn't designed to secure data at rest and in transit. CSPM can't address DBaaS and SaaS environments.

Some great CSPM technologies are available that offer DSPM-light capabilities. But without understanding what data exists, where it is, how it is used, and how it flows through the environment, the data isn't properly secured.

Data Security Posture Management

The DSPM approach enables security teams to build data security programs centered around the data rather than on the environment or outlying technologies. DSPM helps organizations assess, monitor, and reduce the risk associated with sensitive data stored in their cloud environments.

By providing visibility into data assets and ensuring that proper security controls are in place, DSPM can help organizations maintain a strong data security posture. This, in turn, enables them to monitor their cloud data stores closely, make security improvements, and respond to data breaches immediately.

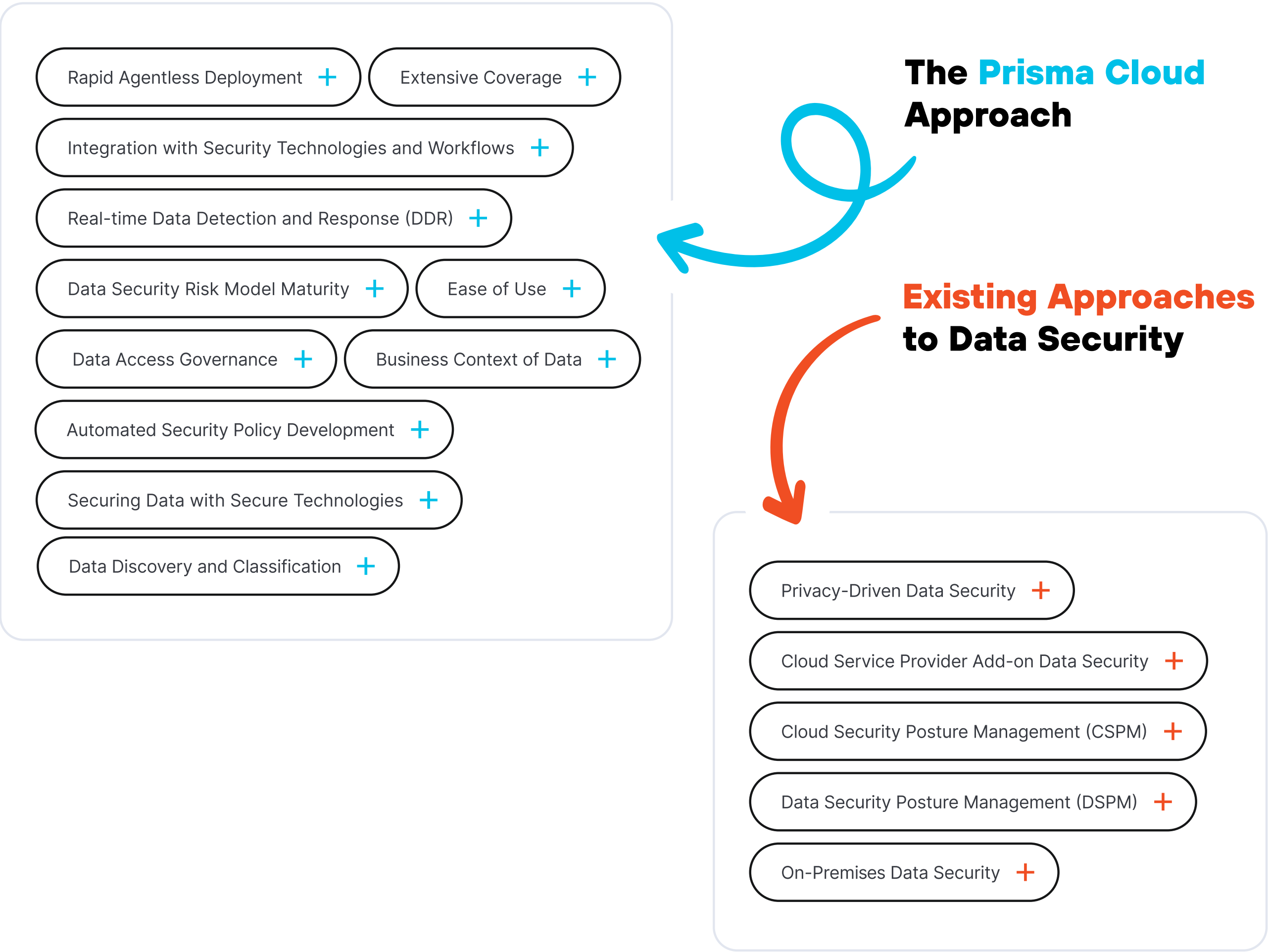
The Prisma Cloud Approach
Rapid Agentless Deployment +
Extensive Coverage +
Integration with Security Technologies and Workflows +
Real-time Data Detection and Response (DDR) +
Data Security Risk Model Maturity +
Ease of Use +
Data Access Governance +
Business Context of Data +
Automated Security Policy Development +
Securing Data with Secure Technologies +
Data Discovery and Classification +
Existing Approaches to Data Security
Privacy-Driven Data Security +
Cloud Service Provider Add-on Data Security +
Cloud Security Posture Management (CSPM) +
Data Security Posture Management (DSPM) +
On-Premises Data Security +

Figure 1: Prisma Cloud's approach to data security

The Prisma Cloud Approach to Data Security

Prisma Cloud offers a comprehensive data security solution that brings out the best in DSPM and DDR. Focusing on cloud environments, Prisma Cloud provides real-time visibility, control, and protection of data assets across any cloud and any data store.

Rapid Agentless Deployment

- Easily integrates as an agentless and proxy-free platform into your business' infrastructure within minutes.
- Reveals where sensitive data is stored, who has access to it, how it is being used, and how it flows through the environment.
- Determines if data is at risk for loss or exfiltration, and showcases what security teams can do to secure it.

Extensive Coverage

- Supports a wide range of cloud platforms, including AWS, Azure, Google Cloud Platform, Oracle Cloud, Databricks, Office365, and Snowflake.
- Ensures consistent data protection across any cloud and any service.

Data Discovery and Classification

- Identifies and classifies sensitive data assets instantaneously with over 150 data classifiers.
- Refines and customizes data classification to meet specific data security criteria and policies.
- Offers a highly accurate data classification engine with classifiers for addressing compliance and privacy frameworks such as HIPAA, PCI-DSS, CCPA, and GDPR.

Business Context of Data

- Understands data from a business perspective and distinguishes critical business contexts.
- Differentiates between employee and customer emails, internal vs. external IP addresses, data ownership, and data that surrounds sensitive data.
- Generates more accurate data security policies, processes, and incident response actions.

Data Access Governance

- Maps users and role access to sensitive data to ensure that a least privileged practice is applied across multi-cloud assets.
- Easily determines when excessive access is granted to individual entities by comparing level of access with actual usage.
- Implements consistent policies and procedures for managing access permissions across different cloud environments and platforms.

Automated Security Policy Development

- Enhances the ability to automate critical security actions with an evolving threat model.
- Learns from data security events to generate and advance policies and enhance a security program.

Data Security Risk Model Maturity

- Provides a purpose-built data security risk model.
- Identifies risks to data, quantifies them, develops rich context around them, and receives alerts to quickly remediate data security incidents.

Real-Time Data Detection and Response (DDR)

- Dynamically monitors and protects against malicious activities targeting sensitive data in the cloud.
- Facilitates triage of data security events with rich data security context.
- Integrates data security workflows into existing SOC workflows and security technologies.
- Enables in-platform cloud data loss prevention (DLP) use cases to stop data breaches in real time.

Integration with Security Technologies and Workflows

- Ground-up solution that integrates with and complements existing customer security technologies and workflows.
- Integrates with SIEM, SOAR, and ticketing solutions to turn alerts into action quickly.
- Reduces mean time to detect (MTTD) and mean time to respond (MTTR) to data security incidents.
- Proactively hunts for malware across cloud environments and data stores.

Ease of Use

- Facilitates data security with a simple and intuitive interface while not sacrificing functionality.
- Requires no extensive training to extract value.

Cloud-Native Technology

- Is purposely built for organizations that store data in cloud environments.
- Offers a specialized and mature cloud data security solution.
- Enables rapid implementation and integration with data stores via API rather than via legacy technologies, such as connectors.

Securing Data with Secure Technologies

- Eliminates vendor risk through agentless deployment.
- Keeps customer data in cloud environments to prevent privacy regulation violations and new data residency or sovereignty issues.

About Prisma Cloud

Prisma® Cloud is the industry's most comprehensive cloud-native application protection platform (CNAPP) with the broadest security and compliance coverage—for applications, data, and the entire cloud-native technology stack—throughout the development lifecycle and across hybrid and multicloud environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate secure cloud-native application development. To learn more, visit us online and request a demo.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com