Prisma Cloud Enterprise Credit Guide

Prisma® Cloud Enterprise is a SaaS-delivered cloud-native application protection platform (CNAPP). Prisma Cloud enables security and DevOps teams to effectively collaborate to accelerate secure cloud-native application delivery from code to cloud.

The Prisma Cloud platform delivers continuous visibility and threat prevention throughout the application lifecycle across multicloud environments. With code-to-cloud coverage that encompasses code, CI/CD pipeline, infrastructure, workloads, data, networks, web applications, identity, and APIs, Prisma Cloud addresses your security needs at every step of your cloud journey. Plus, with over four billion cloud assets secured and over one trillion cloud events processed daily, you can trust Prisma Cloud to protect your cloud at any scale.

Overview

Prisma Cloud Enterprise is a SaaS platform comprising product modules providing distinct security capabilities. These product modules offer organizations flexibility in where and how they secure their code and cloud environments.

Prisma Cloud product modules are utilized via Credits, a universal capacity unit utilized by all product modules ("Credits"). Credits offer the flexibility to use other modules as your needs evolve, access new modules when they are introduced, and secure your code and cloud footprints as they expand, without additional interactions with Palo Alto Networks. Each product module requires a specific number of Credits. Overall usage of Prisma Cloud is measured based on the aggregate number of Credits used across modules.

Cloud Security Plans

Prisma Cloud Enterprise offers plans representing recommended approaches for securing cloud environments.

Cloud Security Foundations is ideal for customers looking for agentless visibility and compliance of their multicloud code, build, deploy, and runtime environments.

Cloud Security Foundations offers:

- Real-time threat and misconfiguration detection for IaaS and PaaS.
- Compliance management.
- Agentless workload scanning.
- Infrastructure as code (IaC) misconfiguration detection.
- Least-privileged access enforcement.

All via an agentless architecture.

Cloud Security Advanced includes the use case coverage from Cloud Security Foundations, plus the flexibility of real-time, prevention-first:

- Host, container, and serverless runtime security
- Web Application and API Security

Table 1: Prisma Cloud Security Plans and Included Modules

Prisma Cloud Capability	Cloud Security Foundations	Cloud Security Advanced
Visibility, Compliance and Governance (includes Threat Detection)	Included	Included
Agentless Workload Scanning (hosts, containers, serverless functions)	Included	Included
IAM Security	Included	Included
Infrastructure as Code Security	Included	Included
Host Security	Available as add-on*	Included
Container Security	Available as add-on	Included
Serverless Security	Available as add-on	Included
Web Application and API Security	Available as add-on	Included
Data Security	Available as add-on	Available as add-on
Data Security Posture Management (DSPM)	Available as add-on	Available as add-on
Cloud Discovery and Exposure Management (CDEM)	Available as add-on	Available as add-on
Software Composition Analysis (SCA)	Available as add-on	Available as add-on
Secrets Security	Available as add-on	Available as add-on
CI/CD Security	Available as add-on	Available as add-on
Prisma Cloud Credit Requirements (for included modules)	2 Credits†	5 Credits‡

* Credit requirements of modules available as add-ons are listed in table 2.

† Per virtual machine (VM) running in public cloud accounts (e.g., Amazon EC2, Azure Virtual Machines, Azure Virtual Machine Scale Sets, Google Cloud Google Compute Engine [GCE], Alibaba Cloud ECS, Oracle Cloud Compute) protected by Prisma Cloud.

‡ Per VM running in public cloud accounts and private clouds protected by Prisma Cloud.

Prisma Cloud Product Modules

Organizations can customize their code-to-cloud security coverage by utilizing individual Prisma Cloud product modules. Table 2 lists credit requirements for individual modules.

Table 2: Prisma Cloud Product Modules and Credits

Prisma Cloud Product Module	Credits
Visibility, Compliance and Governance (including Threat Detection)	1 per VM*
IAM Security	0.25 x Visibility, Compliance and Governance credit usage
Data Security (for Amazon S3 and Azure Blob Storage)	Exposure Scan: 1 per 200 GB scanned Full Scan†: 1 per 33 GB scanned
Data Security Posture Management	IaaS and PaaS data assets: 1 per asset‡ Database as a Service: 1 per TB of data volume‡ SaaS: 0.1 per user‡
Cloud Discovery and Exposure Management	100 minimum or 0.25 x Visibility, Compliance and Governance credit usage, whichever is greater§
Host Security	0.5 per Host Defender deployed
Container Security	5 per Container Defender deployed 1 per App-Embedded Defender deployed
Serverless Security	1 per 6 serverless functions
Web Application and API Security	2 per Defender deployed inline‖ 2 per Defender in out-of-band mode
Infrastructure as Code Security	3 per developer#
Software Composition Analysis (SCA)	4 per developer#
Secrets Security	1 per developer#
CI/CD Security	3 per developer#

* Virtual machines (VMs) refer to those running in public cloud accounts (e.g., Amazon EC2, Azure VMs, Azure Virtual Machine Scale Sets, Google Cloud Google Compute Engine [GCE], Alibaba Cloud ECS, Oracle Cloud Compute) protected by Prisma Cloud.

† Exposure scan, data classification, and malware analysis.

‡ Refer to Prisma Cloud technical documentation for the full list of supported IaaS, PaaS, Database as a Service, and SaaS data assets.

§ Cloud Discovery and Exposure Management requires a minimum of 100 credits.

‖ In WAAS, each protection has an action defined as a user-selected operating mode. Inline WAAS requires Host, Container, or App-Embedded Defender to be deployed. For inline WAAS, we have disable, alert, prevent, and ban; while for out-of-band, we have disable or alert.

\# A developer is defined as an active Git committer (identified through their unique Git author email address) and has contributed to a code repository protected by Prisma Cloud within the last 90 days.

Purchase and Use of Prisma Cloud Credits

Prisma Cloud Credits can be purchased from Palo Alto Networks, our channel partners, and various marketplaces (AWS Marketplace, etc.). Prisma Cloud Credits are applied toward cloud security plans and standalone modules. Once the Prisma Cloud Credits are loaded into your account, they can be used to enable Prisma Cloud plans and/or individual product modules from within the Prisma Cloud console.

Prisma Cloud Credit Usage Measurement

Credit usage is measured every hour (except Data Security). We then roll up to daily, weekly, monthly, and quarterly averages for reporting. This prevents overages based on short-term bursts. On an aggregate basis across all Prisma Cloud modules, if you use more Credits than you purchased, our Palo Alto Networks team will help you procure more. For more details about credit usage measurement, please refer to Palo Alto Networks technical documentation.

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

prisma_prisma-cloud-enterprise-credit-guide_070924