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 multi-cloud environments. With Code to Cloud coverage that encompasses software, infrastructure, workloads, data, networks, web applications, identity and API security, Prisma Cloud addresses your security needs at every step in your cloud journey. With over 10 billion cloud assets secured and over 1 trillion cloud events processed daily, you can trust Prisma Cloud to protect your cloud at any scale.

This document is intended to outline Prisma Cloud's future metering changes. It is intended for information purposes only, does not supersede or amend Palo Alto Networks End User Agreement nor is it intended to be incorporated into any contract. All product offerings are subject to then-current pricing. Please contact your Prisma Cloud sales representative with any questions.

Overview

Prisma Cloud Enterprise is a SaaS platform composed of 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"). 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 multi-cloud code, build, deploy and run time environments. Cloud Security Foundations offers:

- Real-time Threat and Misconfiguration detection for IaaS and PaaS
- Compliance management
- Workload vulnerability scanning
- Infrastructure as Code (IaC) misconfiguration detection
- Least privilege 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

Prisma Cloud Capability	Cloud Security Foundations	Cloud Security Advanced
Visibility, Compliance and Governance (including Threat Detection)	Included	Included
Agentless Vulnerability Management	Included	Included
IAM Security	Included	Included
Infrastructure as Code (IaC) Security	Included	Included
Host Security	Available as add-on[1]	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
Software Composition Analysis (SCA)	Available as add-on	Available as add-on
Secrets Security	Available as add-on	Available as add-on
Prisma Cloud Credit requirements	2 credits[2]	5 credits[3]

1. Credit requirements of modules available as add-ons are listed in the table below
2. per Virtual Machine (VM) running in public cloud accounts (e.g., AWS EC2, Azure Virtual Machines, Google Cloud Google Compute Engine (GCE), Alibaba Cloud ECS, Oracle Cloud Compute) protected by Prisma Cloud
3. 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.

Prisma Cloud product module	Credits
Visibility, Compliance and Governance (including Threat Detection)	1 per VM[4]
IAM Security	0.25 per VM[4]
Data Security (for Amazon S3 and Azure Blob storage)	Exposure Scan: 1 per 200GB Full Scan[5]: 1 per 33GB
Host Security	0.5 per defender deployed
Container Security	5 per defender deployed
Serverless Security	1 per 6 defended serverless functions
Web Application and API Security (WAAS)	2 per defender deployed 1 per defender in out-of-band mode[6]
Infrastructure as Code (IaC) Security	3 per developer[7]
Software Composition Analysis (SCA)	4 per developer[7]
Secrets Security	1 per developer[7]

4. Virtual Machines (VMs) refers to those running in public cloud accounts (e.g., AWS EC2, Azure VMs, Google Cloud GoogleCompute Engine (GCE), Alibaba Cloud ECS, Oracle Cloud Compute) protected by Prisma Cloud
5. Exposure scan, Data Classification, Malware Analysis
6. In WAAS, each protection has an action, defined as a user-selected operating mode. For in-line WAAS, we have: disable, alert, prevent, and ban; while for Out-of-Band, we have disable or alert
7. A developer is defined as an active Git committer (identified through their unique Git author email address) and has made a contribution 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 purchased in increments of 100, and are applied towards 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. This prevents overages based on short-term bursts.

On an aggregate basis across all Prisma Cloud modules, if you use more Prisma Cloud Credits than you purchased, our Customer Success team will help you procure more Prisma Cloud Credits.

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