SERVICE DESCRIPTION

QuickStart Service for Prisma Cloud CWP – Small

1. Introduction

This service description document (“Service Description”) outlines the Palo Alto Networks QuickStart Service for Prisma Cloud – Cloud Workload Protection (CWP) – Small (“Services”).

By placing a purchase order (“Purchase Order” or “PO”) for the Services, customer (“Customer”) is purchasing Palo Alto Networks QuickStart Service for Prisma Cloud CWP – Small and agrees to the terms in this Service Description. The term of the Services shall commence upon Purchase Order acceptance by Palo Alto Networks, Inc. and shall continue for, and must be used within, a period of six (6) months. Any extension of the term must be mutually agreed to by the parties, and neither party shall unreasonably withhold such agreement.

Palo Alto Networks will provide Services on the Customer’s existing security infrastructure to Palo Alto Networks hardware and software offerings (collectively “Products”) described in the Deliverables section of this Service Description.

1.1. Public Sector Customers

Public Sector customers, which term shall include but may not necessarily be limited to customers in and related to the federal government, state and local governments, education (both K-12 and higher education), and other quasi-governmental entities (collectively “Public Sector Customers”) shall purchase the Services in this Service Description through a Palo Alto Networks authorized partner only and not directly from Palo Alto Networks. Any Services performed by Palo Alto Networks through this Service Description will be in support of the partner prime contractor’s contractual obligations. This Service Description shall in no way create a contractual obligation between Palo Alto Networks or its subsidiaries and any Public Sector Customers or government end user. For purposes of Public Sector Customers only, the following sections will not apply: Section 5 (Travel Expenses for On Site Work), Section 8 (Fees and Payment) and Section 9 (Terms and Conditions). Further, any references to payment of travel expenses due to cancellation shall not apply to the extent that any aspect, term or condition of this Service Description contradicts any applicable rule, law or regulation such rule, law or regulation shall take precedence over that term or condition.

2. Scope of Services

The Customer may purchase Services for:

- Prisma Cloud CWP (Cloud Workload Protection)

The scope for Prisma Cloud CWP is documented in Section 2.1.

The Palo Alto Networks part number covered by this Service Description is:

SKU	Description
PAN-CONSULT-PRISMA-CWP-QS-SMB	QuickStart Service for Prisma Cloud CWP for Small Customers

2.1. Prisma Cloud Compute (CWP)

2.1.1. Service Parameters

Parameter	In Scope	Description
Console	1	Self-Hosted Edition: Install Console for single Environment SaaS Edition: Onboard Prisma Cloud Enterprise Users to access Prisma Cloud Console (SaaS)
Defenders (per Kubernetes cluster) or Host Defenders	2	Install defenders within supported platforms (for example, Openshift 3.x/4.x, Kubernetes, Google Kubernetes Engine, Amazon Kubernetes Services, Azure Kubernetes Services) or Host Defender on any cloud platform such as AWS, Azure, GCP, etc.
App Embedded Defenders	1	App Embedded Fargate Defender
Agentless Scanning	1	Enable Agentless Scanning
Auto-Defend for Hosts and Serverless	1	Enable Serverless Auto-Defend for Hosts and Serverless
RBAC Configuration	1	Configure Users and Roles
Registry Scanning	1	Setup Defender to scan appropriate registry
Alert Provider	1	Integrate with alert providers for alerts notifications to one (1) of the following: Splunk, Google Pub/Sub, Google Command Security Center, JIRA, or email
CI/CD Pipeline Integration	1	Integrate twistcli tool for image scanning with one (1) Continuous Integration (CI) tool (for example, Bamboo, Spinnaker, Jenkins)
Cloud Discovery	1	Configure Cloud Discovery to discover unprotected resources
Runtime Policy Tuning	10	Tune or tighten rules and policies. Build rulesets based on Runtime Model. ***Note** - Policy tuning requires a two (2) week "bake-in" period after the Defenders have been deployed to provide sufficient audit events
Runtime/Compliance/ Vulnerability Tuning four (4) hour session	1	One (1) four (4) hour Session to tune vulnerability/runtime/compliance rulesets

Compliance/vulnerability	10	Review events to build additional Compliance and Vulnerability rules
Code Repository	1	Configure Code Repository
Knowledge Transfer four (4) hour Session	1	One (1) session for up to four (4) hours for up to eight (8) participants
As-Built Document	1	As-Built Document to be delivered upon project completion

2.1.2. Planning

Palo Alto Networks will, with Customer's participation, conduct planning activities and a project kick-off call. The project kick-off will include review of the project requirements (new deployment), discuss milestone timelines, identify the Customer's project team members and follow-up action items. Palo Alto Networks will also provide details of all required network connectivity.

Palo Alto Networks will provide a predefined Project Plan, as defined in Section 3, and perform one (1) review with the Customer team for the addition of Customer specific requirements/feedback. The final Project Plan will be mutually agreed to prior to moving to the next phase of the project.

2.1.3. Discover

Palo Alto Networks will provide a Technical Requirements Document ("TRD"), as defined in Section 3. Palo Alto Networks and the Customer will meet using remote web-meeting or conference call to review the following information to prepare the TRD:

- Provide system and integration requirements of Prisma Cloud CWP
- Discuss the access requirements to Prisma Cloud CWP Intelligence stream
- Prepare technical detail gathering sheet for implementation
- Document and review technical details with Customer

Palo Alto Networks will provide a draft TRD for Customer review and feedback. If the Customer does not provide feedback, the draft will be considered accepted. The final TRD will be delivered to the Customer prior to moving to the next phase of the project.

2.1.4. Deployment

Palo Alto Networks will, with the Customer's assistance, perform an initial remote Prisma Cloud CWP deployment. Prior to any deployment activities, the Customer will meet all pre-deployment criteria identified in Section 2.1.9 below. Upon Customer's completion of all the criteria, the deployment will proceed as follows:

- Self-Hosted Deployment
    - Deploy Prisma Cloud Compute Console
    - Download the Prisma Cloud software
    - Modify the console(s) Console.CFG file for any customization of ports/services
    - Create the PersistentVolume prior to Console deployment
    - Generate a YAML configuration file or Helm Chart for Console and deploy the Console

    - Modify Console YAML file ReplicaSet using Kubernetes built-in HA capabilities
    - Configure the Console
    - Register a DNS entry for Console's external IP address
    - Set up a custom certificate or import a Certificate from PKI to secure Console access
    - Update the list of identifies in a Console's certificate that Defenders use to validate Console's identity
    - Integrate Console with a single identity management service, such as Active Directory, SAML, or supported identity directory service

- SaaS Deployment
    - Onboard Prisma Cloud Enterprise Users
    - Map Prisma Cloud Enterprise Groups (RBAC) to Prisma Cloud Compute Console Built-in Roles
    - Create Access Keys in Prisma Cloud Enterprise for CI User role in Prisma Cloud Compute for CI/CD pipeline integration

- Deploy the Defenders
    - Self-Hosted Deployment
        - Configure the following as required (Prisma Cloud Compute Console):
            - Sign into Prisma Cloud Compute Console (UI)
            - Go to **Compute** > **Manage** > **Defenders** > **Deploy** > **DaemonSet**
            - Copy the Defender install script
        - Configure the following CLI commands as required:
            - Generate a defender.yaml file or Helm Chart for Defender Deployment
            - Modify the defender.yaml or Helm Chart for any customizations for ports/services
            - Deploy the Defender type either as a DaemonSet or RASP
            - Deploy the Defender DaemonSet
              ```
              kubectl create -f defender.yaml
              ```
            - Verify the Defenders are deployed
            - Create an external service route to Console (applicable only to OpenShift)
    - SaaS Deployment
        - Configure the following as required:
            - Sign into Prisma Cloud
            - Go to **Compute** > **Manage** > **System** > **Downloads**
            - Copy the URL address under Path to Console
            - Go to **Compute** > **Manage** > **Defenders** > **Deploy** > **DaemonSet**
            - Copy the URL address from the Path to Console step above (the name that clients and Defenders use to access this Console)
- Deploy the Host Defenders
    - Configure the following as required:
        - Log into the Prisma Cloud CWP Console to select the single Defender Deployment
        - Choose the Host Defender Type whether it is for Linux/Windows
        - Choose the Host Defender Listener Type (non or TCP)
        - Download the Host Defender install script
        - Copy the install script for the Host Defender on each Host

(Linux/Windows)

        - Verify the Host Defenders are deployed

- Deploy the Serverless or App-Embedded Defenders
    - Configure the following as required:
        - Log into the Prisma Cloud CWP Console to select the Serverless or App-Embedded Defender Deployment
        - Choose the Auto-protect rules
        - Add new credential that will be stored in the Credential Store
        - Choose Defender Type (Container Defender-app embedded)
        - Deploy App Embedded Defender
        - Create a task definition in AWS
        - Test the AWS task definition
        - Validate the tasks results in the Prisma Cloud Compute Console
        - Verify the Defenders are deployed
- Authentication Configuration (Self-Hosted Edition)
    - Integrate Console authentication against one (1) of the following external services as required:
        - Active Directory
        - OpenLDAP directory services
        - SAML Identity Providers
        - Integrate Google G Suite (SAML)
        - Integrate with Azure Active Directory via SAML 2.0 Federation
        - Integrate with Active Directory Federation Services (ADFS) via SAML 2.0 Federation
        - Integrate with PingFederate via SAML 2.0 Federation
        - Assign roles to Console for RBAC
- Console authentication Hardening Configuration (Self-Hosted Edition)
    - Prisma Cloud lets you set up long-lived tokens for access to the Console web interface and the API
    - Set Console token validity period
    - Set strong password requirements for local accounts (as a backup to IAM)

2.1.5. Integration

Palo Alto Networks will, with the Customer's assistance, perform an initial remote Prisma Cloud CWP integration. Palo Alto Networks will review and validate the configuration and the state of the Prisma Cloud CWP integration of third-party services. The integration parameters are as follows:

- Integrate Prisma Cloud CWP alert providers for alerts notifications to one (1) of the following: Twistlock Splunk App, Google Pub/Sub, Google Command Security Center, JIRA, or email
- Integrate Prisma Cloud CWP tool for image scanning with a Continuous Integration (CI) tool (for example, Bamboo, Spinnaker, Jenkins)
- Configure Prisma Cloud CWP Syslog/StdOut alerts to one (1) Logging and Reporting and alert Provider Integration (SIEM) via Syslog or StdOut (for example, Splunk, Google StackDriver, LogRhythm)

2.1.6. Policy Tuning

Upon completion of all Integration activities identified in Section 2.1.5 above, Palo Alto Networks will work with the Customer to perform policy tuning. Before policy tuning can be completed, it requires a minimum of a two (2) week "bake-in" period after the Defenders have been deployed to collect audit events. Palo Alto Networks will deploy the configuration elements listed below to complete review and tuning default policies based on Runtime Container learning models.

- Review the scanning data with Customer
- Tune the default compliance policy to suit Customer environment or requirements
- Review and investigate the Compliance/Vulnerability explorer events with Customer to build additional Compliance and Vulnerability rules for up to ten (10) rules, if applicable
- Build additional Runtime Defense Rules based on investigating Runtime event anomalies (up to ten (10) Runtime rules). These Runtime events will be triggered by anomalies against the Active Container Models.

Palo Alto Networks will create additional compliance and vulnerability rules from investigating events from Vulnerability/Compliance Explorer, and build additional rules for Runtime Defense. In addition, Palo Alto Networks will create custom vulnerability, compliance, Runtime, and Image Scanning policies, and allow traffic monitoring and review.

Palo Alto Networks will document all non-standard changes in the configuration.

2.1.7. Validation

Palo Alto Networks will review and validate the deployment of Prisma Cloud CWP and review Prisma Cloud CWP Event audits, Vulnerability Explorer, and Compliance Explorer. Palo Alto Networks will then review with the customer, and start applying preventive actions by performing the following actions:

- Review security audits from the Prisma Compute CWP Monitoring Events
- Perform investigation of the Monitoring Events, then apply policies to prevent incidents
- Assess and review results from custom and default policies
- Start applying preventative actions to rules in "prevent" mode based on events from the Monitoring Events
- Assess and review results from Prisma CWP Console's Vulnerability Explorer and Compliance Explorer
- Start applying preventative Vulnerability rules to take action based on the severity of the vulnerabilities (if applicable)
- Start enforcing Compliance rules to take action based on failed compliance checks defined by the customer (if applicable)

2.1.8. Knowledge Transfer

Palo Alto Networks consultant will provide knowledge transfer upon completion of all the tasks identified above in Sections 2.1.2 through 2.1.7. The sessions will include a description of the as-built environment, and a transfer of information on how to manage and operate the environment. Knowledge transfer will be conducted in a single session for up to four (4) hours for up to eight (8) participants. Knowledge transfer activities can include:

- Review as-built environment
- Review the actions and decisions that were taken during the validation phase and work with proper resources for management knowledge transfer
- Review the actions and remediations taken during the different phases of the project to go over an operations knowledge transfer

2.1.9. Service Specific Customer Obligations, Assumptions and Exclusions

Customer Obligations

Prior to creation of the TRD, the Customer must complete the following items:

- Assignment of project lead resource
- Signed, proper non-disclosure agreement requests, if needed
- List of approved Cloud providers and Integrations to be connected for the professional services engagement
- Proper administrative accounts for Cloud providers
- Network diagrams
- Authentication codes and serial numbers registered and activated via Palo Alto Networks support portal site
- Assign proper resources to work with Palo Alto Networks to assist with integrating SAML, Continuous Integration (CI) plugins, and alert providers

Customer is responsible for scheduling proper resources that will be responsible for making decisions based on access and remediation actions for results found from policy reports. Prior to providing the Deployment Services listed in Section 2.1.4 above, Customer will:

- Ensure any necessary proxy, firewall rules, or routing changes are in place to allow all required network communication between Console and Defender
- Ensure any necessary proxy, firewall rules, or routing changes are in place to allow all required network communication between twistcli image scanning tool and the Console, or from the Continuous Integration (CI) to the Console
- Provide service accounts with proper access to alert providers, CI tools, image repositories, and integration with enterprise Secrets Stores (HashiCorp Vault)
- Ensure for scanning images with the twistcli tool, Docker Engine must be installed on the executing machine
- Ensure running an existing provisioned Kubernetes cluster that meets the minimum system requirements and runs a supported Kubernetes version
- Ensure the nodes in Kubernetes cluster can reach Prisma Cloud's cloud registry (registry-auth.twistlock.com)

- Ensure that permissions on the cluster can create PersistentVolumes and LoadBalancers from YAML configuration files
- Provide the Palo Alto Networks resource(s) access to the platform and Kubectl RBAC rights for TwistLock Console and Defender deployment
- Provide the Palo Alto Networks resource(s) HTTPS access to the TwistLock Console Management
- If it is a Public cloud deployment, provide Palo Alto Networks resource(s) the necessary IAM rights for deploying Consoles and Defenders
- Create PersistentVolume for the Console Deployment (required)
- Ensure all details required for configuration of identity Management systems are captured
- Ensure any necessary firewall rules or routing changes are in place to allow all required network communication
- Ensure required NAT policy is fully documented (if applicable)
- Ensure connectivity to mail server and all required authentication servers
- Provide email address and Syslog server settings
- Provide team members to work with the identity management systems integration
- Ensure definitions of external RBAC groups are created
- Provide necessary rights to create Helm Charts for Console and Defender deployments

Prior to providing the Integration Services listed in Section 2.1.5 above, Customer will:

- Make necessary changes on the third-party systems/tools/applications required for the Twistlock implementation:
    - Existing OpenShift and Kubernetes architecture review
    - Configuration of any third-party system/tool/applications
    - Scripting Development
    - Custom reporting generation
    - Continuous Integration/Continuous Deployment (CI/CD) tools

Service Description Definitions

- “Console” - Prisma Cloud’s management interface. It lets you define policy and monitor your environment. Console is delivered as a container image.
- “Defender” - Defenders enforce the policies you set in Console. They come in a number of different flavors. Each flavor is designed for protecting specific types of cloud-native resources and for optimal deployment into the environment, with full support for automated workflows.
- “Kubernetes” - Container-orchestration system for automating application deployment, scaling, and management.
- “WAAS” Web Application and API Security (WAAS) - A web application firewall (WAF) designed for both hosts and containers. WAFs secure web apps by inspecting and filtering Layer 7 traffic to and from the app.
- “CNNF” Cloud Native Network Firewall (CNNF) - A Layer 3 container-aware virtual firewall that utilizes machine learning to identify valid traffic flows between app components, and alert or block anomalous flows.

- “SAML” - When SAML support is enabled, administrators can log into Console with their federated credentials. With SAML users and groups, admins can create granular access control rules that allow or deny specific actions against specific resources for specific users and groups.
- “RBAC” Role-Based Access Control (RBAC) - Prisma Cloud provides broad enterprise identity support for Role-Based Access Control, integrating with Active Directory, OpenLDAP, Ping, Okta, Shibboleth, Azure AD, and G Suite, allowing you to implement central credential management in the Prisma Cloud Platform.
- “StdOut” - Stdout integration, you can optionally enable verbose output. Verbose output records vulnerability and compliance issues in your environment. It also records all process activity.
- “CI/CD” - Generally refers to the combined practices of continuous integration and either continuous delivery, or continuous deployment.
- “Runtime Defense” - Runtime defense is the set of features that provide both predictive and threat based active protection for running containers.
- “Runtime Container Models” - The results of the autonomous learning that Prisma Cloud performs every time we see a new image in an environment. A model is the ‘allow list’ for what a given image should be doing, across all runtime sensors.
- “PersistentVolume (PV)” - A piece of storage in the cluster that has been provisioned by an administrator or dynamically provisioned using Storage Classes.

Assumptions

The following assumptions will apply to the Services:

- Palo Alto Networks will perform all work using remote access
- All Deliverables will be provided in English

Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- Any cloud activities not related to network security using the Palo Alto Networks platform
- Multiple Prisma Cloud Compute Consoles deployments are not supported
- Multi-tenant environments are not supported
- Automation or scripting of Prisma Cloud Compute Console and Defenders will not be covered by this project
- Palo Alto Networks will not provide any guidance on API calls
- Automation or orchestration workflow design and configuration, and automation of policy or Infrastructure as code are excluded from Policy tuning services

3. Deliverables

The following Deliverables will be provided in accordance with the Services:

PROJECT DELIVERABLES	
Project Deliverable	**Deliverable Criteria**
Project Plan	Capture project management requirements ● Milestones ● Task/activities ● Owners ● Timeline
Prisma Cloud TRD	The Technical Requirements Document includes the following: ● Outline the planned production environment of the cloud Security policies and operational procedures with the cloud environment that were agreed on during the initial architectural review phase
As-Built Configuration Document	Document the "as implemented" configuration of the deployed Solution

4. Project Resources and Designated Place of Work

Palo Alto Networks will assign project resources with the appropriate skills to deliver the Services and agreed upon Deliverables including, but not limited to, a project manager to serve as a single point of contact for the administration and management of the Deliverables. Palo Alto Networks resources may be subject to change at any time throughout the project, and Customer will be notified by Palo Alto Networks as soon as practicable of any such changes.

5. Travel Expenses for On-Site Work

The Services will be performed remotely. Travel and Expenses ("T&E") are not included in the price of the Services. Any travel by Palo Alto Networks will be mutually agreed upon before the travel occurs. Fees for travel-related costs are purchased and billed separately.

6. Scheduling

Palo Alto Networks resources work a normal work day of eight (8) hours and will adhere to the Customer's local business hours. In addition, Palo Alto Networks resources will adhere to the local Palo Alto Networks office holiday schedule. Any Services performed after normal business hours and on weekends must be approved in advance by Palo Alto Networks management.

Cancellation of a working session without a minimum of two (2) business days advance notice may cause: (i) delay in the performance of the Services; and (ii) risk the completion of the Services within the term of this Service Description. In the event of a delay due to a late cancellation, Customer may be required to purchase additional Services to complete the project. Any delays due to Customer's late cancellation shall be at no fault of Palo Alto Networks.

7. General Customer Obligations, Assumptions and Exclusions

Palo Alto Networks obligations, and the Services, are subject to Customer complying with the Customer obligations, assumptions, and exclusions listed below. Successful and timely completion of the Services are subject to Customer meeting its obligations under this Service Description and Palo Alto Networks shall not be responsible for any delay due to Customer's non-compliance of its obligations.

Customer Obligations

Prior to the delivery of the Services, Customer will:

- Provide a project manager or other single point of contact ("SPOC") for the project who will be responsible for:
    - Providing all information, as requested by Palo Alto Networks, in a timely manner.
    - Acting as the central point of contact to Palo Alto Networks.
    - Coordination of Customer resources engaged in the project. Customer's technical resources should be qualified on Palo Alto Networks Products.
- Be responsible for procurement of any and all licenses for the Palo Alto Networks Products and provide to Palo Alto Networks professional services consultant(s) upon request.
- Provide Palo Alto Networks professional services consultant(s) with existing and up to date documentation including, but not limited to: topological diagrams, design documentation, up-to-date configurations, and change management policy documentation.
- Advise Palo Alto Networks of any:
    - Special security, health, and safety matters applicable.
    - Relevant project management meetings related to the project and/or Services, and permit Palo Alto Networks to attend such meetings as appropriate.
- Be responsible for managing all other vendors including, if applicable, Customer's managed services partner or systems integrator.
- Be responsible for any and all configuration changes to any non-Palo Alto Networks Products.
- Provide prompt written notice to Palo Alto Networks as soon as Customer becomes aware or has reason to believe that: Customer will not meet any of the Customer obligations under this Customer Obligations section, and/or if any of Palo Alto Networks assumptions will not occur or are inaccurate.
- Provide any additional equipment, such as network analyzers, test equipment, and/or laboratory equipment that are not provided by Palo Alto Networks, but necessary to perform the Services.
- Ensure that Palo Alto Networks personnel may access and use Customer's and third-party licensors' proprietary materials as necessary for Palo Alto Networks to perform the Services. Customer warrants and represents that it has the right and authority to grant such access and use to Palo Alto Networks and hereby grants Palo

Alto Networks the rights to use and access such proprietary materials as needed for Palo Alto Networks to perform the Services.

- Accept as agreed upon and final the detailed software/hardware specifications and scope set forth herein prior to execution of this Service Description.

Assumptions

Throughout the delivery of the Services, Customer will:

- Upon request or as needed, provide access to the skilled subject matter and technical experts within Customer's (or their third-party vendor) organization for Palo Alto Networks to perform the Services.
- Perform all responsibilities and obligations specified under this Service Description in a professional workmanlike manner to facilitate timely completion of the Services.
- Provide direct remote access to the Palo Alto Networks equipment to be worked on via a Palo Alto Networks owned laptop.
  - Where direct remote access cannot be provided to Palo Alto Networks owned laptops, Customer shall provide alternative laptops with appropriate capabilities and connectivity, or other functionally equivalent connectivity.

Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- The Services will not commence until Palo Alto Networks has received a non-cancellable PO for the Services.
- Palo Alto Networks is responsible for providing only the Services with the associated tasks and Deliverables described in this Service Description. Palo Alto Networks shall have no responsibility for other contractors or third parties engaged by Customer or another third-party during delivery of the Services unless expressly agreed to in writing.
- Palo Alto Networks shall not be responsible for any delays caused by Customer or any third-party.
- Services are non-transferrable.

8. Fees and Payment

If Customer is purchasing the Services directly from Palo Alto Networks, payment terms for the Services are subject to the terms set forth in Section 2 of the Professional Services Agreement. Fees for Services purchased through an authorized reseller or distributor shall be paid directly to such authorized reseller or distributor.

9. Terms and Conditions

Palo Alto Networks professional services shall be subject to the Professional Services Agreement, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-professional-services-agreement.pdf, unless the parties have entered into a separate written agreement that is identified as the governing agreement (either, “Agreement”).

In either case, the applicable Agreement shall be incorporated by reference into this Service Description. In the event of any material conflict between the terms in the Agreement and the terms in this Service Description, the terms in this Service Description shall control.

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