Prisma Cloud Security Guide

Table of Contents

Overview

This guide provides Prisma® Cloud customers with a framework that establishes the pillars of security within their cloud journey. It focuses on the Prisma Cloud Enterprise software-as-a-service (SaaS) suite of capabilities. Prisma Cloud Enterprise is a cloud-native application protection platform (CNAPP) that incorporates all the various cloud security disciplines (e.g., multicloud posture management, workload protection, microsegmentation, identity and access management, data security, etc.) into a unified, holistic service for the protection of your cloud resources.

The major cloud service providers (CSPs) each publish a cloud adoption framework (Azure, GCP, AWS). "Securing the cloud" is a pillar in each of these frameworks, and Prisma Cloud is a perfect fit for this pillar. It is a multicloud and hybrid cloud solution that provides visibility and control across CSPs' cloud-based services (code, VM, containers, serverless functions, identity, etc.). Prisma Cloud facilitates and accelerates an organization's cloud transformation journey.

Code & Build, Deploy, and Run

In this guide, we segment the cloud application's lifecycle into the following categories:

- **Code & Build**: The CSPs provide the ability to codify the deployment, maintenance, and removal of cloud services (e.g., VMs, storage buckets, etc.). This is commonly referred to as infrastructure as code (IaC). You are responsible for the secure operation of your cloud services. Continuous integration (CI) is a development lifecycle practice that has expanded with the growth of the cloud. CI provides your organization with the ability to rapidly and continuously develop, update, and maintain your cloud-based applications. The assembly and testing of your code into usable software packages are automated by CI systems (e.g., Jenkins, CircleCI, CloudBees) that integrate with the different code repositories and package management systems. These CI systems produce deployable artifacts, such as IaC, VM images, Docker images, serverless images, etc., that are consumed by the release processes to drive frequent deployments. Prisma Cloud provides visibility and control within your Code & Build processes to identify vulnerabilities and compliance violations before progressing to the next phase of the application's lifecycle.
- **Deploy**: Continuous deployment (CD) provides the automation of testing and the deployment of applications within your clouds' runtime environments. With modern automation, cloud applications are in a continuous cycle of development, testing, and release. This notion of continuous change is a fundamental challenge in managing cloud applications. Prisma Cloud identifies vulnerability and compliance issues within applications that are staged for deployment. With Prisma Cloud, you can enforce policies to ensure that only trusted applications are allowed to launch within the cloud runtime environment.
- **Run**: Applications run across the cloud workload continuum. Regardless of where they are deployed (IaaS, PaaS, SaaS, etc.), the application's runtime actions should be monitored for abnormal behaviors. Overly permissive cloud access roles present opportunities for attackers. Prisma Cloud quickly identifies expected behaviors and prevents anomalous behavior. It secures runtime environments using predictive and threat-based protections.

Foundational, Intermediate, and Advanced

This guide categorizes Prisma Cloud capabilities that are recommended to be implemented within the cloud disciplines of Code & Build, Deploy, and Run. This framework's cloud adoption phases are:

- **Foundational**: Your organization has started its cloud adoption journey. You are presented with the challenge of effectively managing assets within the cloud and on-premises. Prisma Cloud Enterprise provides your organization with the visibility, tools, and knowledge to develop a strong and secure cloud adoption foundation.
- **Intermediate**: Prisma Cloud supports your organization's progression of understanding and adopting cloud-based technologies. Effectively manage the vulnerabilities and compliance of your cloud-based resources. Use Prisma Cloud to secure cloud capabilities that advance beyond the traditional infrastructure as a service architecture.
- **Advanced**: Your organization is innovating its business with the cloud, and this is supported by the industry-leading capabilities of Prisma Cloud Enterprise. Proactively control your cloud operations and identify and remediate issues before they manifest within your runtime environments.

The cloud has introduced a new discipline to cybersecurity and the total cost of ownership. Organizations can quickly utilize technologies that would have taken years to implement in a traditional on-premises environment.

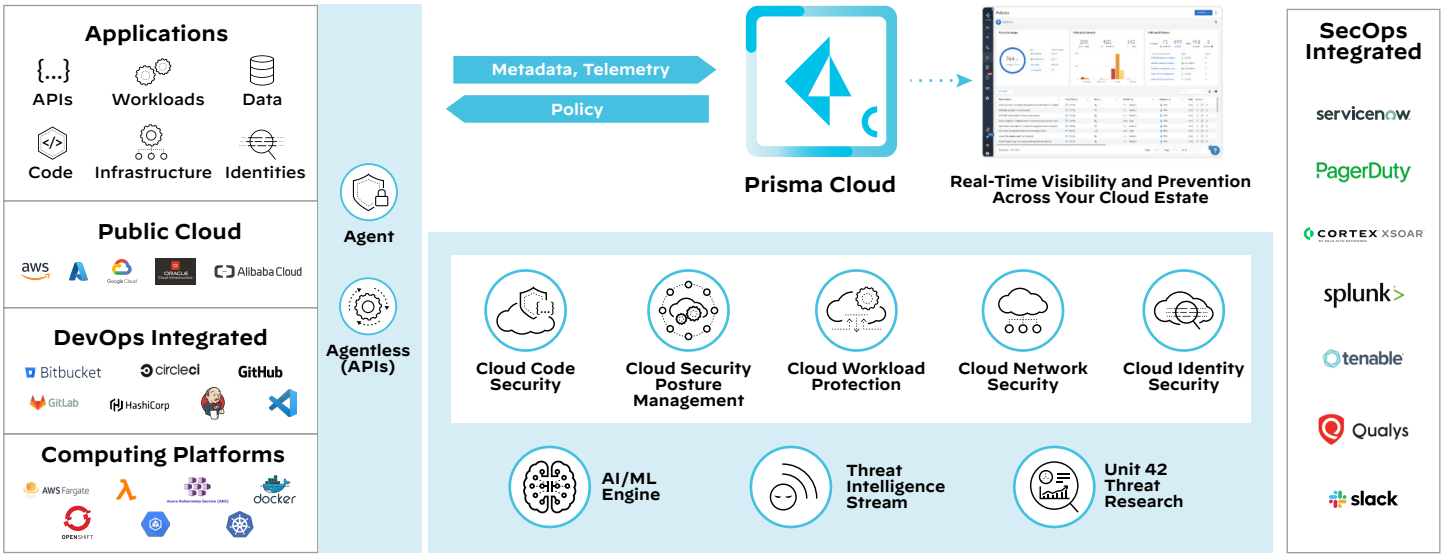


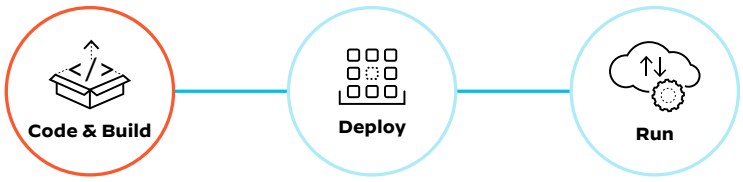
Figure 1: Prisma Cloud architecture

The ownership of responsibility between the CSP and the customer is dependent upon the technology (e.g., IaaS, PaaS, or SaaS). Prisma Cloud provides consistent security across the ownership responsibility gradient dependent upon the technology. It secures all these technologies, giving the customer confidence in their cloud transformation journey. This guide is intended for all organizational cloud stakeholders. With Prisma Cloud, Development, Security, and Operations (DevSecOps) practitioners have a common platform to identify, protect, detect, respond to, and recover their cloud-based infrastructure, services, and workloads.

Palo Alto Networks is the leader in cloud cybersecurity. Internally, our services teams have worked together to create this guide. It is a collaboration of what Palo Alto Networks has experienced and how to address those issues in your environment. Use the Prisma Cloud Field Guide for an in-depth technical understanding of how to fully utilize Prisma Cloud Enterprise. We recommend following the Prisma Cloud blogs for the latest Prisma Cloud announcements.

Code & Build

The cloud has changed how applications are collaboratively developed. The use of version control systems (e.g., GitHub, GitLab, Bitbucket, Azure Repos, etc.) has grown exponentially. The CSPs provide customers with the ability to deploy and maintain their cloud services using scripting languages such as Terraform. These coding technologies and disciplines have introduced the "learn how to configure code security" feature to protect your IaC code opportunity of identifying vulnerabilities and misconfigurations before they are compiled into applications or deployed as insecure cloud services. This approach to securing the development of code is frequently called "shifting left." The building of cloud resources involves various technologies that span computational environments, such as virtual machine images, container images, and continuous integration build tools (e.g., Jenkins, CircleCI, CloudBees, etc.). Prisma Cloud provides DevSecOps stakeholders with the ability to securely build and maintain their cloud-based environments.



Implement the following Prisma Cloud capabilities to provide visibility and control within your organization's cloud coding and building practices:

Foundational

Identify misconfigured infrastructure as code that leads to insecure runtime cloud services.

Insecure IaC directives can ultimately manifest as misconfigured and vulnerable runtime cloud services. Identify common coding mistakes within the code repository. Find secret keys, passphrases, insecure configurations, and more. You need to identify these insecure codified cloud service directives before they get deployed as running services. Prisma Cloud Code Security scans code repositories that generate fully contextualized results. Learn how to configure Code Security to protect your IaC code.

Identify misconfigurations before you commit your code.

Prisma Cloud Code Security makes it possible for you to identify misconfigurations before developers commit their code. Avoid pull requests that will cause builds to fail due to undetected misconfigurations. Use the code analysis tool to scan IaC files from frameworks such as Terraform plan, CloudFormation, Azure Resource Manager (ARM),

secrets, serverless, Dockerfile (only code), and Kubernetes. The integration of Code Security within IDE tools gives you immediate detection of misconfigurations and inline code fixes. Learn how to integrate Code Security within your IDE tools.

Identify supply chain dependencies and Software Bill of Materials (SBOM).

The supply chain capability on Code Security is a code-centric view of infrastructure and application security that visualizes a supply chain graph, starting with the IaC templates, the services, deployed cloud workload resources (including associated permissions), and the runtime configuration on these resources. Prisma Cloud's supply chain graph is a real-time autodiscovery of potentially misconfigured infrastructure and application files, sorted into a concise data model that you can use to prioritize and search. The graph identifies infrastructure, image, open source, and secrets, and combines that data to identify risk chains. Learn more about Supply Chain Security.

Software Bill of Materials is a method for the inventory of software that is present in an industry-accepted format. Prisma Cloud's repository and CI/CD scans inspect open-source packages through the package manager files to generate an SBOM report. The SBOM reports are configurable to contain open-source packages, infrastructure as code, and image packages in either CSV or CycloneDX format. Learn more about SBOMs.

Intermediate

Integrate vulnerability and compliance checks within your CI tools.

Scanning VMs, container images, and serverless functions in their earliest stage will allow you to fix issues before they are running in production. Use the Prisma Cloud CI plugin within the developers' automation tools to scan for vulnerability and compliance issues. For example, developers can scan the packages and binaries that are compiled into the container images and immediately get detailed reports within their build pipelines, thus increasing your developers' security awareness. Learn more about continuous integration with Prisma Cloud.

Detect drift within infrastructure as code cloud deployments.

Drifts are inconsistencies in configuration that occur when resources are modified manually using the CLI or console, and these divergences from the code are not recorded or tracked. The inconsistencies in code configuration can either be an addition or deletion of values from the template configuration in the source code. Code Security periodically scans your repositories to identify drifts that may occur between the Build and Deploy phases and enables you with corrective solutions to handle traceable configuration changes. Learn more about Drift Detection.

Prevent developers from committing hard-coded secrets.

Prisma Cloud detects when secrets are committed from developers' machines, branches, and build jobs. Your code is analyzed using prebuilt secrets detectors, built to identify the API keys, tokens, and passwords developers may be using when developing a cloud-native app. Enforce policy by halting a build process when a secret is found to ensure secrets have not been committed downstream in your CI/CD process and assess if the secret was compromised. Learn how to monitor and manage issues in your code scan.

Define your own vulnerability and compliance policies.

Prisma Cloud includes out-of-the-box policies that enable you to detect misconfigurations and provide automated fixes for security issues across your integrated code repositories. You also have the flexibility to add new custom policies for your repositories and pipelines. As soon as you connect Code Security to your repositories, both out-of-the-box and custom policies are used to scan for potential issues. Learn more about how to create your own custom build policies.

Analyze the runtime behavior of images before running in development and production environments.

You are going to deploy an image into your environment, and you want to ensure that the image's resulting container will not exhibit malicious behavior. With Prisma Cloud's twistcli plugin, you can validate an image's runtime behaviors within a sandboxed environment. Have confidence that your images will not exhibit malicious runtime behaviors before leaving the Build phase. Learn more about image analysis sandbox.

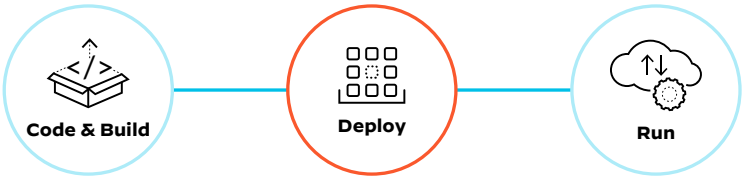
Advanced

Trace a deployment of a cloud resource with tags.

Do you ever wonder which infrastructure as code template was used to deploy a cloud resource? Tags can help you trace the link for your resources deployed from code-to-cloud infrastructure. Detect drift within your codebase and locate the specific resource within a commit that identifies teams and resource owners to help triage a fix in the most timely and cost-effective way. Learn more about IaC tag and trace.

Deploy

Deployment of services has traditionally been the responsibility of the operations group. With cloud technologies, that responsibility is now shared with developers and security practitioners. The cloud has brought these traditionally disparate groups into the DevSecOps operations of today. Prisma Cloud provides your DevSecOps groups with a common platform to visualize, monitor, and deploy cloud-based services.



Implement the following Prisma Cloud capabilities to provide visibility and control within your organization's cloud deployment practices:

Foundational

Discover compliance issues and vulnerabilities on your deployed containers.

To affect deployment policies with your environments, you will need to deploy Prisma Cloud Defenders. A Defender is the component that performs registry vulnerability and compliance scanning, Kubernetes policy enforcement, etc. Learn more about how to deploy Prisma Cloud Defenders.

Scan images stored within container image registries.

To identify vulnerabilities and compliance issues in images stored within your registries, first deploy container Defenders, then configure registry scanning. Prisma Cloud scans images for vulnerabilities and configuration compliance via a schedule or a webhook. New vulnerabilities are automatically updated within Prisma Cloud via the Intelligence Stream service. Prisma Cloud will automatically identify these new vulnerabilities within hosts, images, containers, and serverless functions throughout your environment. Learn more about how to scan your container image registries.

Intermediate

Enforce vulnerability and compliance policies.

Prisma Cloud container Defenders enforce your organization's policies to ensure noncompliant images are not allowed to instantiate as running containers. You can create policies to block specific vulnerabilities and/or compliance findings. You can allow exceptions and grace periods for findings that are migrated through other controls. Enforce your organization's vulnerability and compliance policies, ensuring the secure operations of your services. Learn more about policy enforcement.

Advanced

Enforce Kubernetes operational policies.

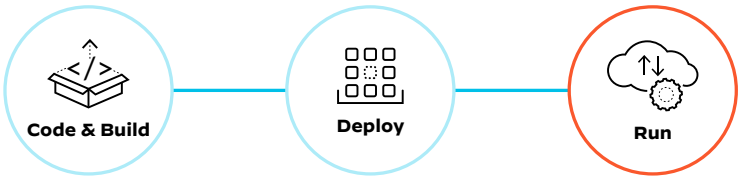
Prisma Cloud provides a dynamic admission controller for Kubernetes and OpenShift that is built on the Open Policy Agent (OPA). Prisma Cloud disseminates your policies to Defenders deployed within a Kubernetes cluster. With OPA rules, you can control the creation, maintenance, and deletion operations within your Kubernetes clusters. Learn more about simplified policy enforcement with managed OPA.

Deploy only trusted containers.

Modern development has made it easy to reuse open-source software. Pulling images from public registries is easy, fast, and convenient. However, it is a practice that is not allowed by most organizations. You should maintain a set of trusted images and registries to ensure that only these images are allowed to be deployed within the runtime environment. You can define the trusted images and registries to ensure that only these images are allowed to run in your environment. Learn more about trusted images.

Run

The runtime environment is the culmination of all the other phases. This is where the immense, diverse cloud computational resources are available and orchestrated by you. Operational discipline is of equal importance to the securing of applications running within the cloud. Prisma Cloud provides real-time visibility and full-stack protection across all the leading public clouds.



Implement the following Prisma Cloud capabilities to provide visibility and control within your organization's cloud runtime environment:

Foundational

Gain visibility into your cloud services and assets running within your cloud environments.

Onboarding allows Prisma Cloud to query your CSP's API endpoints to collect configuration, network, and audit data. This information is used to identify vulnerable configurations, suspicious network traffic, and anomalous behaviors within your cloud infrastructure. Supported cloud service providers are Alibaba Cloud, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure. Learn more about connecting your cloud accounts.

See all cloud resources across all clouds in a single pane of glass.

You need to have complete visibility into every deployed resource and absolute confidence in the configuration status of your multiple cloud environments. Therefore, maintaining a current inventory of deployed resources and gaining centralized visibility across cloud environments are essential for your cloud operations. From the single dashboard, you gain operational insight over all our cloud infrastructure, including assets and services. Prisma Cloud also maintains a history of configuration changes, enabling users to understand exactly when a new security issue was introduced and by whom, to simplify cloud forensics and auditing. Learn more about cloud inventory management.

Quickly identify vulnerabilities without deploying agents.

Agentless scanning lets you inspect the risks and vulnerabilities of a virtual machine without having to install an agent or affecting the execution of the instance. Prisma Cloud supports agentless scanning on AWS, GCP, and Azure hosts for vulnerabilities. Learn more about agentless scanning.

Identify vulnerability and compliance issues within serverless functions.

Serverless computing has gained popularity due to cloud providers dynamically managing the allocation of machine resources. Serverless architectures delegate operational responsibilities to the cloud provider. However, you are responsible for the vulnerabilities in your code and associated dependencies. Prisma Cloud scans your cloud-based serverless functions without the deployment of Defenders. Prisma Cloud supports AWS Lambda, Google Cloud Functions, and Azure Functions. Learn more about serverless function scanning.

Check your cloud environments against compliance standards.

Onboard your cloud accounts to quickly review, manage, and enforce compliance standards across multicloud environments in real time based on your regulated industry's standards. Prisma Cloud supports more than 20 compliance standards, including PCI DSS, HIPAA, GDPR, SOC 2, NIST 800-171, NIST 800-53, NIST CSF, ISO 27002, CCPA, CCM, and custom frameworks. You can create compliance reports and run them immediately or schedule them on a recurring basis to measure your compliance over time. You can also track your vulnerability issues and ensure your cloud environment is secure and void of misconfiguration mistakes. Learn more about compliance standards.

Work toward Zero Trust by reviewing net-effective permissions and removing excessive permissions for all user and resource identities.

In the public cloud, overly permissive roles, poor credential hygiene, and accidental public exposure have caused significant enterprise breaches. Gaining visibility into net-effective permissions across cloud providers is a complex task. The security operations team needs to apply and maintain the principle of least privilege in highly dynamic multicloud environments. Prisma Cloud provides broad visibility into effective permissions, continuously monitors cloud environments for risky and unused entitlements, and automatically makes least-privilege recommendations. You can query all relevant identities, including all the relationships among different entities and their effective permissions, in cloud environments. Learn more about Prisma Cloud IAM Security.

Ensure that data stored in the cloud is secure and does not contain sensitive information or malware.

The near-limitless capacity offered by cloud storage services has enabled organizations to store significant amounts of data, amplifying the challenges of traditional, lengthy, and error-prone manual processes for classification. The risks of cloud storage services, from misconfiguration to sensitive data to malware to suspicious user activities, are challenging to assess and remediate without a single consolidated view. Prisma Cloud Data Security is purpose-built to address the challenges of discovering and protecting data at the scale and velocity common in public cloud environments. It enables the discovery and classification of data stored in AWS S3 buckets and protects against accidental exposure, misuse, or sharing of sensitive data. In addition to protecting your confidential and sensitive data, your data is also protected against threats—known and unknown (zero-day) malware using Palo Alto Networks WildFire® service. Learn more about Prisma Cloud's Data Security capabilities.

Intermediate

Monitor the runtime behavior of your applications.

Applications run across the cloud continuum. Regardless of where they are deployed (hosts, containers, serverless functions, etc.), the application's runtime behavior should be monitored for abnormal behaviors. The security operations team needs to identify those planned behaviors quickly and prevent any other unpredictive anomalous behavior. Prisma Cloud secures runtime environments using predictive and threat-based protection without adding overhead. Threat-based protection includes capabilities like detecting when malware is added to a container or when a container connects to a botnet. Prisma Cloud automatically creates runtime models based on observed processes, networking, and file system behaviors. These runtime models can be adjusted to further refine the monitoring and effect policy responses when events are encountered. In addition, Prisma Cloud captures the forensic details, which provide the history of events that led up to and followed an incident for threat hunting and lifecycle analysis. Learn more about Prisma Cloud runtime defense.

Identify rogue cloud deployments and assess internet exposure risk.

The rapid development of cloud-native applications leaves the doors open to rogue cloud deployments, creating unmanaged shadow cloud assets. These shadow assets compromise cloud security, exposing organizations to many security risks. Attackers can discover and exploit these internet exposures before security teams know about them. To address this challenge, Prisma Cloud delivers cloud discovery and exposure management to identify rogue cloud assets, highlights internet exposure risks, and allows users to quickly onboard unmanaged workloads. Prisma Cloud accurately discovers and attributes internet-exposed assets across multicloud deployments so security teams can investigate and communicate risk to application owners to remediate internet exposure risks. Learn more about Prisma Cloud's Cloud Discovery and Exposure Management.

Identify anomalous network and user activities.

The dynamic, distributed nature of cloud environments can often create alerts that lack context at a volume that can overwhelm security operations teams. Attempting to correlate logs, API metadata, and signature-driven alerts can overwhelm teams with false positives instead of actionable insight. Prisma Cloud employs advanced machine learning to identify the normal network behavior of each customer's cloud environment to detect anomalies. Users who access cloud environments can pose a significant threat if not continuously monitored for unusual activities that could signal possible credential or account compromise. Prisma Cloud continuously monitors and learns each user's activities to identify what's normal and alerts on behaviors that deviate from that baseline. Prisma Cloud provides a comprehensive policy to detect malicious network and user activities. Learn more about Prisma Cloud's Threat Detection.

Prioritize risk management and incident responses.

As alerts start to arrive from Prisma Cloud, it is critical to categorize what is important to avoid alert fatigue. The ATT&CK Explorer and Top Incidents & Risks (view by MITRE ATT&CK) give an excellent overview and categorization of your alerts to easily address any possible issues, including both incidents that map to MITRE as well as misconfiguration risks that could be addressed to make your cloud infrastructure less prone to specific MITRE ATT&CK tactics. The MITRE ATT&CK framework's curated knowledge base and model for cyber adversary behavior is available for your security operations team to easily track down possible incidents and wade through audits/noise to find what is important in your environment. Learn more about Prisma Cloud's ATT&CK Explorer and Top Incidents & Risks (view by MITRE ATT&CK).

Advanced

Safeguard your web applications and APIs from attacks with Layer 7 firewall protection.

Prisma Cloud's Web Application and API Security (WAAS) is a web application and API firewall designed for HTTP-based web applications deployed directly on hosts as containers, application-embedded, or serverless functions. Your web applications running on hosts, containers, or serverless are protected against the most critical OWASP Top 10 risks, including injection flaws, broken authentication, broken access control, security misconfigurations, etc. In addition, you can enable many other security features like access control, file upload control, bot protection, DoS protection, and more. The overall outcome is that you will be protected against vulnerabilities like Log4j. Learn more about Prisma Cloud's Web Application and API Security protections.

Automatically correct misconfigurations.

With complex multicloud environments, the security operations team wants to have automated solutions to resolve security violations, such as misconfigured security groups, to be addressed immediately and effectively. Prisma Cloud can automatically resolve policy violations within the Prisma Cloud console. Learn more about Prisma Cloud autoremediation capabilities.

Continued Reading: Best Practices

This guide's goal is to help you and your organization capitalize on the industry-leading cloud-native application protection platform capabilities of Prisma Cloud Enterprise. We encourage you to engage with your Palo Alto Networks support team to start the journey of protecting your organization with Prisma Cloud Enterprise.

We recommend reading and implementing the Prisma Cloud Field Guide to maximize the utilization of Prisma Cloud Enterprise.

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