Prisma Cloud FAQs

Eliminating Attack Paths Free Trial

408.753.4000 | 3000 Tannery Way, Santa Clara, CA 95054 | paloaltonetworks.com

Q. Why should I opt into this trial?

Risk prioritization and remediation serves as a cornerstone in cloud security strategy. It enables security organizations to allocate resources efficiently, focusing on mitigating the most significant security issues first for robust protection.

Prisma Cloud prioritizes risks by correlating multiple security indicators, providing actionable security context to defend against high-risk threats. This is accomplished with out-of-the-box Attack Path policies, which consolidate several unique indicators of risk (e.g., misconfigurations, vulnerabilities, suspicious activity) to identify harmful combinations that cause impactful risk.

A significant number of Prisma Cloud's attack path policies rely on misconfiguration, overly permissive access, and vulnerability findings generated from Prisma Cloud's Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and Agentless Workload Scanning capabilities.

Customers that have not enabled Prisma Cloud's CIEM or Agentless Workload Scanning capabilities can opt into this free 30-day trial to fully experience improved risk prioritization through Prisma Cloud's out-of-the-box Attack Path policies.

Q. Where can I find more information about Prisma Cloud's attack path policies?

Learn more about attack path policies here, and about risk prioritization here.

Q. Where can I find more information about Prisma Cloud's capabilities for Cloud Infrastructure Entitlement Management (CIEM)?

Learn more about managing permissions and entitlements across cloud environments here.

Q. Where can I find more information about Prisma Cloud's Agentless Workload Scanning capabilities?

Learn more about Agentless Workload Scanning here.

Q. What will happen to my Prisma Cloud credit usage during this trial?

If you have not enabled Prisma Cloud CIEM, opting into the free trial will not result in credit consumption for Prisma Cloud's IAM Security product module.

If you have not enabled Agentless Workload Scanning, opting into the free trial will not result in credit consumption for Prisma Cloud's Host Security or Container Security product modules.

Q. Can I end and leave the trial before the 30-day period?

Yes, you can end the trial at any time. To do so:

- Log in to the Prisma Cloud administrative console.
- Select Profile > View Subscriptions.
- Select End Trial.

Q. After I activate the trial, are there additional configurations I must apply to start using the unlocked functionality?

The trial activates CIEM and Agentless Workload Scanning capabilities.

- CIEM: The trial activation automatically enables the CIEM functionality. No additional steps are required.

- Agentless Workload Scanning: You will need to do some light configuration changes across cloud accounts to use the Agentless Workload Scanning functionality. Once you activate the trial, Prisma Cloud provides in-product guidance to help you with these steps.

- Attack Paths: For optimal experience, you must activate CIEM and Agentless Workload Scanning before you see attack path alerts. New attack path alerts may take 24 hours to generate once both features have been turned on.

Q. What will happen to my Prisma Cloud credit usage after this trial?

The trial will automatically deactivate after a 30-day period.

- CIEM: The trial deactivation will automatically disable the CIEM functionality. No additional steps are required.

- Agentless Workload Scanning: You will need to disable the Agentless Workload Scanning capability in your cloud accounts if you don't want to consume additional credits after the trial is deactivated.

Q. My trial has concluded and I want to continue with CIEM and/or Agentless Workload Scanning. What should I do next?

Please contact your Palo Alto Networks account representative to explore the Prisma Cloud Security Foundations pricing plan, which includes CIEM, Agentless Workload Scanning, and other foundational cloud security capabilities.