



TECHDOCS

Prisma Cloud Compute Edition Release Notes

22.06 (EoL)

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2023-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

March 23, 2023

Table of Contents

Prisma Cloud Compute Edition Release Information.....	5
22.06 Update 7 Release Notes.....	6
Addressed Issues.....	6
22.06 Update 6 Release Notes.....	7
Addressed Issues.....	7
22.06 Update 5 Release Notes.....	8
Addressed Issues.....	8
22.06 Update 4 Release Notes.....	9
Addressed Issues.....	9
22.06 Update 3 Release Notes.....	10
Addressed Issues.....	10
Upcoming Breaking Changes.....	11
22.06 Update 2 Release Notes.....	12
Enhancements.....	12
Addressed Issues.....	13
End of Support Notifications.....	14
Upcoming breaking changes.....	14
22.06 Update 1 Release Notes.....	16
Improvements, Fixes, and Performance Enhancements.....	16
Known Issues.....	17
End of Support Notifications.....	17
22.06 Release Notes.....	18
CVE Coverage Update.....	18
New Features in the Core Platform.....	19
New Features in Container Security.....	22
New Features in Agentless Security.....	31
New Features in Host Security.....	36
New Features in Serverless Security.....	36
New features in Web Application and API Security (WAAS).....	37
DISA STIG Scan Findings and Justifications.....	44
API Changes.....	44
Addressed Issues.....	45
End of Support Notifications.....	46
Supported Host Operating Systems.....	46
Changes in Existing Behavior.....	47
Known Issues.....	48
Upcoming Deprecation Notifications.....	48
Backward Compatibility for New Features.....	49

Get Help.....	53
Related Documentation.....	54
Request Support.....	55

Prisma Cloud Compute Edition Release Information

Prisma Cloud Compute Edition secures your hosts, containers, and serverless functions.

To view the current operational status of Palo Alto Networks cloud services, see <https://status.paloaltonetworks.com/>.

Before you begin using Prisma Cloud, make sure you review the following information:

- [22.06 Update 7 Release Notes](#)
- [22.06 Update 6 Release Notes](#)
- [22.06 Update 5 Release Notes](#)
- [22.06 Update 4 Release Notes](#)
- [22.06 Update 3 Release Notes](#)
- [22.06 Update 2 Release Notes](#)
- [22.06 Update 1 Release Notes](#)
- [22.06 Release Notes](#)

22.06 Update 7 Release Notes

The following table provides the release details:

Build	22.06.234
Codename	Kepler, 22.06 Update 7
Release date	Mar 13, 2023
Type	Maintenance release
SHA-256 digest	f871922e48194c06a6551760a1e4c93ec89f1c22f0f6c1434b0501503266ba83

Addressed Issues

- Addressed the following issues:
 - Fixed [CVE-2023-25173](#) and [CVE-2023-25153](#) (Severity - Moderate): the *containerd* package is used in the Prisma Cloud Defender and for Agentless Scanning. To address the vulnerability, upgrade to *containerd* version v1.6.18 or v1.5.18 as needed.
 - Fixed [CVE-2022-27664](#) (Severity - High): Updated the net module - [golang.org/x/net - Go Packages](https://golang.org/x/net) to version v0.5.0. WAAS deployments were affected if you have a HTTP2 applications and have deployed WAAS to inspect HTTP2 traffic. Upgrade your Prisma Cloud console and deployed Defenders if you use WAAS to inspect HTTP2 traffic.

22.06 Update 6 Release Notes

The following table provides the release details:

Build	22.06.232
Codename	Kepler, 22.06 Update 6
Release date	February 14, 2023
Type	Maintenance release
SHA-256 digest	70df141032c0ac641f74834e835b9c923405d5db56fa77564843c90d9da5e48a

- [Addressed Issues](#)

Addressed Issues

- The *ubi-minimal* base image's packages are updated to the latest.
- *bits-and-blooms/bloom* Go module is updated to v3.3.1 to fix CVE-2023-0247.
- GoLang is updated to version 1.18.9 to fix CVE-2022-41717.

22.06 Update 5 Release Notes

The following table provides the release details:

Build	22.06.229
Codename	Kepler, 22.06 Update 5
Release date	Dec 8, 2022
Type	Maintenance release
SHA-256 digest	b1831ebfbaf70c6724b236e219b1ae646cbcc381d42922efa6cbded755345fd2

- [Addressed Issues](#)

Addressed Issues

- Fixed CVE-2022-42898 vulnerability found in krb5-libs package in Red Hat Enterprise Linux (RHEL) 8 for the Prisma Cloud Console and the Defender.

22.06 Update 4 Release Notes

The following table provides the release details:

Build	22.06.228
Codename	Kepler, 22.06 Update 4
Release date	Nov 20, 2022
Type	Maintenance release
SHA-256 digest	216ccfd64b8ca66f036b811a6b94cdd38aeb8df34b1fd1af324245ed87bac7db

- [Addressed Issues](#)

Addressed Issues

- Addressed the following issues:
 - CVE-2022-1304 out-of-bounds read/write vulnerability found in e2fsprogs package in Red Hat Enterprise Linux.
 - CVE-2016-3709 a Cross-site scripting (XSS) vulnerability found in libxml2 package in Red Hat Enterprise Linux.
- Fixed an error in the credit usage utilization for WAAS. With this fix, when container/host Defenders are disconnected for 24 hours, the usage of the credit is automatically stopped until the Defenders reconnect.
- Setting the collection scope for greater than 6000 collections under runtime policy rules would freeze, this is now fixed.

22.06 Update 3 Release Notes

The following table provides the release details:

Build	22.06.224
Codename	Kepler, 22.06 Update 3
Release date	Nov 7, 2022
Type	Maintenance release
SHA-256 digest	f0451f05951ab28811f99ebc68adcdf58d17fd332f68290d03eab023d4510495

- [Addressed Issues](#)
- [Upcoming Breaking Changes](#)

Addressed Issues

- Fixed an issue with incorrect health state for a Defender deployed on a container.
- Addressed the following issues:
 - CVE-2020-7711 vulnerability detected in a vendor package - *goxmldsig*.
 - CVE-2022-40674 vulnerability detected in a vendor package - *expat*
 - CVE-2022-41716 vulnerability detected in Google Go Windows environment variable - *exec.cmd* syscall
 - Go update to version 1.18.8. The version includes security fixes.
- Improved the reconnection time for multi-tenant deployments when some tenants are disconnected from the central Console.
- Fixed a DNS resolution error when running a twistcli image scan with the *--tarball* option.
- Fixed an issue where errors were reported in Google cloud discovery scan when the scanned service APIs are disabled.

Now when such APIs are disabled on the Google cloud, cloud discovery do not display these as errors in the results. The messages are added to the console logs.
- Fixed an issue with incorrect cluster information in image scan results on **Monitor > Vulnerabilities > Deployed**.
- Fixed the rule scope selection for Out-of-Band WAAS rule.

When adding a new Out-of-Band WAAS rule, you were unable to choose a container name in the rule scope, or save an Out-of-Band WAAS rule with a scope that included a namespace selection, or did not include an image selection. These issues are now fixed.

Upcoming Breaking Changes

- **Alert Profile**—as announced in [Kepler Update 2](#).

22.06 Update 2 Release Notes

The following table provides the release details:

Build	22.06.213
Codename	Kepler, 22.06 Update 2
Release date	Sep 19, 2022
Type	Maintenance release
SHA-256 digest	d780dd3e80152d98f585868e3dd73e5e02e66c5d1d604a4831694e89d9aadabd

- [Enhancements](#)
- [Addressed Issues](#)
- [End of Support Notifications](#)
- [Upcoming breaking changes](#)

Enhancements

HTTPS Proxy Support for Agentless Scanning

Agentless scanning now supports connections over an HTTPS proxy server. If you use custom certificates for authentication, you can now configure custom certificates for the connection to Console when using [agentless scanning](#).

Embed a Defender in a CloudFormation Fargate Task in YAML format

Prisma Cloud Compute now supports embedding a Defender to a CloudFormation Fargate task in the YAML format, in addition to the JSON format.

Also, Prisma Cloud now supports generating a protected Fargate task definition for a full CloudFormation template that contains other resources except for the task definition itself.

Use the Console (Manage > Defenders > Deploy > Defenders) or the APIs (`/api/22.06/defenders/fargate.yaml`, `/api/22.06/defenders/fargate.json`) to complete the workflow.

Update for CVE-2022-36085

As part of this release, Prisma Cloud has rolled out an update to the vulnerability data stream for [CVE-2022-36085](#). After updating to the enhanced intelligence feed, you may see alerts on vulnerabilities in Prisma Cloud components and Defender images of releases 22.06 Update 1 or older versions. We have determined that Prisma Cloud components are not impacted by these vulnerabilities. There is no risk to continue running any of the supported Prisma Cloud releases.

To ensure these vulnerability alerts do not display, we recommend upgrading to the latest 22.06 release where applicable. If you are not ready to upgrade right away, add an exception in the

default Ignore Twistlock Components rule (under Defend > Vulnerabilities > Images > Deployed) to suppress these vulnerability alerts.

Support for Additional Orchestrators on x86 Architecture

- Google Kubernetes Engine (GKE) version 1.24.2 with containerd version 1.6.6
- Elastic Kubernetes Service (EKS) version 1.23.9 with containerd version 1.6.6
- Azure Kubernetes Service (AKS) version 1.24.3 with containerd version 1.6.4+azure-4 running on Linux
- AKS version 1.24.3 running with containerd version 1.6.6+azure on Windows
- Lightweight Kubernetes (k3s) version v1.24.4+k3s1 with containerd 1.6.6-k3s1
- Openshift version 4.11 with CRI-O 1.24.1
- Rancher Kubernetes Engine (RKE) version 1.24.4+rke2r1 with containerd 1.6.6-k3s1

Name Update for Cloud Native Network Firewall (CNNF)

The Cloud Native Network Firewall (CNNF) is now renamed as Cloud Native Network Segmentation (CNNS).

Addressed Issues

- Fixed an issue that caused Defender to incorrectly report the Host OS as SLES15SP1 instead of SLES15.
- Fixed an internal error that failed to refresh the vulnerability statistics under **Monitor > Vulnerabilities > Vulnerability Explorer**.
- Fixed two issues with Defenders running on containerd/CRI-O nodes:
 - Defenders attempted to scan host file systems during image scans for containers that changed to the host mount namespace. This issue is fixed.
 - Defenders attempted to scan the host where the image had a mount point to the host filesystem and some parent directory of the mount point was a symlink.
- Fixed an issue that prevented editing WAAS rules. On upgrade to 22.06, it was not possible to update or modify WAAS rules configured to protect the same port at multiple endpoints with different attributes, such as TLS, HTTP2, and gRPC. With this fix, such rules can now be modified.
- Fixed the "**Missing required VM instance data**" error encountered during agentless scanning on Azure. Azure hosts with unmanaged operating system disks are skipped during the scan. Agentless scanning doesn't support Azure hosts with an unmanaged operating system disk.
- Fixed a high memory usage issue in Linux distributions where CNNF/CNNS was enabled. In addition to upgrading to this release, CNNF/CNNS users are advised to upgrade 4.15.x kernel to >=5.4.x kernel.

End of Support Notifications

- With the end of support for Maven system dependencies, [Defender injection for java functions](#) is now implemented using the bundle as a Maven internal repository. With this update, `<systemPath>` dependency is no longer used.
- With the end of support for compile dependency in Gradle 7.0, [Defender injection for java functions](#) is updated to implementation dependency using an internal repository.

Upcoming breaking changes

On upgrade to the next release, Lagrange, if you have configured an alert profile on **Compute > Manage > Alerts** and enabled the **Image vulnerabilities (registry and deployed) trigger** as well as the **Immediately alert for deployed resources** setting, you will now be getting immediate alerts for vulnerable registry images along with immediate alerts for deployed images.

Edit alert profile [Close]

- Provider ✓
- Triggers ✓
- Settings ✓
- Summary

Select triggers (1 trigger selected)

✉ Email

Vulnerabilities (1 trigger selected) Alert every 24 hours

- Image vulnerabilities (registry and deployed)**
- Select rules to alert on: 2 items selected
- Host vulnerabilities
- VM images vulnerabilities
- Immediately alert for deployed resources**

Compliance (0 triggers selected)

Cloud discovery (0 triggers selected)

Runtime (0 triggers selected)

Access (0 triggers selected)

Previous Next

The volume of immediate alerts that are generated may be much higher than what you've seen in the previous releases because support for immediate alerting for registry images is being added in Lagrange. With this change, the Image vulnerabilities (registry and deployed) option is being separated into two: Deployed images vulnerabilities and Registry images vulnerabilities, and both these triggers will be enabled if the original trigger was enabled in the alert profile.

22.06 Update 1 Release Notes

The following table provides the release details:

Build	22.06.197
Codename	Kepler, 22.06 Update 1
Release date	Jul 27, 2022
Type	Maintenance release
SHA-256 digest	5aa618314e176d03e559e58d2eba50959365cdc145cba99f5d47d90737d233bf

Improvements, Fixes, and Performance Enhancements

- Added support for more orchestrators:
 - Google Kubernetes Engine (GKE) version 1.23.7 with containerd version 1.5.11
 - GKE version 1.24.1 running on ARM64 architecture. For the full announcement, refer to [our blog](#).
 - VMware Tanzu Kubernetes Grid Integrated (TKGI) version 1.14
 - VMware Tanzu Kubernetes Grid Multicloud (TKGM) version 1.5.1 on Photon 3 and Ubuntu 20.04.03 LTS
- Fixed the broken pipe error that occurred while [downloading a large image CSV](#) for secondary consoles when using Projects. The error was fixed by extending the HTTP client timeout value.
- Fixed the welcome tour screen for new users who don't have an administrator role.
- Fixed an issue wherein the Defenders blocked application deployments on SELinux due to incorrect SELinux labeling on proxy *runc*. The issue was fixed by applying the original *runc*'s SELinux label to the created *runc* proxy binary.
- Fixed the validity period error of [self-signed certificates](#). The limit of 365 has been waved off and the value can now be a whole number greater than or equal to 1.
- Fixed an issue where a Defender scanning a non-docker (CRI-O) registry incorrectly reported all custom compliance checks as passed.
- Fixed error that overwrote the communication port after upgrading a Defender with a custom port from the Prisma Cloud Console UI.
- Fixed an issue that showed different fixes for the same CVE on a single image. Each CVE vulnerability is consolidated and grouped according to OS version for each image and package.
- Fixed issue with missing *runc* path in TKGI with containerd. Specify a custom container runtime socket path when deploying Defenders on TKGI with containerd.
- Fixed issue with the scanned images filter. With this fix, the filter lists all the tags when multiple images have the same digest.
- Fixed an issue of duplicate or missing system rules for WAAS.

- Fixed an issue of unprotected web apps and APIs missing from the report (Monitor > WAAS > Unprotected Web Apps and APIs).
- Fixed an issue where XSS is not detected due to query key/value parsing.

Known Issues

- Defenders are not accepting the self-signed proxy certificate configured for TLS intercept proxies.

Workaround: Ensure the following conditions are met to workaround the issue.

- Your proxy trusts the Prisma Cloud Console Certificate Authority (CA).
- Your proxy uses the client certificate of the Defender when the proxy sends requests from the Defender to the console.
- You obtained the certificates of the Defender and the Prisma Cloud Console CA. Use the `/api/v1/certs/server-certs.sh` API to obtain the needed files:
 - The client key of the Defender: `defender-client-key.pem`
 - The client certificate of the Defender: `defender-client-cert.pem`
 - The Prisma Cloud Console CA certificate: `ca.pem`
- You obtained the password for the client key of the Defender using the `/api/v1/certs/service-parameter` API.

End of Support Notifications

- Debian 9 (Stretch) has reached End of Life (EOL), and users of Debian 9 will not receive any CVE security vulnerabilities from the [Intelligence Stream](#) feed associated with this OS version.

22.06 Release Notes

The following table outlines the release particulars:

Build	22.06.179
Code name	Kepler
Release date	June 09, 2022
Type	Major release
SHA-256 Digest	349505f80b50468eb1eab2448a57b43b578bcd57d780b459ea1d6d00803a1091

- [CVE Coverage Update](#)
- [New Features in the Core Platform](#)
- [New Features in Container Security](#)
- [New Features in Agentless Security](#)
- [New Features in Host Security](#)
- [New features in Serverless Security](#)
- [New Features in WAAS](#)
- [DISA STIG Scan Findings and Justifications](#)
- [API Changes](#)
- [Addressed Issues](#)
- [Changes in Existing Behavior](#)
- [End of Support Notifications](#)
- [Supported Operating Systems](#)
- [Known Issues](#)
- [Deprecation Notifications](#)
- [Backward Compatibility for New Features](#)

CVE Coverage Update

As part of the 22.06 release, Prisma Cloud has rolled out updates to its vulnerability data for Common Vulnerabilities and Exposures (CVEs) in the Intelligence Stream. The new additions are as follows:

- Support for Github Security Advisories vulnerabilities including Go, Java, and Python vulnerabilities.
- Increase of 152% new PRISMA-IDs since the Joule major release.

- Faster addition of CVEs (pre-filled CVEs).

The pre-filled CVEs were added to the Intelligence Stream on an average of 56 days before they were analyzed in the NVD. As an example, the SpringShell CVE (CVE-2022-22965) was published on March 31, 2022, and the NVD analysis was completed on April 8, 2022. 'PRISMA-2022-0130' was published for the vulnerability on March 30, 2022, and was changed to the CVE as soon as it was published in the NVD.

New Features in the Core Platform

In addition to familiarizing yourself with the new features and enhancements in this release, review the minimum [System Requirements](#) for versions that are tested and supported on 22.06.

To download the Prisma Cloud Compute Edition release tarball from the Palo Alto Networks Customer Support Portal (CSP):

1. Log in to the [Palo Alto Networks Customer Support Portal](#).
2. Go to **Updates > Software Updates** and select **Prisma Cloud Compute Edition**.

New Filters in the Vulnerability Explorer

On the [Vulnerability Explorer](#), you can now generate a vulnerabilities report using new filters such as CVSS score and severity threshold. In addition to viewing the filtered results for deployed images, registry images, hosts, and functions under **Vulnerability (CVE) results**, on **Monitor > Vulnerabilities > Vulnerability Explorer**, you can also download a detailed report for CVEs in a CSV format or a detailed report for impacted resources in a CSV format from the Vulnerability Explorer.

Vulnerabilities

[Vulnerability Explorer](#)
[Code repositories](#)
[Images](#)
[Hosts](#)
[Functions](#)
[CVE viewer](#)
[VMware Tanzu blobstore](#)

Vulnerability Explorer

Vulnerabilities across your environment.

2
CVSS threshold: 5 x
Severity threshold: High x

x
?

You cannot combine filters for CVE attributes and collections. To filter by collections, remove the CVE attribute filter.

Top 10 Critical CVE results

[Registry images](#)
•
[Registry images](#)
•
[Hosts](#)
•
[Functions](#)

Results for each CVE display the greatest risk across your entire environment. The values do not consider filters or assigned collections and accounts.

More than 100 results. Only the first 100 results are shown. Export to CSV to get the full list or consider refining your search parameters.

	Highest risk score	Highest CVE risk factors	Highest severity	Highest CVSS	All impacted packages
00	90	6	Critical	9.8	libx11:2:1.6.4-3
35	89	6	Critical	9.8	libx11:2:1.6.7-1+deb10u1, libx11:2:1.6.4-3
0888	89	6	High	8.8	php-pear:1:1.10.1+submodules+notgz-9
18	88	5	High	7.5	php7.0:7.0.30-0+deb9u1
88	88	5	Critical	9.8	inetutils:2:1.9.4-2
91	88	5	Critical	9.8	busybox:1.28.4-r2, busybox:1.33.1-r3, busybox:1.26.2-r7
95	88	6	High	8.8	tiff:4.0.8-2+deb9u2
43	88	5	Critical	9.8	php7.0:7.0.30-0+deb9u1
28	87	6	High	7.2	mariadb-10.1:10.1.26-0+deb9u1
24	87	5	Critical	9.8	php7.0:7.0.30-0+deb9u1

Vulnerability Scan Report for Registry Images

With the vulnerabilities report for registry images (**Monitor > Vulnerabilities > Images > Registries**), you can review the [top 10 critical CVEs](#) discovered in your registry images and search by a CVE ID to view the results for both registry and deployed images that are impacted by a CVE.

Vulnerabilities (CVEs)

Registry images  Hosts  Functions Download

Display the greatest risk across your entire environment. The values do not consider filters or assigned collections and accounts.

Risk score	Highest CVE risk factors	Highest severity	Highest CVSS	All impacted packages
90	6	Critical	9.8	libx11:2:1.6.4-3
89	6	Critical	9.8	libx11:2:1.6.7-1+deb10u1, libx11:2:1.6.4-3
89	6	High	8.8	php-pear:1:1.10.1+submodules+notgz-9
88	5	High	7.5	php7.0:7.0.30-0+deb9u1
88	5	Critical	9.8	inetutils:2:1.9.4-2
88	5	Critical	9.8	busybox:1.28.4-r2, busybox:1.33.1-r3, busybox:1.26.2-r7
88	6	High	8.8	tiff:4.0.8-2+deb9u2
88	5	Critical	9.8	php7.0:7.0.30-0+deb9u1
87	6	High	7.2	mariadb-10.1:10.1.26-0+deb9u1
87	5	Critical	9.8	php7.0:7.0.30-0+deb9u1

[Download vulnerability report for an impacted resource](#)

ARM64 Architecture Support

You can now deploy Defenders to protect AWS workloads based on the Linux ARM64 architecture.

With ARM64 support, you can secure your deployments and enhance the cost savings for compute and network-intensive workloads that use cloud-native compute offerings such as the AWS Graviton processor.

To use Prisma Cloud on ARM64 architecture, see the [system requirements](#).

Compliance Alert Triggers for Slack

You can now trigger and send vulnerabilities detected for container and image compliance, and host compliance to your Slack integration.

Learn how to [configure these new triggers for Slack alerts](#).

Integrate with Azure Active Directory Using SAML 2.0

Prisma Cloud Compute now uses the Microsoft Graph API for integrating with Azure Active Directory (AD) resources. This transition is inline with the deprecation notice from Microsoft of the Azure AD Graph API and the Azure Active Directory Authentication Library (ADAL).

For authenticating users on the Prisma Cloud Console, you must replace the *Directory.Read.All* permission for Azure Active Directory Graph with the *Directory.Read.All* permission for the Microsoft Graph API. For the correct permissions to use Azure AD with SAML 2.0, see [correct permissions](#).

OIDC User Identity Mapping

You can map OIDC identities to Prisma Cloud users as required by the specification. Instead of using the default *sub* attribute, you can now use [several more friendly attributes](#) like *email* or *username*.

Improvements in Runtime Protection

The container model learning is improved to reduce false positive audits when a binary is modified during container creation. The grace time for binaries added after the container has started is now at 10 seconds. Additionally, for CI/CD environments where dedicated containers are used to pull images, you can now allow pulling images. For example, if a container was started with podman as one of its startup processes, the Dockerfile will allow this action and ignore runtime audits.

Enhanced Coverage for Certificate Authentication with Azure

You can now authenticate with Azure using a certificate for the following integrations:

- Cloud discovery
- Azure Key Vault
- ACR registry scanning
- Azure serverless function scanning
- Azure VM image scanning

GKE Autopilot Deployment Improvement

When deploying Defenders into your Kubernetes deployment for [GKE Autopilot](#), you have a new toggle in the console and a corresponding `twistcli` flag that makes the workflow easier. The improvements automatically remove the mounts that are not relevant to the Autopilot deployment and enable you to add the annotation required to deploy Defenders successfully.

On the console, **Manage > Defenders > Deploy > Defenders**, select **Kubernetes** and enable the **Nodes use Container Runtime Interface (CRI), not Docker** and **GKE Autopilot deployment**.

The `--gke-autopilot` flag in `twistcli` adds the annotation to the YAML file or Helm chart.

For example, `./twistcli defender export kubernetes --gke-autopilot --cri --cluster-address <console address> --address https://<console address>:8083`

New Features in Container Security

Vulnerability and Compliance Scanning for Workloads Protected by App-Embedded Defenders

App-Embedded Defenders can now scan the workloads they protect for vulnerabilities and compliance issues. They can also collect and report package information and metadata about the cloud environments in which they run.

Go to **Monitor > Vulnerabilities > Images > Deployed** and **Monitor > Compliance > Images > Deployed** to review the scan reports.

Details

ian-app3
 e8014016-8bad-cd8d-dbce-77741ce554b3
 on Alpine Linux v3.15
 3.15.0

- Compliance
- Runtime
- Layers
- Process info
- Package info
- Environment
- Labels

Vulnerabilities by keywords and attributes ? 7 total entries

↓↑	Highest severity	↓↑	Description
	critical		expat version 2.4.1-r0 has 15 vulnerabilities
	high		zlib version 1.2.11-r3 has 1 vulnerability
	high		openssl (used in libssl1.1, libcrypto1.1) version 1.1.1l-r7 has 2 vulnerabilities
	high		libretls version 3.3.4-r2 has 1 vulnerability
	medium		krb5 (used in krb5-libs) version 1.19.2-r4 has 1 vulnerability
	low		xz (used in xz-libs) version 5.2.5-r0 has 1 vulnerability
	low		busybox (used in ssl_client, busybox) version 1.34.1-r3 has 2 vulnerabilities

App-embedded details

App ID: multicontainer-4cad10adf9640d7a85f840c5fb7dc80
 Image: 123456789123.dkr.ecr.us-east-1.amazonaws.com/my-registry/debian10
 Container name: fargateapp-debian10-py

Runtime Environment

Cloud provider: AWS
 Account ID: 123456789123
 Region: us-east-1
 Cluster: ECS-fargate
 Instance ID: 4cad10adf9640d7a85f840c5fb7dc80
 Resource Name: fargateapp-debian10-py
 Image: 123456789123.dkr.ecr.us-east-1.amazonaws.com/my-registry/debian10
 Start time: May 23, 2022 4:10:49 PM

Improved Visibility for CaaS Workloads Protected by App-Embedded Defenders

For CaaS (Container as a Service) workloads protected by the App-Embedded Defenders, you can now view more metadata on the cloud environment on which it is deployed, forensics, and runtime audits on the **Monitor > Runtime > App-Embedded observations** page. You can filter the workloads in the table by a number of facets, including collections, account ID, and clusters.

Runtime

Explorer

Container models

Host observations

App-Embedded observations

Image analysis sandbox

App-Embedded observations

App-Embedded observations are automatically collected for any entity deployed with App-Embedded Defender, including environment metadata, runtime audits, forensics for processes, file system and network details.

✕

? 3 total entries

	↓↑ Image	↓↑ Container	↓↑ Cluster
app:df915f34-3f8d-bb4c-4...	eks-fargate-app		
er:99ac827f88bd4332bf38d...	vulnerables/web-dvwa	web-dvwa	ecs-fargate-cluster
t-defended-4containers:f4ae...	account-id.dkr.ecr.us-east-1.amazonaws.c...	fargateapp-debian1...	ecs-fargate-cluster

Runtime File System Audits for App-Embedded Defenders

App-Embedded Defender runtime defense now includes support for container file systems so that you can continuously monitor and protect containers from suspicious file system activities and malware.

Runtime rule

Enter the rule name

Enter notes

All Click to select collections

- Networking
- File system**
- Custom rules (0)

File system monitoring Enabled

For file system activity, Defenders must be enabled for file system protection during deployment. Enable it by default on [Defender settings](#), and use the [Defenders page](#) to review the file system status for each Defender.

and

Specify list of allowed file system paths

! Denied & fallback

Effect

Alert Prevent

Changes to binaries and certificates On

Detection of encrypted/packed binaries ? On

Changes to SSH and admin account configuration files On

Automatically Extract Fargate Task Entrypoint at Embed-Time

To streamline the embed flow and eliminate manual intervention (that is updating task definitions to explicitly specify entrypoints), Prisma Cloud can automatically find the image entrypoint and set it up in the protected task definition.

Now, when Prisma Cloud generates a [protected task definition](#), it knows the entrypoint and/or cmd instructions of the container image during the first run of the App-Embedded Defender.

The screenshot shows the Prisma Cloud console interface. On the left is a dark sidebar with the 'CLOUD BY PALO ALTO NETWORKS' logo and a navigation menu including 'Radars', 'Defend', 'Monitor', 'Manage', 'Cloud accounts', 'Logs', 'Projects', 'Defenders', 'Alerts', 'Collections and Tags', 'Authentication', and 'System'. The main content area is titled 'Manage / Defenders' and has three tabs: 'Manage', 'Names', and 'Deploy'. Under the 'Deploy' tab, there are three numbered steps: 3. 'Choose the Defender type' with a dropdown menu showing 'Container Defender - App-Embedded'; 4. 'Enable file system runtime protection' with a toggle switch set to 'On'; and 5. 'Deploy App-Embedded Defender'. Below step 5, there are three buttons for 'Deployment type': 'Fargate task' (selected), 'Dockerfile', and 'Manual'. A red rectangular box highlights the 'Automatically extract Entrypoint' section, which includes a toggle switch set to 'On', a help icon, and three options: 'Get Entrypoint from scanned registry results' (marked with a green check and 'Automatically enabled'), 'Get Entrypoint directly from registry using API (Optional)', and 'Registry type' (a dropdown menu showing 'Amazon EC2 Container Registry'). Below this is a 'Credential' dropdown menu. At the bottom of the highlighted section is a 'Use Entrypoint interpreter' toggle switch set to 'Off'.

CloudFormation Template (CFT) Support for Fargate Task Definitions

You can now generate protected Fargate task definitions in the CFT format for embedding an App-Embedded Defender.

Manage / Defenders

Manage Names **Deploy**

Enable file system runtime protection ? On

Deploy App-Embedded Defender

Deployment type **Fargate task** Dockerfile Manual

Automatically extract Entrypoint ? Off

Use Entrypoint interpreter Off

Template type Native Fargate **CloudFormation**

Insert task definition in CloudFormation format, e.g:

```
{
  "Type": "AWS::ECS::TaskDefinition",
  "Properties": {
    "ContainerDefinitions": [ ContainerDefinition, ... ],
    "Cpu": String,
    "NetworkMode": String,
    "Family": String,
    ...
  }
}
```

Generated task definition

Generate protected task

Additional Checks for CIS Benchmark for OpenShift

In 22.06, we've added support for more checks from the CIS OpenShift benchmark.

For more information, see [CIS Benchmarks](#).

Create new compliance rule

00111	master	● high	Docker (CIS v1.3.1) host config	Block	Ensure that the API server pod specification permissions are set to 644 or more restrictive
001111	master	● high	daemon config	Block	Ensure that the etcd data directory permissions are set to 700 or more restrictive
001112	master	● high	daemon config files	Block	Ensure that the etcd data directory ownership is set to root:root
001113	master	● high	security operations	Block	Ensure that the admin.conf file permissions are set to 644 or more restrictive
001114	master	● high	CRI runtime host config	Block	Ensure that the admin.conf file ownership is root:root
			Kubernetes 1.20 (CIS v1.0.0) master worker federation	Block	
			Linux (CIS v2.0.0) host		
			Custom custom		
			Docker (DISA STIG) host config		
			OpenShift (CIS v1.1.0) master worker		

Custom message for blocked requests

Specify customized error string (e.g., Open a ticket at <https://helpdesk.com>)

Terminal output verbosity for blocked requests

Summary Detailed

Reported results

Failed checks only Passed and failed checks

Cancel

Support for Vulnerability and Compliance Scanning for Windows Containers

Windows Container Defender on hosts with the containerd runtime can now scan Windows containers for vulnerabilities and compliance issues. This is supported on AKS only.

In addition, deployed Windows Container Defenders can now be configured to scan Windows images in registries.

twistcli for Windows has also been extended to scan Windows images on Windows hosts with containerd installed.

Support for Google Artifact Registry

You can now scan [Google Artifact Registries](#) using [Prisma Cloud Compute](#).

Add new registry

Version	Google Artifact Registry ▼
Registry	<ul style="list-style-type: none"> Amazon EC2 Container Registry Azure Container Registry CoreOS Quay Docker Registry v2 Docker Trusted Registry Google Artifact Registry Google Container Registry Harbor IBM Cloud Container Registry JFrog Artifactory Red Hat OpenShift Sonatype Nexus
Repository	
Repositories to exclude	
Tag	
Tags to exclude	
Credential	
OS type	Linux x86_64 ▼
Scanners scope ?	■ All Click to select collections
Number of scanners ?	2
Cap ?	5
Version matching pattern	Specify version matching pattern (e.g. *-%d.%d.%d , image-%Y%M%D%H%m)

Cancel Add

Registry Scanning Enhancements

Enhanced registry scanning progress status within the Prisma Cloud Console UI and logs.

The enhancements provide the option to choose whether to stop or continue an in-progress scan when saving the registry settings.

After you [configure registry scanning](#), Prisma Cloud automatically scans the images within for vulnerabilities using an improved flow.

Scan Image Tar Files with twistcli

twistcli can [scan image tarballs](#) for the [Docker Image Specification v1.1](#) and later.

This enhancement enables support for vendors who deliver container images as tar files, not via a registry, and the integration with [Kaniko](#), a tool that builds images in a Kubernetes cluster from a Dockerfile without access to a Docker daemon.

Rule to Allow Activity in Attached Sessions

When you start a session inside pods or containers running in your deployment using commands such as `kubectl exec` or `docker exec`, you can now explicitly specify whether the rule should allow the activity in attached sessions. This option on **Defend Runtime Container Policy > Add rule > Processes** helps you reduce the volume of alerts generated for the allowed activities and processes.

When enabled, process, network, and filesystem activity executed in an attached session such as `kubectl exec`, is explicitly allowed without additional runtime analysis.

Only Defender versions 22.06 or later will support this capability.

...es available. [Review them](#)

Defend / Runtime

Container policy Host policy Serverless policy App-Embedded policy

Container runtime policy

Manually defined rules augment learned models. By default, everything is denied if not within the learned models. Manual rules can be used to control detections and define explicitly allowed lists and/or explicitly denied lists. Explicit allow lists in manual rules override explicit deny lists.

Enable automatic runtime learning On

Filter runtime rules 2 total entries

Rule name	Owner	Scope	Modified	Entities
Per label rule	admin	—	Jan 29, 2022 11:42:15 PM	Sh
Default rule	admin	—	Feb 1, 2022 3:28:41 AM	Sh

New Features in Agentless Security

Support for Microsoft Azure

Agentless scanning is now available for vulnerability scanning and compliance scanning on Azure. To configure and onboard agentless scanning on Azure, see [configure agentless scanning](#).

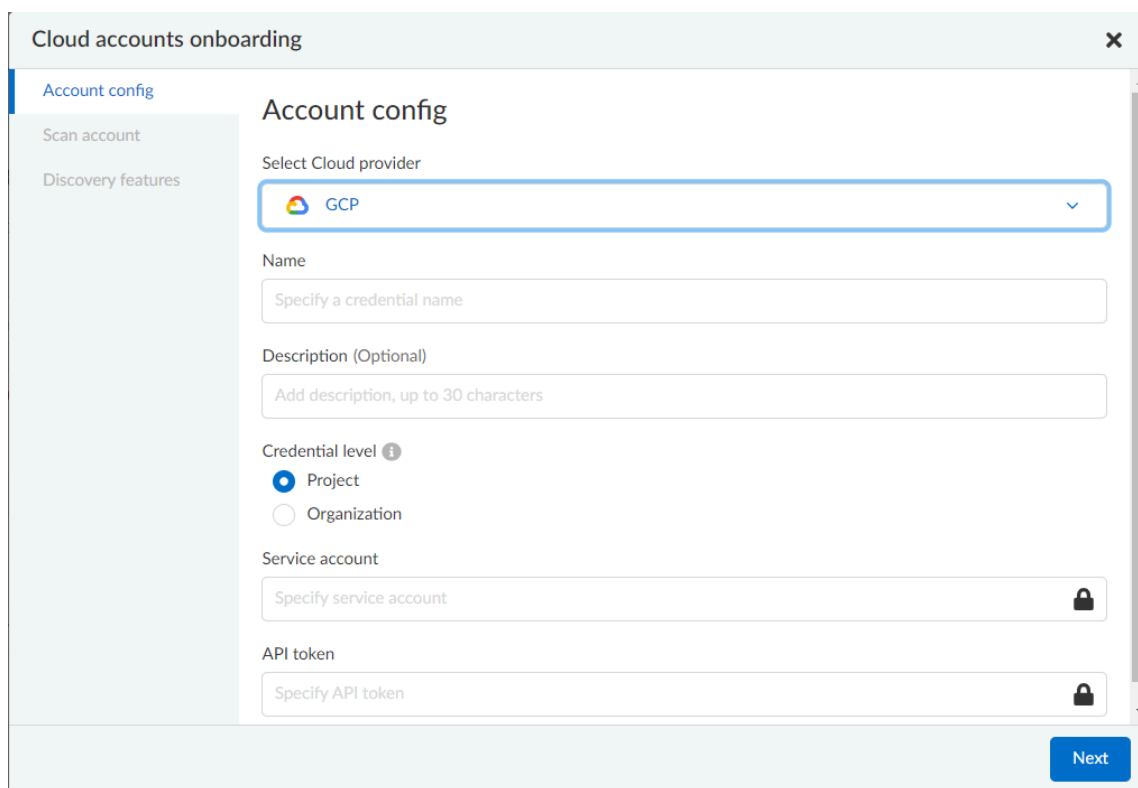
The screenshot shows a web interface for 'Cloud accounts onboarding'. The main heading is 'Account config'. On the left, there is a sidebar with three items: 'Account config' (highlighted), 'Scan account', and 'Discovery features'. The main content area contains the following fields and options:

- Select Cloud provider:** A dropdown menu with 'Azure' selected.
- Name:** A text input field with the placeholder 'Specify a credential name'.
- Description (Optional):** A text input field with the placeholder 'Add description, up to 30 characters'.
- Authentication method:** Two radio buttons: 'Service key' (selected) and 'Certificate'.
- Service Key:** A text input field with the placeholder 'Specify service key' and a lock icon on the right.

A blue 'Next' button is located at the bottom right of the form.

Support for Google Cloud

Agentless scanning is now available for vulnerability scanning and compliance scanning on Google Cloud. To configure and onboard agentless scanning on Google Cloud, see [configure agentless scanning](#).



Compliance and Custom Compliance Support

With agentless scanning you can now scan hosts from all three major cloud providers—AWS, Azure, and Google Cloud—against compliance benchmarks. In addition to out of-the-box checks, you can apply user defined [custom compliance checks](#) and scan against the host file system.

Host details

Hostname	tel-master.c.compute-pm.internal	Provider	GCP
OS distribution	Ubuntu 18.04.5 LTS	Region	us-central1-a
OS release	blonic	VM image	ubuntu-1804-bionic-v20201114
Scan time	Jun 2, 2022 2:52:48 AM		
Docker version	20.10.7		

Vulnerabilities | **Compliance** | Runtime | Package info | Environment

Id	Category	Type	Severity	Description
^ 6143	Linux	host	● critical	(CIS_Linux_2.0.0 - 1.4.3) Ensure authentication required for single user mode
Full description		Single user mode is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.		
Cause		Password should be set for user "root". File: /etc/shadow		
∨ 63512	Linux	host	● high	(CIS_Linux_2.0.0 - 3.5.1.2) Ensure IPv6 loopback traffic is configured
∨ 63511	Linux	host	● high	(CIS_Linux_2.0.0 - 3.5.1.1) Ensure IPv6 default deny firewall policy
∨ 62216	Linux	host	● high	(CIS_Linux_2.0.0 - 2.2.16) Ensure rsync service is not enabled
∨ 6628	Linux	host	● high	(CIS_Linux_2.0.0 - 6.2.8) Ensure users' home directories permissions are 750 or more restrictive

Close

Unpatched OS Detection

In addition to vulnerabilities and compliance scanning, you can now track pending OS security updates in this release with agentless scanning.

Host details

Hostname	del-master-c-compute-pm-internal	Provider	Google Cloud
OS distribution	Ubuntu 18.04.5 LTS	Region	us-central1-a
OS release	bionic	VM image	ubuntu-1804-bionic-v20201014
Scan time	Jun 2, 2022 7:52:48 AM		
Docker version	20.10.7		

Vulnerabilities | **Compliance** | Runtime | Package info | Environment

Filter compliance by keywords and attributes

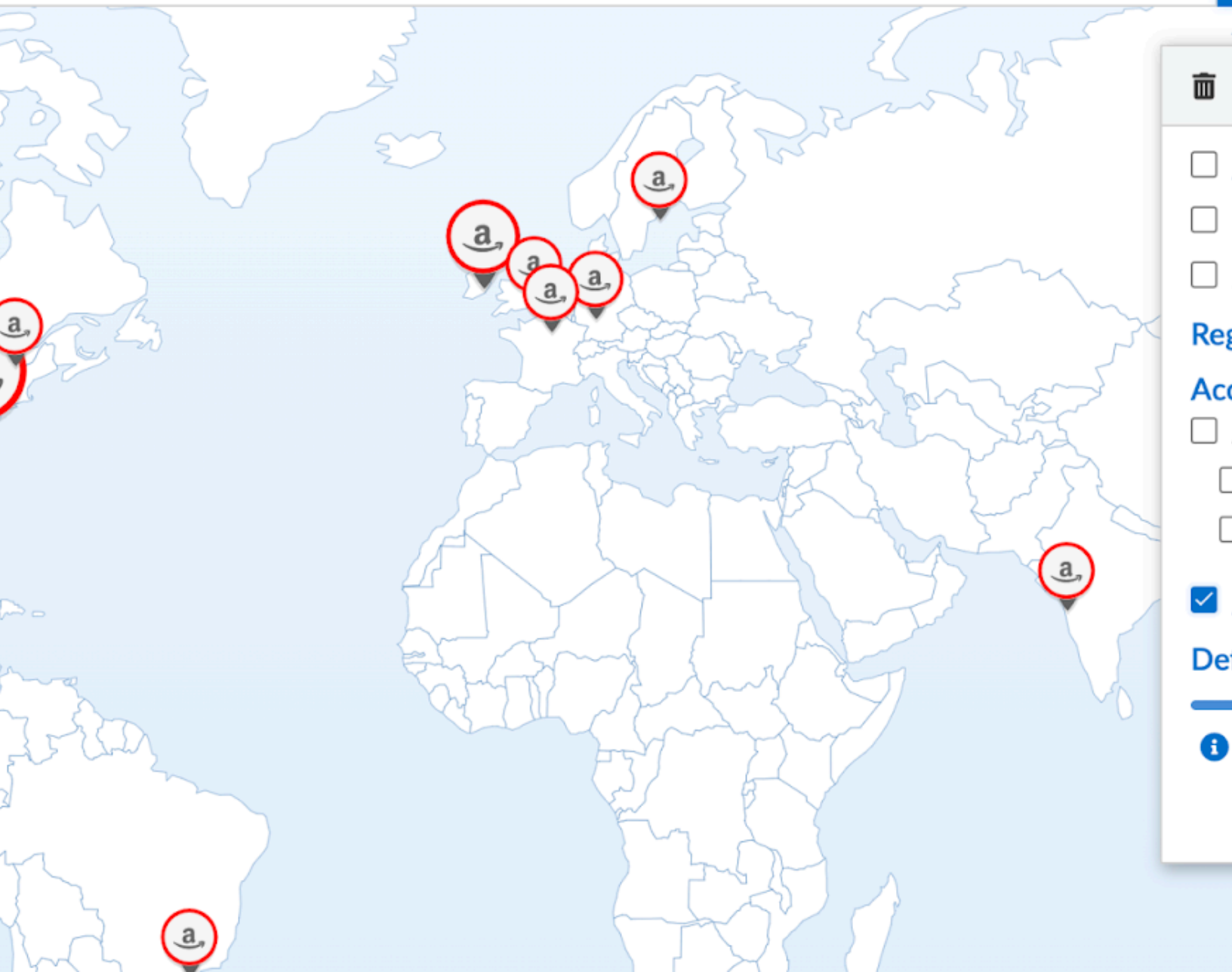
Id	Category	Type	Severity	Description
6112	Linux	host	high	(CIS_Linux_2.0.0 - 1.1.2) Ensure /tmp is configured
656	Linux	host	high	(CIS_Linux_2.0.0 - 5.6) Ensure access to the su command is restricted
449	Twistlock Labs	Linux host	high	Ensure no pending OS security updates
Full description		Keeping your computer's software up to date is the single most important task for protecting your system. It is highly recommended to install official OS security updates as soon as possible		
Cause		The following security updates were detected: distro-info (0.18ubuntu0.18.04.1 Ubuntu:18.04/bionic-updates, Ubuntu:18.04/bionic-security [amd64])		
224	Docker	daemon config	high	(CIS_Docker_v1.3.1 - 2.14) Ensure containers are restricted from acquiring new privileges
211	Docker	daemon config	high	(CIS_Docker_v1.3.1 - 2.12) Use authorization plugin

Close

Unscanned Cloud Account Detection

You can now easily discover regions within AWS, Azure, or Google Cloud accounts where agentless scanning is not enabled, and enable scanning for those cloud accounts.

view



Proxy Support

In this release, you can manage how scanners connect to the Prisma Cloud Console for agentless scanning. If you use a proxy, you can configure the proxy configuration in the scan settings for accounts under **Manage > Cloud Accounts**.

New Features in Host Security

Auto-Defend Host Process Update

When you set up the process to automatically deploy Defenders on hosts, this update ensures that Host Defenders are not deployed on container hosts. Hosts running containers require Container Defenders to protect and secure both the host and the containers on it.

Learn about the [deployment process for auto-defend hosts](#).

CIS Linux Benchmark Update

The CIS Linux Benchmark now includes 13 additional checks. You can find the additional controls in the **Defend > Compliance > Hosts > CIS Linux** template.

New Features in Serverless Security

Runtime Protection for Azure Functions

Serverless Defenders now offer runtime protection for [Azure Functions](#). Functions implemented in C# (.NET Core) 3.1 and 6.0 are supported.

Manage / Defenders

Manage Names **Deploy**

Defenders Host auto-defend Serverless auto-defend

Deploy Defenders

Defenders enforce the policies created in Console. Install Defender on each host you want Prisma Cloud to protect.

Deployment method

Orchestrator

Single Defender

Choose the name that Defender will use to connect to this Console

35.238.63.75

Choose the Defender type

Serverless Defender - Azure

Container Defender - Linux

Container Defender - Windows

Host Defender - Linux

Host Defender - Windows

Container Defender - App-Embedded

Tanzu Application Service Defender

Serverless Defender - AWS

Serverless Defender - Azure

Unzip the bundle in your function's root directory

New features in Web Application and API Security (WAAS)

WAAS Out of Band Detection

Out of band is a new mode for deploying Web Application and API Security (WAAS). It enables you to inspect HTTP messages to an application based on a mirror of the traffic, without the need for setting up WAAS as an inline proxy, so that you can receive alerts on malicious requests such as OWASP top alerts, bot traffic, and API events. It provides you with API discovery and alerting without impacting the flow, availability, or response time of the protected web application.

Out of band detection also allows you to extend your WAAS approach:

- You can monitor your resources deployed on AWS with VPC traffic mirroring from workloads. This option gives you the flexibility to monitor environments without deploying Defenders.

- If you have deployed Defenders in your environment, but are not using the WAAS capabilities on Compute, you can mirror traffic for an out of band inspection without requiring any additional configuration.

After you configure a custom rule for out of band mode (**Defend > WAAS > Out of band**), all the detections are applied on a read-only copy of the traffic. And you can view the out of band traffic details on **Monitor > WAAS > API observations > Out of band observations**.

Host App-Embedded Serverless **Out of band** Network lists Log scrubbing

Out of band WAAS policy

Designed to let you tailor the best-suited protection for the out of band in your environment.

Firewall rules by keywords and attributes × ? 1 total entry

	Description (optional)	Scope	Modified
			Apr 17, 2022 11:17:43

Click to edit scope

Discovery On

Automatically detect ports On

Traffic mirroring Off

Filter applications by keywords and attributes × ?

App ID	HTTP host	Protection layer	Description
There is no data to show			

OpenAPI Definition File Scanning

You can scan OpenAPI 2.X and 3.X definition files in either YAML or JSON formats, and generate a report for any errors or shortcomings such as structural issues, gaps in adherence to security guidelines and best practices.

You can initiate a scan through twistcli, upload a file to the Console, or import a definition file in to a WAAS app. The scan reports are available under **Monitor > WAAS > API definition scan**.

API observations **API definition scan** Unprotected web apps

API definition scan

Issues and misconfigurations.

Search for words and attributes 1 total entry

Source	Issues found	Scan date
Imported from	8	Mar 16, 2022, 6:31:20 PM

Rows Page

Automatic Port Detection of WAAS Applications for Containers or Hosts

When you enable the automatic detection of ports in WAAS **Container**, **Host**, or **Out of band** rules, you can secure ports used by unprotected web applications. The automatic detection of ports makes it easier to deploy WAAS at scale because you can protect web applications without the knowledge of which ports are used. Additionally, you can add specific ports to the protected HTTP endpoints within each app in your deployment.

Create new WAAS rule

Rule name

Notes

Scope

API endpoint discovery On

Automatically detect ports Off

VPC traffic mirroring Off

Customization of Response Headers

You can append or override names and values in HTTP response headers for **Containers**, **Hosts**, and **App Embedded** deployments that are sent from WAAS protected applications.

WAAS app

Import an app by importing an OpenAPI/Swagger spec file or by manually specifying its API endpoints. Importing a spec file will overwrite all previously defined endpoints that were manually defined.

API protection

Response headers

Header	Values	Mode
Content-Type	text/html	<input type="radio"/> Override <input checked="" type="radio"/> Append

Cancel Create

WAAS Actions for HTTP Messages that Exceed Body Inspection Limits

You can now apply the **Alert**, **Prevent**, or **Ban** WAAS actions for HTTP messages that exceed the body inspection limit and ensure that messages that exceed the inspection limit are not forwarded to the protected application.

To enforce these limitations, you must have a minimum Defender version of 22.01 (Joule).

And with custom rules (**Defend** > **WAAS** > **Out of band**), you can apply **Disable** or **Alert** actions for HTTP messages that exceed the body inspection limit.

HTTP body inspection On

HTTP body inspection size limit (in bytes)


 Increasing body inspection limit may have an adverse effect on performance and memory consumption.

HTTP body inspection limit exceeded
Disable
Alert
Prevent
Ban

Attacker IP Addition to a Network List

When a WAAS event includes an attacker IP address, you can now directly click a link to add the attacker IP address to an existing or new network list from **Monitor > Events > Aggregated WAAS events > Attacker**.

WAAS Events

 Alert

1

waas-container

Denied IP

2c4ac4b2da5014361dffa029e3047838942b0db189d01176ea...

/k8s_dvwa_dvwa_dvwa_5a666e45-5914-4583-bced-95c862d6...

infoslack/dvwa:latest

qa-ruby-env1

User-agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10...

Host 34.72.32.31:9001

Url (Show decoded) 34.72.32.31:9001/phpinfo.php

Path /phpinfo.php

Header names Accept, Accept-Encoding, Accept-Language

Response header Cache-Control, Content-Type, Date, Expires


Status code 200

ge

31.154.166.148 matched a denied subnet address 31.154.166.148


Attacker

Source IP 31.154.166.148

Source country  IL


Regex Match in Forensics Message

When defining a custom rule, you can now define a regular expression to match for strings and include the matched information in the forensics message.

test rule 

Specify short description

Attack using HTTP %req.http_version matching on the following payload: %regexMatches

waas-request 

Press OPTION+SPACE to autocomplete allowed event properties, operators and transformations

```
req.http_version = "1.1" and req.path contains /a.*/
```

Defender Compatibility with Custom Rules

To make it easier to review and make sure that all Defenders meet the minimum version requirement for a rule, you can now view the minimum Defender version required to use each rule. The Defender version information is displayed in a new column within the custom rules table.

-9541

- Definition
- App firewall
- DoS protection
- Access control
- Bot protection
- Custom rules**
- Advanced settings

Applied by client IP

Use of "Allow" effect and transformation functions in custom rules is not supported in defenders running versions older than 22.03.139

Search custom rules by keywords and attributes ? 1 total entry [+ Add rule](#)

↓↑	Rule name	↓↑	Owner	Minimum defe...	Effect
est	RULE		admin	22.01	Disable Allow Alert Prevent Ba

WAAS Proxy Error Statistics

On **Radar > WAAS connectivity monitor** you can view WAAS proxy statistics for blocked requests, count of requests when the inspection limit was exceeded, and parsing errors.

WAAS connectivity monitor

Last updated 3/31/22 2:07 PM [Refresh](#)

Aggregation start time 3/31/22 2:00 PM [Reset](#)

⚠ WAAS errors 0 Errors

[Show all rules](#)

WAAS statistics

- 4 Incoming requests
- 2 Forwarded requests
- 2 Blocked requests
- 0 Interstitial pages served
- 0 reCAPTCHAs served
- 1 Parsing errors
- 1 Inspection limit exceeded

Application

- 0 1XX responses
- 0 2XX responses
- 1 3XX responses
- 1 4XX responses
- 0 5XX responses
- 0 Timeouts

DISA STIG Scan Findings and Justifications

Every [release](#), we perform an SCAP scan of the Prisma Cloud Compute Console and Defender images. The process is based upon the U.S. Air Force's Platform 1 "[Repo One](#)" [OpenSCAP scan](#) of the Prisma Cloud Compute images. We compare our scan results to [IronBank's](#) latest approved UBI8-minimal scan findings. Any discrepancies are addressed or justified.

API Changes

GET /stats/vulnerabilities

Introduces a change in the existing API endpoint that fetches the vulnerabilities (CVEs) affecting an environment. The data for each CVE, such as impacted packages, highest severity, and so on, is now based on the entire environment irrespective of the collections filter, assigned collections, or assigned accounts.

Also, the impacted resources and distribution counts are not retrieved and are returned as zero when you apply filters or are assigned with specific collections or accounts.

One more change in this API endpoint is that the value of the *status* field will now be empty. In the context of a CVE, there can be multiple fix statuses, depending on the impacted package. Therefore, providing a fix status per CVE is incorrect and was removed. To get the right fix status according to the package, use additional endpoint to fetch the resources impacted by the CVE and their details.

GET /stats/vulnerabilities/impacted-resources

Introduces new optional query parameters such as **pagination** and **resource type** to the existing API endpoint. To enable backward compatibility, if you don't use these optional query parameters, the API response will display results without pagination and registry images, and similar to the response in the previous releases (Joule or earlier).

Note: Make sure to update your scripts before the Newton release. Starting with the Newton release, the API response will no longer support requests without the pagination and resource type query parameters.

GET /stats/vulnerabilities/download

Introduces a new API endpoint that downloads a detailed report for CVEs in a CSV format.

GET /stats/vulnerabilities/impacted-resources/download

Introduces a new API endpoint that downloads a detailed report for impacted resources in a CSV format.

PUT policies/firewall/app/out-of-band

Introduces a new API endpoint that updates or edits a WAAS custom rule for **out of band traffic**.

GET policies/firewall/app/out-of-band

Introduces a new API endpoint that discovers and detects the HTTP traffic for an existing WAAS out of band custom rule.

GET policies/firewall/app/out-of-band/impacted

Introduces a new API endpoint that fetches the impacted resources list for an existing WAAS out of band custom rule.

POST waas/openapi-scans

Introduces a new API endpoint that scans the API definition files and generates a report for any errors, or shortcomings such as structural issues, compromised security, best practices, and so on. API definition scan supports scanning OpenAPI 2.X and 3.X definition files in either YAML or JSON formats.

GET profiles/app-embedded

Introduces a new API endpoint that fetches the app-embedded runtime metadata.

GET profiles/app-embedded/download

Introduces a new API endpoint that downloads the app-embedded runtime profiles in a CSV format.

GET util/arm64/twistcli

Introduces a new API endpoint that downloads an x64 bit Linux ARM architecture twistcli in a ZIP format.

Addressed Issues

- Fixed an issue where fixedDate for Windows vulnerabilities did not update.
- The Intelligence Stream is updated to fix an issue where some Red Hat Enterprise Linux (RHEL) packages were incorrectly reported as vulnerable.

This issue occurred because Red Hat had duplicate records of the same CVE in their OVAL feed, where one was fixed and the other one was not.

- Security Fixes

In accordance with the [security assurance policy](#), this release contains updates to resolve older vulnerabilities in packaged dependencies:

Console & Defender:

- Upgraded Go Lang version
- Removed mongodb-tools binaries
- Containerd updates for Kubernetes (github.com/containerd/containerd)
- Open Policy Agent updates (github.com/open-policy-agent/opa)
- Runc updates (github.com/opencontainers/runc)
- Kubernetes (k8s.io/kubernetes)
- Mongod
- MongoDB Go driver (go.mongodb.org/mongo-driver)
- AWS SDK for Go (github.com/aws/aws-sdk-go)
- Dependency updates for:
 - Package xz (github.com/ulikunitz/xz)
 - YAML for Go package (gopkg.in/yaml.v3)

Defender

- github.com/docker/distribution
- github.com/tidwall/gjson

Console

- Dependency updates for `com.google.code.gson_gson`

End of Support Notifications

The following list of items are no longer supported in 22.06.

- With the RedHat EOL announcement for OpenShift 3.11, Prisma Cloud no longer supports Openshift 3.11.

Supported Host Operating Systems

Prisma Cloud now supports hosts running x86 architecture on multiple platforms and hosts running ARM64 architecture on AWS.

Review the full [system requirements](#) for all supported operating systems.

x86 Architecture

In this release, Prisma Cloud added support for the following host operating systems on x86 architecture:

- Bottlerocket OS 1.7
- Latest Amazon Linux 2

- Latest Container-Optimized OS on Google Cloud
- Ubuntu 22.04 LTS

ARM64

In this release, Prisma Cloud added support for the following host operating systems on ARM64 architecture running on AWS:

- Amazon Linux 2
- Ubuntu 18.04 LTS
- Debian 10
- RHEL 8.4
- CentOS 8
- Photon OS 4

Changes in Existing Behavior

- For short-lived containers, that is when a container is created and immediately terminated, the image will not be scanned. In previous versions, the image was scanned by monitoring pull events from the registry.
- An additional permission is added to AWS agentless scanning template.

For existing accounts that are enabled for agentless scans you will need to update the permissions.

- Credentials for AWS, GCP, and Azure cloud accounts are now under **Manage > Cloud Accounts**.
- In 22.01 update 2, we updated how the scanning process impacts artifact metadata in JFrog Artifactory. The scanning process no longer updates the **Last Downloaded** date for all manifest files of all the images in the registry.

In 22.06, we've further refined how this works:

As part of the process for evaluating which images should be scanned, in addition to reviewing the manifest files, Prisma Cloud also examines the actual images. Now the **Last Downloaded** date won't change unless the image is actually pulled and scanned.

"Transparent security tool scanning" is **not** supported for anything other than Local repositories. If you select anything other than **Local** in your scan configuration (including virtual repositories backed by local repositories), then Prisma Cloud automatically uses the Docker API to scan all repositories (local, remote, and virtual). When using Docker APIs, the **Last Downloaded** field in local JFrog Artifactory registries will be impacted by scanning.

If you've got a mix of local, remote, and virtual repositories, and you want to ensure that the **Last Downloaded** date isn't impacted by Prisma Cloud scanning, then create separate scan configurations for local repositories and remote/virtual repositories.

- The data collection for incidents in the Prisma Cloud Compute database is capped to 25,000 incidents or 50 MB, whichever limit is reached first.

When upgrading from 22.01 to 22.06, if the size of your incident collection exceeds this limit, then the oldest incidents that exceed the limit will be dropped.

As part of this change, the serial number field for incidents will now be empty. The serial number was a running count of the incidents according to the size of the data collection. Now that the collection is capped, the serial number is no longer available. To uniquely identify incidents, use the ID field instead.

- A new field **category** is now available for incidents alert integration with Webhook and Splunk to identify the incident type.
- With 22.06, all App-Embedded collections including Fargate tasks, will be grouped together in collections using the **App ID** field.

Until now, collections of Fargate tasks were specified using the **Hosts** field in vulnerability, compliance, and incidents pages.

After upgrading to 22.06, update your existing collections to use the **App IDs** field rather than the **Hosts** field to maintain the correct grouping of resources for filtering, assigning permissions, and scoping vulnerability and compliance policies.

Also, the CSV file export for vulnerability scan results, compliance scan results, and incidents has changed. Fargate tasks protected by App-Embedded Defender will be reported under the **Apps** column instead of the **Hosts** column.

Known Issues

- The `--tarball` option in `twistcli` does not scan for compliance checks. Currently, only vulnerabilities are detected successfully.
- When Defender is installed on Windows hosts in AWS, and Prisma Cloud Compute Cloud Discovery is configured to scan your environment for protected hosts, the Windows hosts running Defender are reported as unprotected.
- For custom compliance checks for Kubernetes and OpenShift on CRIO, when **Reported results** is configured to show both passed and failed checks, if a check doesn't run, Prisma Cloud still reports it as **passed**.
- If you have the same custom compliance rule in use in a host policy (effect: alert) and a container policy (effect: block), the rules will enforce your policy (as expected), but the audit message for a blocked container will incorrectly refer to the host policy and host rule name.
- On the Radar > Containers, K3s clusters are not displayed. You can view the containers within these clusters under **Non-cluster containers**.

Upcoming Deprecation Notifications

- Support for Windows Server 2022 will be added with or before the next release, Lagrange. With support for Windows Server 2022, Windows Server 2016 will no longer be supported. Microsoft has announced the [EOL for Windows Server 2016](#) as of January, 2022.

- Support for Docker Access Control is being deprecated along with the Access User role. Support will be removed in the Newton release.
- Support for scanning your code repositories from the Prisma Cloud Compute console (**Monitor > Vulnerabilities > Code repositories**) is being deprecated. Twistcli for code repository scanning is also being deprecated. You can use the Code Security module on Prisma Cloud to scan code repositories and CI pipelines for misconfigurations and vulnerabilities.
Support for code repo scanning using Prisma Cloud Compute will be removed in the Newton release.

Backward Compatibility for New Features

Feature name	Unsupported Component (Defender/twistcli)	Details
Support for Google Artifact Registry	Defender	Old defenders will not be supported for scanning Artifact Registry.
Registry Scan Enhancements	Defender	A new log record was added for Defender finished scanning image, which adds pull, analysis and total duration. For older defenders, the following fields will be zero: ImagePullDuration, ImageAnalysisDuration, ImageScanDuration.
Vulnerability and compliance for Workloads Protected by App-Embedded Defenders	Defender	Old app-embedded Defenders (except for ECS Fargate Defenders) will not be supported for vulnerabilities, compliance, and package info. The images running with these Defenders will not be returned in the GET images API. Also, for old ECS Fargate Defenders, the Environment → Apps tab within the image dialog will be empty, even though there are running tasks and their count is displayed on the main images page under the Apps column.

Feature name	Unsupported Component (Defender/twistcli)	Details
Runtime File System Audits for App-Embedded Defenders	Defender	Old app-embedded Defenders will not be able to have the filesystem capability, so the workloads protected by them can not be monitored for FS.
Rule to Allow Activity in Attached Sessions	Defenders	Old Defenders will not support the new functionality as they don't have the backend implementation part of this toggle
Support ARM: Add vulnerabilities support for ARM to the IS ARM support	Defenders, twistcli, Console and Intelligence Stream	Old defenders and consoles won't support ARM64 since there isn't any the dedicated implementation. The Intelligence Stream is updated with ARM64 CVEs for all consoles, but as we predict, it won't be common to get an ARM related CVE for each x86 CVE. ARM64 Defenders are required to scan ARM-based images. Make sure to assign the appropriate collections in your Registry Scanning Scope for x86_64 images and ARM64 images to prevent errors in the registry scanning. The ALL collection automatically includes the ARM64 Defenders.
Windows defender for Vulnerability and Compliance with Containers	Defenders, twistcli	Old Defenders and twistcli will not support the new functionality as they don't have the updated implementation
Improved Visibility for CaaS workloads protected by App-Embedded Defenders	Defenders	Old App-Embedded Defenders will not be supported, the new capability of fetching the workload cloud metadata to App-Embedded profile

Feature name	Unsupported Component (Defender/twistcli)	Details
Authenticate with Azure Container Registry using certificate	Defenders	We will have a problem with using the new credential in scanning with older defenders, they will not be able to use this credential
Extract Fargate task Entrypoint and Command Params, Support Fargate Task Definition in CloudFormation Template format #33033	twistcli	New implementation for Fargate Task defenders in twistcli
Support image tar files scanning with twistcli	twistcli	Old twistcli version doesn't have this implementation
Support for Azure VMs and Containers being reported into SaaS - Unified Inventory (#tbd)	Defender	Older than Kepler Defenders will not be able to report on Azure VMs, due to the lack of the VM Id in proper format support. It will need users to upgrade their defenders to Kepler.

Get Help

The following topics provide information on where to find more about this release and how to request support:

- [Related Documentation](#)
- [Request Support](#)

Related Documentation

Refer to the following documentation on the [Technical Documentation portal](#) or [search](#) the documentation for more information on our products:

- **Prisma Cloud Administrator's Guide (Compute)** – Provides the concepts and workflows to get the most out of the Compute service in Prisma Cloud Enterprise Edition. The [Prisma Cloud Administrator's Guide \(Compute\)](#) also takes you through the initial onboarding and basic set up for securing your hosts, containers, and serverless functions.
- **Prisma Cloud Compute Edition Administrator's Guide** – Provides the concepts and workflows to get the most out of the Prisma Cloud Compute Edition, the self-hosted version of Prisma Cloud's workload protection solution. The [Prisma Cloud Administrator's Guide \(Compute\)](#) also takes you through the initial onboarding and basic set up for securing your hosts, containers, and serverless functions.*
- **Prisma Cloud Administrator's Guide** – Provides the concepts and workflows to get the most out of the Prisma Cloud service. The [Prisma Cloud Administrator's Guide](#) also takes you through the initial onboarding and basic set up for securing your public cloud deployments.
- **Prisma Cloud RQL Reference** – Describes how to use the [Resource Query Language \(RQL\)](#) investigate incidents and then create policies based on the findings.
- **Prisma Cloud Code Security Administrator's Guide** – Use the [Code Security Guide](#) to scan and secure your IAC templates and identify misconfiguration before you go from code to cloud.

Request Support

For contacting support, for information on support programs, to manage your account, or to open a support case, go to the [Prisma Cloud LIVE community page](#).

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

<https://www.paloaltonetworks.com/company/contact-support>

Palo Alto Networks, Inc.

www.paloaltonetworks.com

