Prisma Cloud AppDNA

LGA Guide

Table of Contents

Overview

Prisma Cloud AppDNA discovers applications and uncovers their boundaries. The application boundary determination helps to intelligently group assets by application. Prisma Cloud then adds metadata on top of the application like owner, business criticality, environment and uses this context for risk prioritization.

With AppDNA Prisma Cloud now also provides the Application Context for your Alerts and Assets.You now have a single source for all the meta information which helps in easy assignment of alert and risk prioritization.

Onboarding

For LGA, AppDNA supports applications defined by K8S Namespace and will provide multiple options/criteria of creation like Tags, APIs, etc.

In order to get visibility into the K8s environment, customers need to install K8s Satellite pod into the K8s cluster so that Prisma Cloud can get visibility into K8s objects and create an application boundary by associating the right cloud assets to the right applications.

Prisma Cloud K8s Satellite is an operator designed to manage and orchestrate the deployment of Prisma Cloud functions that are required for Prisma Cloud to perform different tasks in K8s clusters, such as Configuration Visibility, Application Detection, Asset Tracing, Container Exposure, and Security Posture.

Prerequisites

Your system must meet specific requirements for the Satellite to be successfully installed.

Connectivity
The satellite needs outgoing access to the following Prisma Cloud domains and subdomains.

- prismacloud.io
- amazonaws.com
- gcr.io

If you have firewalls blocking this traffic, add the following values to their allow lists:

- *.prismacloud.io
- gcr.io
- *.amazonaws.com

Host Requirements
At a minimum, Satellite requires a K8s Node that can dedicate 256MB RAM and 900mCPU.

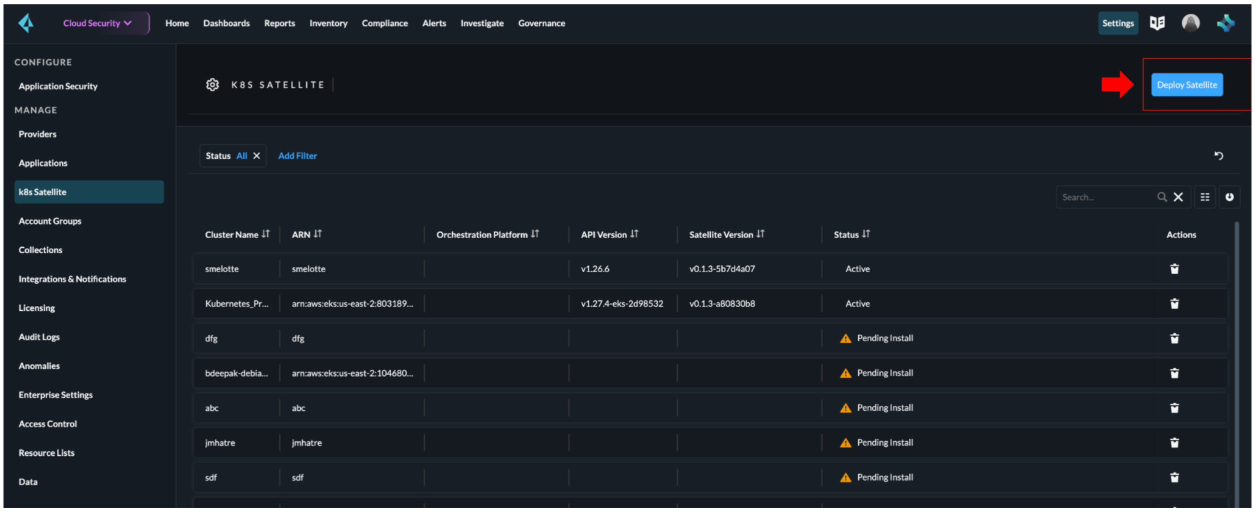
Satellite is supported on the following platforms and versions:

Platform	Version
AWS EKS	1.24, 1.25, 1.26, 1.27

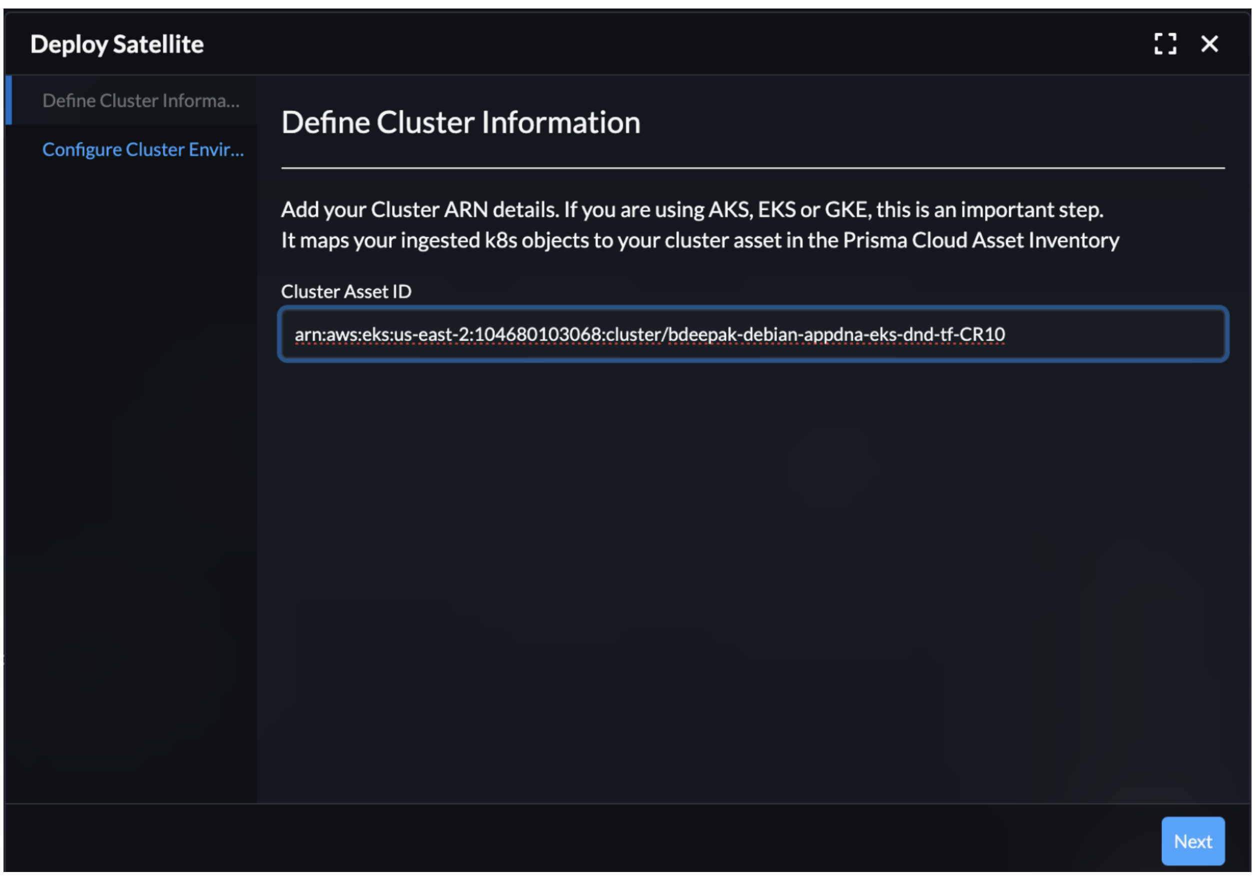
Step 1:Install K8S Satellite

1. Login to Prisma Cloud and navigate to Settings → K8s Satellite Page.

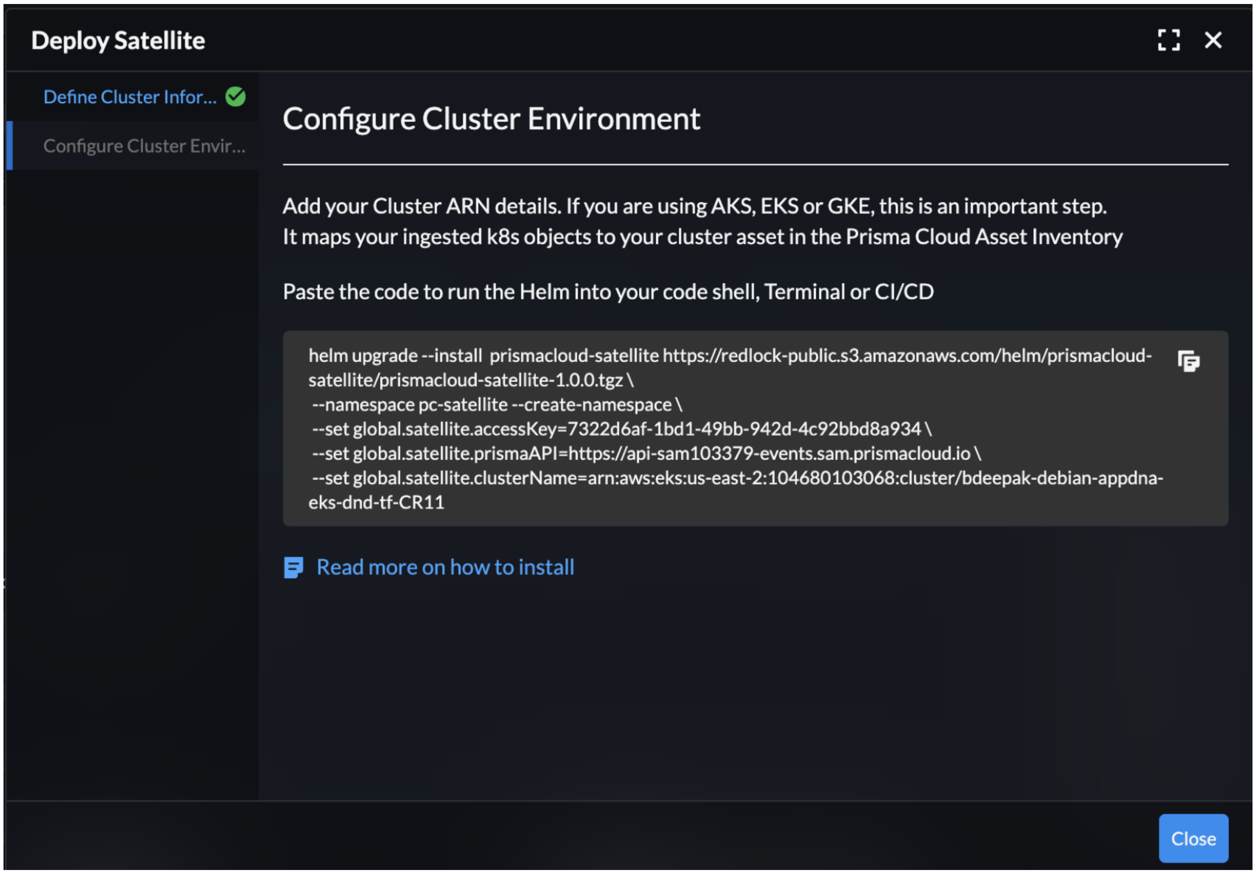
2. Click on Deploy Satellite



3. Provide the Amazon EKS Cluster ARN in the cluster AssetID field and click Next (Find your Cluster Asset ID by referencing the Cluster `Asset ID` field on Prisma Cloud Asset Inventory.)



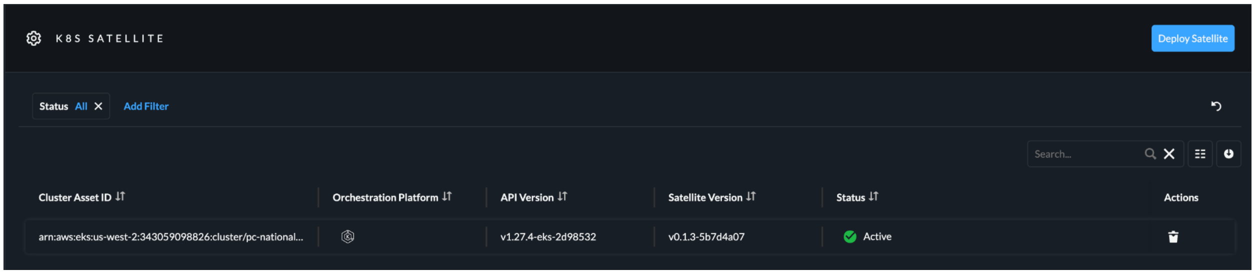
4. Copy the helm upgrade/install command and execute in EKS cluster.
A unique identifier is each time a helm chart is generated and it acts as a cluster identifier, therefore you cannot reuse the helm chart across different clusters.



Right after the helm chart is generated, your cluster will be in `Pending` state, until the Satellite gets deployed and starts reporting to Prisma Cloud.

After the deployment is done, the cluster status will change to a `Ready` state.

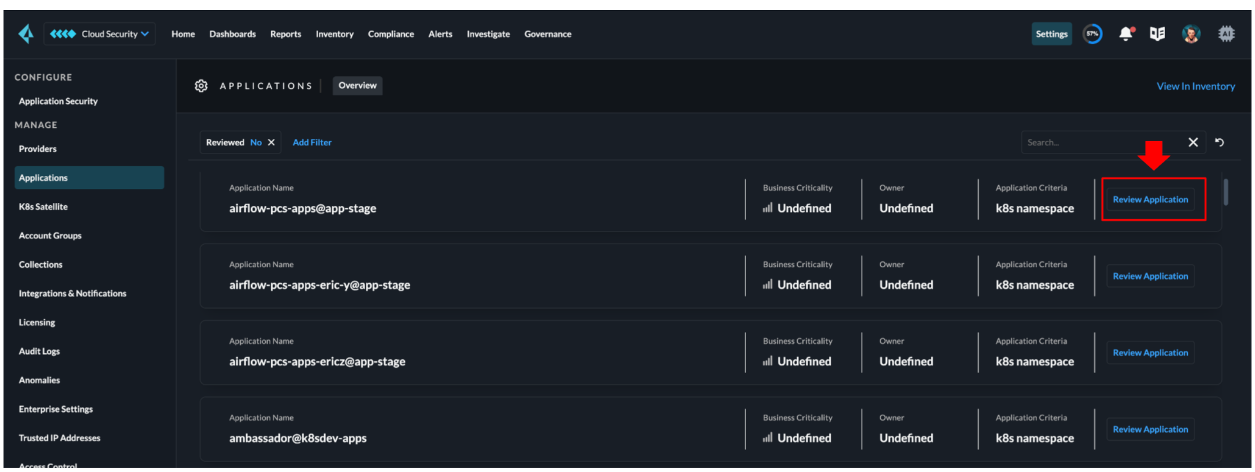
Once a cluster moves to a `Ready` state, it will continuously send keep-alive to Prisma Cloud every 30 minutes. If there's a communication issue or if the Satellite gets removed, the object will move into an `Offline` state until the communication is re-established or the Satellite object is deleted on the Prisma Cloud console.

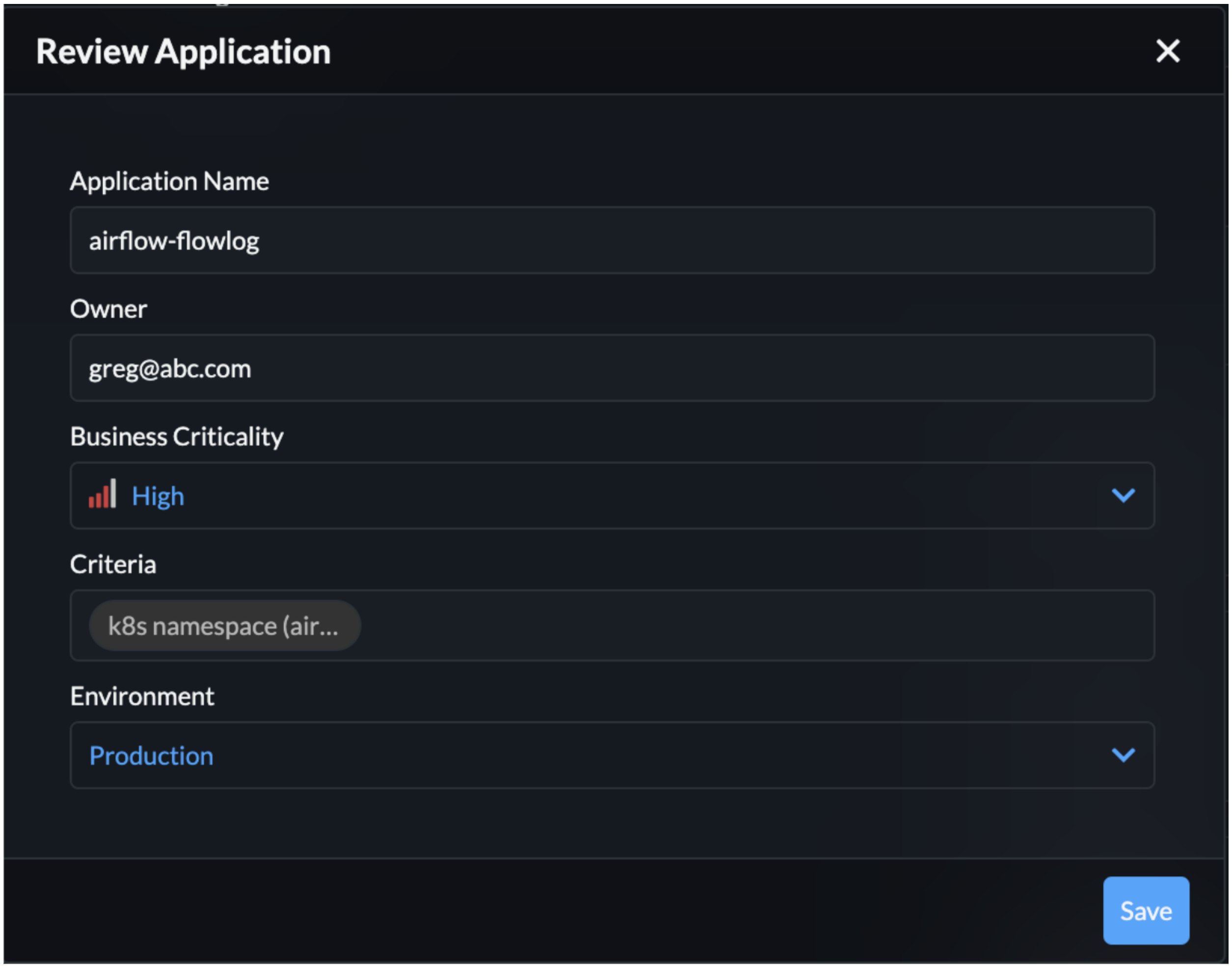


Step 2: Review and update metadata

For LGA the applications can be defined as a K8s Namespace. (The definitions of applications will be expanded in upcoming releases).

Once Step 1 is complete, navigate to **Settings > Applications** to see a list of all the discovered K8s Namespace. Select **Review Application** and update the metadata like Application Display Name, Application Owner, and Business Criticality of the application (High, Medium, Low) based on criteria such as, is the application public-facing, contains sensitive data, the revenue of application, location of application production, staging etc.)



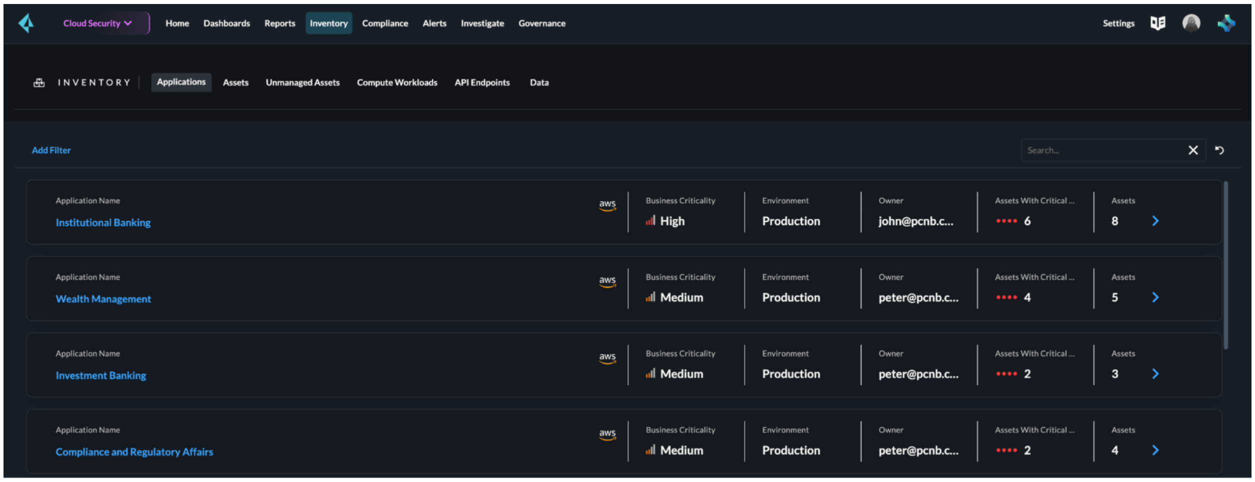


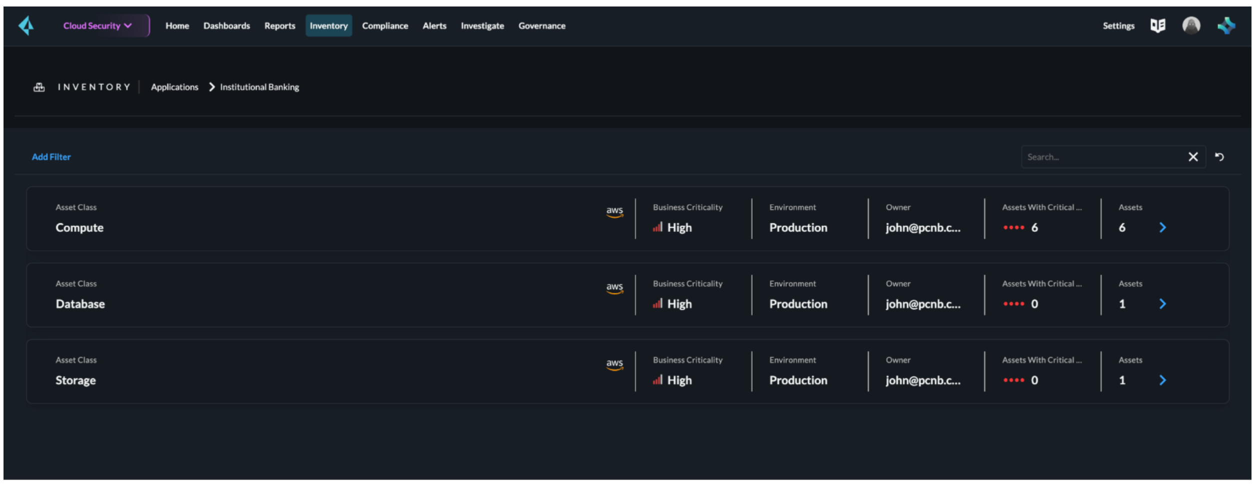
Next Steps

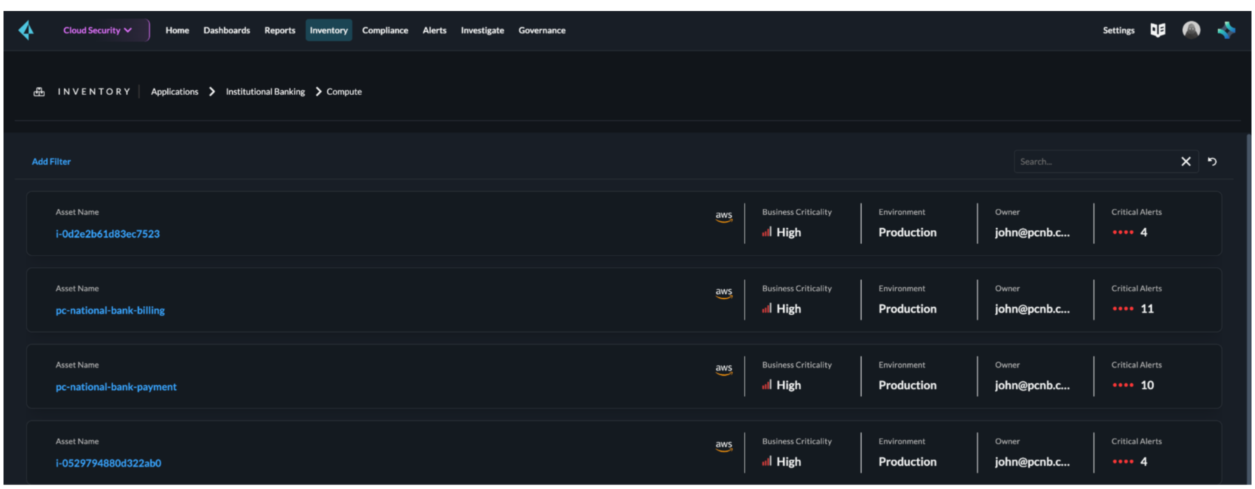
App Inventory

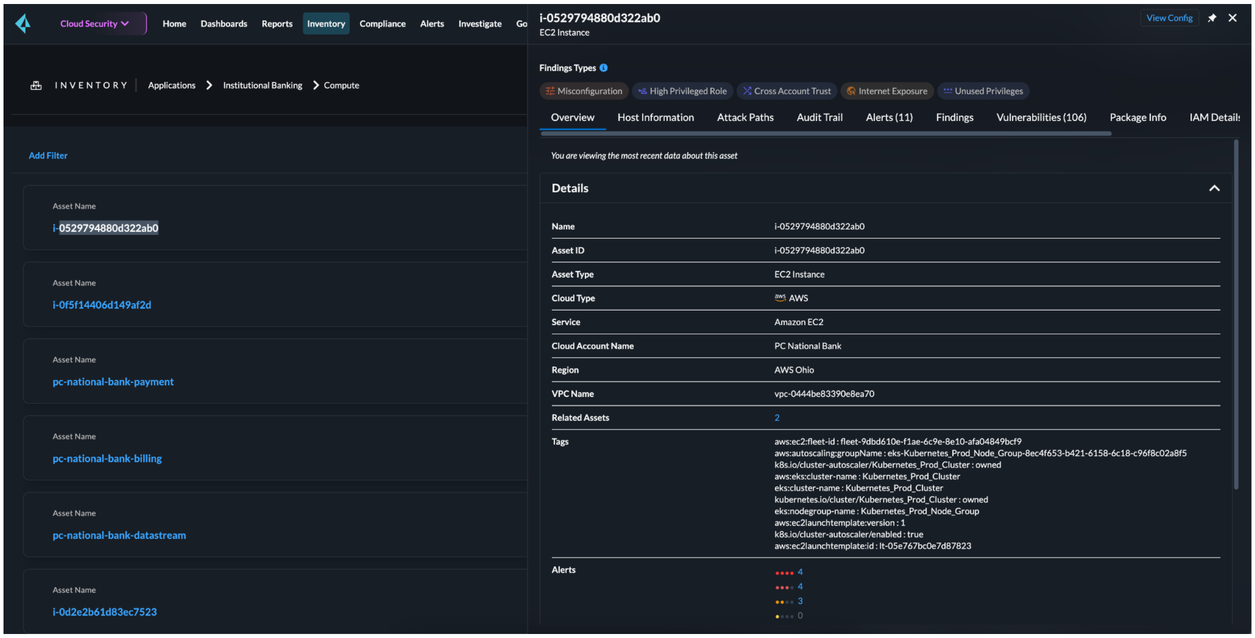
You can get a list of all the Applications under **Inventory > Applications**. Here you can view all the assets of a given application.

The inventory is set in 2 stages, 1st stage will provide a summary of assets on Asset Classes like Compute, Storage, Database etc.


Cloud Security
Home
Dashboards
Reports
Inventory
Compliance
Alerts
Investigate
Governance
Settings
INVENTORY
Applications
Assets
Unmanaged Assets
Compute Workloads
API Endpoints
Data
Add Filter
Search...
Application Name
Institutional Banking
aws
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Assets With Critical ...
6
Assets
8
Application Name
Wealth Management
Business Criticality
Medium
Environment
Production
Owner
peter@pcnb.c...
Assets With Critical ...
4
Assets
5
Application Name
Investment Banking
Business Criticality
Medium
Environment
Production
Owner
peter@pcnb.c...
Assets With Critical ...
2
Assets
3
Application Name
Compliance and Regulatory Affairs
Business Criticality
Medium
Environment
Production
Owner
peter@pcnb.c...
Assets With Critical ...
2
Assets
4


Cloud Security
Home
Dashboards
Reports
Inventory
Compliance
Alerts
Investigate
Governance
Settings
INVENTORY
Applications
Institutional Banking
Add Filter
Search...
Asset Class
Compute
aws
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Assets With Critical ...
6
Assets
6
Asset Class
Database
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Assets With Critical ...
0
Assets
1
Asset Class
Storage
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Assets With Critical ...
0
Assets
1

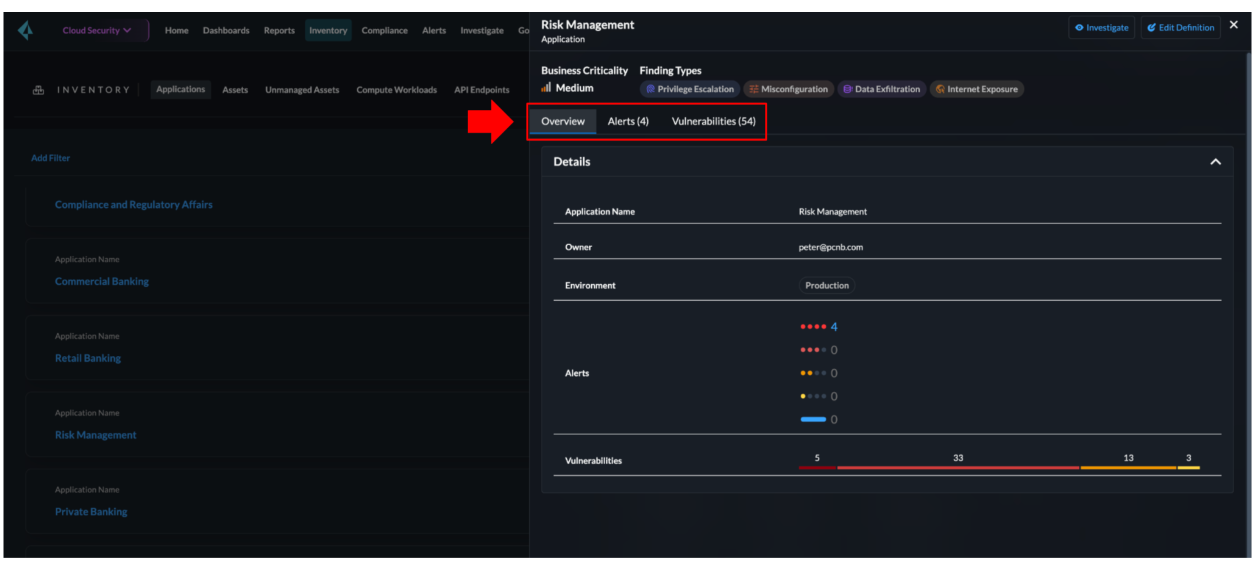

Cloud Security
Home
Dashboards
Reports
Inventory
Compliance
Alerts
Investigate
Governance
Settings
INVENTORY
Applications
Institutional Banking
Compute
Add Filter
Search...
Asset Name
i-0d2e2b61d83ec7523
aws
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Critical Alerts
4
Asset Name
pc-national-bank-billing
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Critical Alerts
11
Asset Name
pc-national-bank-payment
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Critical Alerts
10
Asset Name
i-0529794880d322ab0
Business Criticality
High
Environment
Production
Owner
john@pcnb.c...
Critical Alerts
4

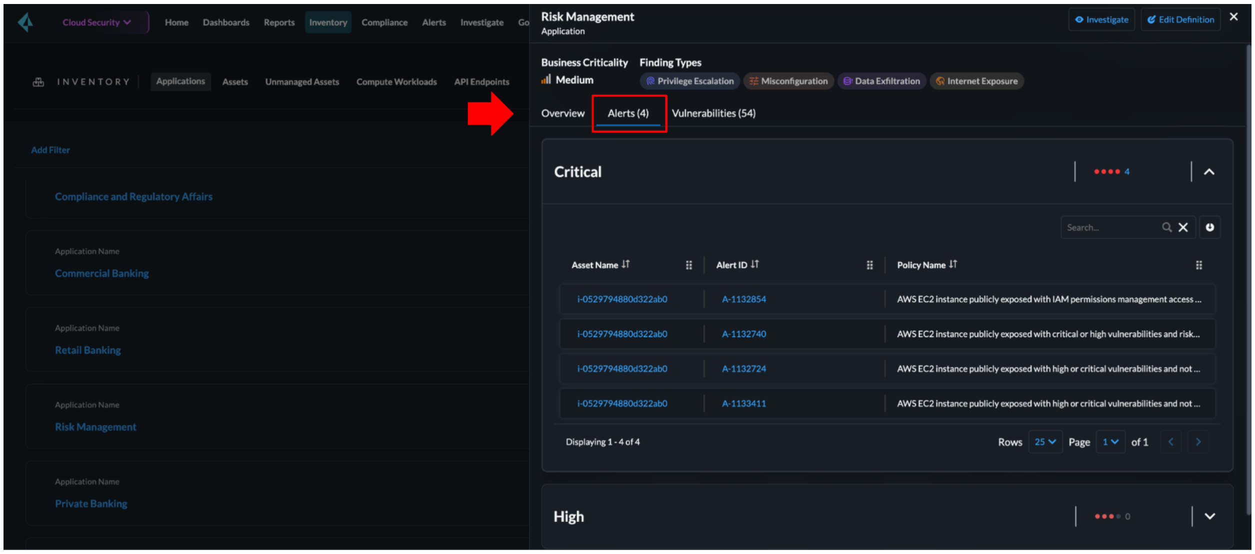


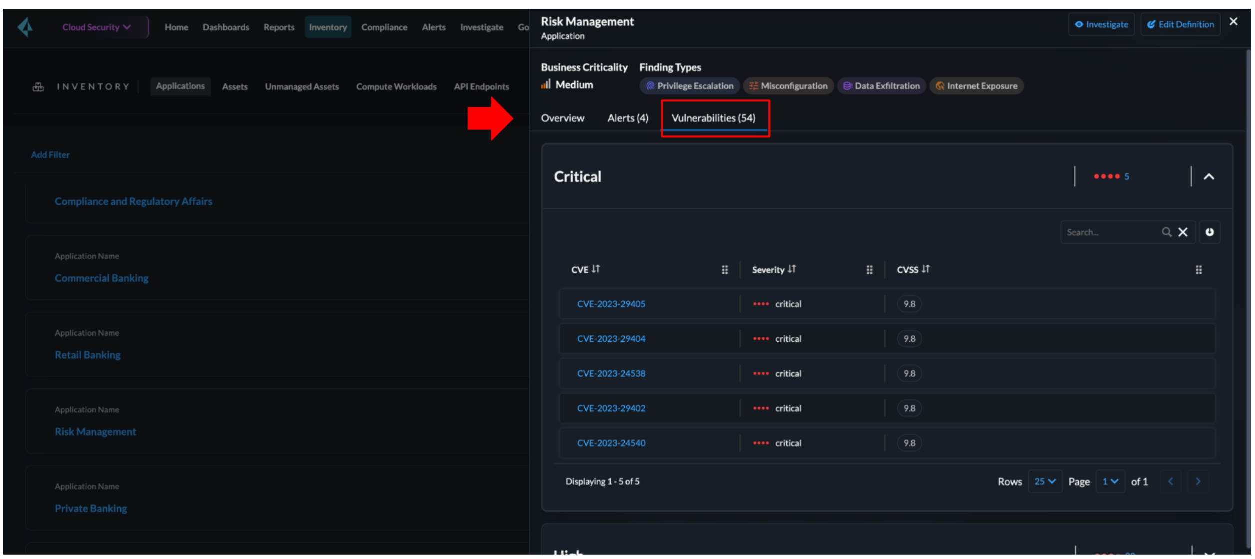
Application Metadata, Alerts, and Vulnerabilities

With Prisma Cloud you can view the list of all the alerts and vulnerabilities associated with the assets of the application. Select **Inventory > Applications** when the user clicks on the application name, the corresponding application sidecar opens up which gives a list of alerts and vulnerabilities reported on an application.

The alerts and vulnerabilities are grouped by 'severity' (more group criteria will be supported later.)

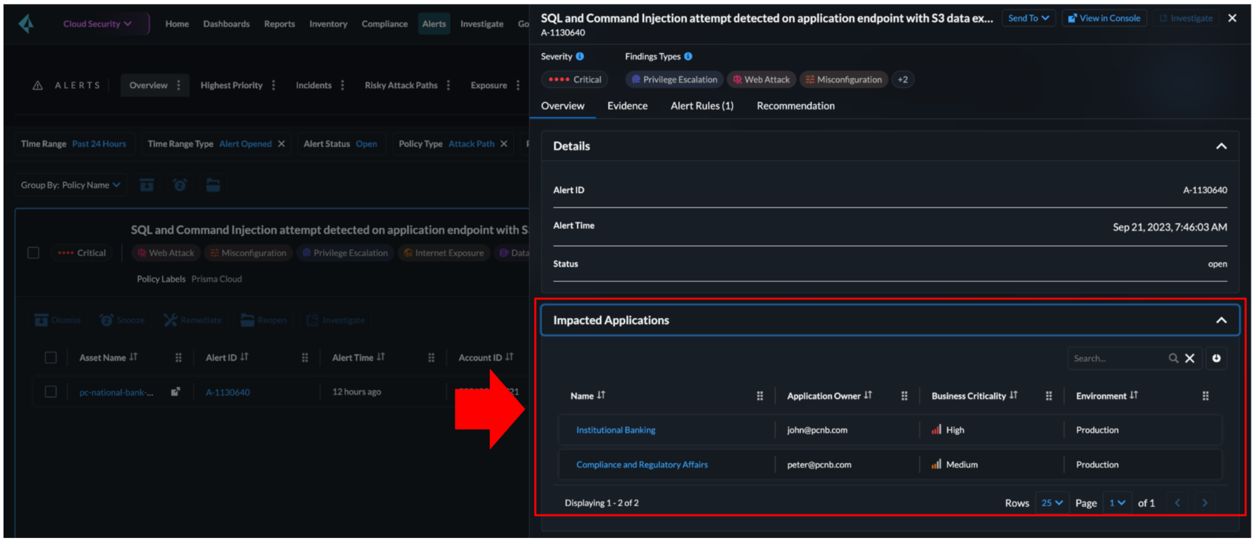






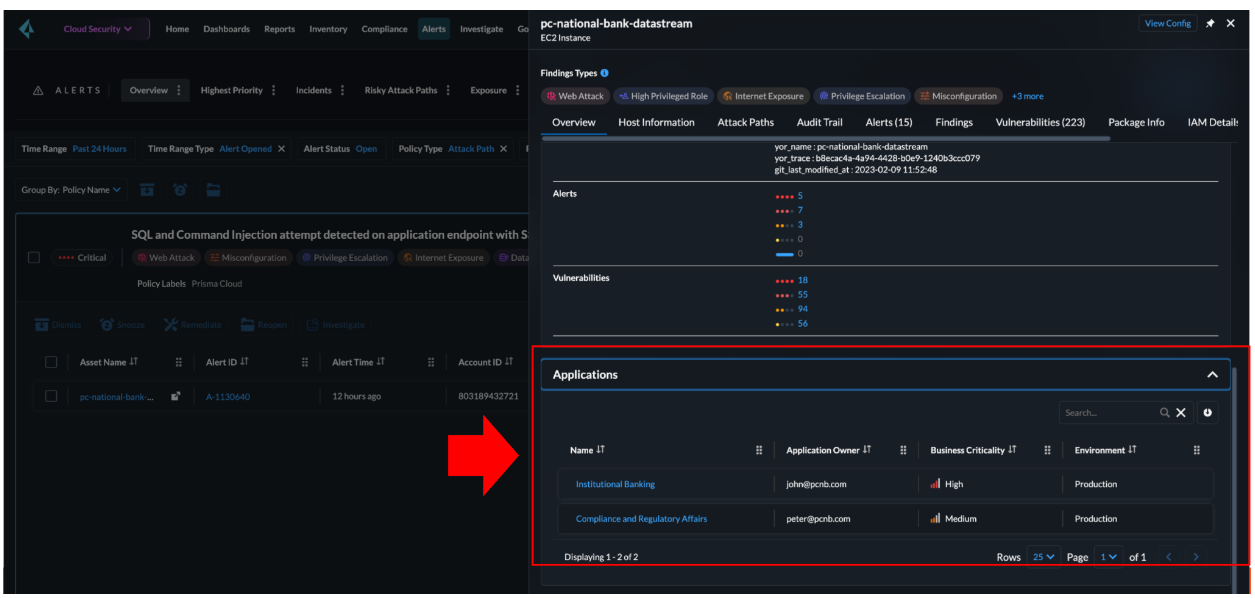
Application Context in Alerts

You can now use application context to prioritize risk in your environment. The application context can now be seen in Alert Sider in Overview under the section ‘Impacted Applications’. For LGA this is available for only Attack Path Alerts as they are the potential exploitable paths for your environment.



Application Context in Assets

Customers can now look up applications the assets belong to. For assets that belong to an application the asset side panel Overview tab will have a section called **Applications** which will display the list of applications.



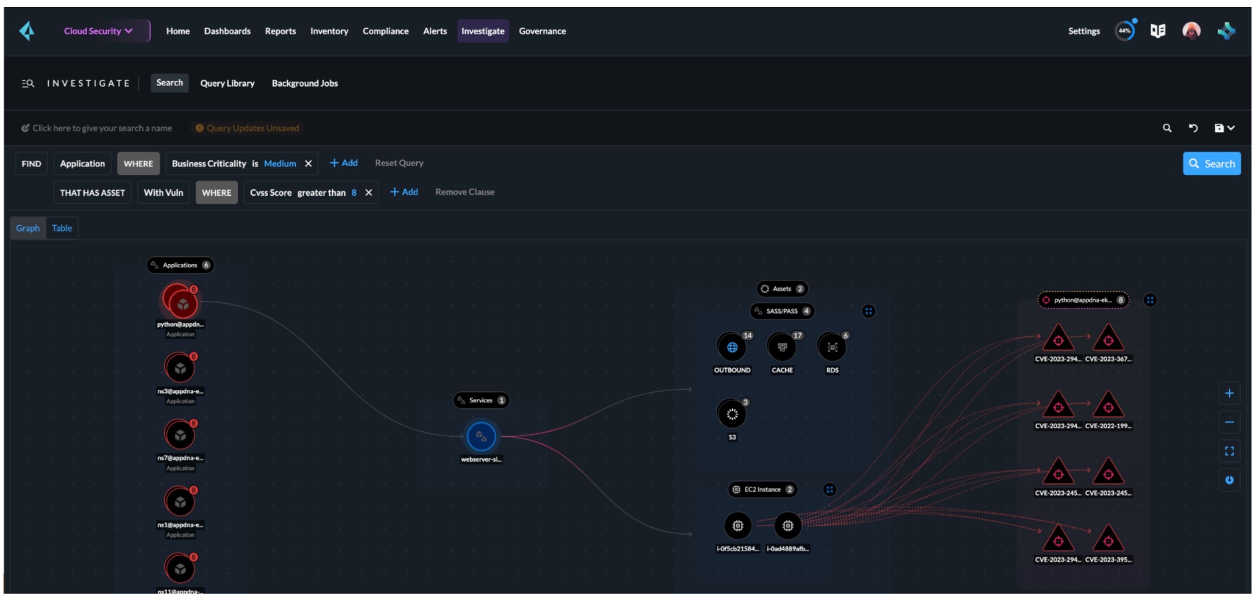
Search and Investigate

You can use **Search and Investigate** for querying applications and their associations. Simplified querying without RQL is also available to further simplify this task.

Following is a list of sample queries:

- Find Applications where business criticality in ‘High’ with Vulnerability / Alert
- Find Applications where environment in ‘Production’’ with Vulnerability

  The graph is applicable for queries with Vulnerability or Alert conditions. The graph displays the services deployed on the application. Select a service to display the interaction of services with cloud assets like Elastic Cache, RDC, S3 bucket and any outbound endpoint which could be third-party applications or other cloud services.



LGA Limitations

- Currently we support applications defined by K8s Namespace. We plan to expand into creating applications by Tags, APIs and other criterias.
- AppDNA is only Available only for System Admins.
- Support is available only for AWS EKS for all AWS regions (all stacks except gov and china stacks).
- **Impacted applications** are displayed for **Attack Paths** only.
- Data refresh (application associations are calculated once in 24 hrs, alerts are near real time)

- Side panel shows only the top ten impacted applications sorted alphabetically by business criticality.
- The **Search & Investigate** graph is available only for queries with Vulnerability or Alert conditions.

Troubleshooting

Scenario: I am not seeing any Applications after onboarding EKS cluster.
>> The Sync happens at 23:30 UTC time everyday. Allow time for the sync to complete.

Scenario: I am not seeing any Applications after onboarding EKS cluster beyond sync time.
>> Execute below commands on the EKS cluster
kubectl create job --from=cronjob/prisma-kubeapi-scraper-cronjob prisma-kubeapi-scrapper-cronjob-test -n pc-satellite
Note: Permanent fix for above will be released shortly.

Scenario: Home > Inventory,only shows Applications but no assets.
>> Onboarding cloud accounts is a prerequisite so that Prisma can map the assets to applications.

Scenario: I don't see RDS, S3, Elastic Cache resources.
>> Enable core DNS logs and ensure there is traffic in the cluster. To validate CoreDnslogs use the command **kubectl logs --namespace=kube-system -l k8s-app=kube-dns -f**

FAQ

Q: How should I share my feedback with the Prisma Team?
A: Please fill out the form.

Q: Does AppDNA consume PANW credits?
A: No, AppDNA does not consume any credits.

Q: Is there a cost for using AppDNA, for example on CSP?
A: Approximately less than $10 per month.

Q: Are there any customer-facing APIs for AppDNA?
A: No public API for AppDNA for LGA.

Q: What cloud regions does AppDNA support?
A: For LGA, AWS cloud and all of its regions are supported.(Azure and GCP will follow shortly).

Q: Why can I see only a few EC2 as a part of the application?
A: For LGA we can determine only the K8s environment and the corresponding cloud services it is communicating with, hence for LGA only K8s Cluster nodes are determined.