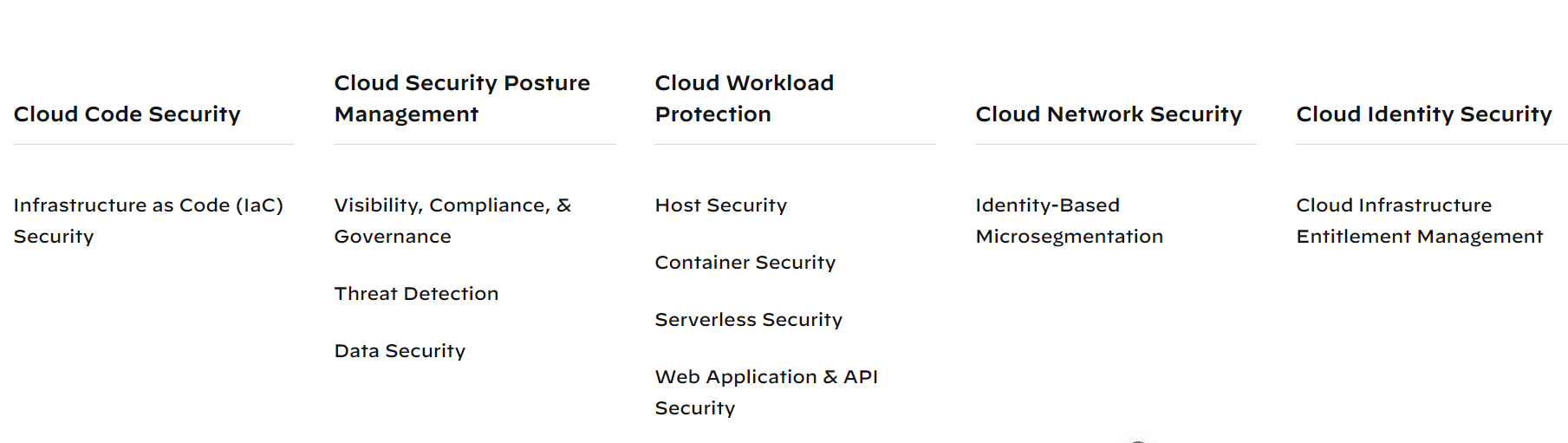
# Prisma Cloud

## What is Prisma Cloud?

Prisma Cloud -> Cloud Infrastructure security solution + Security Operation Center (SOC) enablement tool

## Capabilities of Prisma Cloud

1. Cloud Security Posture Management
2. Cloud Workload Protection
3. Cloud Infrastructure Entitlement Management (CIEM)



g

## How Prisma Cloud works?

Prisma™ Cloud helps identify issues in cloud deployments and then respond to a list of prioritized risks so that we can maintain an agile development process and operational efficiency.

## Highlights of Prisma Cloud

### Comprehensive Visibility

Enables you to view your resources—deployed on multiple cloud infrastructure platforms—from a single console. In addition to providing a consolidated view of the resources across the cloud platforms, Prisma Cloud integrates with threat intelligence feeds, vulnerability scanners.

### Policy Monitoring

Enables you to use Prisma Cloud, which includes Security policies based on industry standards, to continuously monitor for violations. Prisma Cloud provides hundreds of out-of-the-box policies for common security and compliance standards, such as GDPR, PCI, CIS, and HIPAA. We can also create custom policy rules to address specific needs or to customize the default policy rules.

### Anomaly Detection

Automatically detects suspicious user and network behavior using machine learning.

### Contextual Alerting

the service scans for unpatched hosts, escalation of privileges, and use of exposed credentials, and also scans communication for malicious IP addresses, URLs, and domains.

### Cloud Forensics

Enables you to go back to any point in time and investigate an issue within seconds

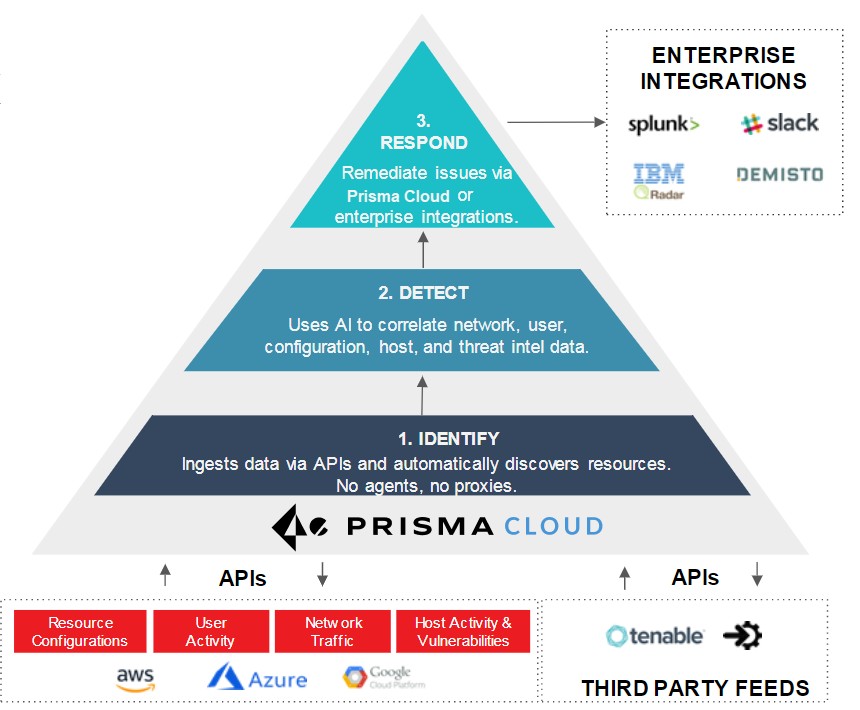
### Compliance Reporting

Reports your risk posture to your management team, to your board of directors, and to auditors.

### Data Security

Scans data stored on AWS S3 buckets and provides visibility on the scan results directly on the Prisma Cloud dashboard. The data security capabilities include predefined data policies and associated data classification profiles such as PII, Financial, or Healthcare & Intellectual Property that scan objects stored in the S3 bucket to identify exposure—how sensitive information is kept private, or exposed or shared externally, or allows unauthorized access.

## Prisma Cloud follows Agile process



## CSPM

\*\*\*\* API based service to enable granular visibility into resources deployed on public cloud

\*\*\*\* API based service to enable granular visibility into network traffic flows to the resources deployed from internet and between instances.

\*\*\*\* provides threat detection and response for resource misconfiguration

\*\*\*\* workload vulnerability

\*\*\*\* Provide visibility into user activity within each cloud environment.

## Prisma Cloud Dashboards

SecOps Dashboard (Out-of-the-box policies)

Asset Inventory

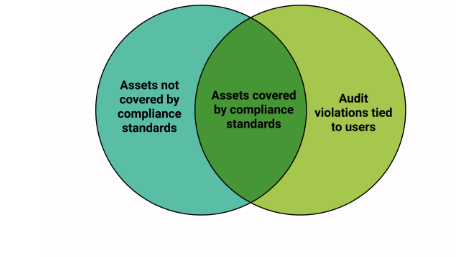
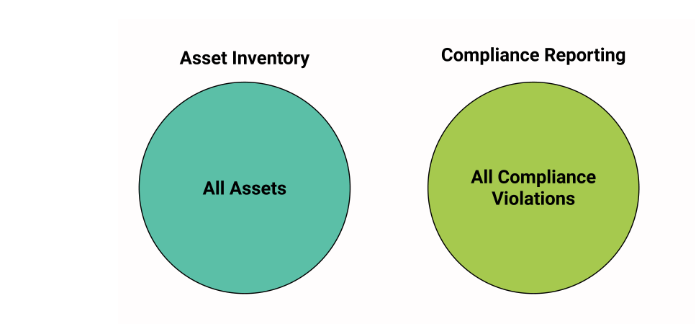
Compliance Dashboard

Prisma Cloud supports the need to keep track of potential risks and threats to your cloud infrastructure with dashboards for your [Asset Inventory](https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-dashboards/asset-inventory.html#idf8ea8905-d7a7-4c63-99e3-085099f6a30f), [Compliance Dashboard](https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/compliance-dashboard.html#idf165a375-fe34-479d-ad88-d76e623cc9d8), and out-of-the-box [policies](https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies.html#idf024bb91-d347-4f55-a407-f0b091d549a5) which generate alerts for

cloud assets that are in violation. When a policy is violated, an alert is triggered in real time.

### Asset Inventory

To know the state of cloud infrastructure, we need visibility into all the assets and infrastructure that make up our cloud environment and a pulse on its security posture.



The Asset Inventory dashboard (on the Inventory tab) provides a snapshot of the current state of all cloud resources or assets that you are monitoring and securing using Prisma Cloud. From the dashboard, you gain operational insight over all our cloud infrastructure, including assets and services such as Compute Engine instances, Virtual machines, Cloud Storage buckets, Accounts, Subnets, Gateways, and Load Balancers.

### Compliance Dashboard

The Compliance Overview is a dashboard that provides a snapshot of your overall compliance posture across various compliance standards. Use the Compliance Dashboard as a tool for risk oversight across all the supported cloud platforms and gauge the effectiveness of the security processes and controls you have implemented to keep your enterprise secure. You can also [create compliance reports](https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-compliance/add-a-new-compliance-report.html#id29559c3b-f4e6-416e-81db-e24dcb3149b2) and run them immediately, or schedule them on a recurring basis to measure your compliance over time.

### SecOps Dashboard

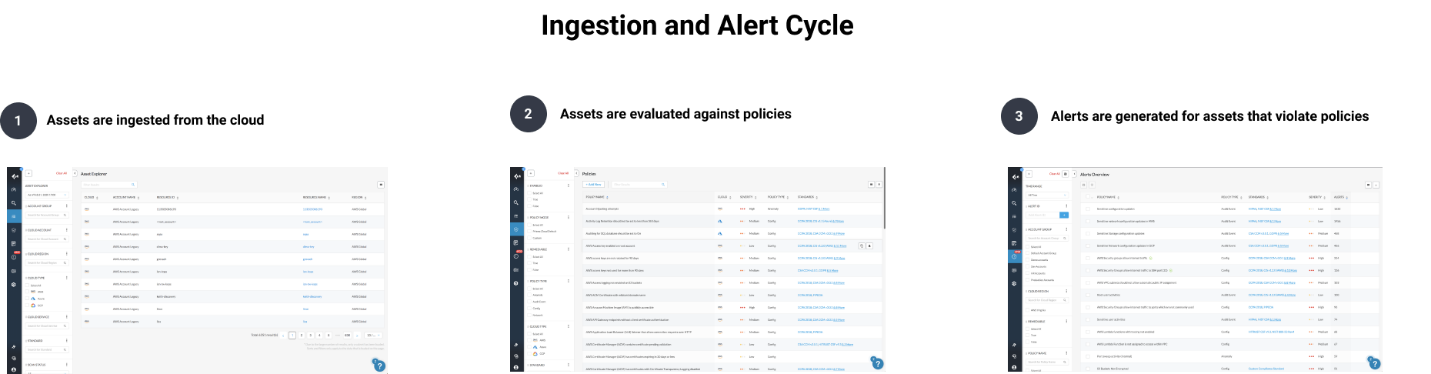
provides a graphical view of the performance of assets that are connected to the Internet, the alerts by policy type over time, the alerts by severity, and the policy violations over time.

### Out-Of-Box Policies

Policies are for risk assessment, and they help to reduce the risk of business disruptions. Prisma Cloud provides policies that map to compliance standards, and a larger set of policies that enable prevention or detection of security risks to which your cloud assets are exposed.

Anomaly policies are an example of policies that are typically not a part of compliance standards, and these policies inform us of actions performed on cloud assets by  *entities*  that are users, services, or IAM roles that have authorization to access and modify your cloud assets, but the entities are not cloud assets.

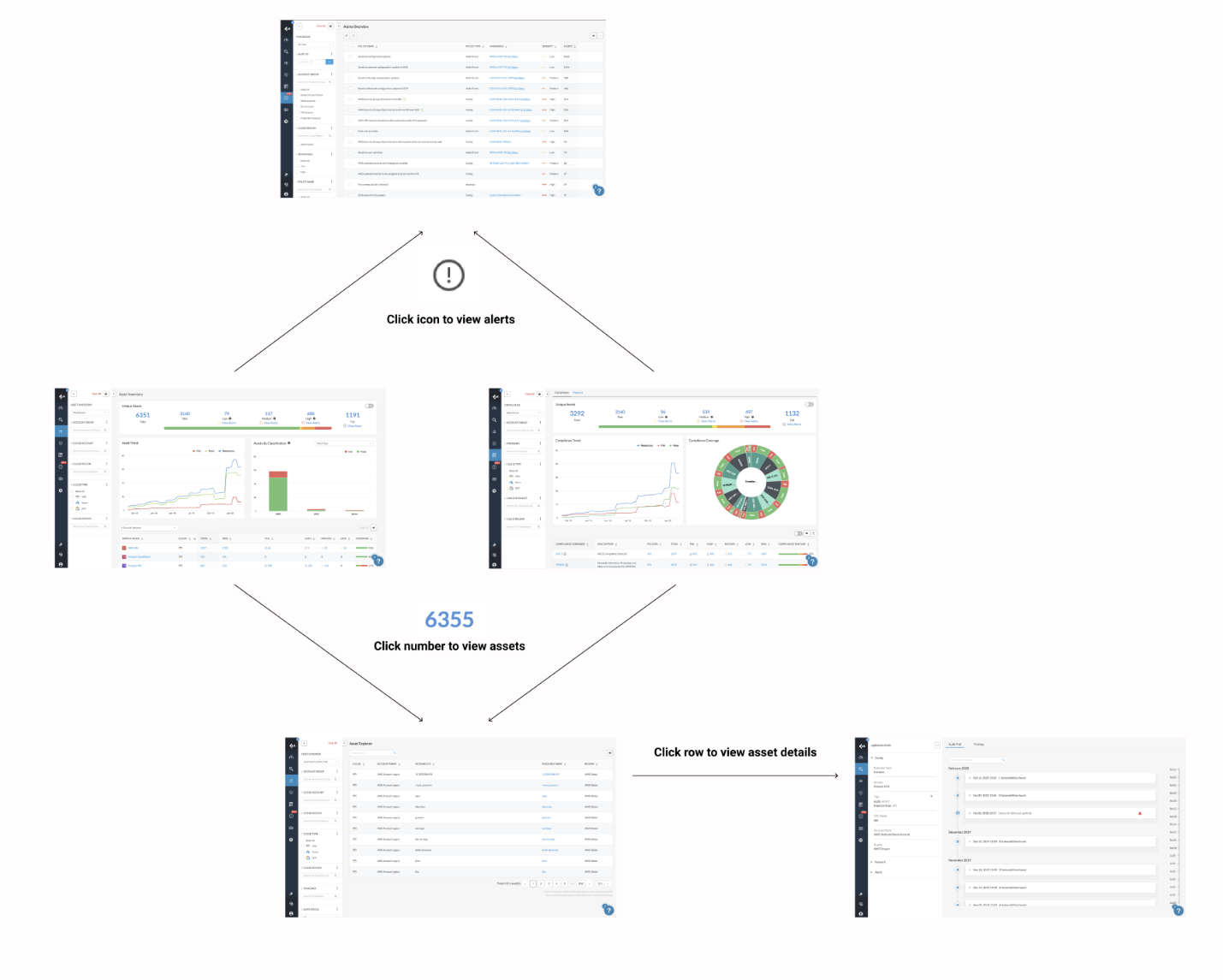




While alerts help you detect policy violations in real time and enable you to investigate what happened, the asset inventory and compliance dashboard are hourly snapshots of your assets and compliance posture for the last full hour.



From the asset inventory and the compliance dashboard, you can directly access all open alerts by severity, and view asset details from the asset explorer as of the last hour.



## What is Prisma Policy?

A policy is a set of one or more constraints or conditions that must be adhered to. Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as PCI, GDPR, ISO 27001:2013 and NIST, and a larger set of policies that enable us to validate security best practices with an impact beyond regulatory compliance. These Prisma Cloud default polices cannot be modified.

In addition to these predefined policies, we can create custom policies to monitor for violations and enforce our own organizational standards. We can use the Default policies as templates to create custom policy. After we set up the policies, any new or existing resources that violate these policies are automatically detected.

## Category of Policies

Incident - An incident is likely a policy that identifies a potential security issue

Risk - A risk is one that checks for risky configurations.

Type - Indicates whether the check is performed against the network logs, audit logs, configuration logs, or user activity logs.

Each policy type has

*subtypes*

 for more granularity, for example, Anomaly policies are split into two subtypes—Network and UEBA.

*Class*

 is another way to logically group policies into buckets such as Misconfiguration or Privileged Activity Monitoring.

## Types of policies

### ***Config***

Two sub types: Build and Run

Build policies enable us to check for security misconfigurations in the IaC templates and ensure that these issues do not make their way into production.

The Run policies monitor resources and check for potential issues once these cloud resources are deployed.

### **Data**

Data policies protect against malware and enable data classification. To identify sensitive data in cloud storage buckets, it uses machine learning and pattern matching

### Network

Network policies monitor network activities in your environment.

### Audit Event

Event policies monitor audit events in environment for potential policy violations. We create audit policies to flag sensitive events such as root activities or configuration changes that may potentially put cloud environment at risk.

### IAM

IAM policies monitor the identities in your cloud environment for excess-or-unused permissions.

Note: - You cannot edit or delete a Prisma Cloud Default policy.

## Managing Prisma Cloud Policies

Prisma Cloud policies enable you to monitor and manage potential misconfiguration or risks across your cloud infrastructure. You can use the graphs and tables on **Policies** to assess your policy coverage and utilization of policies. The graphs help you visualize how many policies are enabled as a number or as a percentage of the total, review the split across different policy types, how many policies of different severities are identified in your infrastructure, and gain greater context on the policy category and Prisma Cloud versus custom policies that are generating alerts.

We can download policy data, clone, enable, delete, or disable policies from the **Policies**  page.

### Cloning Default Policy

Prisma Cloud comes with default policies. If you want to modify any details, you can clone a policy and then modify details.

Cloning a policy is creating a copy of an existing policy. Cloning serves as a quick method of creating a new policy if you choose to change few details of the source policy.

To clone a policy, select the policy and click **Clone**

### Create a Custom Policy on Prisma Cloud

Either build the query using RQL or, Use a saved search to automatically populate the query to match on cloud resources.

Any of the following type of Policies can be created.

Config – Configuration Policy monitor your resource configuration for potential policy violation.

Data –

Network –

Audit Event –

IAM -

### Auto Remediation

If you want to enable auto-remediation, Prisma Cloud requires write access to the cloud platform to successfully execute the remediation commands.

# Prisma Standard

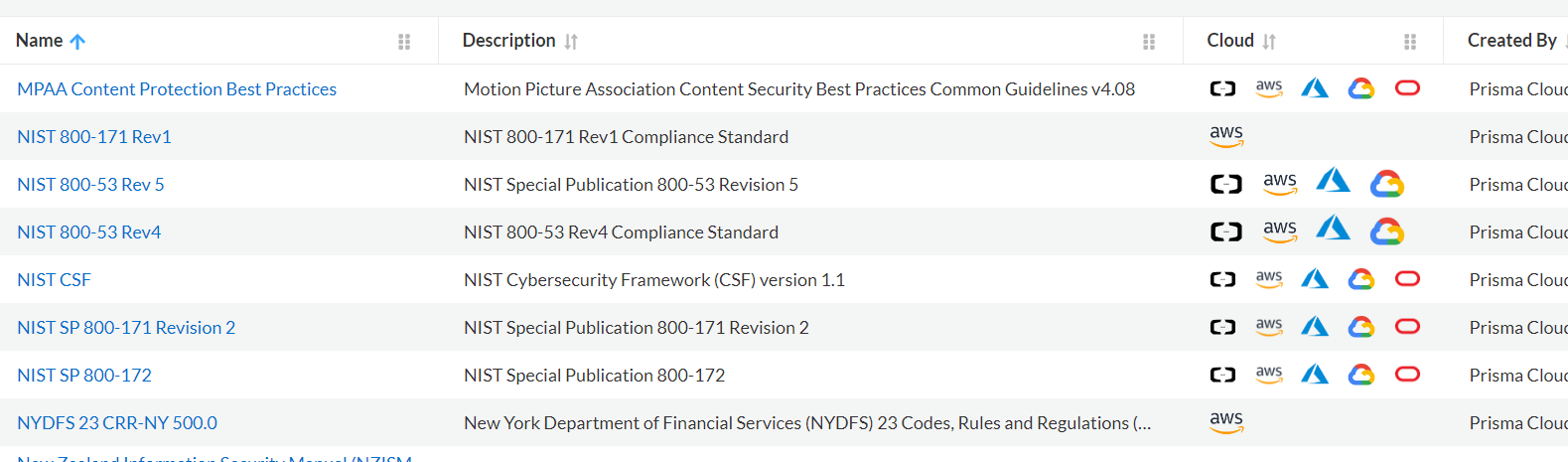
Prisma cloud has 57 compliance standards. HIPAA, GDPR, ISO, NIST and many more.

OCC – Optum Connect Cloud is custom defined standard.

*OCC Policies are mirrored with HCC Launch pad policies.*

*Standard created/supported by Prisma Cloud are as follows:*

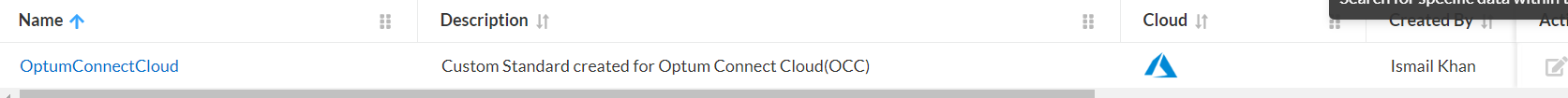
*Go to Compliance -> Standard section from left hand side toggle bar..*



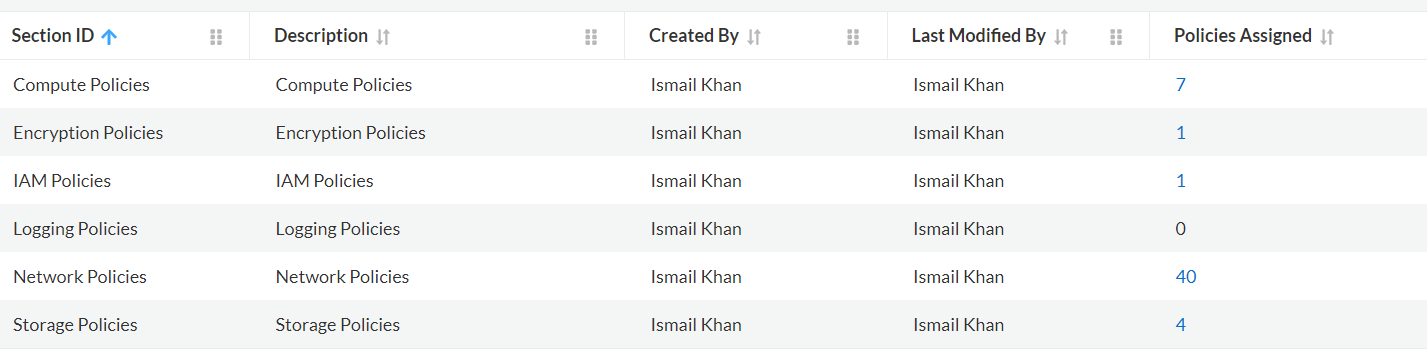


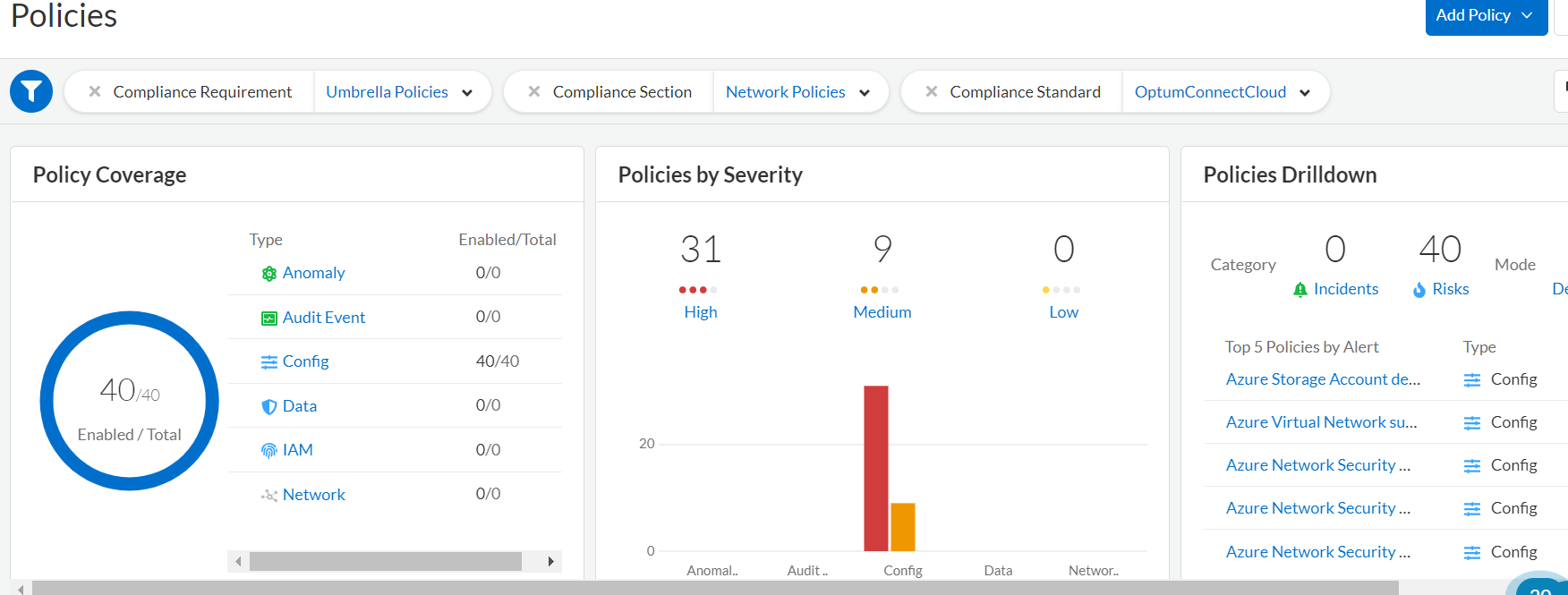
*And many more..*

*Custom one*



*All the Umbrella policies (Policies imported from HCC Launch Pad) have been added in this custom standard.*





### Prisma Out of Box Policy

Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as PCI, GDPR, ISO 27001:2013, and NIST. These Prisma Cloud default polices cannot be modified.

For e.g.

Azure Microsoft Defender for Cloud security alert email notifications is not set

Azure Virtual network not protected by DDoS Protection Standard

Same way, we will have few policies related to GCP and AWS. While we onboard Cloud account, Policies in Azure cloud also come integrated to monitor any violations. These Policies might have been configured through EIS+HCC launch pad.

https://cloud.optum.com/docs/launchpad/azure-policies#azure-virtual-network-using-public-ranges-for-private-addressing-uhg

### What is Launchpad?

**Launchpad** is a configuration deployment and a monitoring tool deployed to all UnitedHealth Group public cloud accounts. Launchpad enables continuous monitoring for security, compliance, application delivery, and business intelligence. It assesses your infrastructure against security best practices and automates many elements of the applications life cycle, including: platform logging, infrastructure compliance, and billing. Launchpad enables enterprise security, and compliance teams to ensure adherence to the necessary obligations across all public cloud applications while providing granular information for application teams to self-service before escalation and to remediate the issues found.

Health Care Cloud and Enterprise Information Security collaborate on an ongoing collection of security policies to identify and address severe security vulnerabilities. The policies help assert adherence to the minimum necessary security controls, helping teams meet those requirements out of the box, and providing an easy path for teams to identify and remediate their severe findings quickly in accordance with our SOX and HITRUST remediation requirements.

### Prisma Policy Automation

Prisma Policy can be imported through terraform. Terraform Registry has the Provider – PaloAltoNetworks/terraform-provider-prismacloud i.e which take care of Policy configuration provided in json files.

Python script has been developed to pull policies from OCC from non-standard policies & HCC non standard policies from Github repository stored as a JSON.

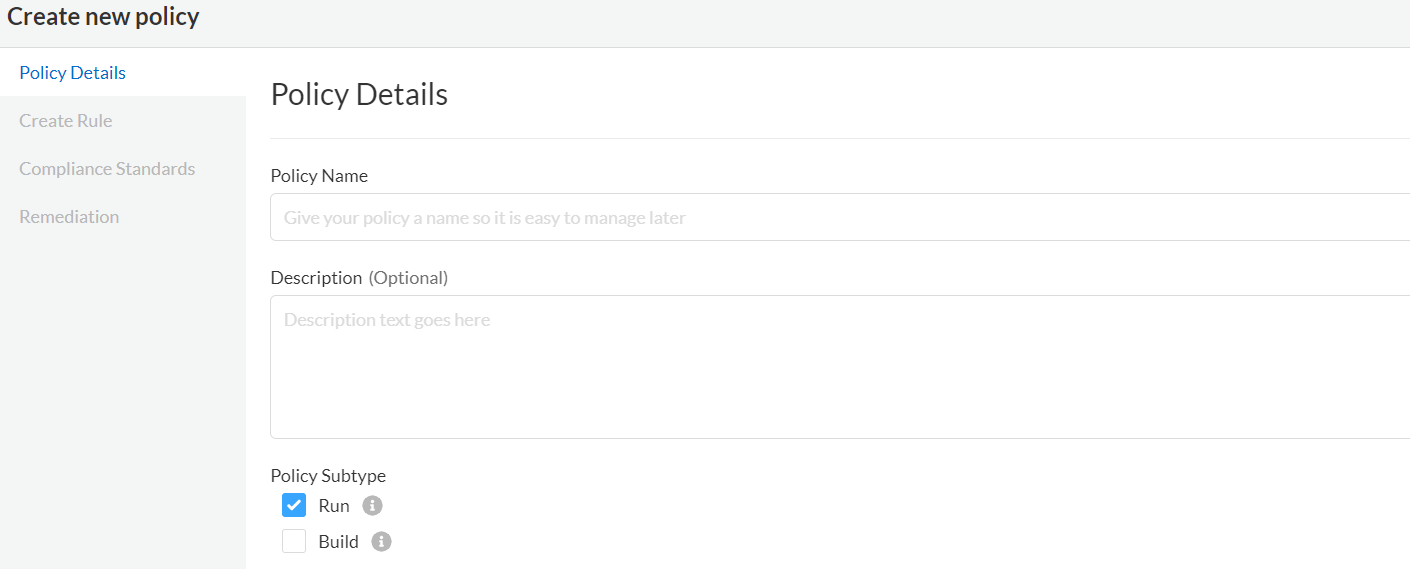
https://github.com/optum-connect/prisma-policies/tree/main/Non-Prod

### How to create Policy?

1. Through Terraform providers by passing policy.json file and import into Prisma Cloud
2. Manual through prisma Cloud console

Go to Policy dashboard -> Add Policy -> Choose type of Policy i.e config or audit or Network

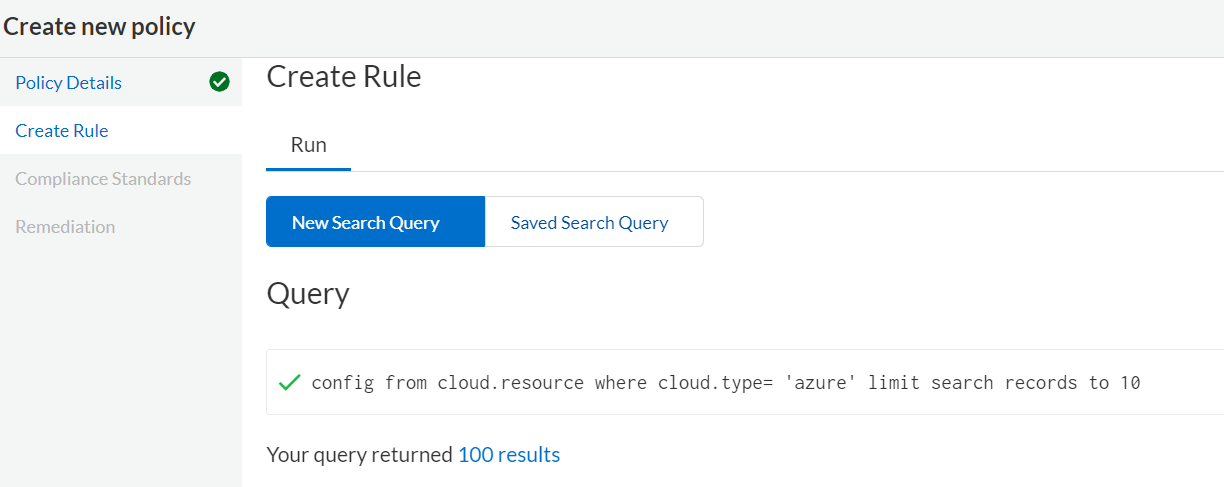
New Create Policy dashboard will be opened.



Policy Subtype

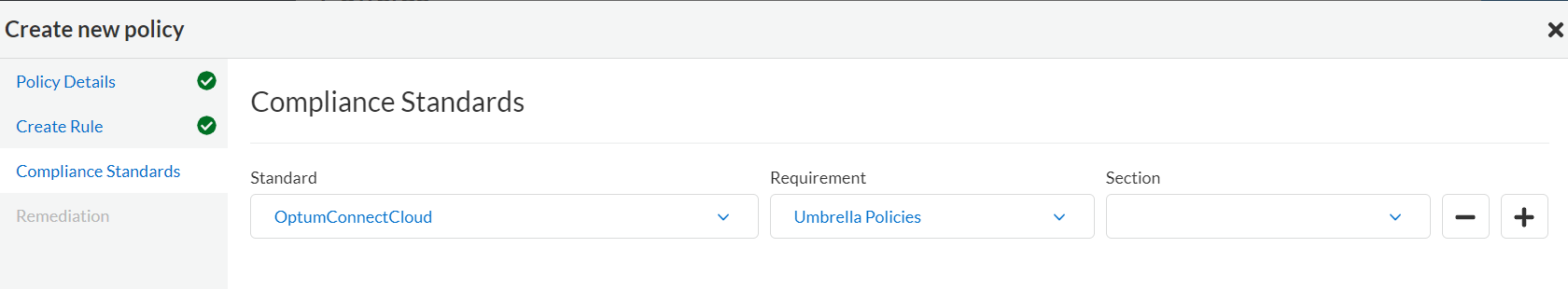
Run :- find and fix misconfiguration in cloud resources that are already deployed

Build :- Scan IaC Code at build time, to find and fix misconfiguration.



If we opt for a Run – Policy Subtype, It give us option to write a query and see output.

Incase of Build, It will write a code. Click Next and



Remediation can be configured parallely. This will contain all the steps required to fix mis configuration.

### How to Edit Policy

Go to Policy Section 🡪 All Policy

Select one policy and select Action Edit

Edit Policy dashboard will open and we can edit all the details.