About Multicloud Defense

About Multicloud Defense

Multicloud Defense is a comprehensive security solution consisting of two primary components: the Multicloud Defense Controller and Multicloud Defense Gateway. These components collaborate to establish a secure multicloud environment

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts. The range of support for these platforms varies.

In essence, Multicloud Defense offers a sophisticated and streamlined security framework, harmonizing controller orchestration, gateway communication, and optimized datapath processing for a robust and efficient multicloud protection mechanism.

Multicloud Defense Naming Conventions

Multicloud Defense interacts with a variety of cloud service providers and in order to provide a universal experience across the platforms, limits the character count when you create gateways and objects. Gateways and objects that exist outside of Multicloud Defense have `ciscomcd` prepended to the name, which may cause issues if the original gateway or object name is too long.

Consider the following character limitations when naming your gateways or objects, both inside and outside of Multicloud Defense:

Table 1: Character Limitation for Naming Convention

Multicloud Defense Feature	Character Limit
Gateway Instance	55
Object Name	63

Note: The values above indicate the character limit for names **without** the prepended Multicloud Defense tag. You are not responsible for including the tag when you name the gateway or object.

Supported Regions

At this time we support all regions for any commercial cloud service provider region for AWS, Azure, GCP and OCI. See your cloud service provider support documentation for more specific information.

If a region appears to not be supported, or a new region is established that is not yet supported, please contact Cisco Support to add support for the region.

Recommended Versions of Multicloud Defense Components

We recommend keeping your components up to date with the latest upgrades and updates for enhancements and new features, as well as bug fixes. For more information on what updates and upgrades are available, and what each package addresses, see the Cisco Multicloud Defense Release Notes.

Third Party Product Support and Versioning

Multicloud Defense utlilizes additional products and functions. For optimal operations, consider using the appropriate versions listed.

Internet Browsers

At this time Multicloud Defense supports and recommends using a **Chrome** browser when viewing the controller dashboard.

Instance Metadata Service For AWS

The Instance Metadata Service (IMDS) is used to access instance metadata from an Amazon EC2 instance. The Multicloud Defense Controller version 23.10 sets up IMDSv2 to be **Required** or **Optional** depending on the corresponding Multicloud Defense Gateway version.

We **strongly** recommend upgrading to a Multicloud Defense Gateway version that specifically supports IMDSv2 in the **Required** mode for optimal security with Amazon EC2 instances.

Note: The Multicloud Defense Controller version 23.10 forces Multicloud Defense Gateway versions 23.04 and later to default to IMDSv2 for EC2 instances.

Use the table below to determine which IMDS version will be setup inside the EC2 instance for your environment:

Multicloud Defense Gateway Version	Required IMDS Version
23.08	IMDSv2 (required)
23.06	IMDSv2 (required)

Multicloud Defense Gateway Version	Required IMDS Version
23.04	IMDSv2 (required)
23.02	IMDSv1 IMDSv2 (optional)
22.12	IMDSv1 IMDSv2 (optional)

For more information on IMDS versions and how to migrate to the version of your choice, see AWS documentation.

Supported Disk Size

Consider the following disk size support for the appropriate gateway versions:

Table 2: Disk Size per Gateway Version

Gateway Version	Supported Disk Size
23.12 and later	128GB
up to 23.10	256GB

Cloud Service Provider Instance Type Support

The recommended instance types for the supported cloud service providers are as follows:

Table 3: Cloud Service Provider (CSP) Instance Type Support

CSP	Instance Type	Max Memory Usage (KB)	Max Bandwidth Usage (Proxy)	Max Bandwidth Usage (Forwarding)
AWS	m5.2xlarge	32,000,000	4,400,000,000	9,000,000,000
	m5.xlarge	9,000,000	2,400,000,000	4,800,000,000
	m5.large	4,500,000	1,200,000,000	2,400,000,000
	m7i	4,500,000	1,200,000,000	2,400,000,000
Azure	Standard_D8s_v3 & Standard_D8s_v5	32,000,000	2,800,000,000	4,000,000,000
	Standard_D4s_v3 & Standard_D4s_v5	9,000,000	1,200,000,000	2,400,000,000
	Standard_D2s_v3 & Standard_D2s_v5	4,500,000	1,000,000,000	1,500,000,000

CSP	Instance Type	Max Memory Usage (KB)	Max Bandwidth Usage (Proxy)	Max Bandwidth Usage (Forwarding)
GCP	e2-standard-8	32,000,000	2,500,000,000	8,000,000,000
	e2-standard-4	9,000,000	1,600,000,000	4,000,000,000
	e2-standard-2	4,500,000	1,200,000,000	2,000,000,000
OCI	VM.Standard.E3.Flex	32,000,000	2,500,000,000	: 8,000,000,000

Multicloud Defense in Cisco Security Cloud Control

Multicloud Defense is now hosted in Cisco Security Cloud Control. Security Cloud Control is a platform that allows you to manage your security products and achieve security outcomes from a single integrated interface. From Security Cloud Control platform, you can manage Multicloud Defense along with other Security products.

When you enroll in a Multicloud Defense, Security Cloud Control creates an account for your tenancy by default to better manage your enterprises across the board. The Security Cloud enterprise supports the following cases: if you have purchased a license and already have a Multicloud Defense account, and if you have purchased a license but currently do **not** have a Multicloud Defense account.

New customers or users of Multicloud Defense can complete the following steps in Security Cloud Control.

1. Create an organization. For details, see the **Create an Organization** topic in the **Organizations and Regions** section of the Getting Started Guide for New Customers of Security Cloud Control.
2. Buy a subscription license. Once you purchase the license, you or the designated system administrator receives an email with a subscription **claim code**. Do not lose this email.
3. Claim the subscription. Enter the claim code in the **Claim Subscription** section of Security Cloud Control application and claim the product. You will receive a confirmation email that Multicloud Defense has been activated on Security Cloud Control. For details, see the **Claim Your Product Subscriptions** section in the Getting Started Guide for New Customers of Security Cloud Control.

Multicloud Defense is provisioned and is available on the default landing page of Security Cloud Control. The navigation pane on Security Cloud Control contains the organization details and menu elements, and the central area contains the dashboard widgets.

Note Customers who provision Multicloud Defense after August 6, 2025 and want to use **Object Sharing** will need to contact Cisco Technical Assistance Center (Cisco TAC) to enable this feature.

For existing users of Multicloud Defense migrating to Security Cloud Control, see Getting Started Guide for Existing Customers of Security Cloud Control.

Multicloud Defense Components

Multicloud Defense uses a common principle in public clouds and software defined networking (SDN) which decouples the control and data plane, translating to two solution components - the Multicloud Defense Controller and the Multicloud Defense Gateway.

Multicloud Defense Controller

The Multicloud Defense Controller is a highly reliable and scalable centralized controller that provides the management and control plane. This runs as software-as-a-service (SaaS) and is fully managed and maintained by Multicloud Defense. Customers access a web portal to utilize the Multicloud Defense Controller, or they may choose to use the Multicloud Defense provider for terraform to instantiate security into the DevOps/DevSecOps processes.

Multicloud Defense Gateway

The Multicloud Defense Gateway is an auto-scaling fleet of Multicloud Defense software deployed as patform-as-a-service (PaaS) into the customers public cloud account/s by the Multicloud Defense Controller. This provides advanced, inline security protections that defend against external attacks, prevent egress data exfiltration and prevent the lateral movement of attacks. Multicloud Defense Gateways include functionality for TLS decryption, intrusion detection and prevention (IDS/IPS), web application firewall (WAF), antivirus filtering, data loss prevention (DLP) and FQDN/URL filtering capabilities.

To facilitate the auto-scaling

- **Autoscaling and Self-Healing**: Operate as autoscaling, self-healing Platform-as-a-Service (PaaS), serving as inline network-based security enforcement nodes. For more information about auto-scaling and how it operates within the construct of the gateway, see below.

- **Simplified Management**: Eliminate the need for constructing virtual firewalls, configuring high-availability setups, or managing software installations.

- **Advanced Security Profiles**: Implement granular security profiles within a single pass datapath pipeline, negating the need for traffic offloading to third-party engines.

Important The Multicloud Defense Gateway does not currently support IP fragmentation because of cloud service provider load-balancer limitations. We **strongly** recommend you adjust the Maximum Transmission Unit (MTU) size so it is consistent across the network to avoid the need for fragmentation.

Multicloud Defense SaaS Controller

Multicloud Defense offers a sophisticated, streamlined security framework, combining robust controller orchestration, gateway communication, and optimized datapath processing to provide efficient and comprehensive multicloud protection. This solution helps organizations secure their cloud workloads and applications from cyber threats while maintaining flexibility and scalability in their cloud environments:

- **SaaS-Based Management**: The Software-as-a-Service (SaaS) controller manages the Gateway stack and includes an API Server for orchestration of CSP load balancers (LBs) and Gateway Instances.

- **Dynamic Scaling**: Facilitates dynamic horizontal scaling through instance additions and removals from the load balancer’s “target pool,” monitored for high availability.

- **Continuous Communication**: Engages in continuous communication with Cloud Service Provider (CSP) accounts to keep security policies up-to-date.

Communications

Multicloud Defense Gateways engage in continuous communication, approximately every 3 seconds, with the Multicloud Defense Controller, transmitting health status and policy updates. This enables proactive health reporting, gateway replacement, and scalability adjustments as needed.

Optimized Gateway Instances

Multicloud Defense Gateway instances operate on highly optimized software, incorporating a single pass datapath pipeline for efficient traffic processing and advanced security enforcement. Each gateway instance comprises three core processes: a "worker" process responsible for policy enforcement, a "distributor" process for traffic distribution and session management, and an "agent" process communicating with the controller. Gateway instances can seamlessly transition "in service" for a "datapath restart," enabling smooth updates without disrupting traffic flow.

Gateway Auto-scaling

Autoscaling in Multicloud Defense is triggered based on the following usage thresholds:

- **CPU Usage**
  - Scale Out: Triggered when CPU usage exceeds 95%.
  - Scale In: Occurs when CPU usage falls below 40%.
- **Memory Usage**
  - Scale Out: Triggered when memory usage exceeds 85%.
  - Scale In: Occurs when memory usage falls below 40%.
- **Bandwidth Usage**
  - Scale Out: Triggered when bandwidth usage exceeds 75%.
  - Scale In: Occurs when bandwidth usage falls below 40%.
- **Connection Usage**
  - Scale Out: Triggered when connection usage exceeds 75%.
  - Scale In: Occurs when connection usage falls below 40%.
- **Load Sustain Period**: Autoscaling actions are triggered if the load conditions are sustained for 120 seconds.
- **Scale-In and Scale-Out Periods**: Both scale-in and scale-out actions have a 120-second assessment period to ensure consistent load conditions.

For information about specific cloud service providers and their instance type support, see Cloud Service Provider Instance Type Support, on page 3.

Advanced Security Profiles

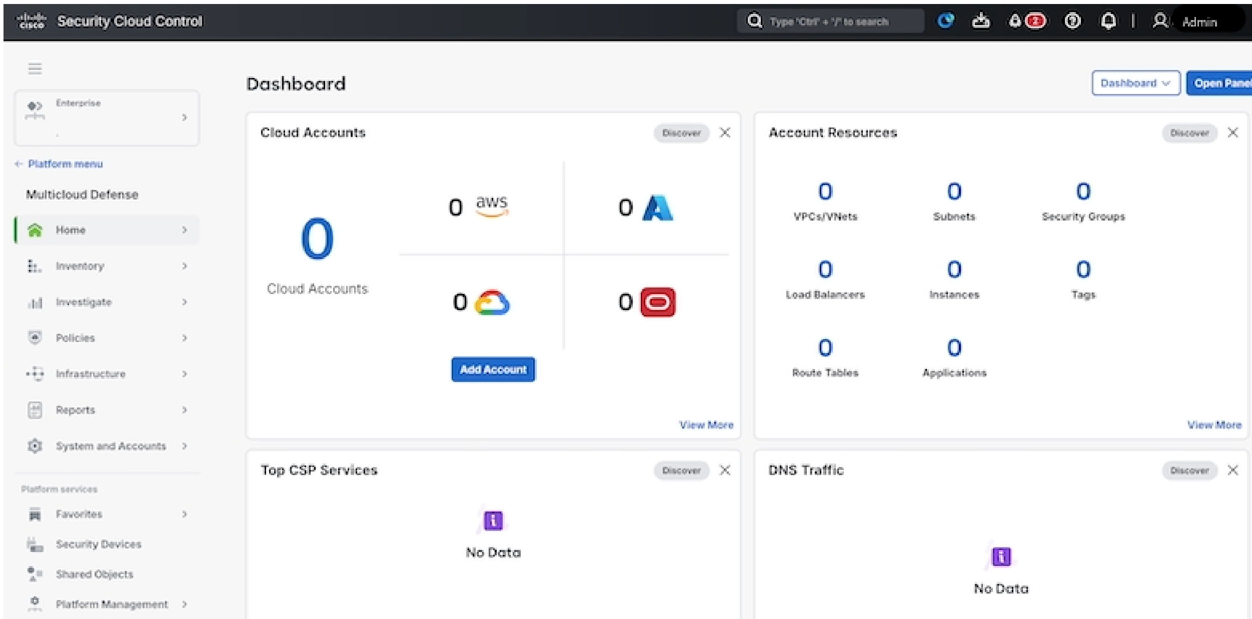
Multicloud Defense Controllers implement granular security profiles within the single pass datapath pipeline, catering to evolving traffic needs. Customers have the flexibility to enable or disable **Advanced Security**

Profiles as required. The pipeline's single pass architecture negates the need for traffic offloading to third-party engines. For instance, full TLS decryption is selectively triggered within the pipeline, ensuring efficient handling without unnecessary data transfers.

In essence, Multicloud Defense offers a sophisticated and streamlined security framework, harmonizing controller orchestration, gateway communication, and optimized datapath processing for a robust and efficient multicloud protection mechanism.

Multicloud Defense Controller Dashboard

The dashboard of the Multicloud Defense Controller has a multitude of widgets to give you a quick snapshot of the current state of your accounts, account resources, and top-hitting policies or profiles.



For your ease, you can drag/drop any of the following widgets to customize and organize the dashboard to whatever fits your needs. You can also click "x" on any of the widgets to remove it from your dashboard view, or "View More" to go directly to the page affiliated with the widget in question. At the top of each widget is an indication as to what function of Multicloud Defense the widget serves: discovery, detection, deployment, or defending.

The following widgets are generated by default:

Cloud Accounts

This is a high-level view to how many cloud accounts you have connected to the Multicloud Defense Controller, and how many of what cloud service provider.

You can easily click "Add Account" from this widget and launch into the connecting wizard to assist onboarding a new cloud service provider.

Account Resources

This is a general list of allocated resources across all of your connected cloud accounts. It displays how many of the following resources are currently used:

- VPC/VNets.
- Subnets.
- Security Groups.
- Load Balancers.
- Instances.
- Tags.
- Route Tables.
- Applications.

Top CSP Services

The Multicloud Defense Controller connects to the cloud service providers and displays a top-down view that generalizes DNS traffic.

DNS Traffic

Similar to "Top CSP Services", this DNS Traffic widget offers a limited view of current DNS traffic for the cloud service providers that are actively processing traffic. We recommend expanding the widget to the full discovery scope for more insight.

VPCs/VNets with Malicious Traffic

This widget displays any recent VPC or VNet that has encountered malicious traffic. For a comprehensive list of events and attacks, expand the widget and view the traffic.

Top Ports with Malicious Traffic

This small snapshot displays whi ports amongst your cloud accounts have the most hits against malicious traffic.

Security Considerations

The Security Considerations widget is a suggestive widget, summarizing which applications, VPCs or VNets, and associated gateways are not protected by the means provided in Multicloud Defense.

System Logs

The System Logs window supplies a recent history of logs that catalogue the accounts affects, the gateway associated, the severity of events or attacks and more. We strongly recommend utilizing this widget, if not the whole System Log page as a valuable resource.

Top Applications

This window accounts for the top-most applications across all cloud service providers that are used.

Threats

View a graph depicting the last seven days of traffic and how much of the incoming traffic was categorized as threats.

Top Countries by Threat

This horizontal bar chart depicts a snapshot of the top 10 countries that during the entirety of the timespan produced the most events, then displayed breaking that volume across the time increments for which the events occurred during the timespan.

Exfiltration Attempts

View a general display of egress data exfiltration that have occurred on the cloud service providers currently connected to Multicloud Defense.

My Profile Information

The User Profile page is the page that details your user information. Access this page by dropping down the **Admin** arrow in the upper right corner of the Multicloud Defense dashboard. Click your username to see the following information:

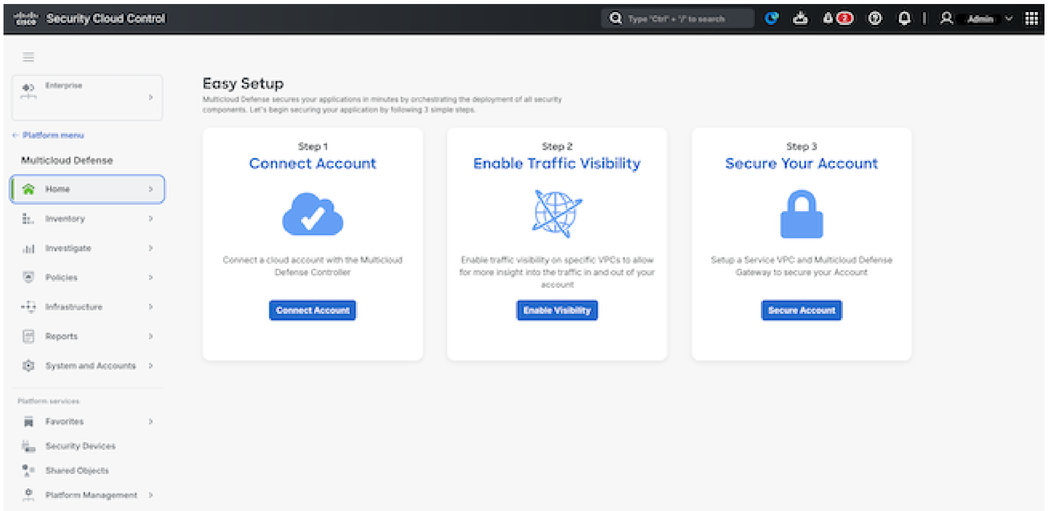
- Your name.
- The email address associated with your Multicloud Defense account.
- The user role you currently have.
- The name of the tenant you are currently logged into.
- Any and all assigned accounts.

This page can be useful for general knowledge, or in the case you reach out for assistance with the Cisco Support team.

Multicloud Defense 90-Day Free Trial

When you log in to your Security Cloud Control tenant, you will see a wizard that guides you through connecting your cloud accounts to Multicloud Defense so that you can manage them with a free 90-day trial of Multicloud Defense Controller. The 90-day trial experience offers the full functionality of a paid-subscription to Multicloud Defense Controller.

Figure 1: Multicloud Defense Easy Setup



Easy Setup

Multicloud Defense secures your applications in minutes by orchestrating the deployment of all security components. Let's begin securing your application by following 3 simple steps.

Step 1
Connect Account

Connect a cloud account with the Multicloud Defense Controller

Connect Account

Step 2
Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3
Secure Your Account

Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

Click **Get Started** to begin your 90-day trial. This begins the process of provisioning the Multicloud Defense Controller.

Note

Easy Setup supports the following Cloud Providers:

- Account Onboarding: AWS, Azure, GCP, OCI
- Enable Traffic Visibility: AWS (Flow Logs, DNS Query Logs), Azure (Flow Logs), GCP (VPC flow logs, DNS Query Logs)
- Create Services VPC/VNet: AWS, Azure, GCP
- Create Gateways: AWS, Azure, GCP

Although Services VCN orchestration is not supported for OCI (requires the user to create the Services VCN using the Cloud Provider console), the Gateway orchestration is supported in Multicloud DefenseMulticloud Defense. Open Multicloud Defense and navigate to **Infrastructure** > **Gateways** > **Gateways**.

Connect Cloud Accounts

After Multicloud Defense Controller is provisioned, the **Connect a Cloud Account** page opens and you can connect any of the types of cloud accounts that are shown to the Multicloud Defense Controller.

The first step is to onboard a set of one or more cloud accounts. This allows the Multicloud Defense Controller to interact with each account by discovering inventory and traffic, orchestrating security deployment, and creating and managing policy.

Follow these instructions to connect your cloud accounts:

- AWS
- Azure
- GCP

- OCI

Enable Visibility

After onboarding, enable traffic visibility for your cloud account. In Multicloud Defense in Security Cloud Control, click **Enable Visibility**.

Enabling traffic visibility provides awareness into the traffic flows within the Cloud Accounts by collecting VPC/VNet Flow Logs and DNS Query Logs. The Flow and DNS Query logs are used by Multicloud Defense to understand traffic flow, correlate with threat intelligence feeds, and provide insight into existing threats that can be protected using Multicloud Defense.

Enabling traffic visibility is a different process for every cloud account type, but typically you will need to identify account characteristics such as your cloud account's region, VPC/VNet that you want to monitor, network security groups, and a cloud storage account for logs.

View Traffic on your Cloud Account

Now that you have enabled traffic visibility, view traffic moving through your cloud account, and look for malicious traffic that needs to be protected against.

1. Log in to Security Cloud Control.
2. In the left pane, click **Multicloud Defense**.
3. In the upper-right corner, click **Multicloud Defense Controller** to open the controller in a new browser tab.
4. In the Multicloud Defense portal navigate to **Investigate** > **Traffic Analysis** > **Topology**.
5. Use the **Filters and Search** bar to find the cloud account you want to monitor.
6. In the **Global View**, add **Malicious Traffic** to your filtering.
7. Click through the malicious traffic bubble to see information in the **Region View** about country of origin, IP address, FQDN, Service and Port that are affected.

Secure Your Cloud Account

Based on your known security needs, and after monitoring traffic, you can secure your account using a centralized hub and spoke model or a distributed model.

Use the **Secure Your Account** wizard to configure a Service VPC and Multicloud Defense Gateway to secure your account.

1. Log in to Security Cloud Control.
2. In the left pane, click **Multicloud Defense**.
3. In the upper-right corner, click **Multicloud Defense Controller** to open the controller in a new browser tab.
4. In the Multicloud Defense Controller dashboard, click **Setup** in the navigation panel.
5. Click **Secure Account** on the **Setup** page.
6. Click **Centralized** or **Distributed**.

7. Click **Next** and continue with the wizard setup.

Relaunching Easy Setup

After you complete the Easy Setup workflow on the Security Cloud Control dashboard to start your 90-day free trial, you can't relaunch it. However, the Easy Setup wizard does exist in Multicloud Defense Controller to help you connect and configure other cloud accounts at a later time.

1. In the left pane of the Security Cloud Control dashboard, click **Multicloud Defense**.
2. In the upper-right corner, click **Multicloud Defense Controller**.
3. On the Multicloud Defense dashboard, click **Setup** in the Multicloud Defense menu bar.

Cloud Explorer

Cloud Explorer, also known as Explorer, is designed to provide users with a graphical visualization of their cloud assets and their relationships. It offers a comprehensive view of the topology of a network, including components such as service VPCs, VPC/VNets, subnets, and instances. This visualization helps users understand and manage the structure and interconnections of their resources within a single interface. Explorer is beneficial for users who want to visualize their cloud infrastructure, manage these assets and their interconnections, and protect them. To manage large amounts of cloud infrastructure and connections, you can create them manually or use Terraform.

The key features of Cloud Explorer are:

- Graphical representation: Displays a clear, visual topology of cloud resources, making it easier to comprehend the relationships between assets.
- Interactive asset management: Enables users to interact with the graphical interface to manage and secure their resources effectively.
- Integrated security posture: Enables users to build and enhance their security posture by protecting assets directly within the Cloud Explorer interface.

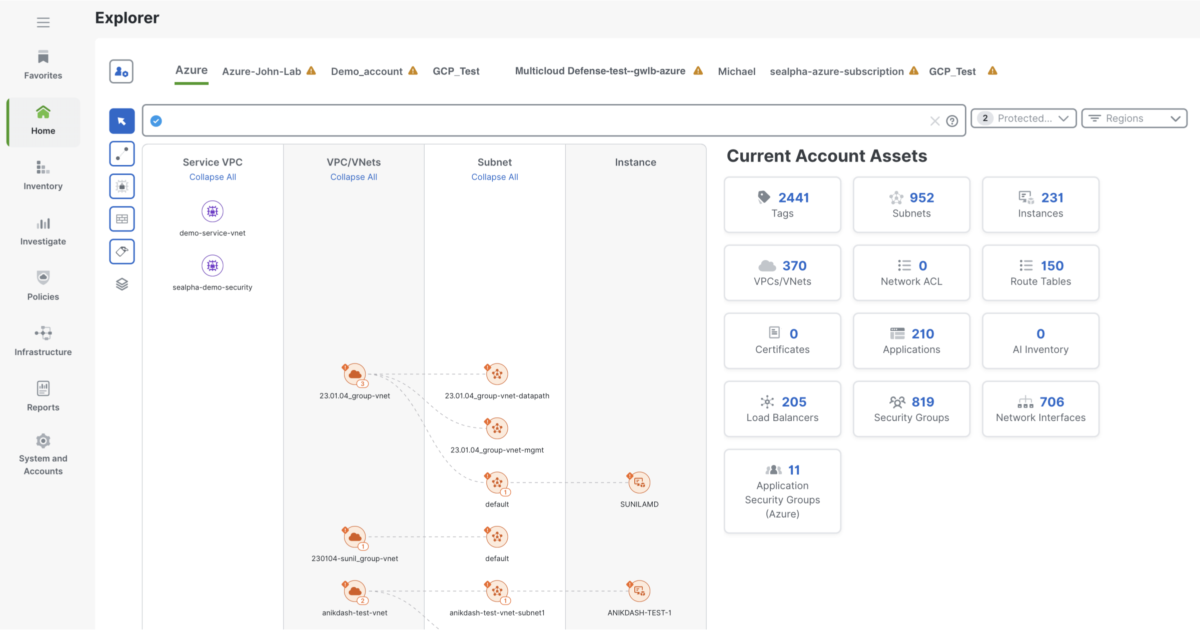
The benefits of Cloud Explorer are:

- Enhanced visibility: Provides a unified view of all cloud assets and their interconnections, simplifying resource management.
- Improved security: Allows users to secure their assets by creating service VPCs and gateways, and by protecting resources through easy drag-and-drop actions and drawing lines to connect assets.
- Ease of use: Simplifies complex configurations with an intuitive interface, enabling users to take immediate actions on their assets.
- Scenario-based utility: Particularly useful in scenarios where users need to understand resource relationships or enhance their security posture dynamically.

To access Cloud Explorer, navigate to **Home** > **Explorer**.

To create an account or select acounts to add to the viewer, click the icon (👤).

Figure 2: Cloud Explorer



Use these icons in the left pane to perform these actions :

- Move ( ): Move your assets between the swimlanes by drag-and-drop actions.
- Secure ( ): Secure your assets by forming connections between them and configuring them on the related screens. For example, click and drag on the Service VPC icon to form a line and connect it to the VPC in the next swimlane. Configure and protect the VPC in the relevant screen that opens up.
- Add SVPC ( ): Click the icon and drop a service VPC into the **Service VPC** swimlane. This opens a drawer for **Create Service VPC** where you can provide details.
- Add Gateway ( ): Click the icon and drop a gateway into the swimlane. This opens a drawer for **Create Gateway** where you can provide details.
- Add Tags ( ): Add tags to selected objects. Click to select up to 3 tags to view in the display.

The central area or canvas contains swimlanes for Service VPCs, VPC/VNets, subnets, and instances. The assets that you include are displayed in the swimlanes. Click the asset and perform actions such as adding a gateway, protecting the asset, or creating a policy for the asset. You can also click an asset to expand or collapse the view of all the asset's connections.