About Multicloud Defense

About Multicloud Defense

Multicloud Defense (MCD) 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 vary.

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.

This documentation has been prepared for practitioners who have a basic understanding of public cloud networking and security concepts, and participate in various functional teams, including:

- Development Operations (DevOps and DevSecOps)
- Security Operation Centers (SOCs)
- Security Architects Info
- Sec Architects Cloud Architects

For more information on the components of this product, continue reading.

Additional Information

You can find additional information about Multicloud Defense in the following documents:

- Multicloud Defense Release Notes

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

We support and recommend the following internet browsers for Multicloud Defense components:

Table 1: Internet Browser Support

Browser	Supported
Chrome	Yes. We **strongly** recommend this browser.
Firefox	Yes.
Edge	Yes.
Safari	Yes.
Inernet Explorer	Yes.

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 Gatewayversion.

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

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 to 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.

Multicloud Defense SaaS Controller

The Multicloud Defense SaaS Controller manages the gateway stack. The controller, equipped with various microservices, includes an API Server facilitating orchestration of CSP LBs and gateway instances. This enables dynamic scaling through instance additions and removals from the load balancer's "target pool," monitored by the load balancer itself.

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.

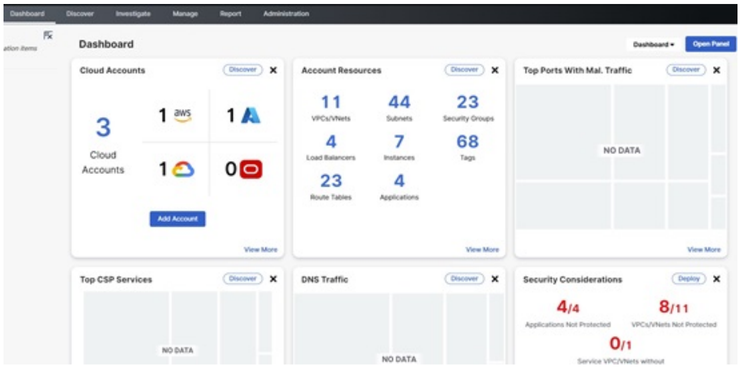
Advanced Security Profiles

Multicloud Defense Gateways 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

This top-down display of cloud service provider services generalizes DNS traffic of the cloud service providers you already have connected to the Multicloud Defense Controller.

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 mlaicious 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.