Multicloud Defense Controller Features and Enhancements (Archives)

Version 25.03 March 28, 2025

Features

The following features are included in this release:

Security Cloud Control Support

Multicloud Defense is now integrated with Security Cloud Control; Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation. You must log into Security Cloud Control and select the Multicloud Defense tab in the navigation pane to launch your Multicloud Defense environment. For more information about Security Cloud Control and what this support means for you, see "About Security Cloud Control".

Gateway Version Notification

The **Infrastructure** > **Gateways** page of the Multicloud Defense Controller now displays whether your deployed gateways are up to date with the recommended gateway version or if they are running a different version. We strongly recommend maintaining your gateways with the recommended version to take advantage of the most recent, stabilized features, enhancements, and fixes.

Version 25.02 February 28, 2025

Features

The following features are included in this release:

AI Defense

Secure your AI assets including the associated activity, types of connections, and number of identities accessing unsanctioned models by enabling AI Defense and integrating the service with your Multicloud Defense tenant.

Resource Tagging

Utilize dynamic objects in your policy rulesets and avoid relying on IP Addresses by tagging your objects as a resource. Either create new objects or select one or more existing objects in your Inventory and click "**Add Tags**"; you can use any key value to tag these resources. Once these tagged objects are attached to a ruleset, Mutlicoud Defense automatically discovers and applies them to incoming traffic.

UDP Fragmentation for Azure Environments

UDP fragmentation refers to the process of breaking down a large UDP (User Datagram Protocol) packet into smaller pieces, called fragments, so that it can be transmitted over a network that has a smaller maximum transmission unit (MTU) than the size of the packet. While fragmentation is not recommended in most scenarios, Mutlicloud Defense Gateways now support UDP fragmentation for Azure environments. Contact Cisco Support to enable this feature on your tenant.

Enhancements

The following enhancements are included in this release:

- Improves the look and feel of the UI.
- Improves general performance.

Version 25.01 January 6, 2025

Enhancements

The following enhancements are included in this release:

- Improves the look and feel of the UI.
- Improves general performance.

Version 24.12 December 2, 2024

Features

The following features are included in this release:

Improved Traffic Summary for Active and Periodic sessions

Previously, an event was only available if a connection session closed or was terminated. Now the traffic summary now posts an event for every five minutes a session is active; this ca help you examine how many ongoing sessions there are at a single time. Merely select the "All Events" checkbox in the summary page to expand the list of open connections, and uncheck it to display only closed sessions.

AI Defense (Private Preview)

Multicloud Defense now supports the private preview of AI Defense to discover and protect your Generative AI application. For more information, contact Cisco.