Multicloud Defense Components

The following components make up the Multicloud Defense experience.

Multicloud Defense Controller

The Multicloud Defense Controller is a Software as a Service (SaaS) component delivered with CDO. It operates as the control plane of the Multicloud Defense and provides administrators the ability to deploy, configure and manage all aspects of Multicloud Defense. It is also the translation layer between operations performed in the Multicloud Defense Controller or terraform provider, and the orchestration of those operations within the cloud service provider.

Capabilities that are provided through the Multicloud Defense Controller include the following:

- Cloud service provider account on-boarding.
- Cloud service provider asset and traffic visibility discovery.
- Services VPC/VNet creation and management.
- Spoke VPC/VNet protection management.
- Gateway deployment, auto-scaling and updates.
- Security policy definition and deployment.
- 3rd party SIEM and Alert integrations.
- Traffic and security event investigation and analysis.
- Discovery and threat awareness report generation.

CDO operations is responsible for updating the Multicloud Defense Controller. Enhancements and updates are provided frequently and can be delivered regularly based on planned release updates, or deployed by way of hot fixes to address critical fixes rapidly.

Multicloud Defense Gateway

The Multicloud Defense Gateway is a platform as a service (PaaS)-delivered component that operates as the data plane deployed in the cloud service provider account to protect public cloud workloads. The Multicloud Defense Gateway is deployed and operates entirely within the cloud service provider account. All traffic processing and security protections reside within the cloud service provider.

Capabilities offered by the Multicloud Defense Gateway include the following:

- Cloud native architecture for protecting workloads.
- Ingress, egress and east-west use-cases.
- Forwarding and proxy-based processing.
- Full decryption for traffic payload inspection.
- Advanced security from a web application firewall (WAF), IDS/IPS, DLP and L7 DOS.
- Filtering via L4, URL/URI, and malicious and geographical IP.
- Orchestration via the Multicloud Defense Controller and terraform provider.
- Multi-cloud, multi-region and multi-availability zone deployment.
- Dynamic auto-scaling based on workload demands.
- Dynamic multi-cloud security policy using cloud constructs.

The customer is responsible for updating the Multicloud Defense Gateway through an upgrade process that is simple, hitless and is completed in minutes. Gateway enhancements and updates are provided frequently.

Multicloud Defense Terraform Provider

The Multicloud Defense terraform provider is a multi-cloud service provider infrastructure-as-code (IaC) orchestration language used to deploy, configure and manage an entire Multicloud Defense deployment via a continuous integration, continuous deployment (CICD) pipeline. It can be used exclusively or in conjunction with the Multicloud Defense Controller and accommodates most operations that are available using the controller.

The customer is responsible for updating their Multicloud Defense terraform provider through referencing the desired terraform release and running a `terraform update` command that loads the referenced version.