Multicloud Defense

(formerly Valtix)

Cisco Partner

https://cs.co/1page

Cisco Multicloud Defense delivers multi-directional protection with ingress, egress, and east-west security. With a single dynamic policy, the solution blocks inbound attacks, mitigates lateral threat movement, and helps stop data exfiltration across your public clouds and workloads.

Benefits:

- Unify control and protection of your public cloud environments, ensuring consistent security policies across AWS, Azure, GCP and OCI.
- Stop inbound threats, block command and control, data exfiltration, and prevent lateral movement with multi-directional protection.
- Deeply understand network behavior and strategically place security controls leveraging continuous asset discovery.
- Save time by reducing policy maintenance in dynamic environments with tag-based multicloud policy management.
- Deploy faster and train less with built-in automation and orchestration.
- Manage, control, and secure cloud infrastructure using Multicloud Defense on Security Cloud Control.

Multi-directional Protection:

Ingress Security: Stop Inbound Threats for Web and Non-Web Apps

Egress Security: Block Command & Control, Botnets, Data Exfiltration

East-West Security: Reduce blast radius and protect against ransomware by mitigating lateral movement.

Where Available: aws Azure Google Cloud ORACLE CLOUD

Use Cases:

Ingress Security protects inbound traffic and provides security capabilities like web application firewall (WAF), IDS/IPS, Layer-7 protection, DoS protection, antivirus, reverse proxy, and TLS decryption.

Egress Security protects outbound and east-west traffic. The egress gateway provides security capabilities like FQDN filtering, URL filtering, data loss prevention (DLP), IPS/IDS, antivirus, forward proxy, and TLS decryption.

Segmentation (East-West) is used in order to mitigate lateral movement. Segmentation provides security capabilities such as Cloud-native Identity, IDS/IPS and antivirus.

URL & FQDN filtering prevents exfiltration and attacks that use command-&-control and enforces URL & FQDN-based filtering in a centralized or distributed deployment model.

Multicloud Defense Packages:

	Advantage	Premier
Visibility	✓	✓
Unlimited Accounts	✓	✓
FQDN Egress Filtering (Outbound)	✓	✓
Malicious IP and Geography-based Blocking	✓	✓
IPS/IDS	✓	✓
Cisco Talos® Threat Intelligence	✓	✓
TLS Decryption	✓	✓
3rd Party Integrations	✓	✓
URL Filtering		✓
DLP (block exfiltration)		✓
Web Application Firewall		✓
API Rate Limiting		✓
Antivirus		✓
Multicloud Connectivity		Coming Soon
Hybrid Segmentation		Coming Soon

Definitions:

Ingress: An application runs in a Virtual Private Cloud (VPC). Traffic enters the VPC from outside (Internet) into the VPC. An Ingress Gateway is deployed to protect the application from external users.

Egress: Instances or Applications that require communication with the external world. To protect/control these clients from egressing traffic to the internet, it is necessary to restrict communication only with certain websites or approved source code repositories.

Edge: The Gateways (Egress and Ingress) can be deployed in Edge or Hub mode. In the Edge mode, the Gateway is deployed in the same VPC as the application(s). If you have 5 VPCs running applications, 5 Gateways are deployed.

Hub: Secure Multicloud creates a new VPC (called Service VPC) and deploys the Gateways inside this Service VPC. All VPCs that are running applications and the Service VPC containing Gateways are connected. Secure Multicloud manages the orchestration of the Transit Gateway, VPC attachments and the routing automatically.

VPC: Virtual Private Cloud (VPC) is a private cloud computing environment contained within a public cloud.

Resources:

SalesResources | Ordering Guide | White Paper | Multicloud Blog | Free Trial

At-a-Glance | Architecture Guide | FAQs | Field Guide | Demo video | Public page

Example SKU: ***FWM-SEC-SUB / MCD-SEC-ADV / MCD-SEC-PRE***