



CUSTOMER SPOTLIGHT:

# TERADATA USES **CISCO** **MULTICLOUD DEFENSE** TO PROTECT AT SCALE

teradata.



# teradata.

**Industry:** Data & Analytics

**Headquarters:**  
San Diego, CA

**Challenges:**

- Required faster security provisioning for customer onboarding
- Desired reduced maintenance driven downtime
- Needed advanced multicloud network security

**Outcomes:**

- Consistent multicloud policy and visibility
- Secure egress traffic at scale
- Modernized solution for secure networking

## Teradata Uses Cisco Multicloud Defense to Protect at Scale

Multicloud data and analytics leader chooses Cisco for improved agility, availability, and security

Dr. Stacy Lanier, Director of Cloud Engineering for Teradata, was faced with a dilemma. Teradata was a fast-growing market leader in delivering multicloud data and analytics. The company's growth and success meant that Stacy needed to evolve his tools stack to keep up with demand while enabling business agility and consistent security policy across each major public cloud.

As Stacy began to define his requirements, he focused on improving security through cloud egress filtering while also enhancing resilience and customer experience. He needed to meet a few core requirement with this new solution.



**Security provisioning in minutes to enhance customer onboarding**

Security couldn't get in the way of service delivery. Stacy wanted his team to not just meet but exceed requirements for customer agility.

**Security rule updates at scale**

Teradata's scale of 1000s of cloud sites meant that many tools would potentially run into issues updating rules fast enough. Waiting hours wasn't an option since that impacted their posture and ability to respond to incidents.

**Low operational overhead through cloud-native**

The amount of troubleshooting and operational headaches couldn't get out of hand. He needed a scalable, cloud-native approach so that his team could spend their valuable time addressing new business priorities, not keeping cloud security infrastructure running.

Stacy also realized that to protect their resources, they required additional security capabilities like decryption and advanced content inspection (e.g. Intrusion Prevention (IDS/IPS), URL filtering) that the CSPs could not fully support.

The business wasn't slowing down. Stacy needed a new solution and he needed it fast.

*"Before we even talked to the Cisco team, we could see the potential fit of their platform with our needs. It was a good sign that we could sign up in minutes on their website."*

**Dr. Stacy Lanier**, Director of Cloud Engineering



# Finding a Modern Solution to Secure Multicloud Networks

One of Stacy's cloud security architects came across Cisco Multicloud Defense while researching new cloud security solutions. Initially, the team signed up to validate against their high-level requirements. As they dug in, they were pleased with what they found and could deploy into a test environment without issue.

Said Stacy, "Before we even talked to the Cisco team, we could see the potential fit of their platform with our needs. It was a good sign that we could sign up in minutes on their website.

The 'a-ha' moment for us was that we could deploy cloud security gateways in minutes, which meant we could remove the bottleneck to customer provisioning. Similarly, security gateway updates could be automated with little downtime and minimal maintenance windows."

Stacy and his team proceeded to set up a meeting with the Cisco team to discuss architecture and run a proof of concept.

"Once we met with the Cisco team, we were impressed by what we found. The Cisco Multicloud Defense architecture was differentiated from other options and our existing solution. This meant that it would not only meet our needs, but could grow as the business grew in the future."

To complete their due diligence, Stacy's team also compared Cisco Multicloud Defense with a solution from a next-generation firewall (NGFW) vendor. What they found further confirmed their direction with Cisco.

- The appliance would take 30 minutes to boot up – a showstopper for a dynamic and changing environment.
- The management and controller architecture would require Stacy's team to manage and maintain another piece of controller software, which was less than desirable.
- The cloud network orchestration required to put the NGFW in the traffic path would create additional implementation and operations burden on Stacy's cloud engineering team.
- High availability (HA) and scale did not meet the operational requirements. The appliance required multiple VMs for HA, which drove cost and complexity, versus a single Multicloud Defense Gateway that could be restarted quickly. In his team's tests, the NGFW failed to deliver at Teradata's scale requirement, thus creating a potential business bottleneck.



# The Cisco Solution: Cloud-Native Architecture to Achieve Agility for Multicloud Networking and Security

After extensive evaluation, Stacy and his team chose Cisco Multicloud Defense to address their needs for an agile, scalable, and robust solution to address their secure cloud networking requirements – now and in the future.

“Cisco Multicloud Defense gives us the best of both worlds. We will be enabled to standardize for consistency across each cloud deployment, reduce operational overhead, and increase our business agility,” said Stacy. “Cisco enables us to do in minutes what previously took hours. When you multiply the many tasks to update gateways, change rules, and support new customers, Cisco Multicloud Defense has the potential to save Teradata in terms of both dollars and hours.”

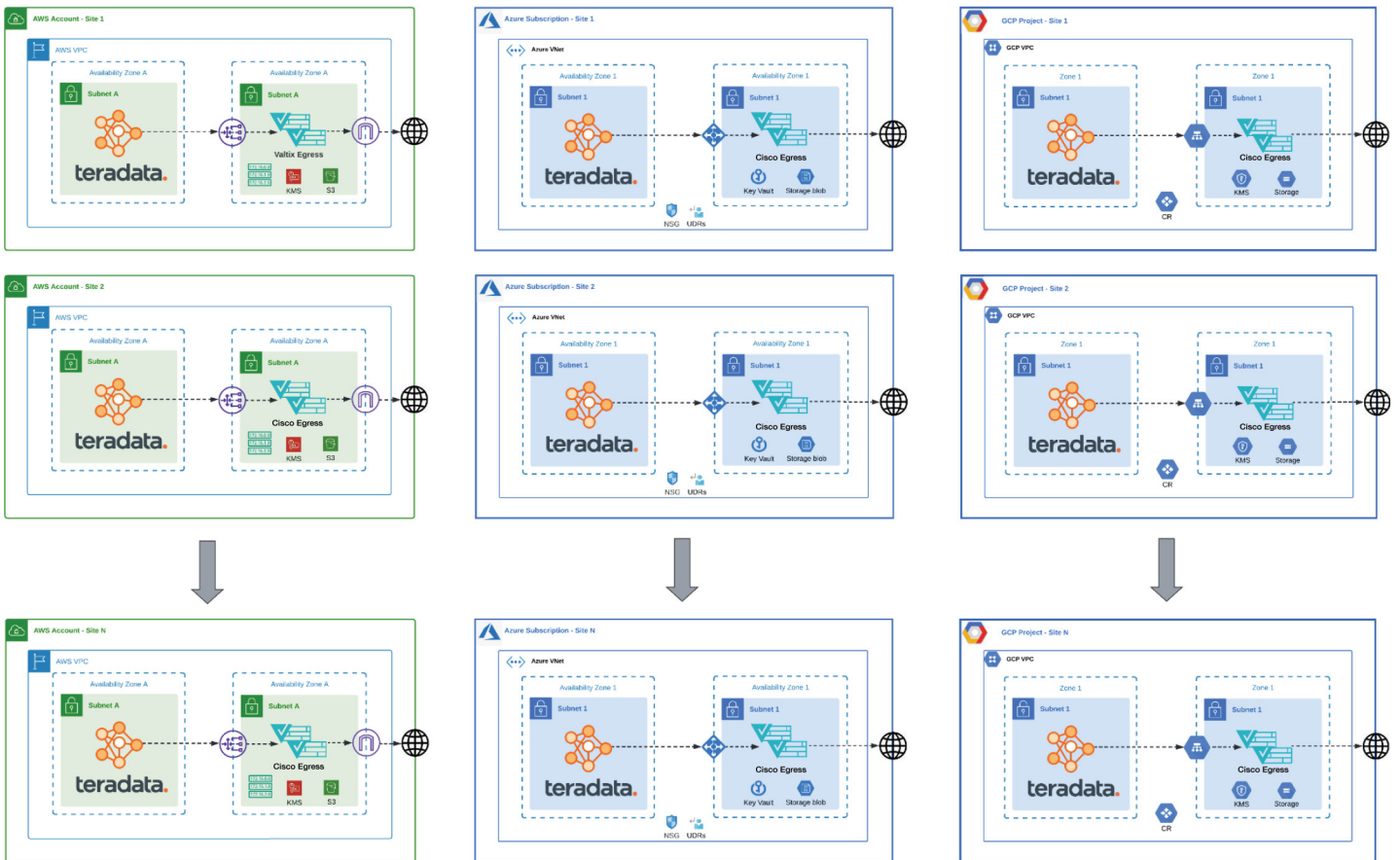
Stacy's team worked with the Cisco team to build a distributed cloud security architecture to support multicloud while keeping data local to each customer account. As a result of the Multicloud Defense Controller and Cloud Gateway architecture (Figure 1), they could meet their business requirements to keep data local to each customer while maintaining consistency and centralized policy management across clouds.

Additionally, the Multicloud Defense Controller, delivered as a SaaS, eliminated maintenance and scale management. Zero controller maintenance improves efficiency and saves time. Also, proactive monitoring provided by the Multicloud Defense Controller with integration into Slack, Datadog and other monitoring tools, enables critical escalations and accelerated workflow.

The Multicloud Defense Gateway provides Teradata with architectural flexibility for distributed and centralized security. This flexibility was essential to support a variety of use cases, including multi-tenant and single-tenant data clouds.

*“Cisco Multicloud Defense gives us the best of both worlds. We could standardize for consistency across each cloud deployment, reduce operational overhead significantly, and increase our business agility. Cisco enables us to do in minutes what previously took hours. When you multiply the many tasks to update gateways, change rules, and support new customers, Multicloud Defense saves us millions of dollars and many man hours.”*

**Dr. Stacy Lanier**, Director of Cloud Engineering



**Figure 1:** The Cisco Multicloud Defense enables multicloud consistency through distributed traffic inspection

Infrastructure as Code (IaC) and policy as code enabled complete automation through Terraform and REST-based API integrations. With Cisco Multicloud Defense, Stacy and his team can achieve the separation of infrastructure and policies that gave them the desired agility.

As a result, Teradata was able to meet its business goals:

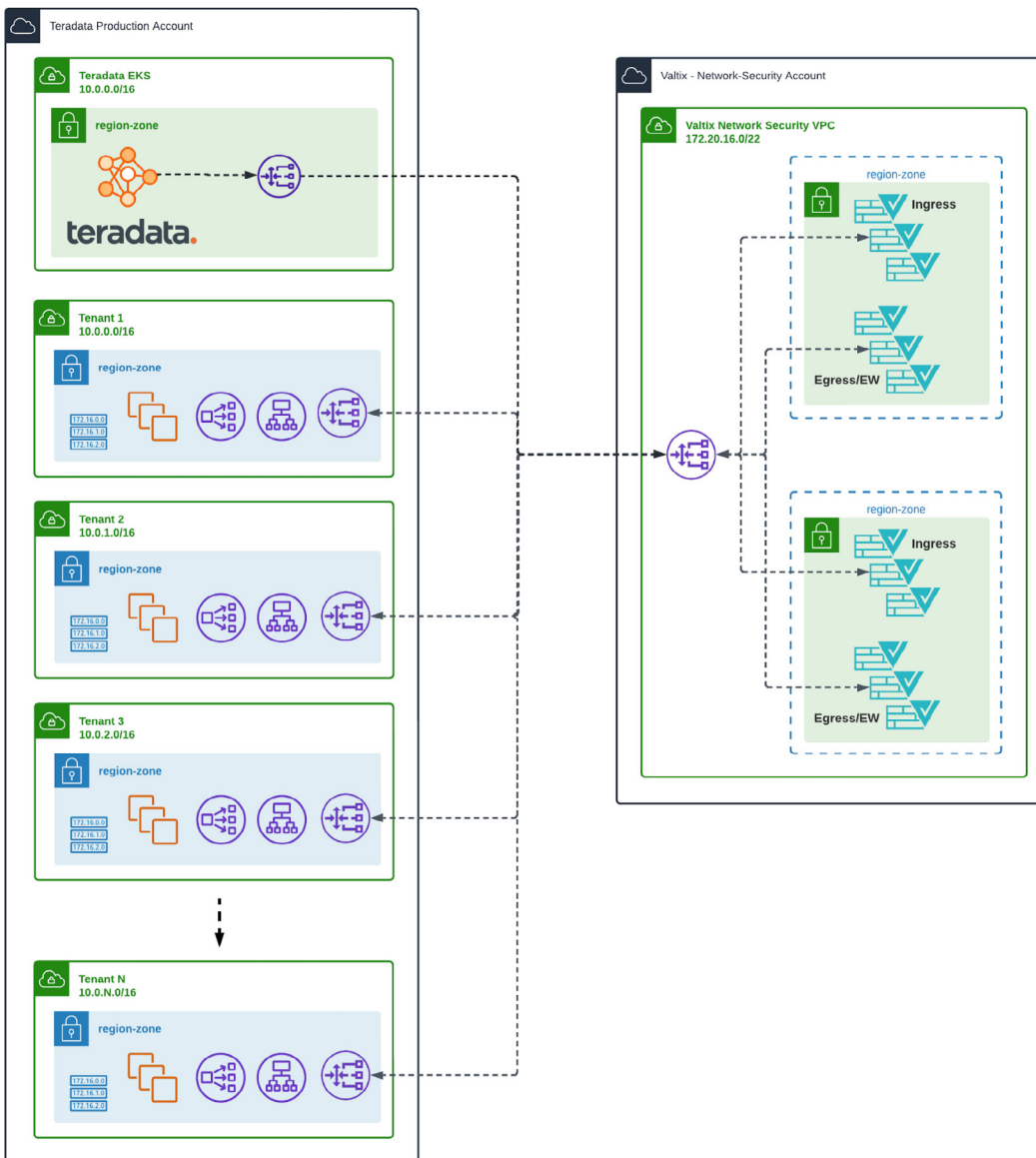
- **No delay for customer provisioning** – Cisco provides Teradata with an approach to achieve security and compliance goals without slowing down business delivery.
- **Increased agility to respond** – Policy updates can be applied in minutes across hundreds of security control points via a centralized multi-cloud security architecture, accelerating incident response.
- **Reduced maintenance and troubleshooting** – Better able to dedicate time to focus on more important security and compliance needs instead of troubleshooting.

Said Stacy, "Cisco Multicloud Defense was the right solution to modernize our secure cloud networking infrastructure. They enable a first-class architecture that centralizes multi-cloud visibility and control across our customer accounts. We're excited to partner with Cisco."

# Opportunities for the Future

While starting with egress security, Stacy was excited about the other opportunities that Cisco Multicloud Defense as a security platform opened up for his team. IPS / IDS was of special interest to block exploit attempts and other threats. The ability to remove other tools and consolidate policy management provides significant agility and economic benefits.

Additionally, Stacy's team needed to create a more centralized security model (figure 2) for both ingress and egress traffic for a new multi-tenant offering. Cisco Multicloud Defense architectural flexibility for both centralized and distributed use cases meant that Teradata could maintain centralized security visibility and control regardless of the security architecture.



**Figure 2:** Centralized security for ingress and egress enables a scalable approach to support Teradata data as a service platform

## What do Ransomware, Botnets, and Cryptomining attacks all have in common?

### ANSWER:

Each of these attacks leverages command and control (C2) frameworks to orchestrate lateral movement, execute attacks, and exfiltrate data.

## What's the best way to detect and prevent command and control (C2)?

### ANSWER:

Securing egress traffic using FQDN (fully qualified domain name) and URL filtering

# What Is Cloud Egress Filtering and Why Is It Important??

Having control over outbound destinations from your cloud workloads and data stores is a fundamental best practice, but too few organizations implement this basic security best practice. If they do, it's usually with so many holes and compromises to be almost completely ineffective.

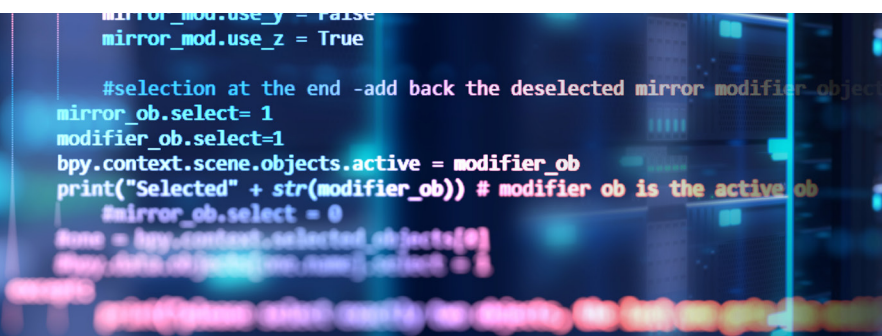
**FQDN (fully qualified domain name) Filtering** – FQDN filtering operates on the destination name to either allow or deny an outbound request based on a set of parameters. Outbound connections can be allowed or denied based on a list of known good domains (whitelisting) or known bad domains (blacklisting).

**URL Filtering** – URL filtering works by analyzing web traffic and filtering it based on the URLs (e.g. https://domain.com/URL) that are accessed. This involves identifying the URLs accessed by your applications and then comparing those URLs to a list of known malicious or potentially harmful URLs or known good URLs.

URL filtering requires TLS decryption since the URL is part of the TLS-encrypted HTTP traffic. FQDN (domain) filtering doesn't require decryption, although it does require category-based domain intelligence that most solutions don't provide.

A great example of a domain where you also need to care about the URL is github.com. Whether the URL is github.com/MyOrganization vs. github.com/MaliciousSite is a pretty important detail when implementing a secure egress strategy. Clearly, FQDN filtering will not help in this case. You need to filter based on URL.

[Read More About URL Filtering](#)



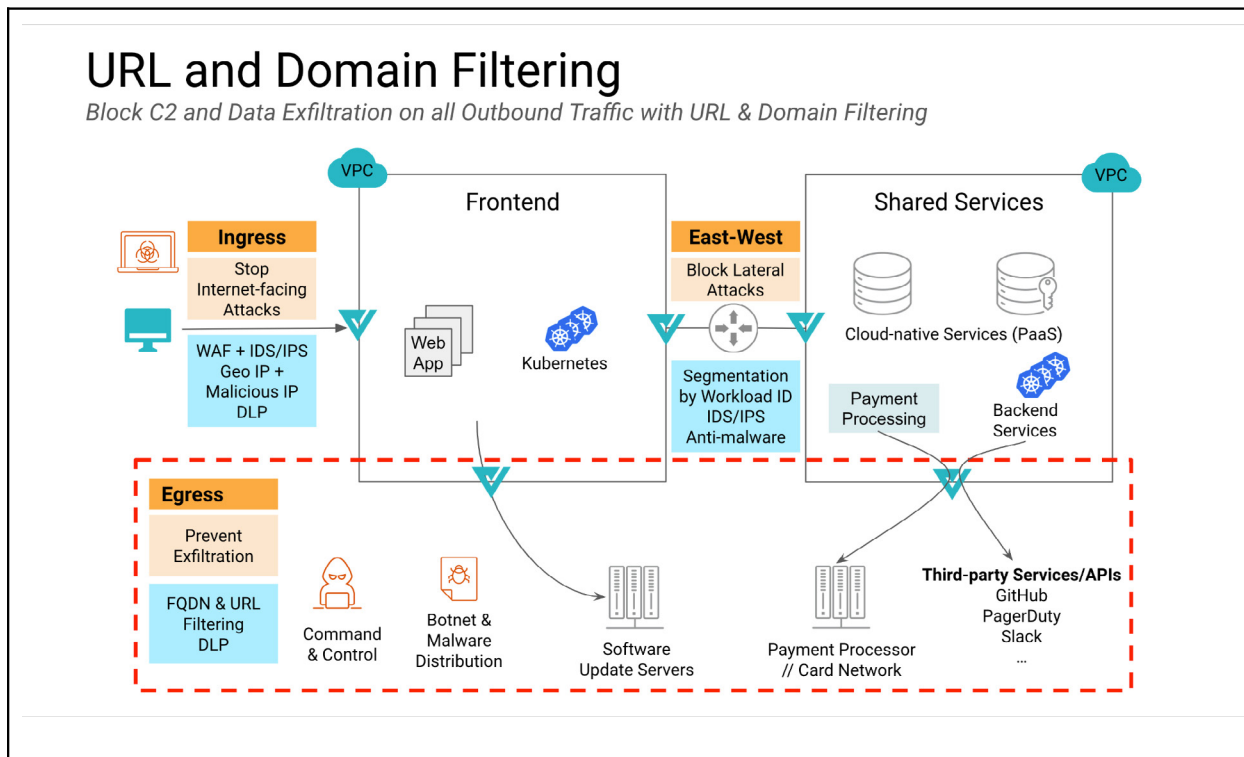
```
mirror_mod.use_y = False
mirror_mod.use_z = True

#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
#name = bpy.context.selected_objects[0]
#obj_data_ob[modifier_ob.name].select = 1
```



**Domain and URL category classification** is provided by a service built into your security platform that can classify any domain/site and URL in real time. This means that you don't have to explicitly list the specific ones you want in your policy out of the millions of domains and billions of URLs. So you can:

- Block all malicious categories like malware, phishing, botnets, and so on.
- Allow only approved pre-defined categories like Financial Services, AWS Cloud Services etc.
- Allow only approved customer-defined categories: My Payment Processors, My Third-Party Vendors



**Figure 3:** URL and domain filtering



CUSTOMER SPOTLIGHT:

# TERADATA USES CISCO MULTICLOUD DEFENSE TO PROTECT AT SCALE

teradata.

## ABOUT TERADATA

*Teradata is the connected Multi-cloud data platform for enterprise analytics company. Our enterprise analytics solve business challenges from start to scale. Only Teradata gives you the flexibility to handle the massive and mixed data workloads of the future, today. Learn more at [Teradata.com](https://www.teradata.com).*