# Solution Overview of Cisco Secure Agile Exchange

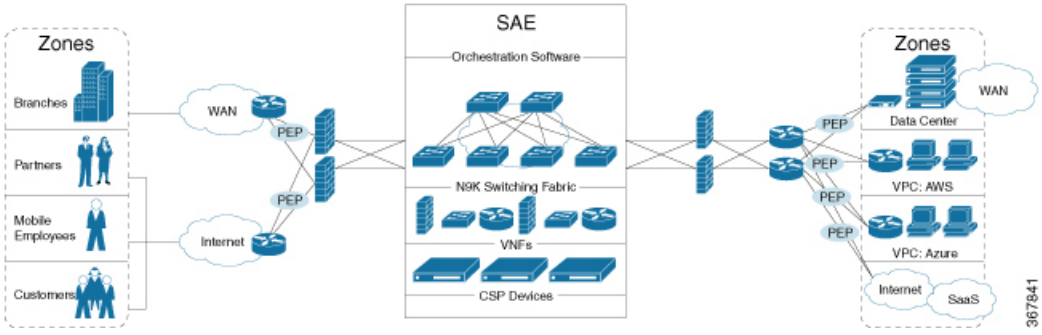
Cisco® Secure Agile Exchange (SAE) is a solution that enables enterprises to interconnect users to applications quickly and securely by virtualizing the network edge (DMZ) and extending it to colocation centers, the crossroads of Internet traffic.



## About Cisco Secure Agile Exchange (SAE)

Cisco® Secure Agile Exchange (SAE) provides orchestration and automation of Cisco products like CSR and ASAv, along with third-party VNFs using Cisco Cloud Services Platform (CSP). CSP is an open Cisco Network Function Virtualization (NFV) appliance.

The flexible architecture of this solution connects distributed consumers with distributed data and applications that potentially reside in many clouds and private data centers.




This single-vendor, turnkey solution reduces the operational complexity of deploying different services from multiple vendors.

# Problem Statement

The interconnections between users and applications are evolving to complex digital business architectures due to emergence of multi-cloud IaaS and SaaS vendors. This requires the network to be both fast and flexible to meet the expanding changes and demand.

## Current Landscape

### Distribution of Applications from Data Centers to IaaS and SaaS

Applications reside in multiple locations, including the private data center; in the cloud in the form of infrastructure as a service (IaaS) with providers like AWS, Azure, and Google Cloud Platform; or as software as a service (SaaS) with providers such as ServiceNow and Salesforce, Box, Office 365, to name a few. Regardless of an organization's cloud strategy, most will have applications across all locations.

Digitization is placing unprecedented demands on IT to increase the speed of services and products delivered to customers, partners, and employees, all while maintaining a high level of security. With the adoption of multi-cloud infrastructure, the need to connect multiple user groups in an agile and secure manner places additional demands on the IT teams.

## Challenges

- It is becoming increasingly difficult to apply security policies uniformly across multi-cloud applications.
- Some IaaS and SaaS vendors may not provide the required security options.
- The IaaS and SaaS providers that do the security options you need may not necessarily do so in a way that is consistent with your enterprise policy.
- There is inconsistency in application of policies across products and applications.

## Business Impact

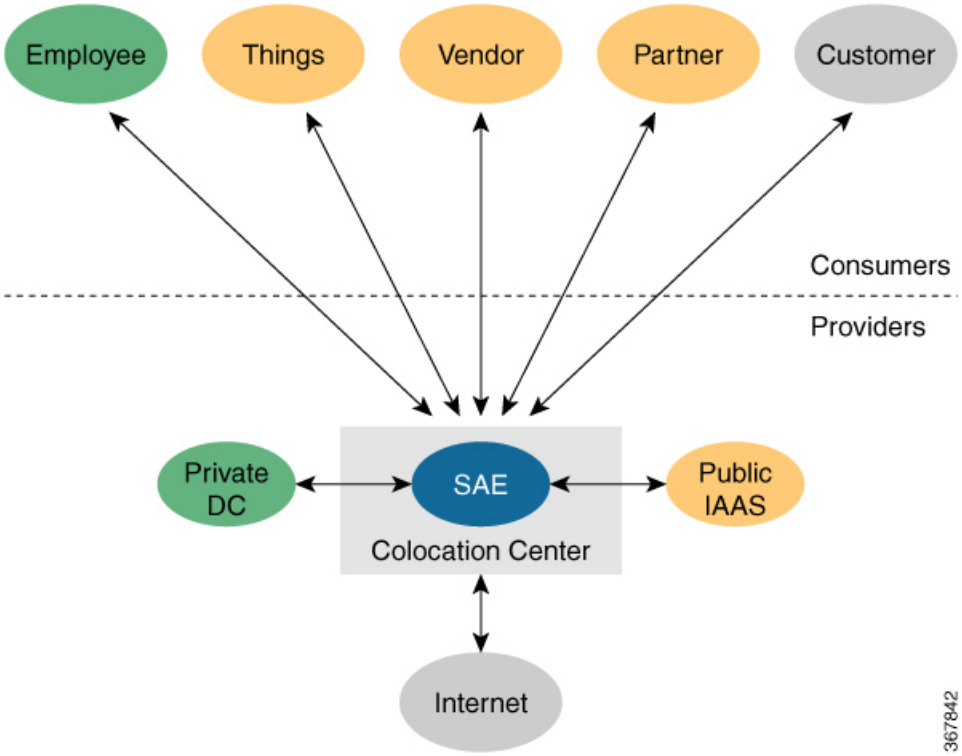
The business impact of the rising complexity resulting from multi-cloud adoption and the increasing demand for flexibility and security can be categorized as follows.

- **Latency and Increased Costs:** As enterprises embrace cloud, they are required to backhaul traffic to their data centers to apply security policies and to gain visibility in the incoming and outgoing IaaS and SaaS traffic. This hairpinning of traffic causes latency and increases costs.
- **Inefficiency:** A majority of changes that are being implemented in response to the changing IT landscape are still being implemented manually. This lack of network agility and automation has led to inefficiency in service enablement.
- **Under-utilization** The existing infrastructure is designed for maximum capacity, but has low utilization.
- **Security:** The attack surfaces are expanding due to increasing numbers of security vendors and connectivity to cloud-hosted services. This has led to an increased time in detecting and remediating network attacks.

### How SAE can Help Overcome the Challenges

As enterprises adopt a multi-cloud strategy, they must look at optimizing traffic patterns for experience, securing interactions, reducing circuit costs, and providing flexibility.

The success of multi-cloud solutions depends on a new cloud-edge capability, where all consumer networks terminate in a carrier-neutral facility and security policies can be enforced centrally.




This is where SAE comes in. SAE offers the capability of virtualizing your network edge and extending it to colocation centers. SAE provides segmentation, virtualization, automation, and orchestration for your enterprise within a carrier-neutral facility.

Virtualization, automation, and orchestration are foundational to SAE. Virtualization negates the need to design infrastructure for future requirements of scale by providing an agile way of scaling up and down as required.

**Note** It is possible to place SAE in your private data center; however, we recommend deploying SAE in a carrier-neutral facility to truly benefit from the agility it offers. Deploying SAE in a carrier-neutral or colocation facility offers the following benefits.

- Proximity to clouds, which helps maintain app SLAs
- Security and telemetry across multiple clouds
- Single location to view and audit traffic and user-app relationships

# Benefits of SAE

**Security:** Centralized policy enforcement offers simple and secure access, deployment, and control.

**Scale-out Architecture:** The flexible architecture of SAE allows you to scale out the VNFs and compute as required. Cloud Servces Platform (CSP), the x86 compute platform negates the need to order, cable, rack, and stack dedicated appliances when capacity needs to increase or changes need to be made.

**Performance Agility:** The ability to spin up networks and VNFs on demand offer improved performance agility. You can optimize application performance by strategically placing SAE in colocation centers that are closest to your Saas and IaaS cloud providers.

**Flexibility:** The solution supports both–Cisco VNFs and third-party VNFs that Cisco supports.

**Cost Savings:** By having a central location to connect to various clouds (including private clouds), enterprises can optimize the costs of circuits to connect their users to applications. Circuit costs for a colocation facility are significantly lower than in a private data center.

# Components of SAE

The SAE solution consists of the following components and services, which integrate to address the challenges described in the previous sections of this guide.

- **Orchestration:** SAE core function pack provides network services orchestration. SAE core function pack enables VNF workflow management, fabric configuration, routing of layer 2 and 3 networks and inter-virtual devices. The core function pack also provides intelligent VNF placement logic that is based on the availability of compute resources and high availability (HA) requirements.
- **CSP NFV Appliance:** CSP, a x86 Kernel-based KVM platform is used to host VNFs. CSP supports high-throughput internal switching technologies such as Single Root I/O virtualization (SR-IOV) and 10 GBPs physical network cards (pNICs). It also uses a central network file system (NFS) to host the images of shared VNFs and configuration templates.
- **Nexus 9000 Switching Fabric:** The SAE switching fabric is built in a carrier-neutral facility and uses high-performance Cisco 9000 series switches. SAE switching can be built in either standalone topology or spine-leaf topology. The Nexus 9000 fabric supports the following:
  - Full redundancy with port channels and virtual port channel (vPC)
  - Multi tenancy with VRFs
  - VLAN and VXLAN
- **Virtual Network Functions (VNFs):** The solution has been tested with both, Cisco VNFs and third-party VNFs that are supported by Cisco.