illumio

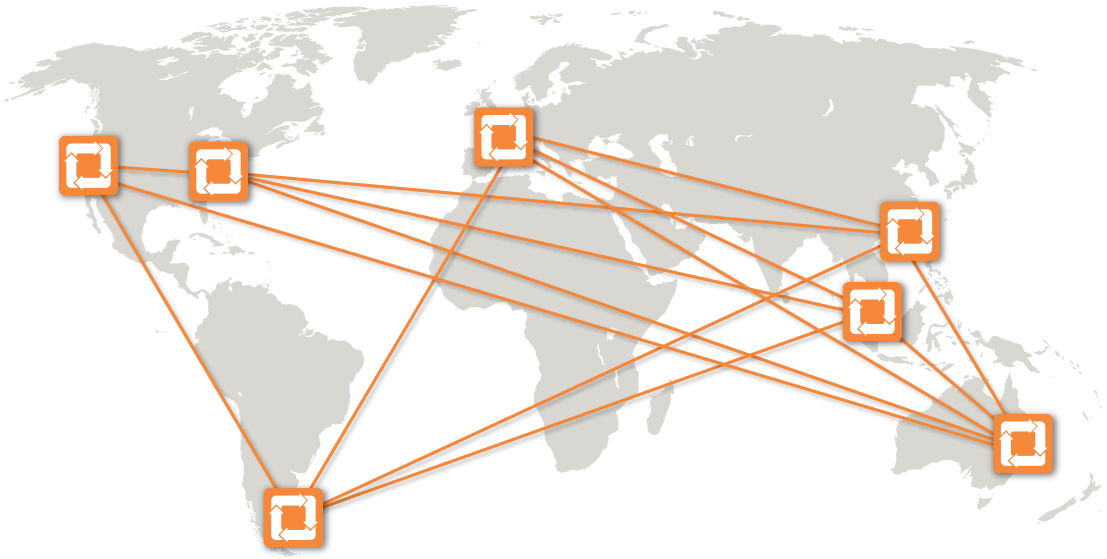
SOLUTION BRIEF

PCE Supercluster: Managing Global Security Policies at Scale

This solution brief discusses the benefits of using PCE Supercluster™ to deploy a federated micro-segmentation architecture with centralized policy management and global visibility at scale. For more details on the Illumio Adaptive Security Platform® (ASP) and its capabilities, please read the Illumio ASP datasheet.

SECURITY CHALLENGE

A very large global enterprise's operations can span across multiple regional data centers. Its data center footprint may be hundreds of thousands of workloads sprawled across a combination of private and public cloud using bare-metal and VM servers and containers. Such organizations want Zero Trust security at a global scale but struggle to achieve it. Using any combination of SDN, data center firewalls, and networking technologies is expensive and complex to deploy and operate. Keeping track of VLANs, IP addresses, and subnets, and managing policies and firewall rules to prevent the lateral movement of bad actors inside the data center and for regulatory compliance will require re-architecting infrastructure.



The organization increasingly recognizes that it is smarter to separate networking from security and wants to:

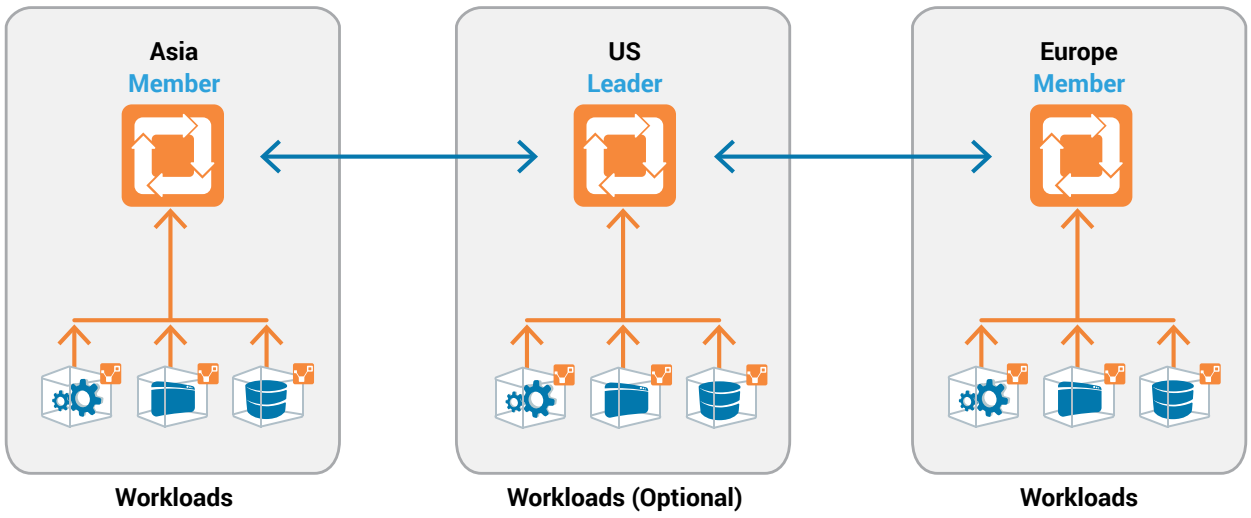
- Enable Zero Trust security at a global scale to meet various global compliance obligations and prevent the lateral movement of bad actors inside its data centers.
- Get global, real-time visibility into its managed workloads and the unmanaged workloads connecting or trying to connect with the managed workloads.
- Centralize global management of security segmentation policies.
- Enable security policies to follow the workloads everywhere at a global scale.
- Enable firewall rules to be applied locally based on contextual information about the environment, workloads, and processes.

This design will allow them to minimize network chokepoints and support disaster recovery and high availability objectives.

> *The organization wants to accomplish these Zero Trust security, high availability, disaster recovery, and network bandwidth efficiency goals without having to re-architect its infrastructure or hire a huge organization to maintain its global Zero Trust security operations.*

ILLUMIO ADAPTIVE SECURITY PLATFORM WITH PCE SUPERCLUSTER

A Policy Compute Engine (PCE) Supercluster consists of a single administrative domain that spans two or more replicating PCEs.



The PCE Supercluster architecture consists of a leader PCE and member PCEs, where the leader PCE provides a central portal into visibility (via Illumination), manages global policies, and distributes changes in policies to member PCEs.

Each PCE in the PCE Supercluster is independent – even a complete failure will not affect other PCEs. If the leader PCE fails, one of the member PCEs can become the leader. Policies will revert to the last version that was distributed from the old/failed leader PCE.

There are also disaster recovery scenarios where VENs will need to be paired with a global load balancer. When the local PCE to which the VEN is paired fails, the global load balancer can make failover decisions and route the VEN to another PCE in the PCE Supercluster. Illumio ASP uniquely offers this capability.

Examples of data center scenarios where the PCE Supercluster is most relevant:

- **An organization has between 25,000 to 185,000 critical workloads distributed across multiple regional data centers.** The organization wants to maintain global visibility and centrally manage policies to enable environmental, application, and workload segmentation for Zero Trust security. To eliminate WAN bandwidth bottlenecks and optimize network resources, it wants a local PCE to manage the workloads (VENs) and program the enforcement points in those workloads. Local PCEs are continuously synced with the leader PCE.
- **An organization has multiple PCEs, its disaster recovery/availability design is Active/Active, and PCEs are considered tier 0 applications.** The volume of workloads managed per PCE may be less than 25K. In this scenario, PCEs are collocated with the workloads (VENs) it manages. To support the organization's recovery time objectives (RTOs), policies are continuously synced across member PCEs and the leader PCE.
    - When a data center goes down, its workloads are immediately restored to another site with all of its security policies in place. These restored workloads are managed by another PCE in the PCE Supercluster.
    - When a local PCE goes down, management of the workloads is immediately transferred to a member PCE in the PCE Supercluster so that security policies remain intact.

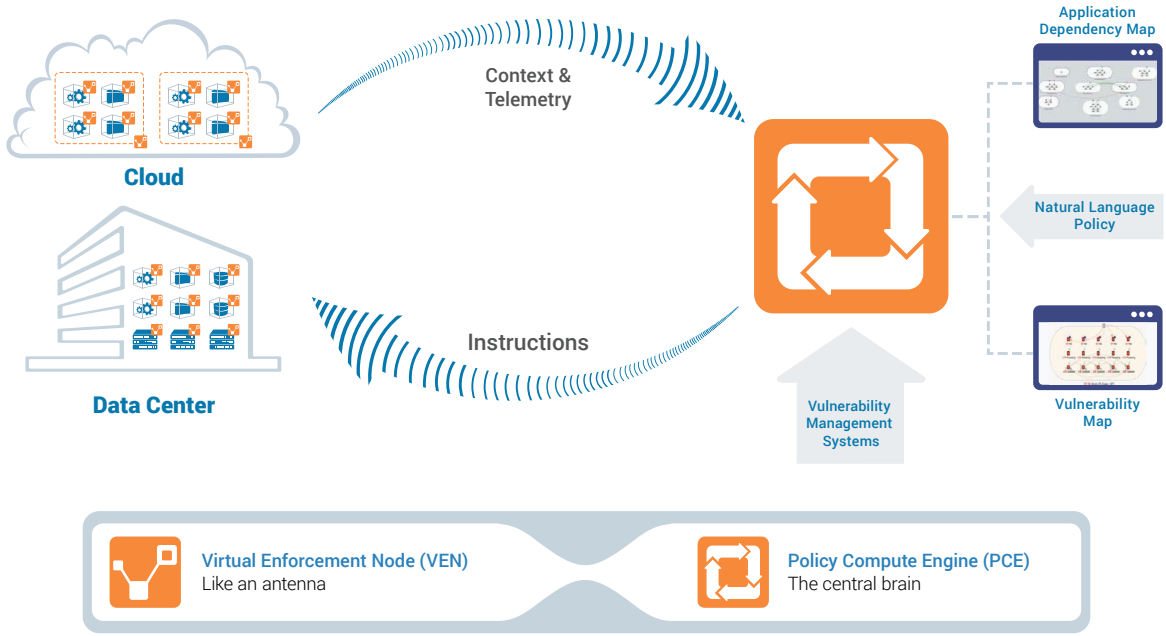
Key Benefits of PCE Supercluster

PCE Supercluster is designed for enterprise-scale, globally distributed environments. It allows organizations to manage Zero Trust policies globally but enable local PCEs to manage the workloads and program its enforcement points. Compared to a single PCE, a PCE Supercluster provides multiple independent PCE failure domains and support for greater numbers of workloads.

It delivers:

- Global real-time visibility across managed and unmanaged workloads at very large scale.
- Centralized policy management across a federated micro-segmentation architecture.
- Zero Trust security operations in multi-region PCE deployments, at scale, using existing enforcement points, avoiding significant infrastructure and management overheads.
- Alignment of Zero Trust security practices with fault isolation, high availability, and disaster recovery objectives.

ILLUMIO ASP ARCHITECTURE



Illumio ASP is comprised of two core components:

Virtual Enforcement Node (VEN): The VEN is a lightweight agent that is installed in the guest OS of the host. The VEN does not enforce firewall rules or route traffic. It collects and transmits information about the workload's connections, flows, and processes to the Policy Compute Engine, enabling security to baseline an application's behavior and create rules to detect for unauthorized connections and deviations from policies. It also takes instructions on the applicable firewall rules from the PCE and programs the host's native Layer 3/Layer 4 stateful firewalls.

Policy Compute Engine (PCE): The PCE is the brain that collects all the telemetry information, visualizes it via application dependency maps (Illumination), and then creates the optimal firewall rules based on contextual information about the environment, workloads, and processes. These rules are transmitted back to the VENs, which in turn program each host's Layer 3/Layer 4 firewalls. Policies automatically adapt to changes in the application environment to maintain consistent security.

LEARN MORE

- Illumio ASP Datasheet

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve visibility behind the firewall, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com