SECURING HYBRID INFRASTRUCTURES

UNIFORM SECURITY POLICIES ENABLE MULTI-VENDOR INFRASTRUCTURES AND HYBRID CLOUD DEPLOYMENTS

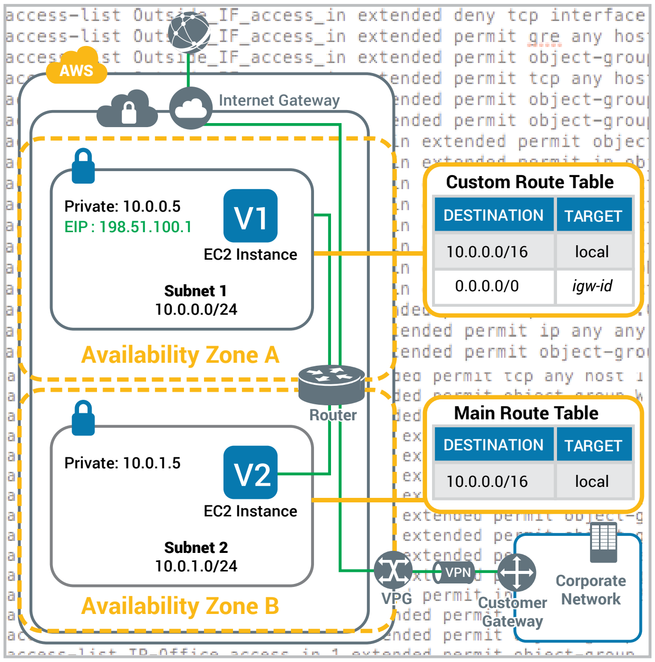
Enterprises need to secure data centers with a mix of bare metal-servers and virtual machines from multiple vendors and public clouds from different cloud providers. The Illumio Adaptive Security Platform (ASP)™ secures hybrid deployments with natural-language policies that don't depend on the network.

Before Illumio

- No control over the network in public cloud—network-centric security doesn't work
- Risk of breaking applications without visibility to traffic flows
- Non-uniform security policies between data center and public cloud make security hard to set up and maintain

After Illumio

- Uniform security policies across all infrastructures or cloud environments
- Securely auto scale applications with orchestration tools (e.g., Chef, Puppet, Ansible)
- Security automatically adapts to changes in application, environment, and location
- Instantly encrypt data in motion (IPsec) between any Linux/Windows workloads, across any environment



Custom Route Table

DESTINATION	TARGET
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main Route Table

DESTINATION	TARGET
10.0.0.0/16	local

Figure 1: Organizations don't have control over the network in a public cloud, making it difficult to implement security and keep it uniform across their environments.

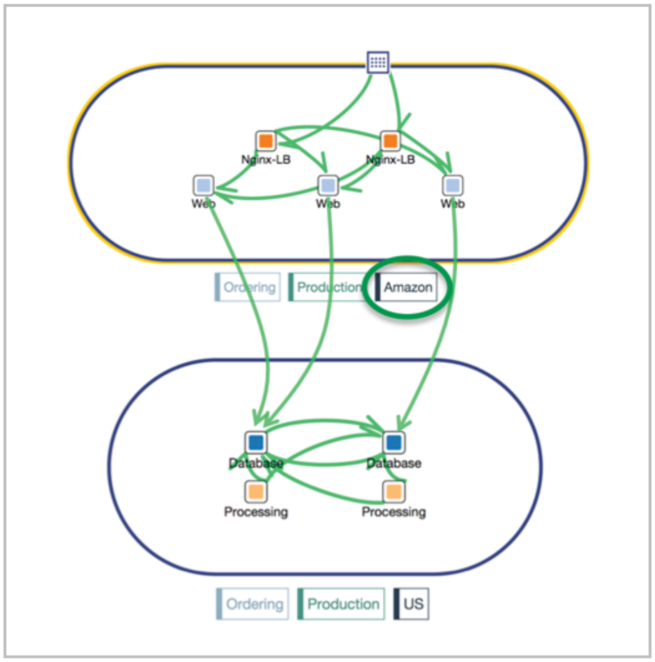
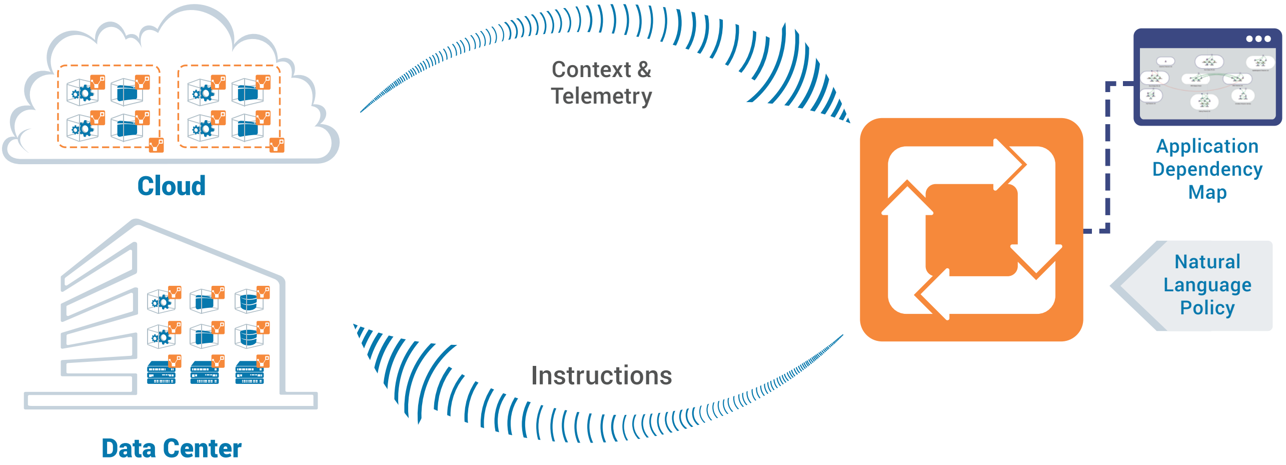


Figure 2: Illumio ASP securing an ordering application deployed across a hybrid environment with complete visibility of traffic flows.

RELATED ASSETS

For additional information on securing hybrid infrastructures, visit www.illumio.com/use-case-overview. You can also download white papers on this and other topics at www.illumio.com/resources.

The Illumio ASP architecture consists of lightweight Virtual Enforcement Nodes (VENs) installed on workloads residing in any data center or cloud. The VENs act as antennas and send telemetry information about the workloads to a Policy Compute Engine (PCE) that acts as the central brain of the platform. The PCE builds a graph of all dependencies between workloads and their applications and computes precise security policies that are instrumented into the native security capabilities (iptables or Windows Filtering Platform) in every workload. Anytime applications or environments change, Illumio ASP automatically adapts by recomputing and updating the policies.



Virtual Enforcement Node (VEN)
Like an antenna

Policy Compute Engine (PCE)
The central brain

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 environmental separation, 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