illumio

WHITE PAPER

IT ENVIRONMENT SEPARATION

CONTENTS

OVERVIEW

BUSINESS DRIVERS

Separating the operating environment to prevent cross contamination for applications is a best practice in the systems development life cycle. By doing so, enterprises can prevent software from being used in production before it is ready. Poor separation of operating environments can lead to problems like the recent data breach at HealthCare.gov caused by an incorrectly configured development server.

By isolating application environments, IT/DevOps teams can help to avoid outages, errors, and compliance violationsthat can negatively impact a business's revenue or reputation, and cause financial penalties.

Environment separation is commonly used to address business scenarios like:

- Preventing unwanted customer access to business-critical servers
- User acceptance testing of applications before deployment
- Isolation of applications through the life-cycle stages
- Performing compliance audits
- Isolating security vulnerabilities

CURRENT CHALLENGES WITH IT ENVIRONMENT SEPARATION

- Manual errors in identifying workloads with their environments can cause unauthorized access to critical resources.
- Reconfigurations of network infrastructure are required to move applications across environments as part of the application development lifecycle.
- Migrating to public clouds is difficult due to the reliance on network infrastructure to isolate environments.

THE ILLUMIO SOLUTION

- Security policies are based on application context instead of network parameters like IP addresses.
- Security and IT ops teams can isolate application environments with precise security policies, independent of the underlying infrastructure.
- Environment isolation is adaptable to application or infrastructure changes, empowering IT and DevOps teams to be responsive.
- Automated, fine-grained security enforced at the level of individual workloads follows workloads when movements or changes occur preventing inadvertent or malicious access to incorrect applications.
- Continuous computation of security based on real-time application context ensures accurate policy enforcement, while accounting for application migrations through the development life cycle.
- Visualization of application workloads and their interactions lets enterprises detect suspicious activities in business-critical environments.

CURRENT APPROACHES TO ENVIRONMENTAL SEPARATION

Organizations that have at least one data center and an application deployment life cycle test applications prior to deploying them into their production environment. Enterprises that develop their own applications usually employ the classic four-stage development-to-production process.

Enterprises typically use one of the following approaches to isolate application environments:

PHYSICAL NETWORK ISOLATION

Organizations implement physical isolation between different environments with a separate pod within the data center. The primary advantage of this physical separation is clear: it provides a high degree of isolation. A choke-point firewall separates environments from each other, and separates each environment from the outside world. In many cases, the network interconnecting the workloads is very simple, since there is no need to isolate traffic and applications. Test and development environments are often the "Wild West," and simply separating them from staging and production provides reasonable assurance of isolation. Some organizations use public cloud platforms for their test and development environments and their private data center for their staging and production environments.

LAYER-2 NETWORK SEGMENTATION

Originally designed to isolate and maintain broadcast domains, VLANs provide a layer-2 segmentation model and have been adapted to isolate environments within a data center. Intermediate network switches must be configured to extend VLANs to virtualized servers that have workloads from different environments or to dedicated interfaces on bare-metal servers. VLANs are frequently mapped into security zones, and traffic passing between zones must pass through a firewall. The firewall enforces the segmentation rules between the environments.

Layer-2 segmentation provides good use of resources since traffic between all environments is multiplexed over the same network infrastructure. It works well in environments that are static, with limited workload movement between environments, low scalability needs (i.e., auto scale policies), and limited need to span across VLANs or security zones.

SOFTWARE-DEFINED NETWORKING (SDN)

In order to get the benefits of network multiplexing, but at the same time get the network out of the way, SDN creates tunnels that overcome the limitations of creating and stringing VLANs. For example, layer-2 networks are dynamically created using layer-3 tunneling. This effectively builds another layer-2 domain using layer-3 tunnels.

FIVE CHALLENGES WITH EXISTING SOLUTIONS

1. VLANs: Limited flexibility due static networking

If workload capacity or communication needs exceed a VLAN's reach, the network gets in the way. The time it takes to provision a new VLAN, extend that VLAN to a security zone, or create a new zone, can be hours, but for large enterprises with complex networks, it can be days or weeks. In addition, there may be new firewall rules needed for the new VLAN or zone. This means that while spinning up new workloads only takes minutes, the changes to the network are what slows down the process.

2. Firewall rule explosion and out-of-sync security policies

Depending on the amount of motion, scale, and change there is in a data center, layer-2 segmentation can lead to "Swiss cheese" firewalls. Manually maintaining large firewall rule bases and making frequent data center changes leads to out-of-date rules. But, organizations are remiss to reconcile defunct rules out of fear of breaking existing applications. Since firewalls lack the context of workloads behind the perimeter, they organically grow out of sync with the rest of the network.

3. SDN: Complexity and scalability issues and vendor lock-in

It has been difficult to scale SDN solutions, and they are not commonly found in large production environments. While it does reduce the reliance on VLANs for provisioning, SDN also has its pitfalls. For example, it makes troubleshooting tricky since it relies on an underlying L2/L3 fabric that is working correctly. If anything goes wrong, each layer of the stack needs to be validated. In addition, because any motion or change in the infrastructure can create (or tear down) tunnels, a tremendous amount of state information must be maintained. Additionally, many SDN solutions are tied to a vendor's specific hardware appliance or hypervisors and require investment over existing infrastructure.

4. VLANs and SDN are not extensible to public clouds

Layer-2 segmentation limits an enterprise's ability to move to the public cloud since the cloud provider has control over all of the switches and their associated VLANs. Similar to layer-2 segmentation, SDN requires the enterprise to have control over the virtual switches in a network. This works well when an enterprise controls all of the switches and hypervisors in a data center, but it is not open to an enterprise once it moves to public cloud or virtual private cloud. SDN also relies on intermediate gateways to tie in bare-metal servers, has limited to no visibility into the network infrastructure, and does not offer a way to span across public cloud providers.

5. Lack of workload context

All of the current solutions rely on the network to perform segmentation, and on orchestration to put the right workload into the right environment. If orchestration erroneously takes a workload in development or QA and places it into the production environment, it is almost impossible for a choke-point firewall that controls access between VLANs or security zones to understand what is happening on that individual workload. The firewall does not know the workload's state, what is running on it, its operating system, or any changes that have happened since it was placed in the wrong environment.

Some current solutions are tied to specific hypervisors and integrate only with vendor-specific orchestration tools. They claim to gain context by reading labels within the orchestration tool. However these approaches have disadvantages:

- They rely on users to label workloads within the automation tool, which can be error prone since the label generation is disconnected from the actual workload.
- They cannot account for changes in the workload.
- They still rely on traffic from that workload to be brought to an enforcement point.

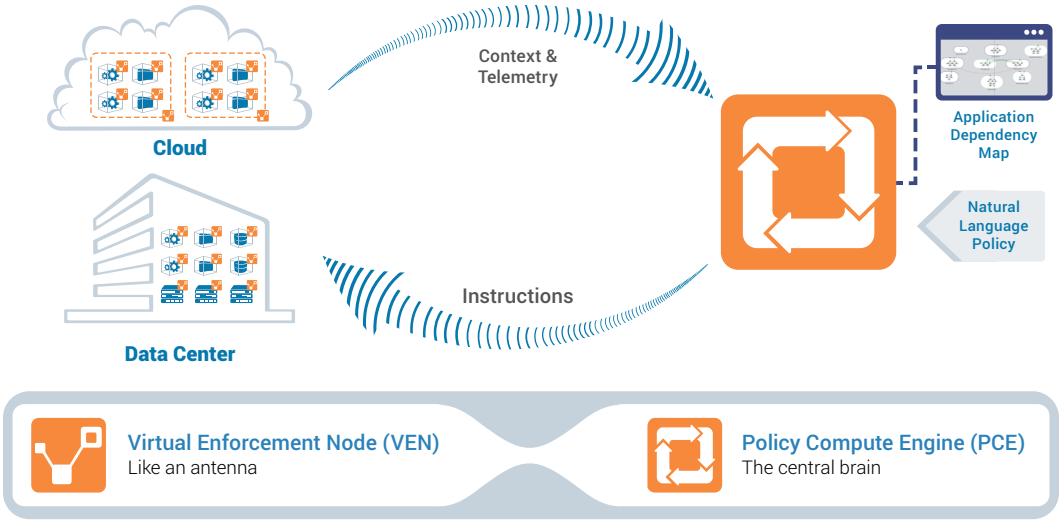
So, the existing network policy remains in place and the misplaced workload could still access anything, or be accessed.

THE ILLUMIO SOLUTION

Illumio Adaptive Security Platform (ASP)™ secures enterprise applications in data centers and private, public, or hybrid cloud environments by decoupling security from the underlying infrastructure. The platform continuously computes security for enterprise applications by using the dynamic context of individual workloads running on virtual machines or physical servers.

The **Illumination** service provides visualization of applications and workload interactions with a graphical view of application topology to help inform security and policy decisions.

The **Policy Compute Engine (PCE)** is a centralized controller than manages all of the state and policies of the computing environment it visualizes and protects. It examines the relationships among workloads, computes the rules required to protect each workload, and distributes those rules out to the **Virtual Enforcement Nodes (VENs)** on the workloads.



Fine-grained security at the most accurate enforcement point

Illumio ASP takes the enforcement of environmental separation down to every workload, which avoids reliance on physical or logical environmental separation. Since security (and separation) is attached to each workload, if a workload is placed into the wrong environment, Illumio ASP will enforce rules based on the workload, not on the network or labels from an orchestration tool. If legacy separation techniques are in place, Illumio ASP can still work alongside those techniques with the full benefits of adaptive security.

Infrastructure-agnostic isolation and security

Since Illumio ASP provides enforcement at the individual workload, rather than using the network, organizations can have environmental separation inside of their existing data center, a public cloud environment, or a hybrid deployment. Illumio ASP works across bare-metal servers as well as hypervisors since a VEN attached to each workload resides in the guest OS. Enterprises do not need to rearchitect or change their existing segregation technology—they can simply integrate Illumio ASP and then allow existing separation technology to provide connectivity and forwarding fabric.

Context-aware security enforcement

Illumio ASP is fully context aware. It understands the context and relationships of each workload, which ensures that the centralized PCE gets accurate security policies every time. The flexible, multi-dimensional labeling mechanism lets organizations define a workload, based on its role (database, web server, mail server, etc.), the application that it serves (Payroll, Sales, etc.), the environment it runs in (dev, test, production, etc.), and its location (US, Atlanta, Rack #3, etc.). This approach allows administrators to define security based on a framework to express the relationships between workloads in the form of human-readable, explicitly allowed policies. The Illumio PCE maps the labels and configured rules to dynamically compute the graph of relationships between workloads. The policies defined based on context are resilient to changes since the workload automatically inherits the correct policies when it migrates across environments as part of the application development life cycle.

Application visualization and policy validation

The Illumination service reveals granular details of application flows between specific workloads, allowing the discovery of interactions across applications and between the tiers within applications. The application-specific flow visualization is also correlated to configured rules. This allows operators to validate and test the security policies against existing (legitimate) flows before they are enforced on the workloads. Flows that do not match the configured rules are flagged, enabling operators to detect any suspicious activities from misplaced and/or compromised workloads in business-critical environments.

USE CASE: ACHIEVING ENVIRONMENTAL SEPARATION WITH ILLUMIO

To better understand how to use Illumio's adaptive security policies to enforce isolation between two internal environments, consider a two-tier Online-Store application consisting of a web tier and a database tier. The application is being used in two environments:

- Production: The current in-service environment, used for running the Online-Store application.
- Staging: A functional duplicate of the Production environment, to test a next-generation version of the Online-Store application.

The Online-Store application requires the following permitted application flows:

- Apache service provided by the web tier of the Production Online-Store application is open to everyone.
- Apache service provided by the web tier of the Staging Online-Store application is open to a select set of IPs in the company headquarters.
- MySQL services provided by the database servers are accessible from their respective web tiers in both Staging and Production environments.

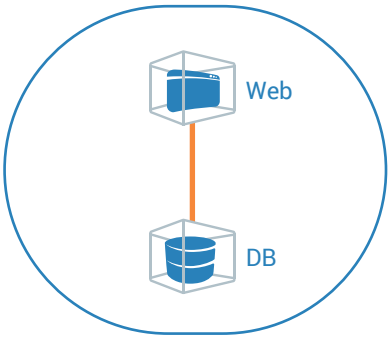
The objective is to ensure that any workload running in the Staging environment is not allowed to communicate with workloads in the Production environment.

CONSTRUCTING SECURITY POLICIES

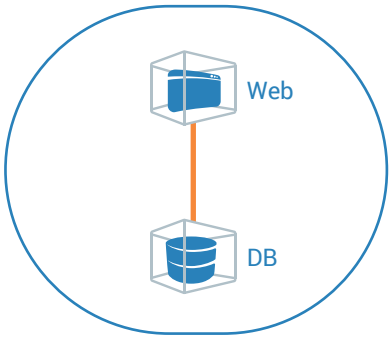
LABELS AND WORKLOAD IDENTIFICATION

Illumio ASP allows administrators to create a library of labels that are unique to their environment. These labels are used to describe the role, application, environment, and location for every workload.

The Online-Store workloads running in Production and Staging environments are labeled as follows:



Online-Store : Staging : US



Online-Store : Production : US

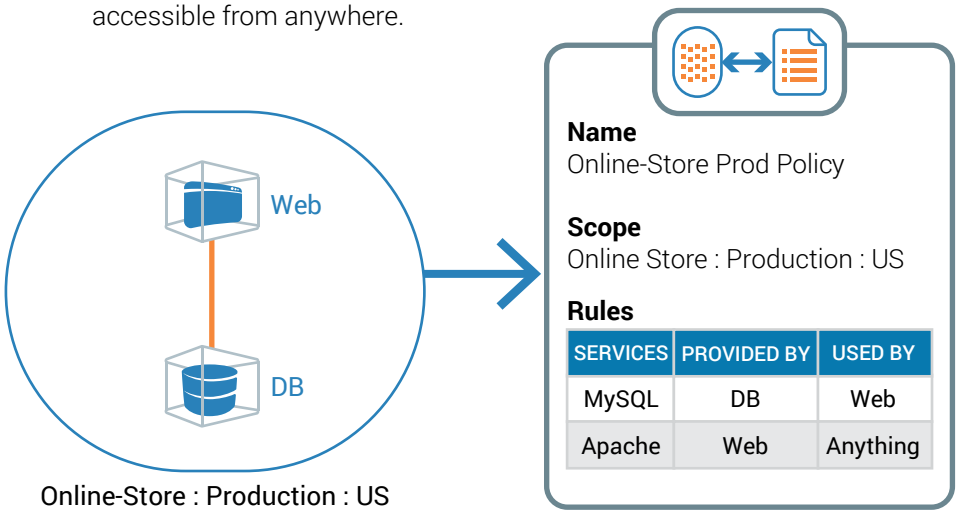
	ROLE	APPLICATION	ENVIRONMENT	LOCATION
Online-Store : Production				
Web workloads	Web	Online-Store	Production	US
Database workloads	DB	Online-Store	Production	US
Online-Store : Staging				
Web workloads	Web	Online-Store	Staging	US
Database workloads	DB	Online-Store	Staging	US

The workloads of the Production and Staging applications are distinguished based on the values assigned to the environment label.

WRITING SECURITY POLICIES BASED ON LABELS

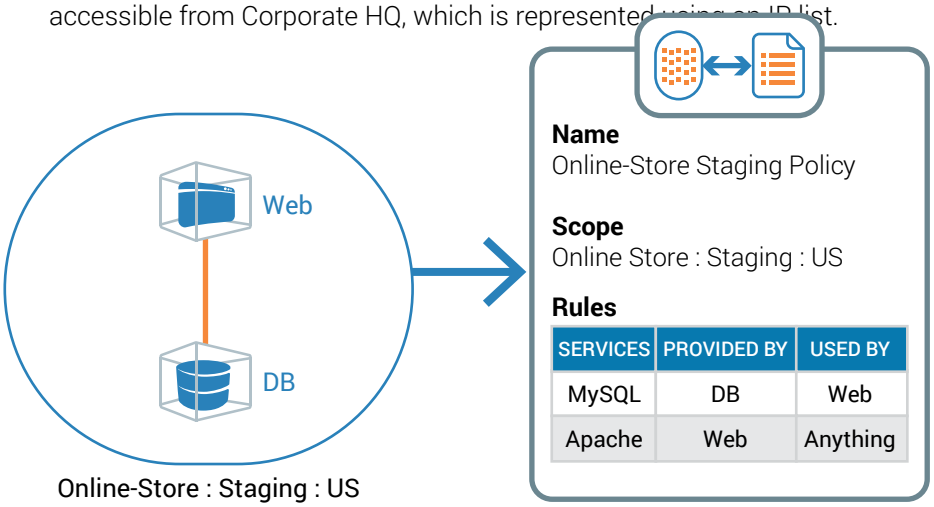
Once the workloads have been labeled, security policies can be written to capture the explicitly allowed interactions (whitelisted policies) between the workloads. Interactions that are not expressed as security policies are simply denied. The figure below shows the rulesets that describe the relationships between the workloads of the Online-Store application running in the production environment.

- **RULE 1:** The MySQL service running on the database servers will only be accessible from the web servers.
- **RULE 2:** Only the Apache service running on the web servers will be accessible from anywhere.



The figure below shows the rulesets that describe the relationships between the workloads of the Online-Store application running in the Staging environment.

- **RULE 1:** The MySQL service running on the database servers will only be accessible from the web servers.
- **RULE 2:** Only the Apache service running on the web servers will be accessible from Corporate HQ, which is represented using an IP list.



The rules assigned to the Staging environment differ from the Production environments in terms of the extent of access granted to the web tier.

THE SCOPE OF SECURITY POLICIES

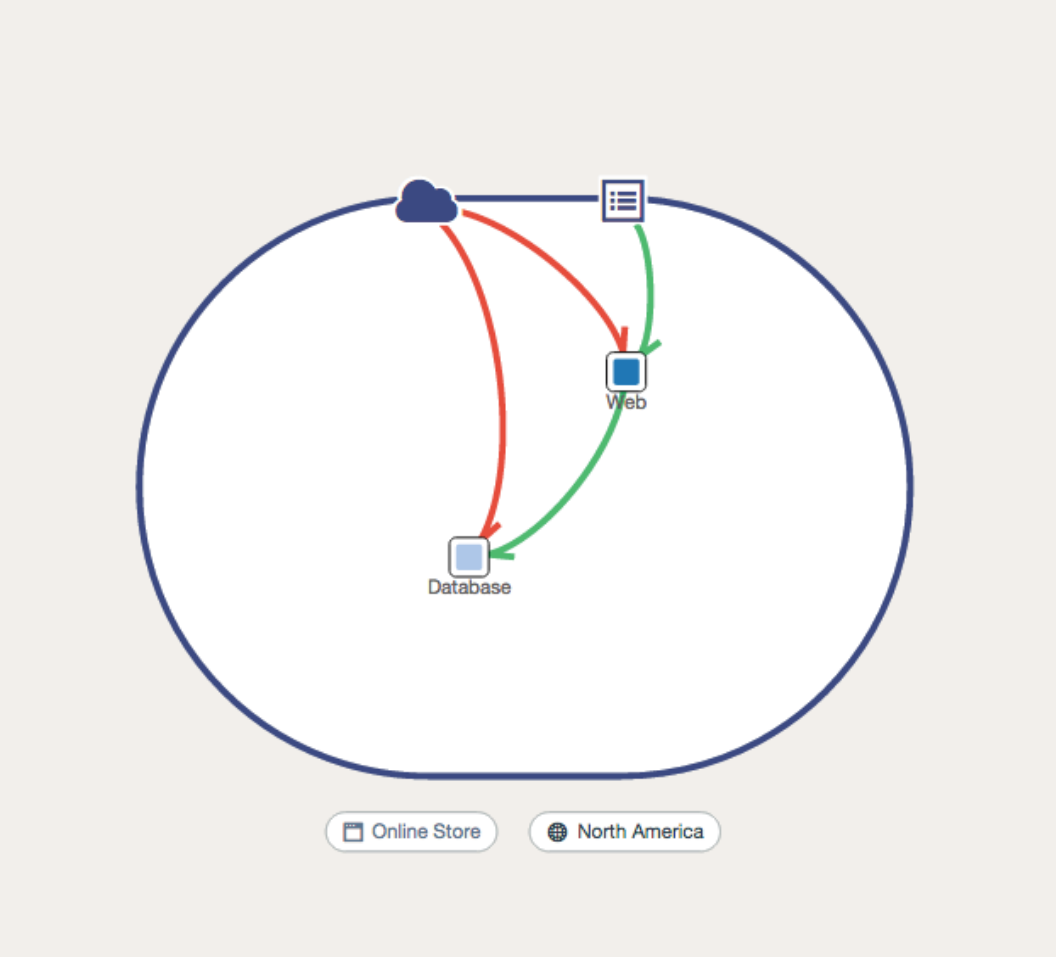
The scope identifies the set of workloads on which the security rules are applied. In the above example, the rules are applied across the workloads of the Online-Store application based on their environment. Since there are no security policies configured to explicitly permit traffic flows between Production and Staging environments, the Online-Store workloads of these environments cannot communicate with each other.

When the Staging application is ready to be rolled out into Production, the assigned security policy is easily portable to the production environment. Besides opening up access of the web tier to everyone, the only required policy-related change is switching the environment label from Staging to Production.

VISUALIZING APPLICATION FLOWS WITH ILLUMINATION

Illumination can be used to visualize the application flows specific to the Production and Staging environments of the Online-Store application. The traffic flows can be used to verify the enforced security policies. For example, in the case of the Online-Store application in the Staging environment traffic flows should show that:

- Online-Store DB allows access to MySQL for the web workloads.
- Apache service on the web workloads is accessible from a list of IP addresses representing the company headquarters. Any traffic flows that do not match the configured rules should show up "red" indicating that these are blocked.



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