illumio

WHITE PAPER

NANO-SEGMENTATION

CONTENTS

OVERVIEW

BUSINESS DRIVERS

As applications have become increasingly critical to business success, enterprises are building network-centric security constructs to protect them. These constructs include VLANs, firewalls, firewall zones, and pseudo layer-2 constructs like software-defined networking (SDN). The goal of all of these approaches is to prevent bad actors from having access to sensitive resources by isolating business-critical applications, or their functional tiers, from one another.

Segmenting applications and the workloads that comprise them improves an enterprise's defense posture and reduces the surface area of a potential attack by restricting workloads to permitted communication paths and isolating applications from each other. Because data breaches and attacks have become more common, businesses are looking at segmentation to improve security and control.

CURRENT CHALLENGES WITH APPLICATION SEGMENTATION

- Segmentation using the network prevents organizations from moving to the cloud.
- Adding layer-2 networking adds many manual steps, making it the slowest part of deploying a new application.
- Layer-2 segmentation increases network complexity, which begets configuration errors that can compromise security posture or application availability.
- The ideal state of segmentation is to have enforcement at each workload, but this would require a VLAN per workload instance, which is both difficult and impractical.
- Lack of validation and visualization tools makes it difficult to enforce fine-grained security policies.

THE ILLUMIO SOLUTION

- Delivers fine-grained security enforcement at the level of individual workloads or processes, enabling segmentation at the most granular level.orm.
- Segmentation automatically adapts to data center moves, additions, and changes since security is attached to workloads from their inception until decommission.
- Security is continuously computed and applied using the dynamic context information collected from all managed workloads. Policies do not need to be manually adjusted as underlying networking parameters change (e.g., when migrating to public cloud).
- Security is completely decoupled from any VM, physical server, or network for both the specification of security policies and their enforcement.

- Works on top of an enterprise's existing segmentation or isolation strategies.
- Visualization of application dependencies lets organizations build security policies and test them against existing flows before enforcing any rules.

CURRENT APPROACHES TO SEGMENTATION

IP ADDRESS RULES

The simplest form of segmentation has been to lump all workloads and applications into a single broadcast domain, and to perform enforcement using IP address rules. This coarse enforcement is generally between the outside world and the data center, but few organizations actually have a simple security strategy.

IP address rules are simple, but they do not provide segmentation. Without some form of application-specific segmentation, core applications are exposed. As threats have evolved, companies have started using segmentation to guard against threats spreading laterally through a data center from compromised workloads. Most organizations have multiple levels of control. For instance, their web servers are separated from application processing tiers using VLANs and firewall zones; and databases are similarly separated from processing tiers and the web tiers.

VLANS

VLANs were originally designed to create logical broadcast domains. But since firewalls—which provided enforcement at layer 3—were very expensive, organizations began extending layer-2 broadcast domains up to an interface on a firewall, providing IP-level security.

As applications have become more complex, enterprises have segmented their data centers using a combination of VLANs and firewalls. In fact, some organizations actually have more VLANs than physical servers in their data centers. As organizations continue down this path, maintaining a map of layer-2 domains becomes difficult—and can actually overrun the limit of 802.1Q VLAN tags.

FIREWALL ZONES

Firewall zones were introduced to simplify the writing of rules for communication between groups of workloads. Zones enabled security administrators to group workloads into a logical zone. For instance, administrators could group all of their databases in one zone and their web workloads in another zone.

Rules would then be written to allow interactions between zones. In the example above, zone-1 workloads (web) are allowed to talk to zone-2 workloads (databases). While they do simplify rule writing, firewall zones are still tied to the physical (or logical) network, so they do not overcome the limitations of VLANs.

SOFTWARE-DEFINED NETWORKING

SDN was originally designed to create logical networks inside of a service provider's infrastructure. Rather than requiring the physical provisioning of separate infrastructure for different data center tenants, SDN enables service providers to provision logical networks that overlay the physical network.

SDN technology has migrated its way into enterprise networks as a way of segmenting applications and workloads in the data center. While SDN does create a level of abstraction that can enable segmentation, it has not seen any widespread adoption by enterprises for this purpose.

FIVE CHALLENGES WITH EXISTING SOLUTIONS

Current segmentation strategies require time to provision and configure, which slows down the deployment and scale of applications. In addition, each new level of segmentation increases the level of complexity since it requires network reconfiguration. Segmentation requires a deep understanding of the overall layout and configuration of the network. This may be easy in a smaller network, but keeping track of subnets, zones, VLANs, and the state of all workloads at scale is almost impossible.

1. Current segmentation technologies are tied to the network

Provisioning new layer-2 domains takes time since it requires manual configuration. In today's data centers, workloads and applications can spin up in minutes, but provisioning new layer-2 domains takes a disproportionate period of time. This slows down the deployment and scale of applications.

2. Security architecture and policies are not uniform

Organizations looking to put their workloads into public clouds find themselves unable to protect layer-2 domains, since cloud providers control the infrastructure. Cloud service providers have created virtual private clouds that attempt to match the idea of a layer-2 domain, however companies are forced to manage security policies in their own data center differently than with the cloud provider. This lack of uniformity between the data center and public cloud provider also increases the probability of misconfiguration.

3. Layer-2 domains don't know what's changing

As workloads spin up and down, the layer-2 domain providing segmentation has no understanding of those changes. Because the segmented layer-2 domains lead to firewalls that control the interactions of traffic going into and out of the domain, many organizations have "stale" firewall rules—or policy debt—that become a security vulnerability.

4. The lack of integrated verification tools

Application segmentation is a great approach to reducing the attack surface area and limiting damage from security breaches. But a conceptual approach alone is not enough. Without understanding the interactions between the workloads, applying fine-grained controls using segmentation can block legitimate application flows. Integrated tools to correlate, visualize, and adjust security-related changes to business application flows across multiple end points don't exist. This makes it difficult to implement a segmentation strategy where every workload is only accessing resources that are necessary for its legitimate purpose.

5. Coarse segmentation isn't adequate

Because segmentation approaches involve constructs that are based on the network, administrators commonly lump multiple workloads of the same type into the same VLAN, zone, or subnet. This simplifies rule writing since an administrator can "separate" application tiers (e.g., separate web workloads from data base workloads). But, trying to drive fine-grained segmentation by application and workload role requires more VLANs and enforcement rules. Moreover, without segmentation at the level of individual workloads, bad actors can still spread attacks laterally within an application.

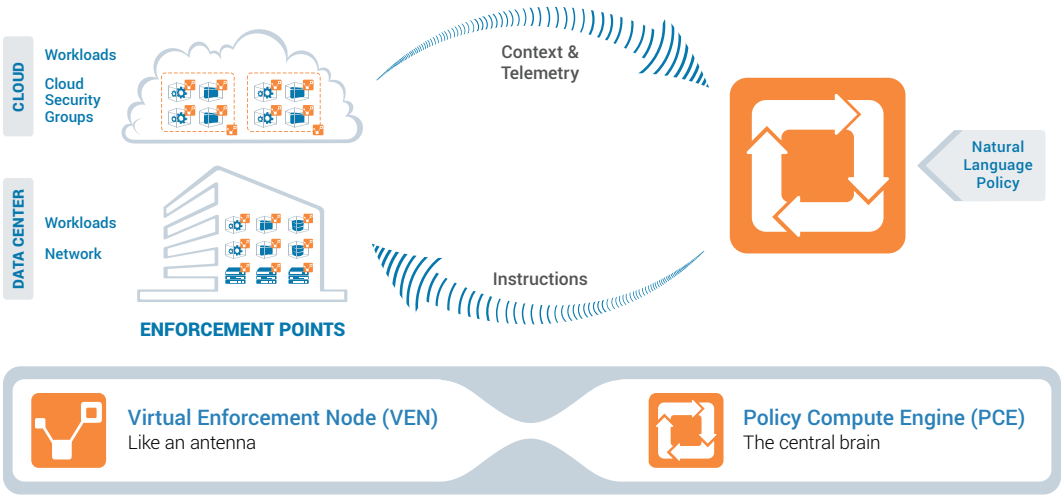
THE ILLUMIO SOLUTION

The **Illumio Adaptive Security Platform (ASP)™** includes nano-segmentation, the most granular segmentation of data center and cloud applications in the industry. Nano-segmentation makes it possible to segment multiple applications down to processes on a single host. By enforcing relationships between workloads, applications can be segmented without relying on the network.

Illumio ASP delivers enforcement at the workload via the **Virtual Enforcement Node (VEN)**. The VEN is not in the data path; it resides within the workload operating system, and enforces policy using the instruments that are in the operating system (i.e., iptables for Linux operating systems and Windows Filtering Platform [WFP] for Windows servers).

Policies are computed using the centralized **Policy Compute Engine (PCE)**, which receives context information about workloads as telemetry from the VENs. The PCE uses the "relationships" between different workloads to determine what security policies should be put into iptables or WFP.

Because security policies are not based on network parameters, there is no reliance on the network for security. Any existing VLANs, physical separation, or segmentation can remain in place—there is no network change required. However, once Illumio ASP is implemented, organizations no longer need to rely on those constructs; they can remain in use or be removed. Illumio ASP gives them the agility to move workloads without worrying about the underlying network architecture.

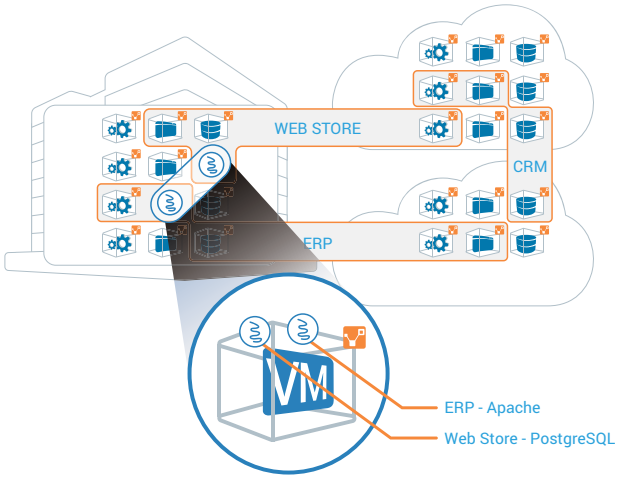


ADAPTIVE, FINE-GRAINED SECURITY ENABLES NANO-SEGMENTATION

Illumio ASP dynamically computes security based on the context of workloads. A flexible, multi-dimensional labeling mechanism is used to define a workload based on its role (database, web server, mail server, etc.), the application it serves (Payroll, Sales, etc.), the environment in which it runs (dev, test, production, etc.), and its location (US, Atlanta, Rack #3, etc.). All dimensions can have an infinite depth; as more labels are needed within a dimension, they can simply be added.

The Illumio PCE maps the labels and configured rules to dynamically compute workload-specific rules using the telemetry provided by the individual VENs. The human-readable syntax for policy specification allows security policies to adapt to changes to applications or the underlying network infrastructure. Once the rules are pushed to individual VENs, the only traffic that is allowed is the traffic that is permitted by the ruleset creating a container around each application.

This effectively createsnnano-segmentation. Illumio enables the segmentation of multiple applications down to processes on a single host. As an example, two instances of the Apache process on a single workload could be segmented across two different applications.



INFRASTRUCTURE INDEPENDENT

Many organizations are splitting their applications between public cloud and their existing data centers. For instance, consumer packaged goods companies often host the web tier of a marketing application in a public cloud to ensure ample bandwidth while keeping other tiers in their private data center. Traditional segmentation approaches fail in this architecture since the enterprise has no way to create a layer-2 segment in the public cloud.

The Illumio PCE creates rules using the context and relationships of application workloads irrespective of where the workloads reside. This is because enforcement rules are instrumented directly on the workload with rules written into iptables or WFP.

VALIDATING SECURITY BEFORE ENFORCING IT

Since Illumio ASP has complete visibility to workloads and their context, it can dynamically compute the graph of relationships between the workloads. This interactive graph is displayed by the Illumination service and provides powerful insight into workloads and all of their communications. Using Illumination, any policy changes can be evaluated against existing application flows before they are enforced.

Illumination effectively improves the accuracy and speed of deployments since it enables simulation of security policies without breaking the desired application behavior and communication patterns. This enables the implementation of fine-grain controls where every workload is only accessing resources that are necessary for its legitimate purpose.

NO NETWORK CHANGES

Many segmentation approaches require administrators to change the underlying network. For instance, some approaches require additional VLANs, or the administration of overlay networks. Since Illumio ASP does not operate at layer 2, it obviates the need to make any network changes.

USE CASE: ACHIEVING NANO-SEGMENTATION WITH ILLUMIO ASP

To better understand how to implement nano-segmentation using Illumio ASP, consider a three-tier Order Processing application:

- The web tier services business partners over Apache.
- The web tier uses Tomcat to interact with the processing tier.
- The processing tier accesses the database tier using the MySQL service.

Here is how Illumio ASP can secure these instances with a single ruleset, without requiring the installation of any additional security appliances or modifying the network infrastructure.

USING LABELS IN SECURITY POLICIES

Illumio ASP allows administrators to create a library of labels that are unique to their environment. These labels are then used to describe the role, application, environment, and location for every workload, and can be automatically assigned as part of pairing the workload (i.e., bringing it under management) using Pairing Profiles.

Below are the labels assigned to the workloads of the Order Processing application.

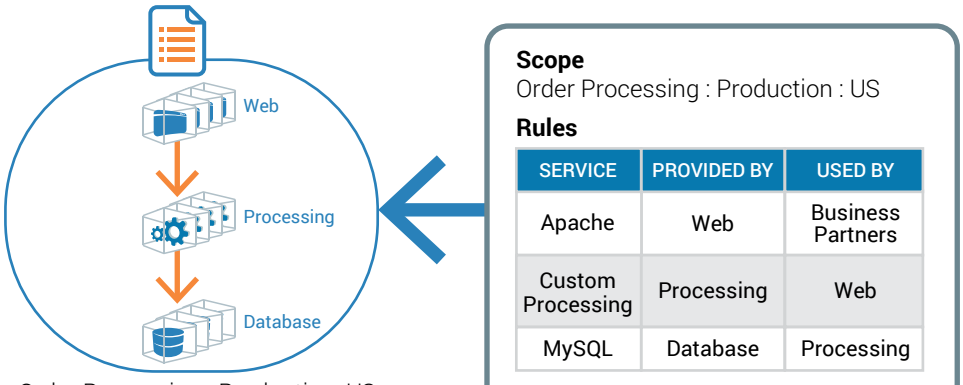
	ROLE	APPLICATION	ENVIRONMENT	LOCATION
Web workloads	Web	Order Processing	Production	US
Processing workloads	Processing	Order Processing	Production	US
Database workloads	Database	Order Processing	Production	US

WRITING SECURITY POLICIES BASED ON LABELS

Users do not need any knowledge of layer-2 or layer-3 topology to write a rule for the Order Processing application with Illumio ASP. Instead, they simply describe the relationships and rely on the PCE to calculate the optimal security topology and send it down to individual workloads.

The figure below shows the ruleset that describes the relationships between the workloads of the Order Processing application running in the production environment across all locations.

- **RULE 1:** Apache service running on the web workloads will be accessible by a set of business partners (represented by an IP list).
- **RULE 2:** The Custom Processing service running on the processing workloads will be accessible from the web workloads.
- **RULE 3:** The MySQL service running on the database workloads will only be accessible from the processing workloads.



Order Processing : Production: US

THE SCOPE OF SECURITY POLICIES

The scope identifies the set of workloads to which the security rules apply. In the above example, the rules will apply to the Order Processing application in the Production environment in all locations where the application runs. Consistent and accurate security is enforced regardless of the number of workloads instantiated as part of the application. If any of the workloads are migrated or decommissioned, these changes are automatically detected by the PCE. Related security policies will be adjusted instantly without any manual reconfigurations.

ABOUT ILLUMIO

Illumio, recently named to the CNBC Disruptor 50 list, stops cyber threats by controlling the lateral movement of unauthorized communications through its breakthrough adaptive segmentation technology. The company's Adaptive Security Platform™ visualizes application traffic and delivers continuous, scalable, and dynamic policy and enforcement to every bare-metal server, VM, container, and VDI within data centers and public clouds. Using Illumio, enterprises such as Morgan Stanley, Plantronics, Salesforce, King Entertainment, NetSuite, Oak Hill Advisors, and Creative Artists Agency have achieved secure application and cloud migration, environmental segmentation, compliance and high-value application protection from breaches and threats with no changes to applications or infrastructure. For more information, visit www.illumio.com or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Join Illumio on G+
- 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.