illumio

WHITE PAPER

AUTOMATING SECURITY WITH DEVOPS

CONTENTS

OVERVIEW

Business drivers

Businesses are innovating fast and want their IT organizations to meet their needs—without trading off security. DevOps practices are driving IT operations at many enterprises to improve cross-functional collaboration, release times, and quality. While DevOps brings together IT infrastructure and application development teams, security discussions are still being held back by static policies and lack of tools or APIs that might help automate security management. DevOps is perceived as a practice focused on streamlining IT and accelerating business, while security is often seen as a roadblock.

The impetus to automate security through DevOps is compelling:

- Security is no longer the bottleneck.
- Balancing security with business goals in a continuous software delivery model enables strategic alignment to the business.
- Standardizing security configurations enables secure and quick application deployments.
- Automating security and auditing development environments minimizes errors by identifying and isolating risky changes before they are implemented in production.
- The morale of infrastructure and operations teams improves as they no longer have their backs to the wall trying to respond to application rollouts.

Current challenges with automating security using DevOps practices

- Security policies are dependent on static network parameters. This leads to inflexible security architectures that cannot adapt to infrastructure or application changes.
- Hundreds of firewall rules have to be reconciled—in many cases manually—when changes occur or new applications are introduced.
- Current solutions lack APIs to automate security management through integration with DevOps tools.
- Lack of validation and visualization tools to verify configuration changes before they are enforced makes it difficult to make well-informed security decisions.

The Illumio solution

- Security policies are built based on application context instead of IP addresses, enabling DevOps teams to define and include security changes early in the application development life cycle.
- Rich set of APIs provides easy integration with third-party orchestration tools such as Puppet and Chef.
- Visual verification of security policies before they are enforced provides a stepping-stone to trust.

- Applications, including newly launched workloads, automatically inherit accurate policies based on their context.
- Application developers are freed from delays caused by security considerations since security does not dependent on the underlying infrastructure.

CURRENT APPROACHES TO AUTOMATING SECURITY

Network-centric security solutions

Enforcing security using network-based appliances relies on bringing traffic from the workloads to the enforcement point where statically configured IP-based firewall policies are applied to application flows crossing security zones. From a networking perspective, there may be specific policies that dictate which VLANs the application workloads need to be placed in. Then, the appropriate security policies are added or modified on a variety of network switches (ACLs) or perimeter security appliances (firewall policies) that are in the traffic flow. This process is repeated for every new application being launched, migrated, or decommissioned as part of the application development life cycle.

Many of these security changes require manual intervention from IT and ops teams, which slows down application rollouts. With workloads increasingly moving from dedicated physical servers to multiple virtual machines, an application can be instantiated anywhere in the data center, and can be migrated to a different data center or a public cloud infrastructure. With no intelligence about the context of the workloads they are protecting, these network-based appliances tend to go out of sync when changes occur "behind" them. Updating and maintaining them requires manual oversight, policy audits, and approvals of responsible teams.

Software-defined networking (SDN)

SDN-based solutions operate by leveraging an overlay network built on top of existing network layer-2 and layer-3 technologies to provide application isolation. These solutions offer RESTful APIs that can be used to integrate with third-party orchestration and automation tools. However with this approach, IT must not only monitor the physical network but also the SDN-based virtual overlays. This makes problems harder to troubleshoot, diagnose, and manage, including root-cause analysis for compliance and forensics. Moreover, SDN-based solutions cannot be extended to a public or hybrid cloud environment, since they require complete control over the entire network infrastructure.

THREE CHALLENGES WITH EXISTING SOLUTIONS

1. Lack of standards-based APIs

DevOps drives speed and efficiency through collaboration between development and operations teams. DevOps teams rely on tools for rapid prototyping of application changes and to automate configurations of workloads. Given the lack of standardized APIs for integration with most firewall platforms, security management is done via scripting, SSH access, and command-line processes. But this is not sustainable, since firewall vendors change commands and their syntax with each new version of their software—making script maintenance and programming policies difficult. Even though firewalls from different vendors serve a similar purpose, there is a general lack of standardization. For instance, security zones are required for some firewalls, but are not used in others. This means creating scripts to manage security may require customizations for each of these solutions.

2. Risk of human error and delays due to manual configurations

Manual configurations to security policies require careful coordination between the application, network, and security teams, which can slow down application deployments. Due to the risk of errors and misconfigurations leading to potential security holes, many businesses have created standard operating procedures for security rule changes, requiring approvals at several levels of the organization. Custom scripts with vendor-specific commands to prepare network infrastructure and account for security changes is cumbersome and error prone. With server virtualization and rapid setup of compute resources, the actual application provisioning can be accomplished in minutes. However, accounting for security of the application extends the process significantly.

3. Lack of integrated verification tools to validate configuration changes

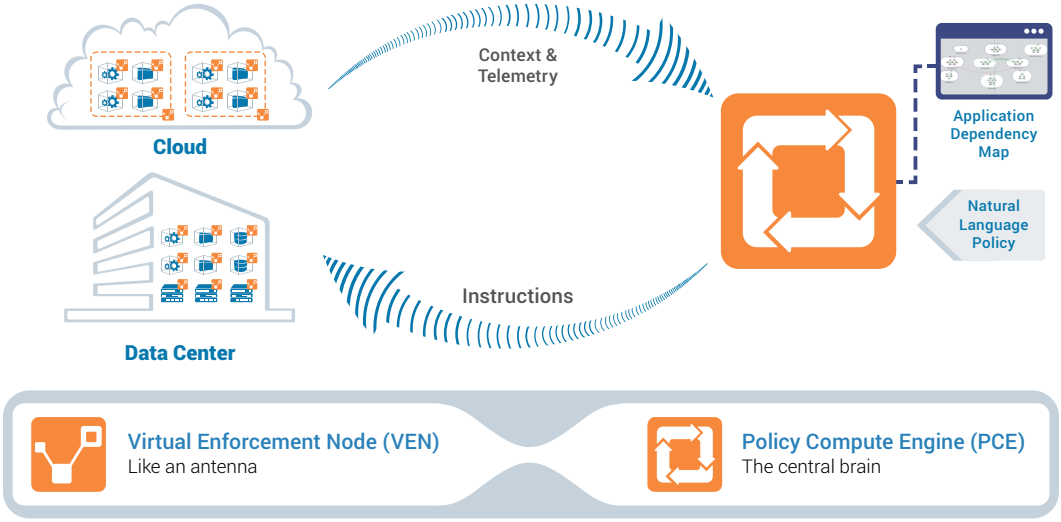
Security administrators tend to be wary of changes orchestrated through security automation tools. Changes must be painstakingly verified before security teams can hand them off and they are committed into production environments. And there are no tools to correlate, visualize and adjust security-related changes to business application flows across multiple end points. This accounts for a big part of the pain felt both by DevOps and security teams—the former wants things done quickly and the latter has the responsibility for security without the tools to help them move fast.

THE ILLUMIO SOLUTION

The **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.



Ease of automation through granular policy association

Illumio ASP creates the most accurate enforcement point by attaching security policies directly to the individual workloads. Security policies can follow the workload life cycle and are automatically attached to workloads from inception to decommission. This simplifies security planning since DevOps teams can be assured that precise security policies automatically apply to newly launched application workloads based on their context. These policies migrate with the workloads wherever they go and are automatically cleaned up as soon as the workloads are decommissioned.

Context-aware security that adapts to application changes

Illumio ASP dynamically computes security based the context of workloads (i.e., their intrinsic properties and relationships to other workloads). Illumio ASP also uses a flexible, multi-dimensional labeling mechanism to define a workload based on its role (e.g., database, web server, mail server, etc.), the application that it serves (e.g., Payroll, Sales,

etc.), the business environment it runs in (e.g., dev, test, production, etc.) and its location (e.g., US, Atlanta, AWS, Azure, etc.). Using dynamic application attributes rather than static network parameters allows DevOps and security teams to define security early in the development cycle. The human-readable syntax for policy specification allows security policies to be resilient to changes to applications or the underlying network infrastructure.

Automation through integration with RESTful APIs

Illumio ASP was designed from the ground up as a simplified, programmable security solution. A full-featured Representational State Transfer (REST) API enables automation of security deployments and easy integration with third-party-automation and DevOps tools like Puppet, Chef, and Ansible.

Validating security using Illumination

The interactive graph displayed by the Illumination capability provides powerful insight into workloads and all of their communications. Illumination displays fine-grained details of traffic flows between specific workloads and the services they provide to each other. The tool allows DevOps teams to verify and troubleshoot application policies before they are actually enforced. Illumination effectively improves accuracy and speed of deployments since it enables simulation of security policies without breaking the desired application behavior and communication patterns. This allows security and DevOps teams to implement security automation confidently.

Decoupling security from infrastructure allows focus on application

By enforcing security on the workload using its context and policies abstracted from the network, Illumio completely decouples security from the underlying network infrastructure. This enables enterprises to secure applications running on bare-metal servers, VMs, and Linux containers across private data centers and public cloud infrastructures including AWS, Rackspace, and Google Compute.

USE CASE: AUTOMATING SECURITY WITH ILLUMIO

To better understand deployments of security policies using the Illumio solution, consider ABC Corp., an enterprise launching a two-tier Online-Store application. ABC Corp. will use Illumio's flexible labels to configure security policies for the application as it goes through the development life cycle, from Dev-Test to Staging and Production. The company also will use Chef recipes to pair workloads and automatically assign preconfigured security policies (and labels) as soon as they are instantiated.

ABC Corp.'s Online-Store application needs the following security policies:

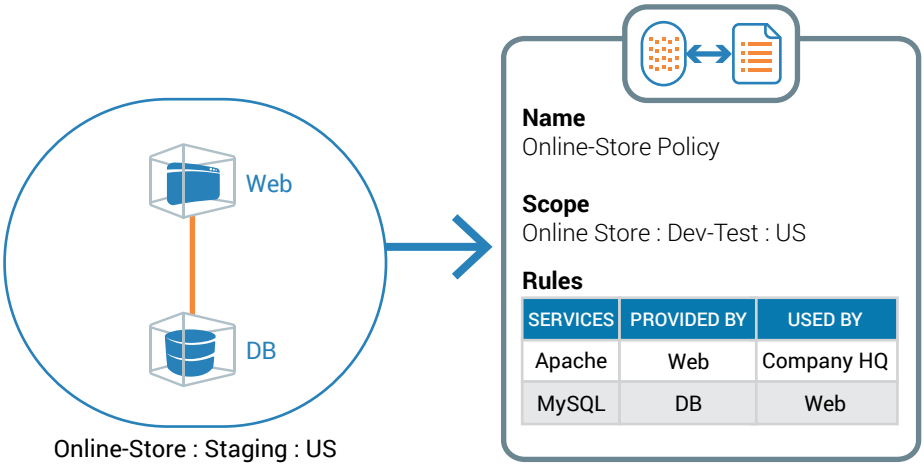
- Apache service hosted on the web tier is open to the Internet. In the Dev-Test and Staging environments, this access will be limited to a select set of IPs.
- MySQL service hosted on the database tier is accessible only from the web tier.

PRE-CONFIGURING SECURITY POLICIES

ABC Corp. will use Illumio policies to capture the explicitly allowed interactions between the workloads of the Online-Store application. These policies can be preconfigured in the system before any workload is even deployed. Alternatively, ABC Corp.'s application teams can configure these policies at an early stage in the app development life cycle (in this example, Dev-Test).

The figure below shows the ruleset that describes the relationships between the workloads of the Online-Store application running in the Dev-Test environment.

- **Rule 1:** Apache service running on the web servers will be accessible from a select set of IPs in the company headquarters.
- **Rule 2:** The MySQL service running on the database servers will only be accessible from the web servers.



THE SCOPE OF SECURITY POLICIES

Scope identifies the set of workloads to which the security rules apply. In the above example, the rules are applied across all the workloads of the Online-Store application running as part of the Dev-Test environment in the United States. If the application also exists in the production environment, these rules would not apply since those workloads would be out of the scope of these rules.

HOW POLICIES ARE INHERITED BY NEWLY INSTANTIATED WORKLOADS

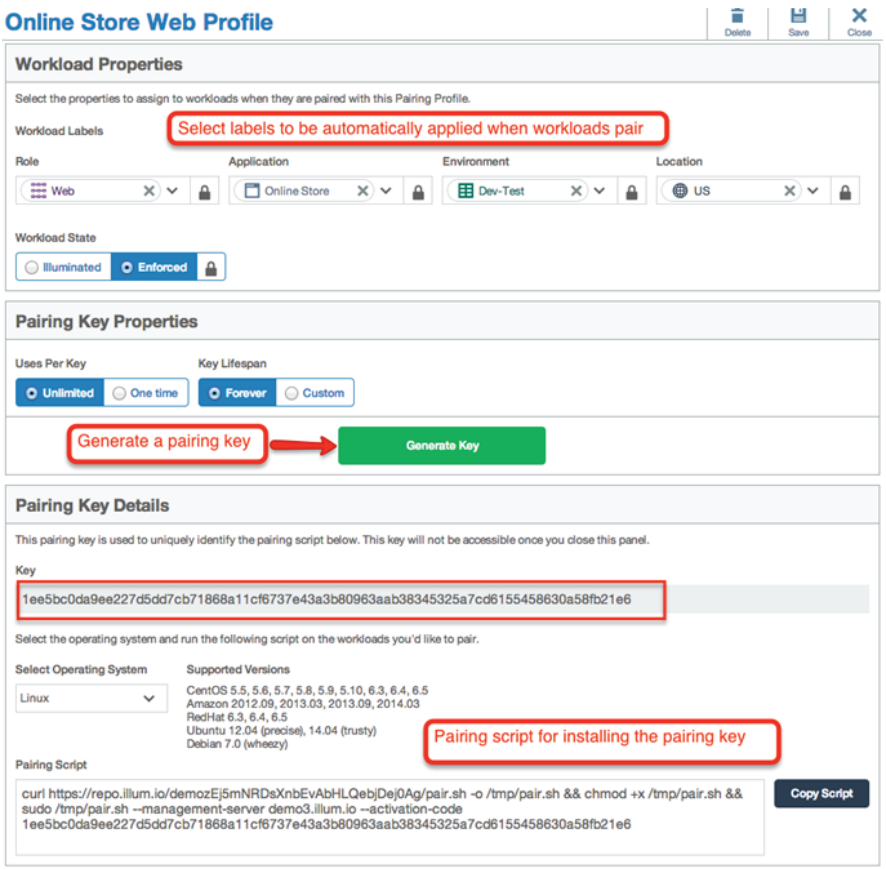
Pairing Profiles are used to replicate workload attributes when the workloads are paired with the PCE. They are used to associate newly instantiated workloads with the correct labels and rulesets.

PRECONFIGURING LABELS USING PAIRING PROFILES

The Pairing Profile is a configuration template that specifies labels that are to be applied to newly instantiated workloads. The Pairing Profile can also be used to generate unique pairing keys that are used by the newly instantiated workloads for identifying themselves to the PCE. When the new workloads are paired, they acquire the labels and the associated security policies within the scope of their labels.

ABC Corp. has defined the following Pairing Profile for the individual tiers of the Online-Store application:

	ROLE	APPLICATION	ENVIRONMENT	LOCATION
Web Profile	Web	Online-Store	Dev-Test	US
Database Profile	DB	Online-Store	Dev-Test	US



INTEGRATING WITH DEVOPS TOOLS FOR SECURING NEWLY INSTANTIATED WORKLOADS

The pairing key generated as part of the Online-Store (web and database) profiles can be baked in to the recipe of DevOps configuration management tools to set up the initial configuration of the newly instantiated workloads.

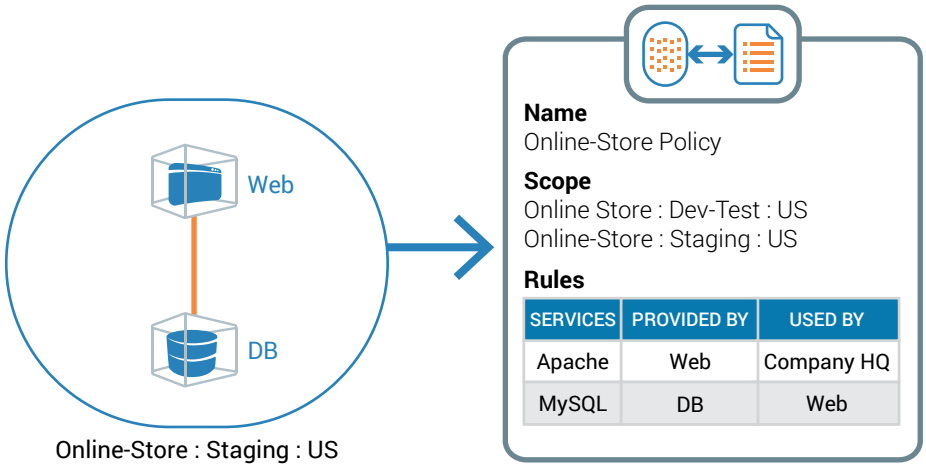
Here is a sample Chef recipe that installs and activates the VEN:

```
#
# Cookbook Name:: pair-node
# Recipe:: default
#
# Copyright 2014, ILLUMIO
#
# All rights reserved - Do Not Redistribute

pair_script = remote_file "#{Chef::Config[:file_cache_path]}/illumio_pair.sh" do
# download from the remote file
  source
"https://#{node["illumio"]["repository"]}/sPl1tOExo0FIEphoewIujIucrLaTOAS3/pair.s
h"
  owner "root"
  mode "0755"
end

# execute the following command
execute "#{Chef::Config[:file_cache_path]}/illumio_pair.sh -m #{node["illumio"][
"management_server"]} -a #{node["illumio"]["activation_code"]} --app
#{node["illumio"]["application_name"]} --env #{node["illumio"]["environment"]} --loc
#{node["illumio"]["location"]} --role #{node["illumio"]["role"]}" do
# check if the node is already paired?
    not_if do FileTest.directory?("/opt/illumio") end
end
```

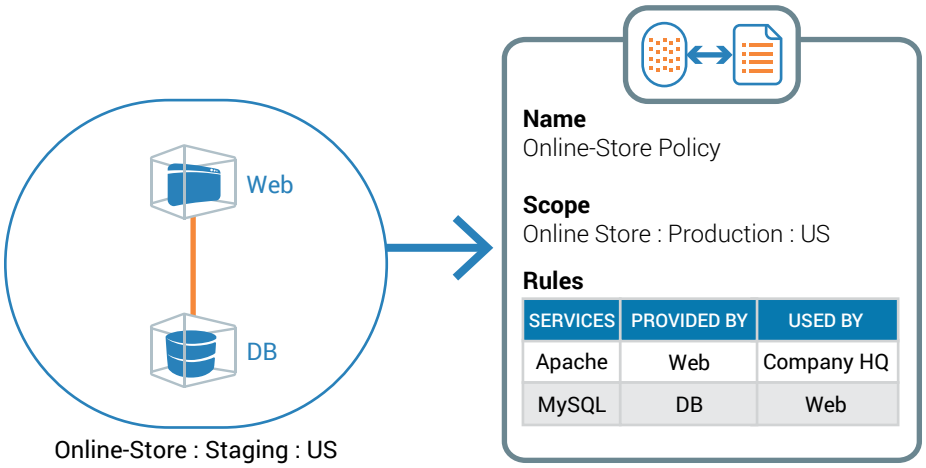
When ABC Corp. is ready to launch the Online-Store application in the Dev-Test environment, the above Chef recipe can be run to secure the workloads as soon as they are instantiated. The pairing key included as part of this script will be used to identify and associate the workloads with the their respective (Online-Store) pairing profile. These workloads instantly inherit the predefined labels (Web or DB / Online Store / Dev-Test / US) as soon as they are brought under management. Any rulesets associated with these labels are instantly propagated to the newly instantiated workloads.

PORTING SECURITY POLICIES THROUGH THE APPLICATION LIFE CYCLE

When ABC Corp. is ready to roll the application into staging, this security policy can be easily reused by adding the details of the new environment to the scope of the ruleset. Any workloads of the Online-Store application that have been newly spawned for the Staging environment will automatically inherit these security rules as soon as they are assigned the appropriate labels.

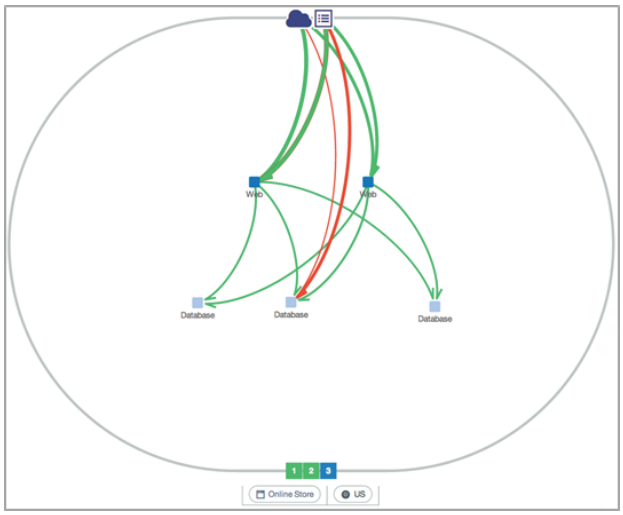


The above ruleset can be easily modified to secure the Online-Store workloads when they are ready to be launched into Production. Besides modifying access to the web tier to allow access from anywhere, the only other policy change would be to switch the context to reflect the new environment label (Production). All the workloads of the Online-Store application that have been newly spawned for the Production environment will automatically inherit these security rules.



POLICY VALIDATION USING ILLUMINATION

Illumination can be used to visualize the application flows between the workloads. For example, in the case of the Online-Store application running in the production environment, traffic flows (indicated by green links) would show that:



- Online-Store DB allows access to MySQL for all the web workloads.
- Apache service on the web workloads is accessible from anywhere.

ABC Corp. can use this graph to validate the policies and ensure that only legitimate traffic flows are allowed to pass through. If ABC Corp. uses the Illumination service to configure its security policies in "test" mode, where traffic flows that do not match the configured rules, it will generate alerts without blocking these flows. In this way, AVC Corp.'s administrators can validate their configuration changes against existing traffic flows before they are enforced.

DevOps represents the coming together of development, operations, security, and quality assurance teams to help improve agility for application rollouts. However to make this a reality, security tools need to interface with automation tools and be adaptable to changes in infrastructure and applications. The adaptive context-aware security enabled by Illumio ASP transforms the way security controls are implemented and automated working with DevOps tools.

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. 160 San Gabriel Drive, Sunnyvale, California 94086 Tel (669) 800-5000 www.illumio.com