

# AUTO SCALING APPLICATIONS SECURELY

## CONTENTS

<b>OVERVIEW</b>	<b>3</b>
Business drivers	3
Current challenges with auto scaling	3
The Illumio solution	3
<b>CURRENT APPROACHES TO AUTO SCALING APPLICATION SECURITY</b>	<b>4</b>
Network-based security appliances	4
Software-defined networking (SDN)	4
<b>THREE KEY CHALLENGES WITH EXISTING SOLUTIONS</b>	<b>4</b>
1.Limited scalability and agility due to static network	4
2.Errors and delays due to manual processes	5
3.Inconsistent security policies across data centers or clouds	5
<b>THE ILLUMIO SOLUTION</b>	<b>5</b>
1.Fine-grained policy association	6
2.Context-aware security enforcement	6
3Automatic enforcement of security policies	7
4.Infrastructure-agnostic security	7
<b>USE CASE: SECURE AUTO SCALING OF APPLICATIONS WITH ILLUMIO</b>	<b>7</b>
Labels and workload identification	8
Writing security policies based on labels	8
The scope of security policies	9
Securing new workloads with Pairing Profiles	9
Securing scaled-out applications using an image	10
Securing application scale outs using DevOps tools	12
<b>ABOUT ILLUMIO</b>	<b>13</b>

## OVERVIEW

### BUSINESS DRIVERS

Enterprises rely on auto scaling to adjust the number and/or size of workloads during demand spikes to ensure application availability and performance. Once demand recedes, applications can be dynamically scaled down to reduce expenses and to reallocate the resources. Enterprises need consistent and accurate security policies for scaled workloads.

### CURRENT CHALLENGES WITH AUTO SCALING

- Security policies don't necessarily change to accommodate auto-scaled workloads.
- Network infrastructure changes are required when the scaling of workloads goes beyond a VLAN or security zone, or if a workload moves to the cloud.
- Manual security policy adjustments are prone to errors and delay scale-out operations.
- Most solutions don't allow for uniform security policies that work across data centers and public or private clouds.

### THE ILLUMIO SOLUTION

- The Illumio Adaptive Security Platform (ASP)<sup>TM</sup> ensures that auto-scaled workloads are secured as soon as they are provisioned. It adapts automatically to application and infrastructure changes.
- Security policies are built based on continuous computation of application context instead of network parameters like IP addresses. Newly launched workloads are automatically assigned context-specific security policies.
- Fine-grained security policies are attached to individual workloads to provide the most accurate policy enforcement from workload inception to decommission.
- Security is decoupled from infrastructure, which means new workloads can be secured on any VM, bare metal server, or container across data centers and private or public clouds.
- Security policies do not need to be manually reconfigured when workloads scale.

## CURRENT APPROACHES TO AUTO SCALING APPLICATION SECURELY

### NETWORK-BASED SECURITY APPLIANCES

Network-centric security appliances, whether virtual or physical, secure traffic using statically configured IP-based rules and firewall zones tied to VLANs. In this scenario, workloads are placed on the VLAN that matches their application or application tier, and the VLANs are then mapped to security zones. Traffic between workloads within a zone is “trusted,” with no security controls governing these flows. This approach works for environments that are relatively static and require limited application movement and scale out, but it doesn’t adequately address traffic inside the security zone or VLAN.

Moreover, the IEEE 802.1Q standard imposes a 4,096-VLAN limit, which may not provide enough addresses for today’s highly scalable and dynamic data centers and clouds.

### SOFTWARE-DEFINED NETWORKING (SDN)

Software-defined networking (SDN) technology leverages tunneling to overcome some of the limitations of VLANs. An overlay network built on top of existing network layer-2 and layer-3 technologies is used to isolate application workloads and can theoretically be used to create millions of logical layer-2 domains. Some virtual firewalls also integrate with vendor-specific SDN solutions to detect and secure newly instantiated workloads resulting from application scale outs using tags. A downside to this approach is that IT departments must monitor not only the physical network but also the SDN-based virtual overlays, which further complicates management and increases the risk of misconfigurations.

SDN also requires the enterprise to have control over the virtual switches and hypervisors in a network. Public cloud providers are not open to enterprises assuming administrative control over their infrastructure, which prevents these solutions from being extended to public or hybrid cloud environments.

## THREE KEY CHALLENGES WITH EXISTING SOLUTIONS

### 1. Limited scalability and agility due to static network

Network-based security solutions are generally static and cannot match the agility needed for highly scalable and dynamic data centers and clouds. With network-based security enforcement, application scale outs must remain limited within the boundaries of security zones and their associated VLANs. As soon as application needs exceed a VLAN’s scope, the network starts getting in the way. Manual configuration is required to add new VLANs and extend existing security zones or create new ones—which also entails related firewall policy changes. Once application demand recedes, these configurations must be manually cleaned up to remove any extraneous security policies that might open up unintentional access to business critical information.

## 2. Errors and delays due to manual processes

When there are big changes in workloads, network-centric security approaches require changes to VLAN configurations, zones, and firewall rules. These rules are specified using specific IP addresses and security zones and require careful evaluation to ensure that the rules are accurate. Manual configuration changes across switches, routers, and network firewalls significantly increase the risk of errors and misconfigurations. Many enterprises have put extensive validation processes in place, requiring careful coordination between application, network, and security teams. These processes introduce delays when responding to application scaling needs or new projects and slow down the business.

## 3. Inconsistent security policies across data centers or clouds

Security policies that are tied to network chokepoints are not portable. With current solutions, security policies have to be rethought and rewritten when workloads move across data centers or to the cloud. For instance, VLANs cannot be extended to the public cloud infrastructure, since cloud providers control the network. This means the security policies previously written for a workload need to be rewritten for the cloud. This problem is not addressed with SDN technology either, since it requires complete control over the entire network infrastructure.

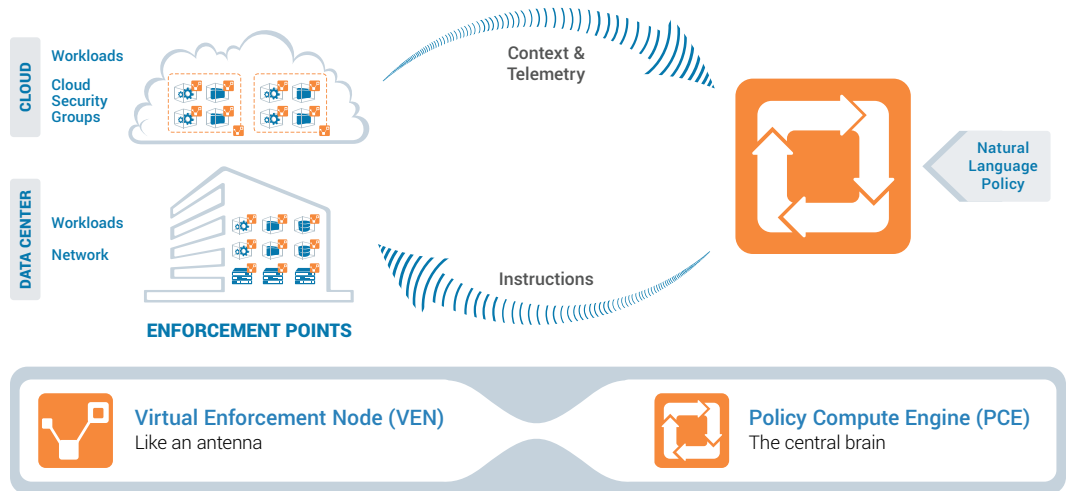
In order to support auto-scaling requirements and elastic workloads, enterprises need a security solution that works across public, private, or hybrid cloud networks without any dependencies on the underlying infrastructure. Consistent and accurate security policies should be automatically applied when new workloads are spawned and when workloads migrate regardless of the infrastructure on which they are deployed.

## 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 that 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.



Illumio directly addresses the limitations of current solutions for auto scaling applications without compromising speed or security.

## 1. Fine-grained policy association

Illumio removes the dependency on the underlying physical or virtual network.

Security policies are attached to individual workloads to provide the most accurate enforcement point. With this approach, security policies follow the workload and are automatically attached to workloads from inception through decommission across data centers, public clouds, or virtual private clouds.

## 2. Context-aware security enforcement

The use of network segmentation with IP-based firewall rules creates an inflexible security architecture that makes it difficult to accommodate workload context changes (such as interface IP changes) and auto scaling needs. By contrast, Illumio ASP provides a simplified, yet adaptive, approach to security using the context of each workload. Illumio ASP uses a flexible, multi-dimensional labeling mechanism to define a workload's context based on its role (database, web server, mail server etc.), the application that it serves (Payroll, Sales, etc.), the business environment it runs in (dev, test, production, etc.), and its location (US, Atlanta, AWS, Azure, 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, whitelisted policies.

The Illumio PCE maps the labels and configured rules to dynamically compute the graph of relationships between workloads. The policies are then automatically implemented by the system with modifications (depending on the OS) to the underlying IP tables or the Windows Filtering Platform in the workload. The policies defined based on context are resilient to changes since the workload automatically inherits the correct policies for its new context. This provides automatic "policy scaling" and replication when auto scaling application workloads.

### 3. Automatic enforcement of security policies

Newly launched application workloads are automatically assigned preconfigured security policies as soon as they are brought under management (i.e., paired). This ensures that auto-scaled workloads always stay within the prescribed security posture, without any human intervention, regardless of the number of workloads or the underlying infrastructure.

### 4. Infrastructure-agnostic security

By enforcing security on the workload using natural-language policies that do not depend on network configurations or parameters, Illumio ASP 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 Amazon AWS, Rackspace, and Google Compute.

## USE CASE: SECURE AUTO SCALING OF APPLICATIONS WITH ILLUMIO

To illustrate how Illumio ASP can be used to auto scale applications securely, consider ABC Corp., an enterprise with an Online-Store application that consists of a web tier and a database tier. During seasonal demand spikes, the web tier needs to be auto scaled. Consistent and accurate security policies must be provisioned and enforced on scaled web workloads as they instantiate.

ABC Corp.'s Online-Store application has the following security constraints:

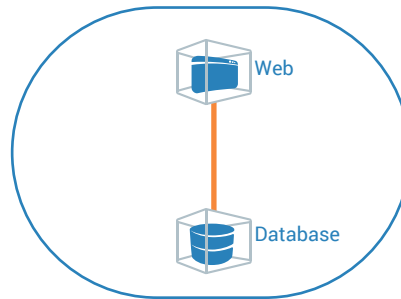
- Apache service hosted on the web-tier is open to the internet
- MySQL service hosted on the database tier is accessible only from the web-tier.

## HOW LABELS ARE USED IN SECURITY POLICIES

### Labels and workload identification

ABC Corp. uses Illumio ASP to create a library of multi-dimensional labels that are unique to its environment. The labels in the library are then used to describe the role, application, environment, and location for every workload.

The workloads for ABC Corp's Online-Store application are labeled as follows.



Online-Store : Production : US

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

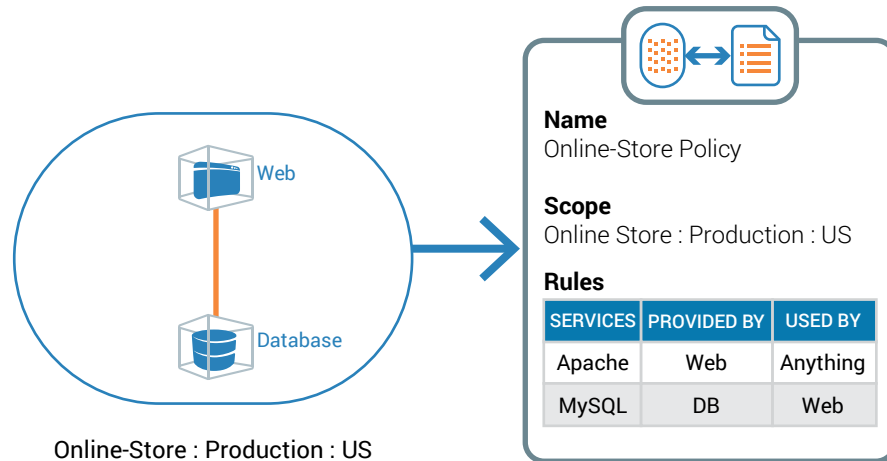
### Writing security policies based on labels

Once ABC Corp. has labeled its workloads, it can write security policies to capture the explicitly allowed interactions (whitelisted policies) between the workloads. Interactions that are not captured are simply denied. The figure below shows the ruleset that describe the relationships between the workloads of the Online-Store application.

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



Once configured and provisioned, this ruleset is applied to all the workloads of the Online-Store application as well as any new workloads that are instantiated as part of a scale-out operation.



### *The scope of security policies*

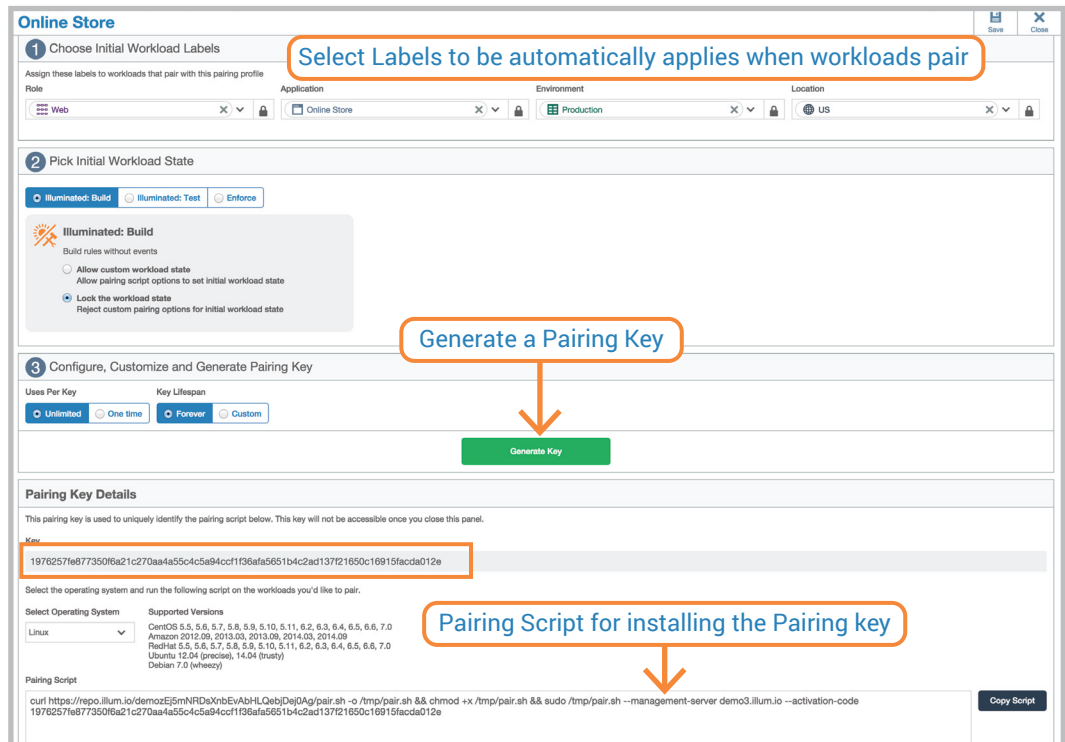
The scope identifies the set of workloads to which the security rules apply. In the above example, the rules are applied across all the workloads of the Online-Store application running as part of the production environment in the United States. Assuming that the application also exists in the test environment,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

### *Securing new workloads with Pairing Profiles*

ABC Corp. uses Pairing Profiles to associate newly instantiated workloads with the correct labels and rulesets.

The Pairing Profile is a configuration template that specifies labels that are to be applied to newly instantiated workloads. The Pairing Profile is used to generate unique Pairing Keys that are used by newly instantiated workloads for identifying (for authentication and for applying the labels) 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.

The following image shows the Pairing Profile for ABC Corp.'s Online-Store web tier, which will be used to generate the pairing key and script.



The screenshot shows the 'Online Store' configuration interface with three main steps:

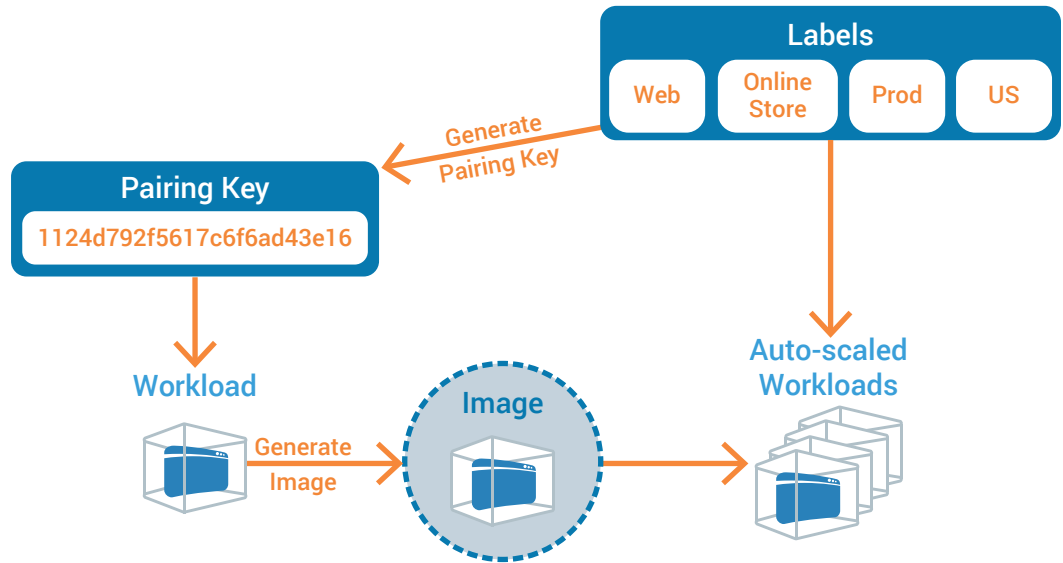
- 1 Choose Initial Workload Labels:** A callout box says 'Select Labels to be automatically applies when workloads pair'. The interface shows filters for Role (Web), Application (Online Store), Environment (Production), and Location (US).
- 2 Pick Initial Workload State:** The 'Illuminated: Build' state is selected. A callout box says 'Generate a Pairing Key' with an arrow pointing to a green 'Generate Key' button.
- 3 Configure, Customize and Generate Pairing Key:** The 'Forever' key lifespan is selected. A callout box says 'Pairing Script for installing the Pairing Key' with an arrow pointing to a 'Copy Script' button. The 'Pairing Key Details' section shows a key: `1976257e877350f6a21c270aa4a55c4c5a94ccf1f36afa5651b4c2ad137f21650c16915facda012e`.

## Securing scaled-out applications using an image

An image (e.g., AMI in Amazon AWS or VM templates in VMware) of the Online-Store web workload can be used to instantiate new workloads as part of the auto-scale operation.

The following procedure is used to prepare the workload before the creation of an image:

- Copy and edit the generated pairing script to replace all occurrences of "pair.sh" with "prepare.sh".
- Execute this script on the workload to install and program the VEN to use the Online-Store web-pairing key.
- Generate an image from this workload.



When application availability demands require auto scaling, preconfigured instances are launched using the workload image. As soon as the workloads are instantiated, they get automatically paired using the unique pairing key of the Online-Store web profile and inherit the predefined labels (Web/Online Store/Production/US). As a result, the rulesets associated with these labels are instantly propagated to the newly instantiated workloads.

## Securing application scale outs using DevOps tools

The pairing key generated as part of the Online-Store web profile can be baked in to the recipe of DevOps configuration management tools like Chef to set up the initial configuration of the web workloads instantiated as part of an application scale out. The pairing keys can be expired after a configurable time to ensure their secure use.

Below 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"]}/sPl1t0Exo0FIEphoewIujIucrLaT0AS3/pair.sh"
  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
```

The above Chef recipe is executed against the scaled-out web workloads as soon as they are instantiated. The pairing key included as part of this script identifies and associates the workloads with the Online-Store web pairing profile. Consequently, the labels (Web, Online-Store, Production, US) and rulesets associated with these labels are instantly propagated to secure the workloads.

With Illumio, automatic enforcement of security across elastic applications is possible independent of the underlying infrastructure. No manual processes are needed, thus reducing the risk of errors and simplifying the auto-scaling operations.

## 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](http://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](mailto:illuminate@illumio.com) or call 855-426-3983 to speak to an Illumio representative.

Illumio Adaptive Security Platform and Illumio ASP are trademarks of Illumio, Inc. All rights reserved.