ILLUMIO ADAPTIVE SECURITY PLATFORM™

HIGHLIGHTS

Adaptive Segmentation Prevents APTs
Segmentation is attached to your workloads, allowing you to secure individual applications and processes without the pain of changing any of your network or virtualization infrastructure. Policies can be as granular as needed and adapt immediately to any changes to workloads and applications.

Traffic and Policy Visibility
Illumio ASP discovers and visualizes all application workloads and their traffic, including the processes being accessed. This live visibility lets you create well-informed security policies based on how applications actually work.

Consistent Security on Any Compute, Any Environment
Illumio decouples security from the network and the hypervisor giving you the freedom to work on any combination of computing—bare-metal, virtualized platforms, and containerized workloads—across any combination of data centers and public clouds. Policies travel with the workload.

On-Demand, Policy-Based Encryption Protects Critical Assets
Implement AES 256-bit IPsec connections for applications across environments with a single click. Protect sensitive communications of traffic in motion based on segmentation policy.

Security for Agile Organizations
Brownfield data center or greenfield cloud environment, Illumio's REST API integrates seamlessly with orchestration and automation tools. All management can be done via API or using Illumio ASP's intuitive management allowing developers and security to go fast.

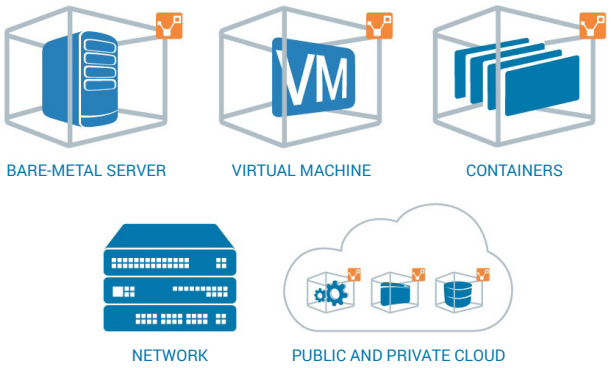
Enterprise Scale and Reliability for the Largest Data Centers
Illumio ASP is built for distributed scale out of hundreds of thousands of workloads with a self-healing, redundant architecture.

Simplicity of Operations For Any Sized Organization
Illumio Segmentation Templates can be deployed in minutes, simplifying the definition and implementation of policy while reducing errors and preventing security gaps for widely-used, business-critical applications.

Stop Bad Actors in Their Tracks
See unauthorized workload communications (policy violations) in seconds, not weeks or months. Stop activity and quarantine with one click or through automation.

The growth of distributed application architectures and cloud computing has permanently transformed IT operations. The implications for data center security teams is profound: an organization's most critical assets are increasingly vulnerable as traditional detection and perimeter security technologies prove inadequate in today's risk environment. Organizations must rethink how to stop the lateral spread of unauthorized communications while still meeting the needs of today's agile, DevOps IT practices. And all of this must happen at scale, from dozens to hundreds of thousands of workloads.

The Illumio Adaptive Security Platform (ASP)™ is the first cybersecurity system that delivers unprecedented live visibility and micro-segmentation services across the broadest range of computing assets (bare-metal, virtualized platforms, containerized workloads and behind network devices) and environments (data centers, private and public clouds) by delivering the optimal security for every workload and application running across the application environments. The patented Policy Compute Engine (PCE) is the only system that adapts in real-time to changes in your applications environment—whether that is the movement of workloads, changes to security policies, or unauthorized communications among your applications.



Customers are using Illumio ASP to:

- Map Application Dependency: gain visibility, improve understanding of risk, and aid in policy creation.
- Micro-segment Applications: control communications and protect applications without dependencies on the infrastructure.
- Nano-segment Applications: control communications down to the process level for dynamic applications like Active Directory.
- Segment Environments: separate and secure environments such as development and production without the need for any complex or fragile network configuration changes.
- Secure New Data Centers: meet security and agility requirements without the cost and complexity of traditional segmentation approaches.

- Securely Move to Public Cloud: migrate applications with policy that adapts and moves with your applications to any data center or cloud.
- Segment Users: prevent unauthorized access to applications based on user identity.

Discover your applications in data centers and the cloud

Illumination provides a live application dependency map across your environments showing workloads, applications, and traffic flows so you can see how applications communicate and identify violations quickly.

Define the most granular adaptive security through a descriptive policy

Illumio policy is defined using declarative, natural language without network constructs, such as VLANs, zones, and IP addresses, for a model that is easy to create and easy for all security, infrastructure, or application teams to understand. Write once and enforce everywhere with policy that adapts automatically to changes in the application environment. Auto recommendation of policy helps teams quickly determine the best policy for the environment and enforce protection quickly.

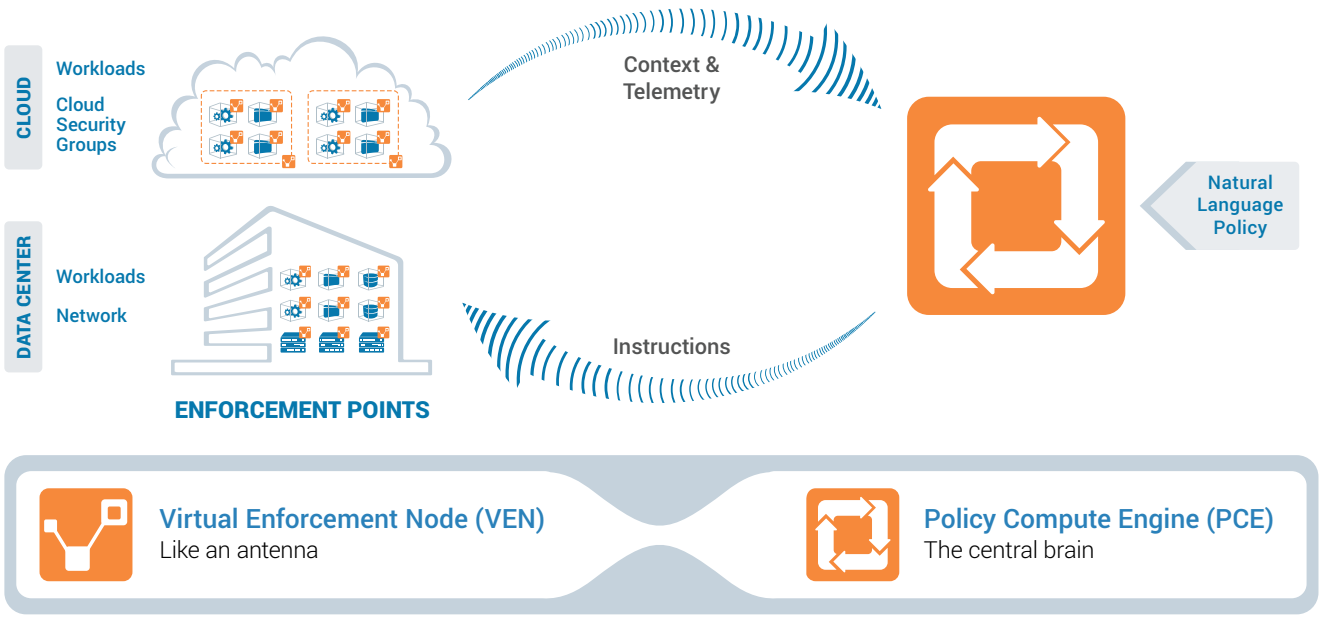
Defend your most trusted assets

Illumio adaptive segmentation is designed to apply the exact level of protection needed to the environment, application, or workload by providing a range of segmentation granularity options applied in the workload, network, or through cloud security controls.

With Illumio, you can segment large environments like production and development with a single rule, micro-segment a specific critical high-value application, define granular policy for control down to the process level, and even encrypt traffic between workloads and environments with a single-click policy.

ILLUMIO ASP ARCHITECTURE

The Illumio ASP patented architecture is built to scale, adapt to changes in real time, and protect applications with centralized policy and coordinated enforcement of adaptive segmentation policy in the workload, network, and through cloud security controls. The Illumio platform is comprised of the following components:



POLICY COMPUTE ENGINE (PCE)

The PCE is the central point of visibility and policy that is deployed on premises or available as a SaaS service hosted by Illumio. The PCE continually collects and aggregates workload context (IP addresses, services, ports, and traffic flows) from all VENs across application environments and uses it to build and display the live Illumination application map.

The PCE translates declarative, natural language policy into instructions used to program pre-existing firewalls on the workloads, Access Control Lists (ACLs) in data center switches, or cloud security groups in cloud services for enforcement—eliminating the need for administrators to use network constructs, such as IP addresses or VLANs, in the creation of adaptive segmentation policy. The PCE adapts to changes across the application environment by updating the Illumination view and automatically recalculating policy to ensure consistent and continuous protection.

VIRTUAL ENFORCEMENT NODE (VEN)

The VEN is a lightweight agent deployed in a workload (a.k.a. operating system) that could be run on bare-metal servers, virtual machines on any hypervisor, or container platforms in a private data center or any public cloud. The VEN is in continuous contact with the Illumio PCE to provide up-to-date workload context across the application environment.

The VEN receives up-to-date instructions from the PCE to program the pre-existing local firewall on the workloads (iptables or Windows Filtering Platform), or ACLs in data center switches to enforce the adaptive segmentation policy at every enforcement point in or across private data centers or the cloud.

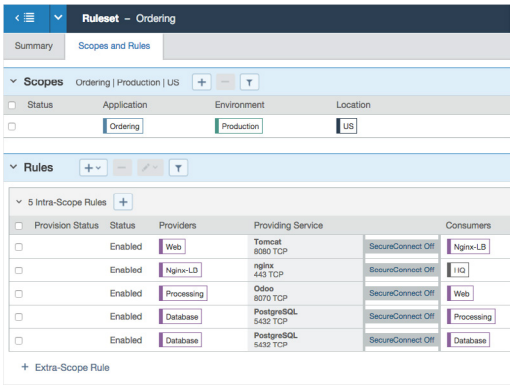
ILLUMIO ASP SERVICES

Illumio ASP delivers two core services that provide an industry breakthrough in protecting applications inside and across your data center and cloud environments.

Enforce Adaptive Segmentation

Illumio adaptive segmentation is designed to apply the exact level of protection needed to the environment, application, or workload by providing a range of segmentation granularity options applied in the workload, network, or through cloud security controls.

With Illumio, you can segment large environments like production and development with a single rule, micro-segment a specific critical high-value application, define granular policy for control down to the process level, and even encrypt traffic between workloads and environments with a single-click policy.



Illumio Enforcement Allows You To:

- Secure and control application traffic with adaptive segmentation at every workload, in the network, or through cloud security controls.
- Ensure consistent and continuous protection that automatically adapts to changes (movement of workloads or new capacity across application environments).
- Enable AES-256 IPsec encryption for data in motion between a mix of Windows and Linux workloads with a single click and without additional hardware or custom software.

Gain Live Visibility

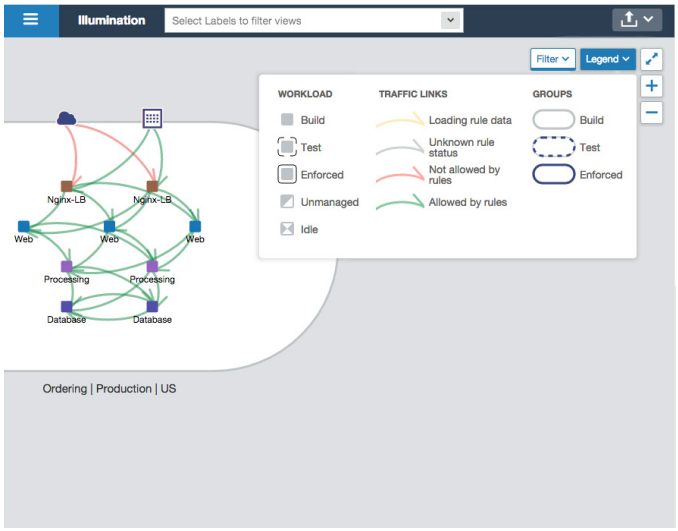
Illumination provides a live application dependency map across your environments showing workloads, applications, and traffic flows so you can see how applications communicate and identify violations quickly.

In addition to being an important cybersecurity tool, Illumination is a tightly integrated component of the Illumio ASP workflow used to:

- Discover applications in both brownfield and greenfield environments.
- Build better, more efficient policies without breaking applications.
- Confirm enforcement of policy.

With Illumination, You Will:

- Eliminate blind spots inside and across your data center and cloud environments with a comprehensive view of application traffic.
- Gain understanding of application behavior and dependencies on common services (e.g., Active Directory, Exchange, database platforms).
- Gain granular visibility into workload relationships with details down to the flow and service level.
- Model security policy and receive visual feedback in real time to eliminate risk of breaking applications with new policies.
- Pinpoint unauthorized communications and stop them immediately with the ability to quickly quarantine workloads.



ILLUMIO LABELS & POLICY MODEL

Illumio's unique approach to labeling workloads enables application-centric visibility and a simplified, understandable, and adaptable model for policy.

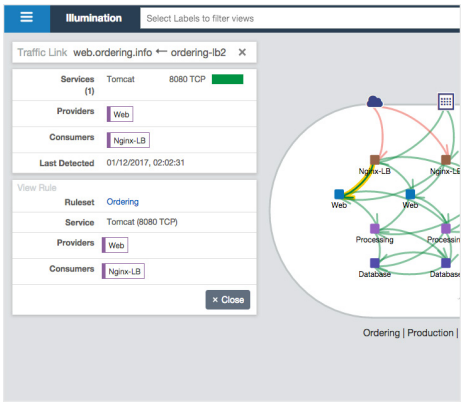
Labels

- Labels allow for classification of workloads in four dimensions using Role, Application, Environment, and Location.
- With labels, the application environment can now be organized and visualized with more context showing a view of applications and their components.
- Labels become the foundation of policy for a model that is both simple to define and adaptable to changes while eliminating dependencies on the infrastructure.

Role	Application	Environment	Location
Web	Ordering	Development	US
Web	Ordering	Production	US
Web	Ordering	Development	US
Web	Ordering	Production	US
Web	Ordering	Development	US

Policy

- Illumio policy is defined using declarative, natural language without network constructs, such as VLANs, zones, and IP addresses, for a model that is easy to create and easy for all security, infrastructure, or application teams to understand.
- Write once and enforce everywhere with policy that adapts automatically to changes in the application environment.
- Auto recommendation of policy helps teams quickly determine the best policy for the environment and enforce protection quickly.



SYSTEM REQUIREMENTS

VEN

Linux workloads

- Amazon Linux
- CentOS 5, 6, 7
- Debian 7, 8
- Oracle Linux 6, 7 (UEK and RHCK kernels)
- Red Hat Enterprise 5, 6, 7
- SUSE Enterprise 11, 12
- Ubuntu 12, 14, 16 (LTS only)

Windows workloads

- Windows Server 2008 R2, 2012, 2012 R2
- Windows 7, 10

Environments

- Any hypervisor (e.g., VMware ESXi, Microsoft Hyper-V, Nutanix AHV, KVM)
- Bare-metal servers
- Private data centers
- Any public cloud (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform)

PCE

Delivery methods

- Illumio Secure Cloud
- Software (RHEL or CentOS 6.x)
- Virtual Appliance (VMware ESXi 5.0, 5.1, or 5.5)

Browsers for web console

- The PCE web console is supported on the most current versions of Chrome and Firefox, and on Internet Explorer 10 or later.

ILLUMIO ASP BENEFITS

BENEFIT	DESCRIPTION
Eliminate blind spots	Gain visibility inside data centers and the cloud, and regain control of your application environment.
Protect the 80% of traffic invisible to perimeter firewalls	Control east/west communications and activity behind perimeter firewalls in your data center and cloud.
Stop the spread of attacks	Immediately detect unauthorized activity and stop breaches in their tracks.
Eliminate service delivery delays	Deploy applications with security as soon as they are deployed versus days to weeks.
Decrease firewall rules by over 95%	Reduce complexity with natural language policies and decrease the number of firewall rules that need to be created and managed inside the data center.
Make security detection solutions more effective	Reduce investigations of unauthorized communications.
Single solution to protect your applications	Protect applications running in bare-metal, virtualized, or containerized environments on premise, in the cloud, or across hybrid cloud deployments.

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.