FAQs

What is the Illumio Adaptive Security Platform® (ASP)?

Illumio ASP is a software solution that secures any computing platform (bare-metal servers, virtual machines, and containers) in any environment (data center, private cloud, public cloud – like Amazon Web Services, Google Compute Engine, Microsoft Azure, OpenStack – or hybrid cloud) without any dependency on the underlying network.

It does this by providing:

- Live visibility of applications, their components, traffic flows and vulnerabilities across all environments, including private data centers and public and hybrid clouds.
- Adaptive micro-segmentation that continuously adjusts to changes in the application environment to keep segmentation enforcement intact.
- On-demand, policy-driven encryption of data in motion between workloads.

Illumio ASP understands all the ports, processes, and connections among an application's workloads including their interrelationships and potential vulnerabilities and uses this information to compute and enforce accurate security. Illumio ASP adapts to computing environment changes, the movement of workloads across data centers and clouds, and IP address changes. It also adapts to application and infrastructure changes and prevents the lateral spread of attacks.

Illumio ASP user segmentation capabilities can control the communications between desktops and applications running in the data center.

What are the key benefits of using Illumio ASP?

Key benefits include:

- Eliminate blind spots inside data centers and the cloud, and regaining control of your application environment.
- Protect the 80 percent of data center and cloud traffic that is invisible to perimeter firewalls.
- See potentially vulnerable connections: prioritize patching and inform micro-segmentation policy.
- Immediately detect unauthorized activity and stop breaches in their tracks.
- Eliminate service delivery delays and deploy applications with security in hours versus days to weeks.
- Decrease the number of firewall rules inside the data center by over 95 percent.
- Make your investments in security detection solutions more effective by reducing investigations of unauthorized communications.
- A single solution to protect your applications running in bare-metal, virtualized, or containerized environments on premises, in the cloud, or across hybrid cloud deployments.

Why does security need to be "adaptive"?

Without adaptive security, businesses are slowed down due to the overwhelming number of firewall rules, manual changes required to policies, and the possibility of errors leading to outages or serious vulnerabilities and breaches. Adaptive security automatically accounts for moves, scale, and changes to applications and infrastructure that are typical of modern data centers.

Illumio ASP is a software solution built around the specific and accurate context of the workload and application. Illumio listens to and understands the services and active network connections that are running on a workload.

Illumio ASP constantly computes workload relationships and adapts to any changes in context. Administrators specify the desired interactions between workloads using natural-language terms. Then, Illumio ASP computes and enforces the precise security for each workload in the application by combining workload context with the defined policies. As workload context changes (moves, scale up, scale down, IP address changes, etc.), Illumio ASP computes and distributes the incremental policy changes to the impacted workloads.

How is Illumio ASP different from existing security solutions?

Illumio ASP enforces security policies for workloads running in any bare-metal server, virtual machine, or containerized host without any dependencies on the underlying network (VLANs, subnets, zones, physical or software defined, etc.), hypervisor, or environment (data centers and private, public, or hybrid clouds). Illumio does not simply automate or repurpose existing security capabilities, it applies security in a unique and innovative way.

Illumio ASP enables IT to write policies in natural language based on the role, application, environment, and location of the workload. These policies are then translated into granular security rules, without the need to specify IP addresses, subnets, VLANs, or zones.

Policy Generator can be used to automate segmentation policy creation and includes inputs such as requested policy granularity and exposure of workloads and vulnerabilities. This saves time, accelerates security workflows, and reduces the risk of human errors.

Illumio micro-segmentation can be applied at the beginning of the application life cycle by integrating with configuration management and orchestration tools such as Chef, Puppet, Ansible, and ElasticBox—or they can be applied to an existing environment.

How are customers using Illumio?

Organizations are using Illumio ASP to prevent the spread of breaches, improve understanding of risk, and simplify security operations for applications inside and across data center and cloud environments.

Here are the eight primary ways organizations are improving security and IT efficiencies with Illumio.

- **Vulnerability-based micro-segmentation** as a compensating control to mitigate vulnerabilities, reduce East-West exposure, prioritize patching efforts, and prevent the spread of breaches.
- **Application micro-segmentation** to secure your most valuable applications and data in hours versus days or weeks – within or across any data center or public cloud. Read More
- **Environmental micro-segmentation** to address challenges of separating and securing environments without impact or dependencies on the network or underlying infrastructure. Read More
- **User micro-segmentation** to dynamically enforce user connectivity to applications so users can only see the applications they're authorized to access. Read More
- **Nano-segmentation** to create and enforce adaptive micro-segmentation policy tied to a specific process for the ability to secure dynamic applications without compromising functionality or protection. Read More

- **Map application dependencies** to visualize relationships across your application environment to better understand risk and improve adaptive segmentation policy creation. Read More
- **Secure a new data center** with the ability to bypass the restrictions, complexity, and expense of legacy segmentation solutions with adaptive segmentation that meets your requirements for security and agility. Read More
- **Securely move to public cloud** by creating adaptive micro-segmentation policy that moves with your applications to any data center or cloud infrastructure. Read More

Who uses Illumio ASP?

Our customers span organization of all sizes, verticals, and geographies, including nine of the largest 15 financial institutions in the US and four of the top seven global Software-as-a-Service companies. Our customers include the likes of Morgan Stanley, Salesforce, BNP Paribas, Oracle NetSuite, Plantronics, NTT, Creative Artists Agency, and Oak Hill Advisors.

Learn more about the customers using Illumio.

What are the core components of Illumio ASP?

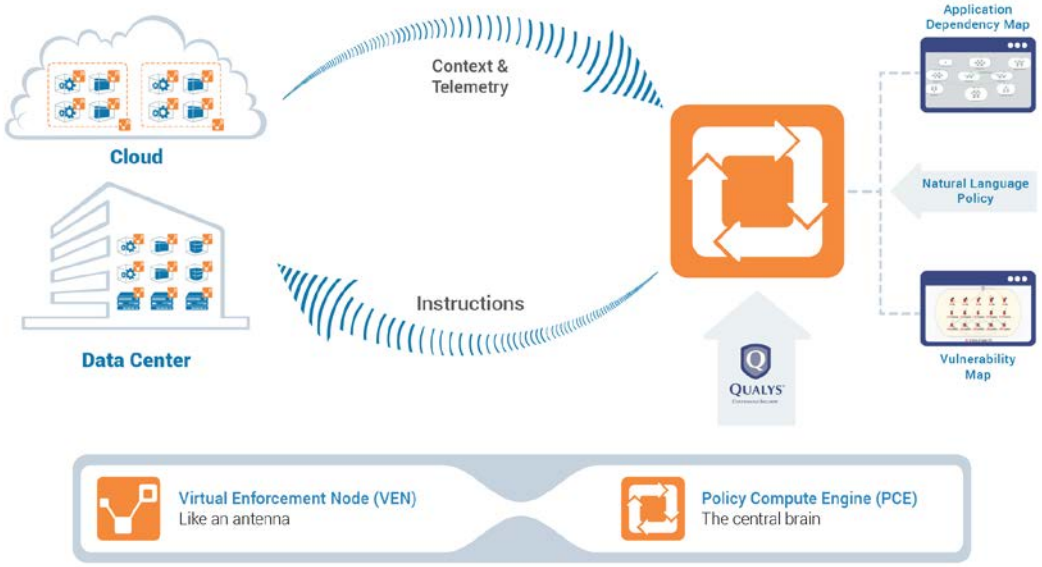
There are two main components to Illumio ASP:

- The **Policy Compute Engine (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, 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.

  See this video for an overview on the PCE.

- The **Virtual Enforcement Node (VEN)** is a lightweight agent deployed in a workload (a.k.a. operating system) or on a networking device. The operating system (e.g., Linux, Windows, AIX, Solaris) could be running 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, Windows Filtering Platform or IPFilter), 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.

  See this video for an overview on the VEN.



Illumio offers three core services to protect applications inside and across the data center and cloud environments:

- **Visibility** with Illumination providing a live application dependency map across environments that shows workloads, applications, traffic flows and vulnerabilities to quickly see how applications communicate, see how exposed vulnerabilities are to a breach, and identify risky connections quickly. In addition to being an important cybersecurity tool, Illumination is a tightly integrated component of the Illumio ASP workflow used to discover applications, build better, more efficient policies without breaking applications, and confirm enforcement of policy. See this video for more on why visibility is important for adaptive segmentation.
- **Enforcement** of micro-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, and even define granular policy for control down to the process level – all without changes to applications or the network.
- **Encryption of data in motion** with SecureConnect for on-demand, policy-driven encryption between workloads without the headaches of manual configuration or expensive, complex hardware solutions. With one click of a button in the Illumio management console, IPsec tunnels between any two workloads can be easily instantiated wherever they are running in private data centers, public cloud or hybrid environments. See this video for more on SecureConnect.

Watch these videos for an Illumio ASP deep dive.

What are vulnerability maps?

Vulnerability maps combine third party vulnerability and threat insights from companies like Qualys with Illumio's application dependency map to help teams see which applications are connecting into vulnerable ports in real time. This enables application security teams, vulnerability

management teams, and segmentation teams to understand not only the vulnerability of a workload but, more importantly, the paths that bad actors can leverage to exploit vulnerabilities.

See this video for a demo of Illumio ASP vulnerability maps.

Why are vulnerability maps needed?

Vulnerability management and micro-segmentation are both foundational security controls and critical to a successful cybersecurity strategy. The combination of vulnerability data and the application dependency map shows how an attacker looks at exploiting vulnerabilities in the data center. This insight helps teams to prioritize patching efforts and the application of compensating controls like micro-segmentation.

What is an Exposure Score?

Illumio vulnerability maps include an East-West exposure score that is shown per workload and is a calculation of how many workloads can potentially exploit the individual vulnerabilities on any given workload that has a VEN. The lower the score, the lower the chance that a bad actor can exploit vulnerabilities on a given workload. This insight can be used to prioritize and generate precise micro-segmentation policies as a compensating control and to help prioritize patching efforts.

How can Illumio micro-segmentation be used as a compensating control?

Vulnerability-based micro-segmentation can be used as a compensating control to reduce East-West exposure by reducing or eliminating unnecessary pathways that may be used to take advantage of vulnerabilities. Compensating controls are used when patching cannot be performed, such as in the case where a patch is not available or patching would impact the availability of a critical application.

Illumio vulnerability-based micro-segmentation quantifies risk reduction before and after policy is deployed. When vulnerability-based micro-segmentation is used as a compensating control, Illumio provides detailed reports on the reduction of vulnerability exposure.

Does Illumio work with my existing security solutions (firewall, IPS/IDS, etc.)?

Yes. Illumio ASP works alongside existing firewall and network security solutions. No changes to the network technology or topology are required to integrate Illumio ASP into a data center or cloud environment.

Is there any dependency on specific hardware or software infrastructure for enforcement of micro-segmentation policy?

No. Illumio ASP secures a broad range of operating systems on bare-metal servers, virtualized servers, or containerized hosts in private data centers or private, public, or hybrid clouds.

Read our data sheet for details on supported platforms.

Does Illumio ASP change server or VM configuration?

No. Illumio ASP does not require any changes to standard OS or VM configurations.

How secure is this solution?

Illumio ASP performs enforcement using the native capabilities within the host operating system – iptables in Linux servers and the Windows Filtering Platform in Windows servers. If the Illumio VEN is tampered with, an alert is sent to the PCE. The PCE will attempt to reestablish control of the

VEN. If attempts to reestablish control of the VEN are unsuccessful, the PCE can update security rules to instruct all other workloads in the environment to shun the workload in question.

What is a workload?

A workload equates to a discrete operating system instance. It can run on a bare-metal server, in a virtual machine, on a containerized host, or in a cloud environment.

What does Illumio mean by "workload context"?

Workload context includes system properties (operating system, IP address, ports, running processes, etc.), relationships and dependencies to other workloads within the application and beyond, and the ecosystem (location, application details, life cycle, environment, etc.). The context of a workload changes as the application that the workload is a part of moves, changes, and scales up or down.

Is the VEN installed inside the hypervisor or as a VM?

The VEN resides in the guest OS. Both Linux and Windows workloads are supported.

Watch this video for more details on the VEN.

Illumio Adaptive Security Platform FAQ

Will my workload traffic be blocked as soon as I install the VEN?

No. The VEN can be installed in a mode that allows you to gain live visibility of the application environment without having to enforce any rules. You can use this option to model/build policy and move to enforcement after you are confident of the results.

Watch this video for more details on the VEN.

Illumio Adaptive Security Platform FAQ

What visibility is provided by Illumination?

Illumination provides live insights to help you visualize application dependencies, view how exposed vulnerabilities are, and automatically recommend optimized policies for applications running across data centers and clouds. With Illumination, you will gain live visibility into the Layer 4 connections between workloads, including details about the flows – source, destination IPs, port protocol, and process names. In addition, vulnerability maps provide a view into potentially vulnerable workloads and connections.

Watch this video for the four reasons why visibility is critical to adaptive segmentation.

Illumio Adaptive Security Platform FAQ

What do you mean by "natural language" policy?

Illumio ASP allows administrators to assign four dimensional labels to workloads to identify their role, application, environment, and location. These labels can then be used to apply security policies to specific parts of the application environment. The PCE converts these label-based policies into rules that can be applied to the OS level firewall of the workload.

Why is label-based policy better than my traditional policy?

Once you define a label-based policy, the PCE dynamically computes the appropriate rules for each workload in the environment. The PCE also dynamically re-computes a policy when new workloads are added to or removed from an environment or when workload IP addresses change. This enables the freedom and flexibility to design security policies without relying on networking details

that may change. This also helps to drastically reduce the complexity of rules, the number of rules created, and the number of rules managed.

Watch this video to learn more about why labels are important to adaptive segmentation.

Illumio Adaptive Security Platform FAQ

What types of enforcement do you support?

Illumio ASP is built on a whitelist enforcement model where only connections that are explicitly defined by policy are accepted and allowed. All other connections are inherently blocked. Policy can be defined at various levels of granularity including environment, application, and port/process level allowing for the right level of policy to be defined and applied for the use case. With this model policy might protect an environment like development by controlling the connections into and out of that environment but allowing all workloads in development to communicate.

How do I deploy Illumio ASP? How long does it take?

Illumio ASP is available in three deployment types:

- Illumio ASP Cloud: Illumio hosts and manages the PCE infrastructure used to provide Illumio ASP services.
- Illumio ASP On Premises:
    - PCE Virtual Appliance: Illumio ASP is deployed as a virtual appliance in the customer's data center.
    - PCE Software: Illumio ASP is deployed as software on the servers in the customer's data center.

Workloads in the customer data center or in any cloud environment are secured by installing the VEN software agent on the workload and establishing a connection to the PCE. Most customers are up and running in hours.

What is user segmentation?

User segmentation builds on Illumio's earlier capabilities of workload- and process-level segmentation to control which data center applications a user can see and connect to. It extends VEN coverage to include Windows 7 workloads and creates new user-based policies within the PCE.

What are the benefits of user segmentation?

Organizations are worried about the "inside man" problem where a laptop can connect to a range of unauthorized servers/applications in a data center or public cloud.

For example, a company that has its VDI implementation located in its data centers would like to control what a user can connect to, thereby limiting the ability of a bad actor to steal credentials or leverage weak passwords to gain access to sensitive applications and data.

How is Illumio ASP sold?

Illumio is offered as an annual subscription.

How do I get a demo of or purchase Illumio ASP?

Contact Illumio Sales at sales@illumio.com.