ILLUMIO ADAPTIVE SECURITY PLATFORM FOR FEDERAL

Organizations are under constant pressure to remain agile. While your data centers evolve and extend into public clouds, containers, and new types of compute resources, you need to ensure that your organization remains compliant with regulations and meets industry security standards. At the same time, security frameworks like NIST and MITRE ATT&CK™ recommend that it is sound security practice to assume your perimeter defenses will be breached and to take appropriate actions to limit the movement of bad actors inside your data center and cloud environments. To address these frameworks while still remaining agile, many organizations are adopting Zero Trust security to reduce attack surfaces and mitigate exposure from different types.

BENEFITS

- Build a foundation for Zero Trust security with micro-segmentation
- Enable compliance and prevent the lateral movement of bad actors inside your data center
- Enable micro-segmentation on a global scale with PCE Supercluster™
- Enable real-time visibility into your application dependencies with Illumination® application dependency maps
- Enhance patching strategy and use micro-segmentation as a compensating control with vulnerability maps
- Use enforcement points from your existing infrastructure investments

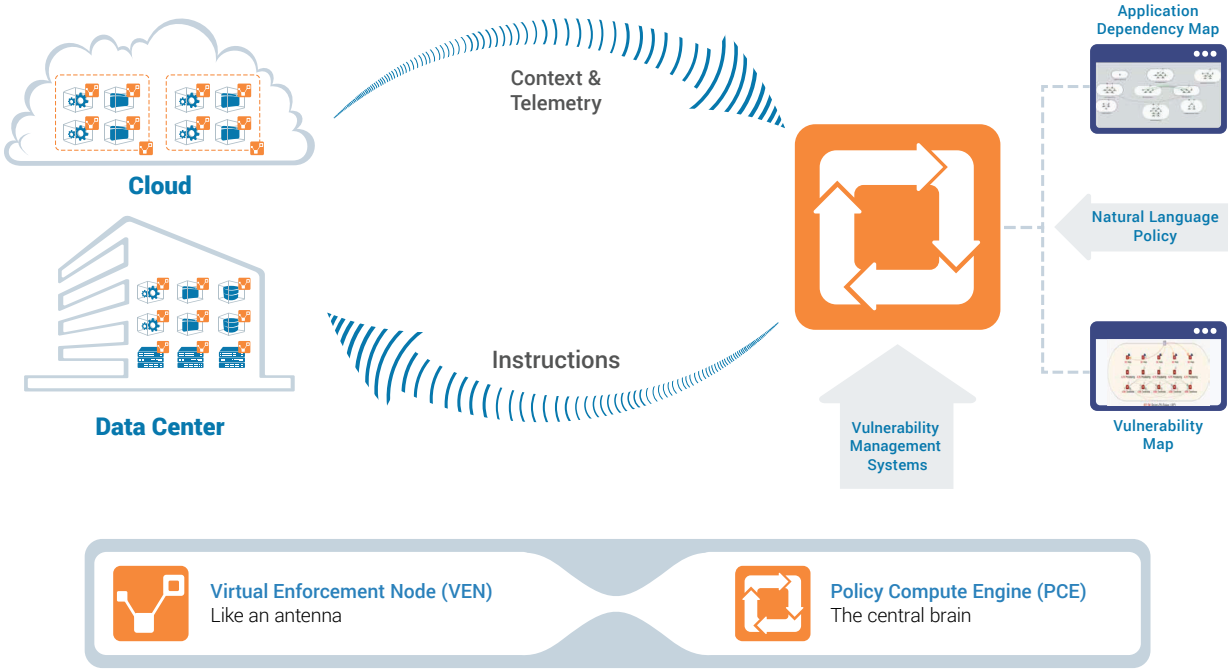
ILLUMIO ADAPTIVE SECURITY PLATFORM (ASP) OVERVIEW

Illumio ASP delivers real-time application dependency mapping and micro-segmentation to prevent the lateral movement of bad actors inside your data center and cloud environments. It provides real-time visibility into the connectivity between workloads across heterogeneous compute environments, generates optimal micro-segmentation policies based on how workloads communicate, and programs the native stateful enforcement points in each host to enforce applicable firewall rules.

Illumio ASP is unique because its architecture enables you to use the sensors and enforcement points that are natively available in your compute environment, eliminating the overhead of having to re-architect your network and deploy more networking/SDN and data center firewalls to secure your micro-perimeters. Illumio ASP delivers visibility and enables micro-segmentation for Zero Trust security at any scale. Since policy creation does not require deep familiarity with networking terminologies, you can empower different teams within your organization to create micro-segmentation policies, but retain governance over what gets provisioned.

The features section of this datasheet offers more details on the differentiation ASP delivers to customers.

ILLUMIO ASP ARCHITECTURE AND CORE COMPONENTS



Illumio ASP is comprised of two core components:

Virtual Enforcement Node (VEN): The VEN is a lightweight agent that is installed in the guest OS of the host. The VEN does not enforce firewall rules or route traffic. It performs two key functions:

- It collects and transmits information about the workload's operating system, interfaces, processes, and flows to the Policy Compute Engine (PCE). Each VEN functions as a point of visibility and a sensor that detects violations. This capability enables security to baseline an application's behavior and create rules to detect unauthorized connections and deviations from policies.
- It receives applicable firewall rules from the PCE and programs the host's native Layer 3/Layer 4 stateful firewalls. VENs program supported operating systems (Windows, Linux, AIX, Solaris) and containers, as well as ACLs for switches, load balancers, and security groups for clouds (public, private, hybrid).

Policy Compute Engine (PCE): The PCE is the brain that collects all the telemetry information from the VEN, visualizes it via real-time application dependency maps, and then calculates and recommends the optimal firewall rules based on contextual information about the environment, workloads, and processes. These rules are transmitted back to the VENs, which in turn program each hosts' Layer 3/Layer 4 firewalls. The PCE can be deployed via Illumio's SaaS platform, on premises, and in a virtual private cloud.

PCE SUPERCLUSTER FOR ENTERPRISE SCALE AND HIGH AVAILABILITY/DISASTER RECOVERY (HA/DR)

PCE Supercluster is designed for enterprise-scale, globally distributed data centers with more than 25,000 VENs deployed. It provides organizations with global visibility into the connections and flows across multiple data centers, and enables them to centralize policies across federated PCEs. Compared to a single PCE, a PCE Supercluster provides multiple independent PCE failure domains and support for a significantly greater numbers of workloads.

KEY FEATURES

Real-Time Application Dependency Maps (Illumination)

Visualizes information on the connections, flows, and processes running in each workload.

Illumination offers real-time visibility into your applications, their behavior and interdependencies; enables application baselining to detect for anomalous behavior; and enables you to model segmentation policies with visual feedback prior to enforcement to ensure applications don't break when moved and/or when policies are enforced.

Who uses Illumination? Illumination facilitates collaboration across IT operations, application owners, and security teams by giving them a centralized real-time view of application behavior and enables them to use this information to perform their jobs while still maintaining access governance. (Figure 2)

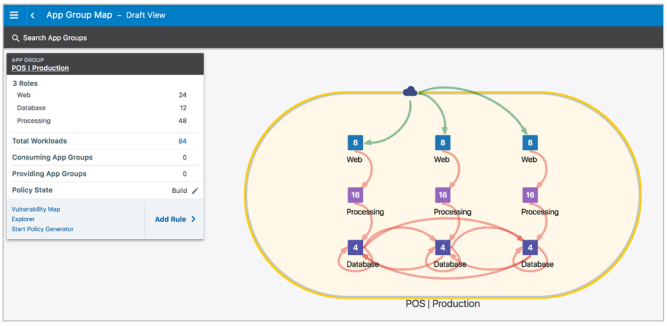


Figure 2: Illumination View in Build Mode

Policy Generator

Uses flow history to create and recommend optimal micro-segmentation policies for every workload and application regardless of the location or type of workload.

Policy Generator accelerates policy development while still giving you control over what gets approved and pushed into production. (Figure 3)

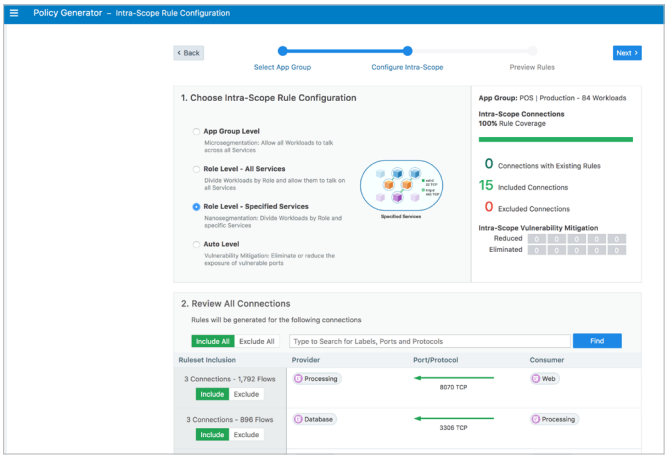


Figure 3: Policy Generator

Vulnerability Maps

Combines application dependency maps with vulnerability scan data from third-party vulnerability scanning tools to provide insights into the exposure of vulnerabilities and attack paths across applications running in your data centers and clouds.

With vulnerability maps, you can see the potential attack paths that could be exploited by a bad actor; get an East-West exposure score that calculates how many workloads can potentially exploit vulnerabilities; and apply vulnerability-based micro-segmentation as a compensating control to reduce East-West exposure. (Figure 4)

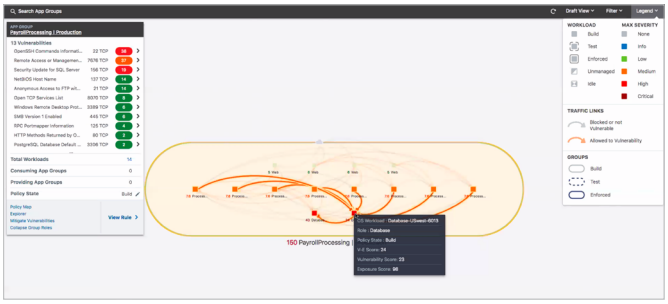


Figure 4: Vulnerability map with East-West exposure score

KEY FEATURES (continued)

Role-Based Access Control (RBAC)

Delivers security at an enterprise scale by assigning users the least required privilege they need to perform their jobs, implementing separation of duties and granting access to users based on multiple label dimensions (roles and scopes).

RBAC streamlines cross-functional processes, giving authorized users the access they need so that they can do their jobs while maintaining separation of duties for governance.

Explorer

Using RBAC, authorized users can use Explorer to query the PCE's historical traffic database to analyze flows for auditing, reporting, and troubleshooting.

Users can view search results as a vertical list of consumers, providers, and ports being used; as a table to show which flows were allowed, blocked, or potentially blocked based on policies; or as a list of unmanaged IP addresses that are connecting to a host.

SecureConnect

Enables encryption of data in motion when data is transmitted within the VLAN data center or PCI environment, or from a cloud location to an enterprise data center.

SecureConnect enables host-to-host traffic encryption between paired workloads by using the built-in encryption libraries of host operating systems. SecureConnect is policy driven and managed by the PCE. CERTIFICATIONS

KEY BENEFITS

- Enables Zero Trust security via micro-segmentation to suit your data center design, size, and complexity, and works across heterogeneous compute environments at any scale.
- Gives you real-time visibility of application behavior and connections and leverages this to drive your micro-segmentation strategy.
- Uses the enforcement points in your existing infrastructure investments, saving you management and cost overheads associated with re-architecting.
- Enhances your patching strategy and vulnerability management programs by helping you visualize and identify the potential pathways attackers could exploit and use micro-segmentation as a compensating control.
- Enables you to gain real-time global visibility and maintain a single control plane for managing micro-segmentation policies at a global scale while supporting high availability and disaster recovery objectives.

CERTIFICATIONS

NIAP COMMON CRITERIA

Common Criteria is an internationally recognized set of security standards which are used to evaluate the Information Assurance (IA) of IT products offered to the government by commercial vendors. For Illumio ASP, the Target of Evaluation, which was evaluated and certified by an authorized third party lab, included the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). Illumio is the first enterprise micro-segmentation vendor that is certified against the NIAP protection profile for Enterprise Security Management, Policy Management v1.2.

DHS CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

Illumio is listed on the Department of Homeland Security's Continuous Diagnostics and Mitigation Approved Products List. The Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) program includes cybersecurity tools and sensors that are reviewed by the program for conformance with Section 508, federal license users, and CDM technical requirements. Illumio ASP conforms with the Phase 3 BOUND technical requirements addressing, "How is the network protected?"

FIPS 140-2

The Federal Information Processing Standard Publication (FIPS PUB) 140-2 is a U.S. government computer security standard used to approve cryptographic modules. An authorized cryptographic equipment assessment laboratory has tested and verified that the Policy Compute Engine (PCE) and Virtual Enforcement Node (VEN) faithfully incorporate the use of cryptographic functions provided by the FIPS 140-2 validated modules as it applies to data in transit.

LEARN MORE

- Learn about enterprise-scale micro-segmentation with PCE Supercluster. (illumio.com/blog/pce-supercluster-security-at-scale)
- Gain visibility and plan your micro-segmentation strategy with real-time application dependency mapping. (illumio.com/product-feature-illumination-application-dependency-map)
- Take a Test Drive – experience application dependency mapping and create micro-segmentation policies in your own environment. (illumio.com/test-drive-landing-page)

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.

CONTACT US

For more information about Illumio ASP and how it can be used to achieve environmental segmentation, email us at illuminate-at-illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 illumio.com