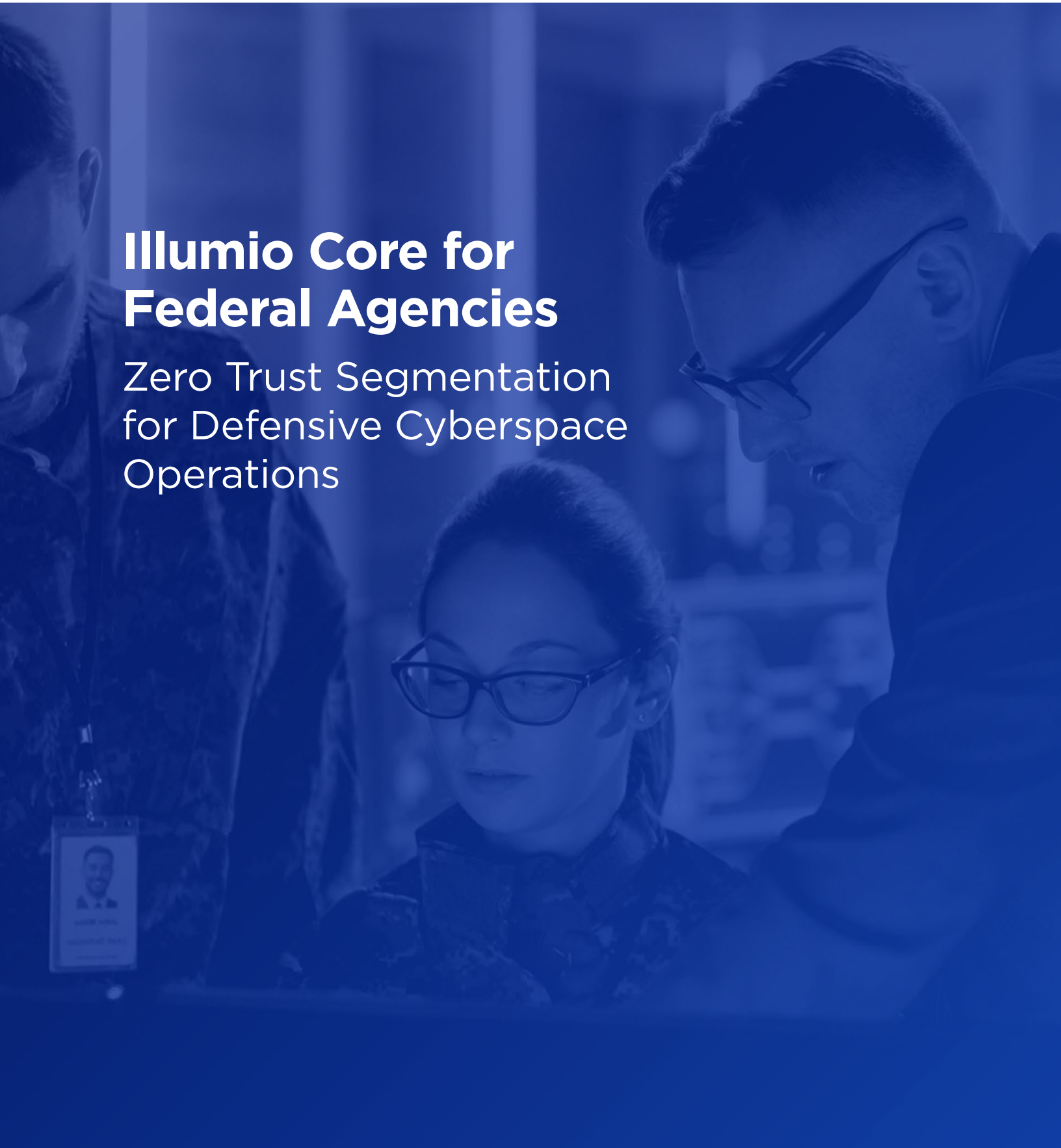
illumio

SOLUTION BRIEF



Illumio Core for Federal Agencies

Zero Trust Segmentation for Defensive Cyberspace Operations

The Zero Trust mindset assumes that breaches will occur and therefore focuses on eliminating automatic access to resources. Even internal network traffic cannot be trusted without prior authorization and authentication of the user, machine/device, and workload identity. Interest in Zero Trust among federal agencies has accelerated.

Several notable developments support this trend:

- August 2021: DISA Releases Request for White Papers (RWP) for Thunderdome Zero Trust Solution. The RFI is seeking a multi-vendor Zero Trust security stack. It specifically calls out 'the ability to provide micro-segmentation and prioritizing specific traffic flows.' It also states the requirement for 'preventing lateral adversary movement.'
- May 2021: The White House Executive Order on improving the nation's cybersecurity mandates that federal agencies adopt Zero Trust security and make plans to implement a Zero Trust architecture that aligns with NIST SP 800-207 guidelines.
- April 2021: The Defense Information Systems Agency (DISA) publishes the unclassified version of the DoD Zero Trust Reference Architecture 1.0.
- February 2021: DISA Zero Trust Reference Architecture released. It calls out designing from the 'inside-out' and a focus on critical data and resources to improve cyber resiliency and visibility. It specifically calls out micro-segmentation under the applications/workloads pillar to reduce the attack surface.
- August 2020: NIST released the final publication of SP NIST 800-207, which discusses the core logical components that comprise a Zero Trust architecture.
- July 2020: The Defense Information Systems Agency (DISA) and National Security Agency (NSA) announced a collaboration to release an initial Zero Trust reference architecture by the end of 2020.
- June 2019: DoD Digital Modernization Strategy (DMS) FY19-23 specifically referenced Zero Trust under DMS Appendix A: Technologies Offering Promise.

Benefits

- Accelerate Zero Trust visibility and enforcement for the data center, hybrid, multi-cloud endpoints, and containers to enable defensive cyberspace operations (DCO).
- Gain intelligent real-time visibility into application behavior with the application dependency map.
- Reduce the dynamic attack surface by continuously monitoring IP connections and integrating micro-segmentation with IT and security operations.
- Ensure Zero Trust at birth of new workloads and containers via integration of micro-segmentation with DevOps and container orchestration.
- Enable faster and less risky Zero Trust by avoiding the deployment of more hardware firewalls and re-architecture of networking infrastructure.
- Realize cost efficiencies by using the native enforcement points of your existing infrastructure investments.
- Enable Zero Trust on a global scale with PCE Supercluster.

Illumio Core Architecture Overview

Illumio Core™ delivers real-time application dependency mapping and micro-segmentation by programming the native Layer 3/Layer 4 firewall of each host. Illumio uses an allow-list model, which means that all traffic is blocked by default. A workload is allowed to connect with another workload only if there is an explicit rule that permits this traffic.

This approach prevents lateral movement of cyberattacks, obstructs ransomware, and enables Zero Trust across on-premises data centers, public clouds, private clouds, and containers. Visibility and micro-segmentation are core to Zero Trust and enable federal agencies to effectively achieve their DCO objectives.

Illumio Core is unique because its architecture allows you to use the enforcement points natively available in your compute environment — eliminating the need to re-architect your network and deploy more networking/SDN and data center firewalls to secure your micro-perimeters. Since policy creation does not require deep familiarity with networking constructs, you can empower different teams within your organization to create micro-segmentation policies while retaining governance over what gets provisioned.

Illumio Core comprises two main components:

Virtual Enforcement Node (VEN): The VEN is a lightweight agent installed in the guest OS of the host. The VEN is not in-line to traffic. It does not enforce firewall rules, nor does it route traffic. It performs two key functions:

- It collects and transmits telemetry data about each managed workload, such as its operating system, hardware, hostname, IP addresses, interfaces, processes, and flows, to the Policy Compute Engine (PCE). It also collects traffic data about workloads and devices connected to or attempting to connect with the managed workload. Each VEN functions as a point of visibility and a sensor that detects violations and changes in IP connections. This capability enables security to baseline an application's behavior, create rules to detect unauthorized connections and deviations from policies. In legacy or brownfield environments, VENs are continuously monitoring the environment for new connections, changes in IP address, and new attempts to connect and transmit this information to the PCE. This continuous monitoring helps ensure that the PCE is able to quickly detect changes and recalculate the applicable changes to the firewall rules. This enables the agency or command to maintain its segmentation posture, even as workloads move or new IP connections are added to the application environment. In greenfield environments, the VEN helps ensure that Zero Trust micro-segmentation policies are provisioned "at birth" for each new workload.
- It receives applicable firewall rules from the PCE and programs the host's native Layer 3/Layer 4 stateful firewalls. Illumio Core is OS-compute infrastructure agnostic and VENs can program supported operating systems (Windows, Linux, AIX, Solaris) and containers (Docker, Kubernetes, Red Hat OpenShift), as well as ACLs for switches (NEN), storage filers, and load balancers.

Policy Compute Engine (PCE): The PCE is the brain that continuously collects all the telemetry information from the VEN and 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 host's Layer 3/Layer 4 firewalls. The PCE can be deployed via Illumio's SaaS platform and in a virtual private cloud, including the customer's on-premises data center.

ILLUMIO CORE ARCHITECTURE

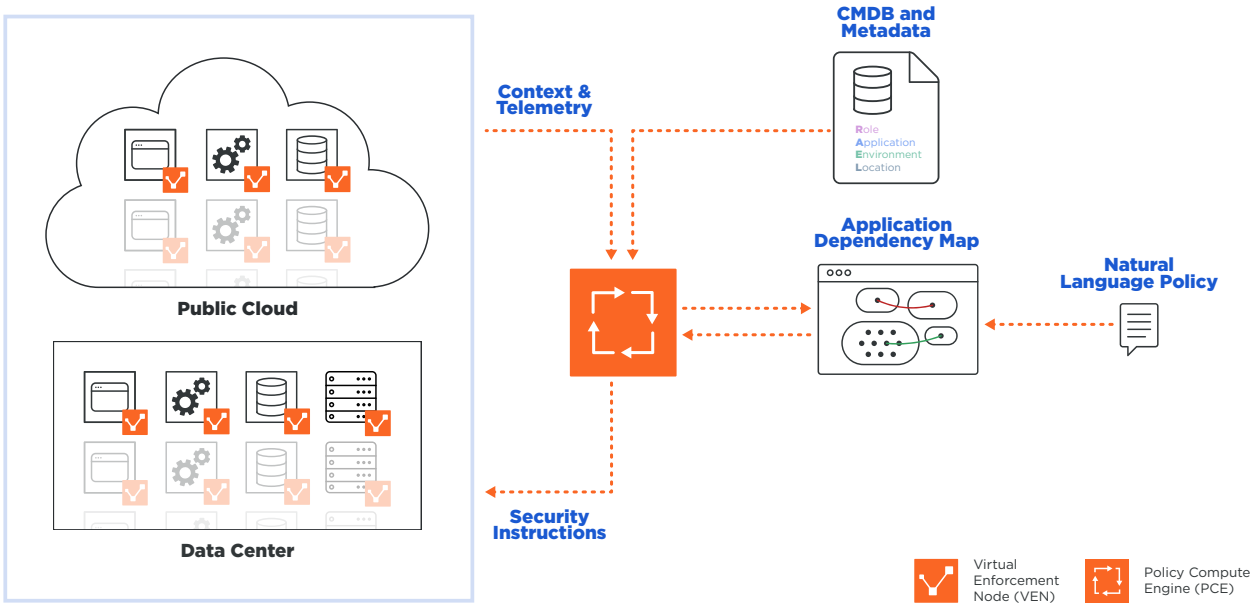


Figure 1

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 per data center. 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 number of workloads.

Key Features

Real-time application dependency map (Illumination)

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

A key tenet of Zero Trust is knowing what you need to protect. 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.

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 separation-of-duties (Figure 2).

ILLUMINATION VIEW IN BUILD MODE

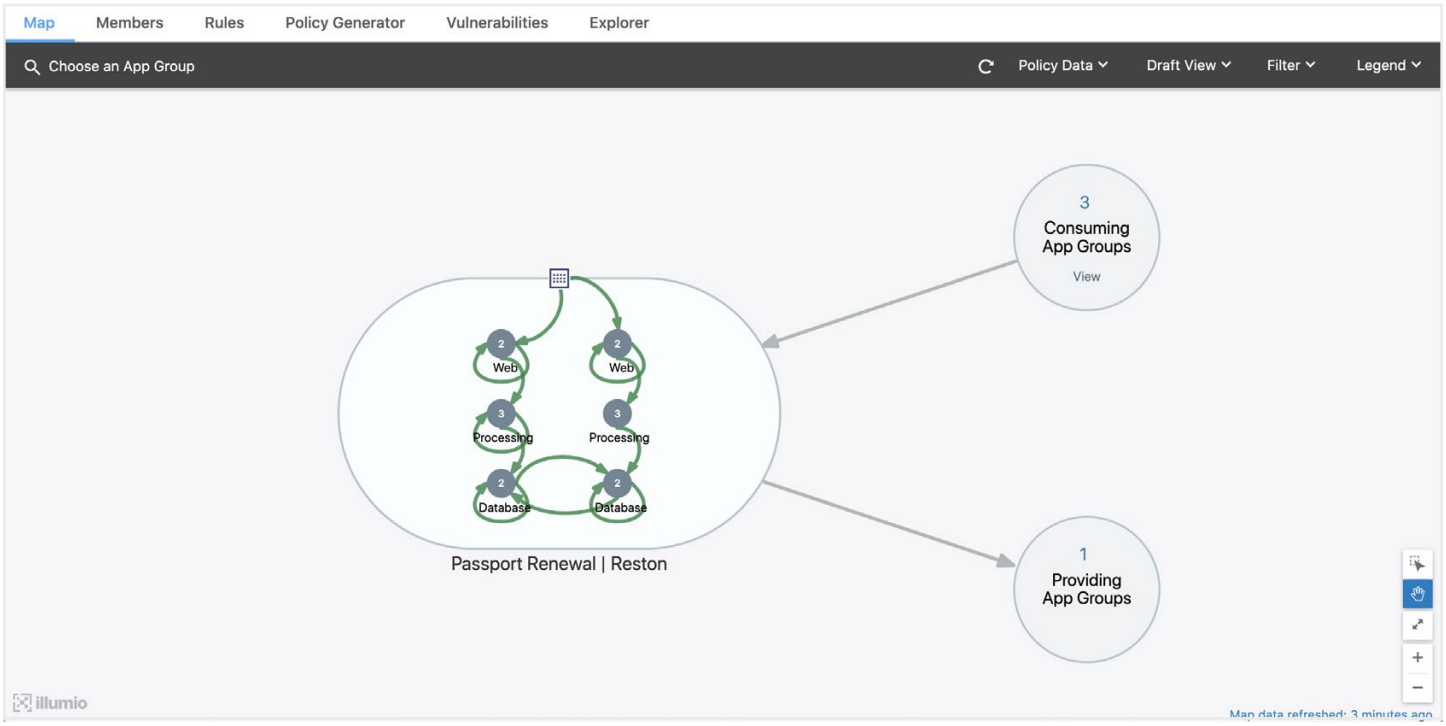


Figure 2

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 design and policy development while still giving you control over what gets approved and pushed into production. The authorized user can create policies without knowing networking constructs like IP addresses, subnets and VLANs, and keep track of the priority order of firewall rules (Figure 3).

POLICY GENERATOR

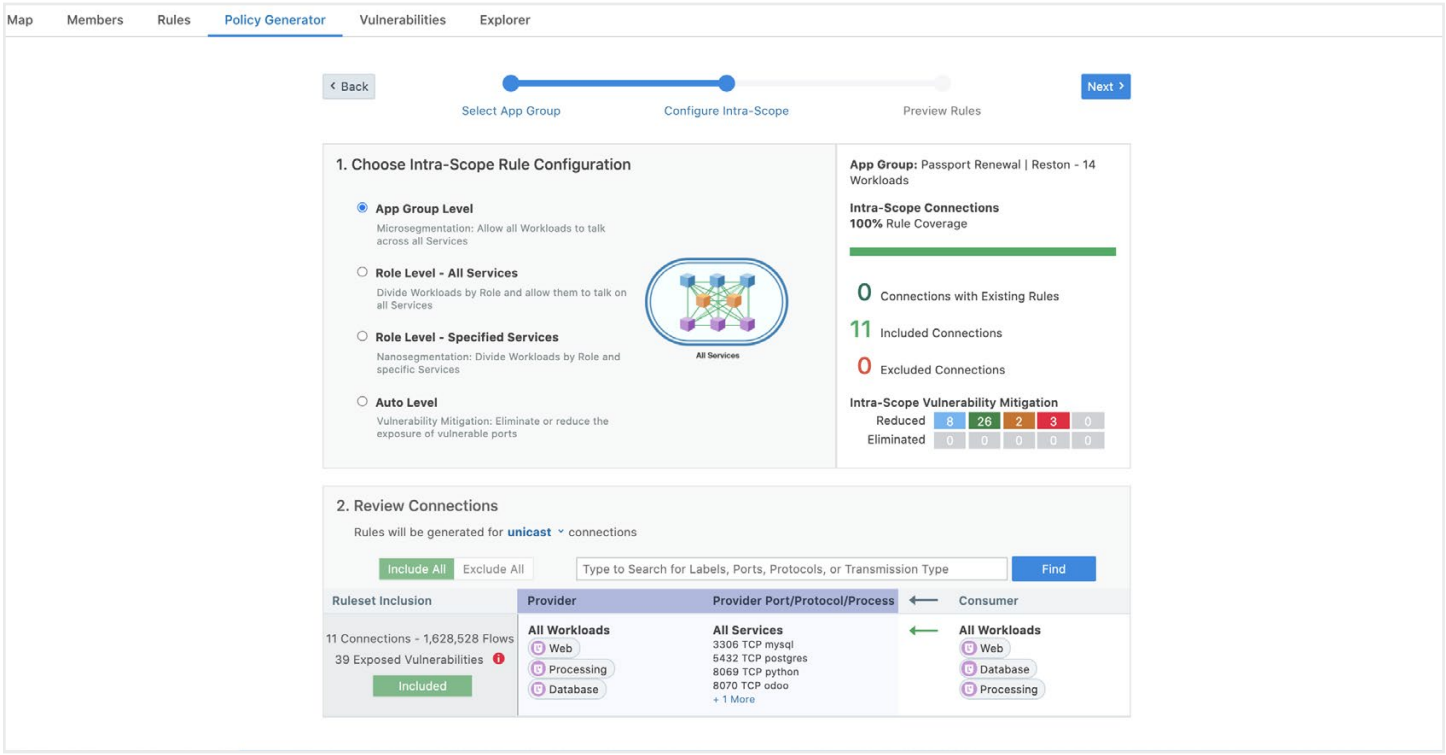


Figure 3

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).

VULNERABILITY MAP WITH EAST-WEST EXPOSURE SCORE

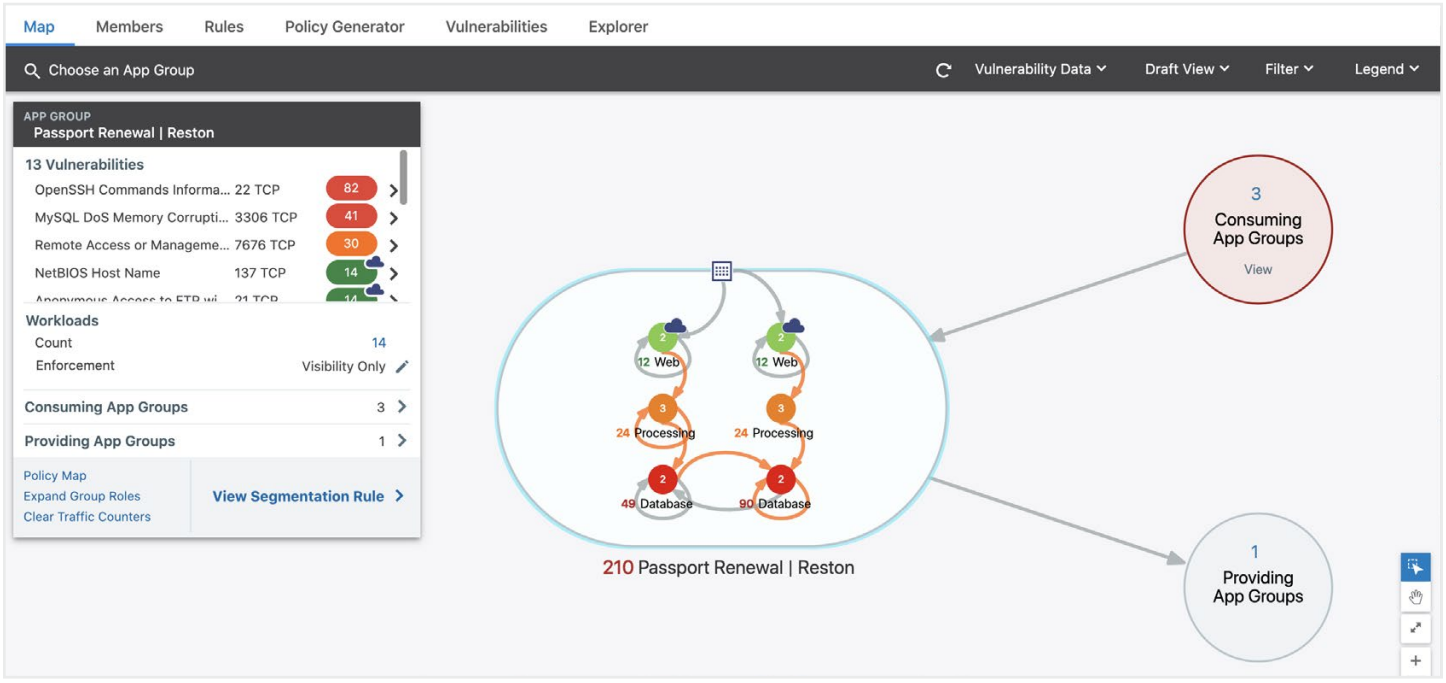


Figure 4

Role-based access control (RBAC)/app owner view

RBAC delivers security at enterprise scale by assigning users the least required privilege needed 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 to do their jobs while maintaining separation of duties for governance.

This means that you can assign what authorized users can see or do based on rules. For example, PCI application owners can see only the PCI environment and design the segmentation policies; security owners have a broader view of the environment and can review, approve, and provision the policies.

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 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. This feature is FIPS 140-2 validated.

FQDN-based visibility and enforcement

Rules based on Fully Qualified Domain Names (FQDN) provide visibility and explicitly define how legitimate traffic is allowed to flow between managed workload services such as SaaS, PaaS, or external registries.

FQDN-based rules also enhance visibility and control of container-to-container and container-to-server workload traffic. This capability enhances security by preventing IP address spoofing. Illumio Core will also dynamically conform policy to any changes, such as a domain name resolving to a new IP address.

RESTful API and connectors

Illumio Core offers robust APIs and plug-ins for key IT Ops, security operations, CMDB, CI/CD, and container orchestration platforms.

These integrations are useful for automating workflows that continuously maintain the Zero Trust segmentation posture, security incident response, and threat mitigation. Details on Illumio's ecosystem of partner integrations can be found at illumio.com/partners.

Illumio product documentation (docs.illumio.com) has a complete list and detailed description of all Illumio Core features.

Key Benefits

Illumio enables federal agencies to accelerate Zero Trust and achieve DCO objectives by delivering the following benefits:

Provides intelligent real-time visibility

- Enables the critical first step to Zero Trust, which is "knowing with precision, what you need to protect."
- Unified and comprehensive collection of traffic telemetry and event data across on-premises data center, public, hybrid and multi-cloud with both agent-based and agent-less approaches.
- Integration with IT systems of record and IT ops/cloud ops orchestration platforms to present traffic data with business context (Illumio Application Dependency Map) and enable governance of metadata and tags.
- Unlike network maps, which use IP addresses, hostnames, and networking constructs to describe workloads and traffic flows, Illumio's real-time application dependency map organizes and describes workloads and permitted connections in easy-to-understand language (location, application, role, and environment).
- Directly meets requirements in various federal security standards and best practices such as OMB 17-09, FISMA, NIST 800-53, NIST 800-171/CMMC, NIST 800-207, DoD Digital Modernization, and DHS CDM, which contain explicit policies to maintain an accurate map and inventory of in-scope resources.
- Continuous monitoring of workloads and their connections to maintain and validate the application flow maps and inventory of in-scope components.
- Governance of metadata and labels facilitates automation and orchestration of Zero Trust workflows for dynamic policy management and security operations, including threat hunting and incident response.

Reduces the dynamic attack surface

- Supports real-time and continuous evaluation and validation of Zero Trust posture. Illumio continuously monitors and transmits telemetry data, including blocked and failed attempts to connect, to validate the segmentation posture and recalculate the applicable firewall rules, if needed.
- In legacy or brownfield environments, integrates with IT operations and CI/CD operations so that firewall rules are able to keep up with change, provisioning, and release management. Illumio Core also integrates with SIEM and security operations.
- In greenfield environments, Illumio Core integrates with DevOps, CI/CD, and container orchestration platforms to ensure that segmentation is provisioned "at birth" of a new workload or container.
- Micro-segmentation contains the rapid propagation of ransomware and obstructs lateral movement attacks.

Enables faster implementation

- Accelerates and simplifies path to Zero Trust with automated enforcement of security policy across a small number of workloads to an entire organization.
- OS-compute infrastructure agnostic so that you can design and execute micro-segmentation to suit your data center design, size, and complexity — working across heterogeneous compute environments at any scale. A full list of supported platforms is available on the public Illumio product page.
- Integrates and co-exists with your existing networking, SDN and firewall investments, plus uses the enforcement points in your existing infrastructure investments. This combination saves you the management and cost overhead associated with re-architecting the networking and data center firewall environment, avoiding the need to deploy more hardware.
- Automated enforcement allows you to quickly get to enforcement and create a smart deny-list. This helps you avoid the operational risks, complexity and errors associated with firewall change management operations that rely on a combination of deny-lists and allow-lists.
- 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 used to evaluate the Information Assurance (IA) of IT products offered to the government by commercial vendors. For Illumio Core, 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 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 (DHS) Continuous Diagnostics and Mitigation (CDM) program includes cybersecurity tools and sensors reviewed by the program for conformance with Section 508, federal license users, and CDM technical requirements. Illumio Core directly meets the security capability requirements to manage assets (boundary protection and encryption), and supports the vulnerability management requirements.

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

- Find out why Illumio is the market leader in the Forrester Wave™: Zero Trust Platform eXtended Ecosystem Platform Providers, 3Q 2020: illumio.com/resource-center/research-report/forrester-wave-zero-trust-2020
- Operationalizing Zero Trust with Illumio: illumio.com/solutions/zero-trust

Illumio is a cybersecurity software company enabling end-to-end Zero Trust in Defensive Cyberspace Operations. The company helps agencies, commands, and organizations achieve Zero Trust and prevent attacker lateral movement by protecting high-value assets, critical applications, and workloads through real-time application dependency mapping, coupled with host-based micro-segmentation. Illumio is FIPS 140-2 validated and NIAP Common Criteria Protection Profile Certified. Illumio can be placed in multi-vendor hardware environments, using existing infrastructure to improve agencies' cybersecurity postures and effectively accomplish their missions.

Gartner peerinsights™

See what customers have to say about Illumio.

gartner.com/reviews/market/cloud-workload-protection-platforms/vendor/illumio