



# Mapping Illumio to NIST SP 800-207 Zero Trust Architecture

## Challenge

Relying on a perimeter network security approach is no longer an effective option for securing high value assets (HVAs). Attackers will always be one or more steps ahead. Attacks are increasingly sophisticated, and the goal is to stop the lateral movement of malware.

Federal agencies and commands are adopting Zero Trust as a strategy for securing their critical systems and HVAs. NIST announced the final publication of NIST Special Publication (SP) 800-207, which details the high-level architecture and core logical components of the Zero Trust architecture (ZTA).<sup>1</sup>

Organizations and federal agencies have existing infrastructure, network, and security investments, including software-defined networking (SDN) for coarse-grained segmentation and trust zones, perimeter firewalls, identity and access management, endpoint security, and other security tools. Most of these organizations and agencies have multi-cloud and hybrid cloud infrastructures where each application stack runs on different compute resources and is also geographically dispersed for resiliency. Automation and orchestration are everywhere. Using IP addresses to keep track of each workload's identities and Zero Trust boundaries will result in management and scalability issues if there is a mismatch between the ZTA approach and each agency's or organization's data center environment.

<sup>1</sup> [csrc.nist.gov/publications/detail/sp/800-207/final](https://csrc.nist.gov/publications/detail/sp/800-207/final)

## Key Benefits

Achieve end-to-end Zero Trust for Defensive Cyberspace Operations by:

- Providing real-time visibility
- Reducing the dynamic attack surface
- Enabling faster Zero Trust implementation

Design and execute a scalable, NIST 800-207-compliant Zero Trust architecture using host-based micro-segmentation



## Overview of Zero Trust Architecture Approaches

The appropriate Zero Trust architecture must consider each agency's and organization's current environment and desired future states. Understanding the various NIST-defined ZTA approaches and how they fit into current and desired future IT states is a critical first step in designing and executing a Zero Trust roadmap.

Figure 1 offers an overview of the three main ZTA approaches outlined by NIST.

OVERVIEW OF ZERO TRUST ARCHITECTURE POLICY ENFORCEMENT APPROACHES


Zero Trust Architecture	Description	Sample Vendor
<b>Enhanced Identity Governance</b>	Access policies are based on identity of actors and assigned attributes (device used, asset status, environmental factors). Essentially, an integrated ICAM and Endpoint Security solution.	Okta with MobileIron, MSFT Intune with Microsoft AD
<b>Software Defined Perimeter (SDP) Infrastructure</b>	SDP approach that applies SDN and intent-based networking concepts to enforce Zero Trust. Overlay network approach so that authorized users can only see cloud and data center resources that they are authorized to see (ZTNA).	Zscaler, Illumio Edge
<b>Micro-Segmentation</b> 		
<b>NGFWs, intelligent routers &amp; switches</b>	Uses intelligent switches, routers, NGFWs, and special purpose gateways to secure unique segments	VMware NSX, Palo Alto NGFW, Fortinet
<b>Host-based micro-segmentation</b>	Uses agents to program the native firewalls in each host or endpoint to design and enforce Zero Trust perimeters	Illumio Core, Cisco Secure Workload

Figure 1

Source: NIST SP 800-207, August 2020

Figure 2 summarizes the pros and cons of each approach.

#### ZERO TRUST ARCHITECTURE POLICY ENFORCEMENT APPROACHES- PROS VS. CONS

ZT Architecture	Pros	Cons
<b>Enhanced Identity Governance</b>	<ul style="list-style-type: none"> <li>• More granular control of traffic between authenticated users, devices, and applications</li> <li>• Device status and identity factor into access policies</li> </ul>	<ul style="list-style-type: none"> <li>• Does not address lateral movement attacks via server-to-server or server-to-container traffic</li> </ul>
<b>SDN &amp; Network Infrastructure</b>	<ul style="list-style-type: none"> <li>• More granular control of traffic between authenticated users, devices and applications.</li> <li>• Easier user experience (especially for remote workers)</li> <li>• Device status and identity factor into access policies</li> </ul>	<ul style="list-style-type: none"> <li>• User experience for hybrid remote work/ in-network use may be sub-optimal based on deployment model of the ZTNA solution</li> <li>• Does not address lateral movement attacks via server-to-server or server-to-container traffic</li> </ul>
<b>Micro-Segmentation</b>		
 <b>NGFWs, intelligent routers &amp; switches</b>	<ul style="list-style-type: none"> <li>• Technology is well understood by firewall and network engineers</li> <li>• Extra services can be deployed (e.g., IPS, URL filtering, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>• Management of large number of rules can be complex and encourage mistakes</li> <li>• A virtual or distributed firewall is required for each host</li> <li>• Lack of visibility</li> <li>• Large deployments can be expensive</li> <li>• Granular micro-segmentation is very complex</li> </ul>
<b>Host-based micro-segmentation</b>	<ul style="list-style-type: none"> <li>• Decoupled from the network architecture</li> <li>• Simple to deploy</li> <li>• Easily scalable</li> <li>• Easily deployed in any architecture (cloud, containers, bare-metal, etc.)</li> <li>• Offers agent-based and agentless visibility across hybrid IT, multi-cloud/ hybrid cloud from a single control plane</li> <li>• OS-compute and network fabric agnostic.</li> <li>• Enables security to decouple from the networking architecture.</li> </ul>	<ul style="list-style-type: none"> <li>• Agent deployments can be a big task</li> <li>• Agent trust</li> <li>• Rule scale</li> </ul>

Figure 2

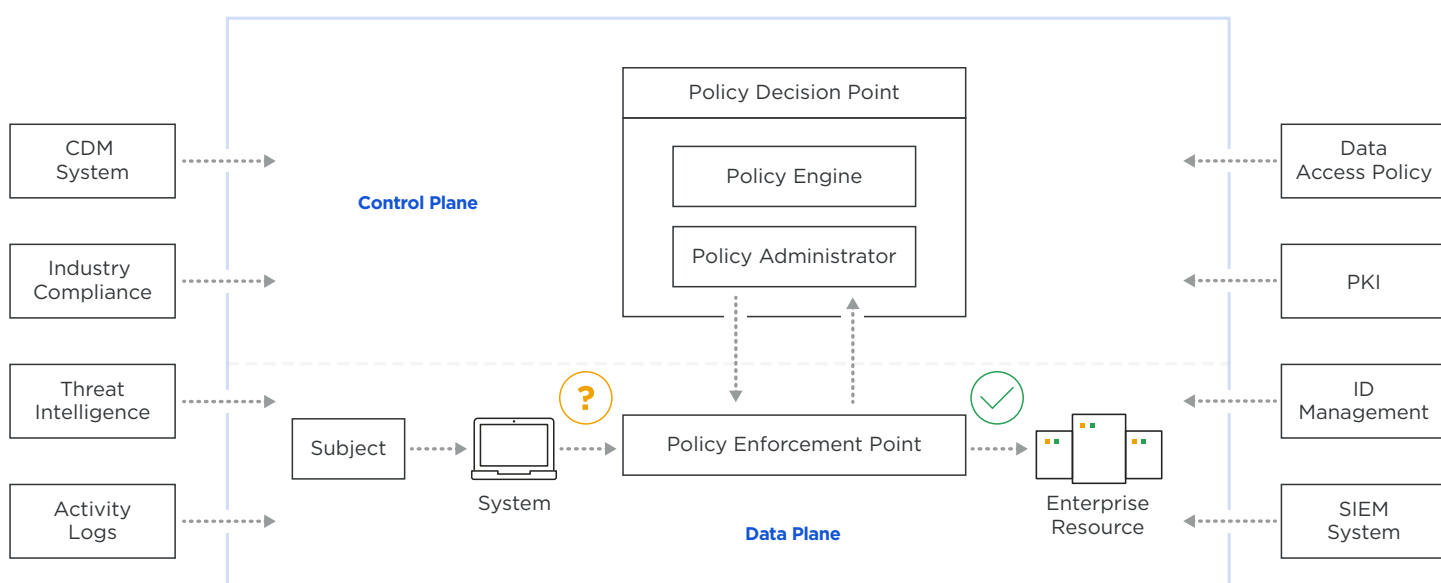
## Overview of NIST SP 800-207 ZTA Logical Components

Regardless of the approach and the deployment model, NIST SP 800-207 has identified the core logical components of a Zero Trust architecture.

The ZTA logical components describe the critical capabilities necessary to operationalize Zero Trust across an agency's environment. The components include capabilities that enable the creation and management of Zero Trust perimeters and policies and support continuous monitoring and enforcement of a Zero Trust posture.

Figure 3 shows a conceptual overview of the logical components and how these interact.

## OVERVIEW OF THE ZERO TRUST ARCHITECTURE LOGICAL COMPONENTS



According to NIST SP 800-207, the three main logical components of the Zero Trust architecture are:

Policy engine (PE): This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.

Policy administrator (PA): This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service; here, it is divided into two logical components. The PA communicates with the PEP when creating the communication path. This communication is done via the control plane.

The policy engine and policy administrator make up the Policy Decision Point (PDP).

Figure 3



**Policy enforcement point (PEP):** This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA.

In addition to the core logical components, there are a multiple third-party systems that provide input and policies that are fed into the policy engine that influence the access decisions. SP 800-207 offers a description of these various sources of policy information which include CDM, GRC and industry compliance, IAM/PKI, SIEM, and more.

Source: NIST Special Publication 800-207, August 2020

## Technical Solution: Mapping Illumio to the Zero Trust Architecture

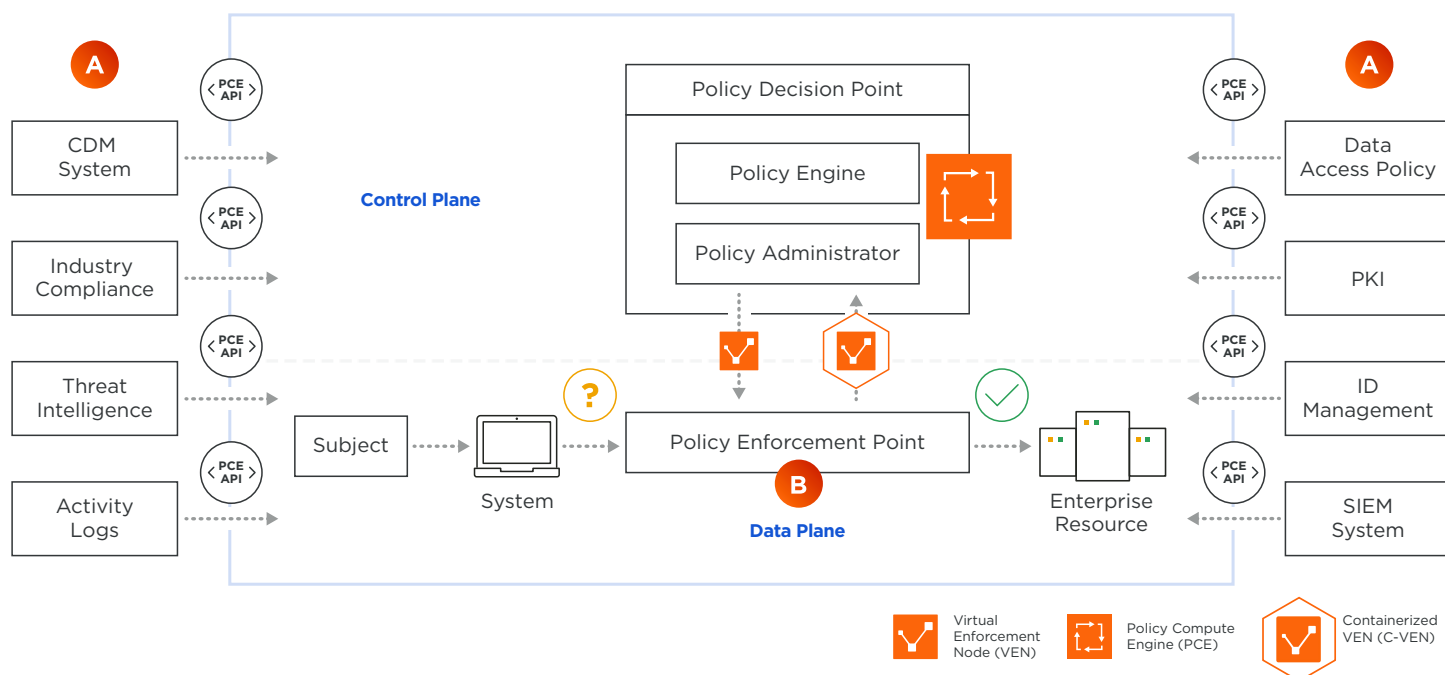
Illumio enables a scalable Zero Trust architecture via host-based micro-segmentation. Illumio delivers real-time visibility into application dependencies and connections and using this information and contextual information from other systems to design and execute the applicable Zero Trust boundaries. These boundaries are enforced by programming the native Layer 3/Layer 4 firewalls of each workload.

Illumio is OS compute-infrastructure agnostic, so the Illumio agent (VEN) can be deployed on-premises (bare-metal and virtualized workloads), in public and private clouds, and containerized hosts. In addition, Illumio integrates with storage filers, switches, routers, and firewalls to program ACLs.

Illumio directly maps to the core logical components of the Zero Trust architecture.

Figure 4 offers a high-level mapping of the Illumio components to the NIST SP 800-207 Core Zero Trust Logical Components.

### MAPPING ILLUMIO COMPONENTS TO THE ZERO TRUST ARCHITECTURE LOGICAL COMPONENTS



**A** Policy Information Points are external feeds that send policy and contextual information to the Policy Engine

**B** Host native stateful firewalls, load balancers, and switch ports

Figure 4

The Illumio products (Illumio Core and Illumio Edge) are comprised of two major components:

- Policy Compute Engine (PCE) – The PCE is the central manager for visibility and micro-segmentation policies.
- Virtual Enforcement Node (VEN) – The VEN is a lightweight agent installed in the host of each workload that Illumio will manage. The VEN collects telemetry data about each host, which the PCE uses to translate and calculate policies into the applicable firewall rules. The VEN also takes the firewall rules calculated by the PCE and uses these to program the native Layer 3/Layer 4 stateful firewall rules for each managed workload. For example, in Linux OS, the VEN programs the iptables, and in Windows OS, it programs Windows Filtering Platform (WFP). The firewall rules define the allowed inbound and outbound connections to each managed workload.

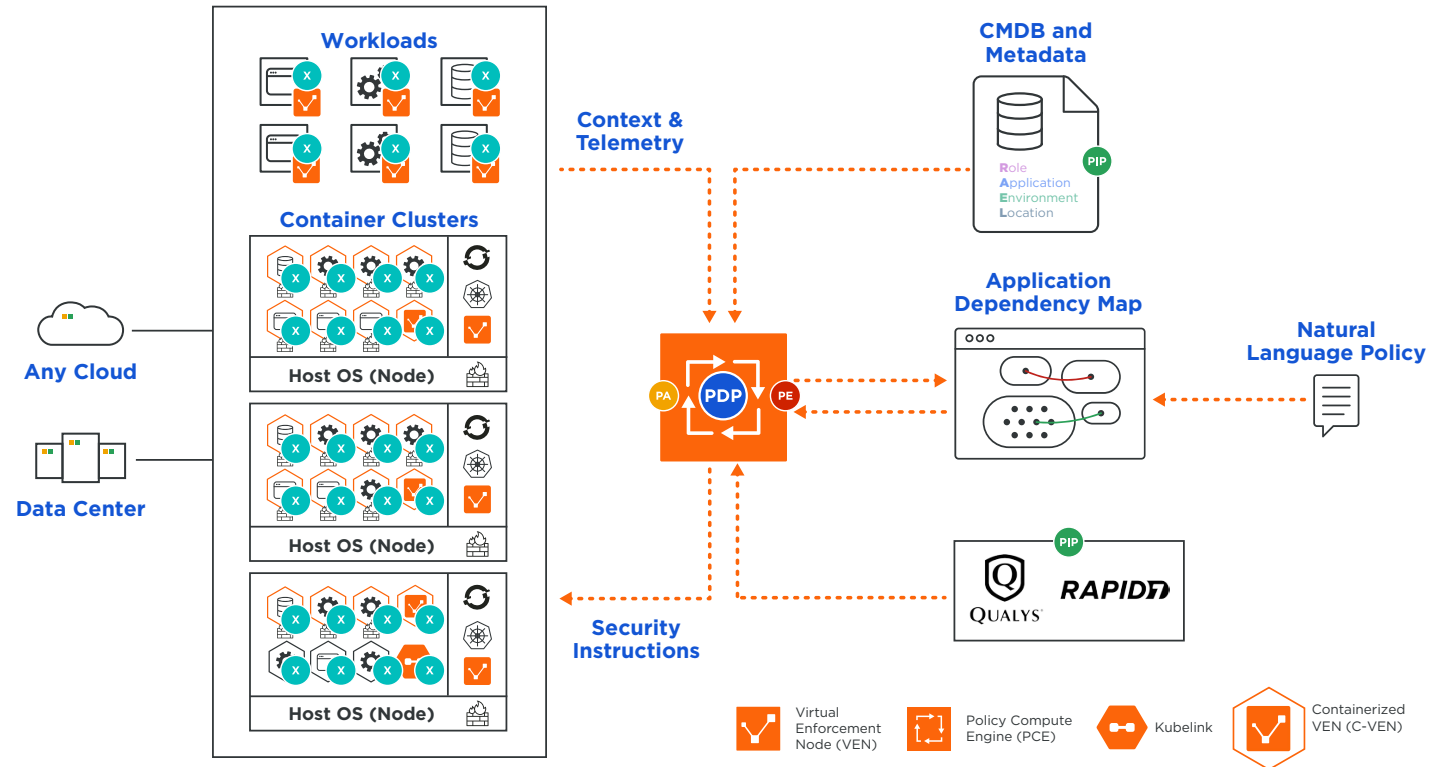
Illumio operates under an “allowlist” model. If there is no “allow” rule for a specific outbound or inbound connection between servers or workloads, that specific traffic is not allowed to proceed.

## Mapping NIST 800-207 ZTA Logical Components to Illumio Software Architecture

ZTA Core Components	Illumio Components	Description
Policy Decision Point (PDP)	Policy Compute Engine	The PCE is the “brain” of Illumio. The PCE offers a workflow to design Zero Trust policies, create Zero Trust perimeters, and enforce Zero Trust boundaries. Enterprise RBAC controls the authorized individuals that can see traffic, design policies, and provision/approve Zero Trust. This ensures enterprise segmentation and governance.
Policy Engine (a component of the PDP)	Policy Compute Engine	The PCE takes the real-time telemetry data from the VEN and uses it to calculate the rules that would allow or deny traffic connection (access) to a workload. For example, if the VEN detects a change in IP address or a new connection attempt, the PCE will calculate the applicable action (example: deny traffic).
Policy Administrator (a component of the PDP)	Policy Compute Engine	This part of the PCE uses the real-time telemetry and contextual data and the rules calculated to eventually transmit to the VENs if the applicable firewall rules have been updated. The VEN takes the instructions from the PCE to program each host IP tables (Linux/Aix/Solaris) or WFP (Windows).
Policy Enforcement Points (PEP)	Host native firewalls (iptables or Windows Filtering Platform) ACLs (load balancers, switch ports, storage filers)	In Illumio, the PEP is the local stateful (Layer 3/Layer 4) firewall already installed within the host operating system. Every system is an inbound and outbound Policy Enforcement Point. Communication between the PCE (PDP) and the host-based firewalls and ACLs (PEP) are done via the control plane.

Figure 5 shows the visual mapping of Illumio Core to the NIST Zero Trust Architecture logical components.

#### MAPPING ILLUMIO CORE TO ZERO TRUST ARCHITECTURE LOGICAL COMPONENTS



**PDP** Policy Decision Point (PDP): Processes the authorization request and evaluates it against the organization's access policies. The PDP is made up of the Policy Engine (PE) and Policy Administrator (PA). In Illumio, the PDP is the Policy Compute Engine, which implements the local policy on the host. It includes policy creation and governance. The PCE then distributes the policy to the VENs for implementation into the Policy Enforcement Points.

**PE** Policy Enforcement Point (PEP): In Illumio, the PEP is the local stateful (L3/L4) firewall already installed within the host operating system. Every system is an inbound and outbound PEP.

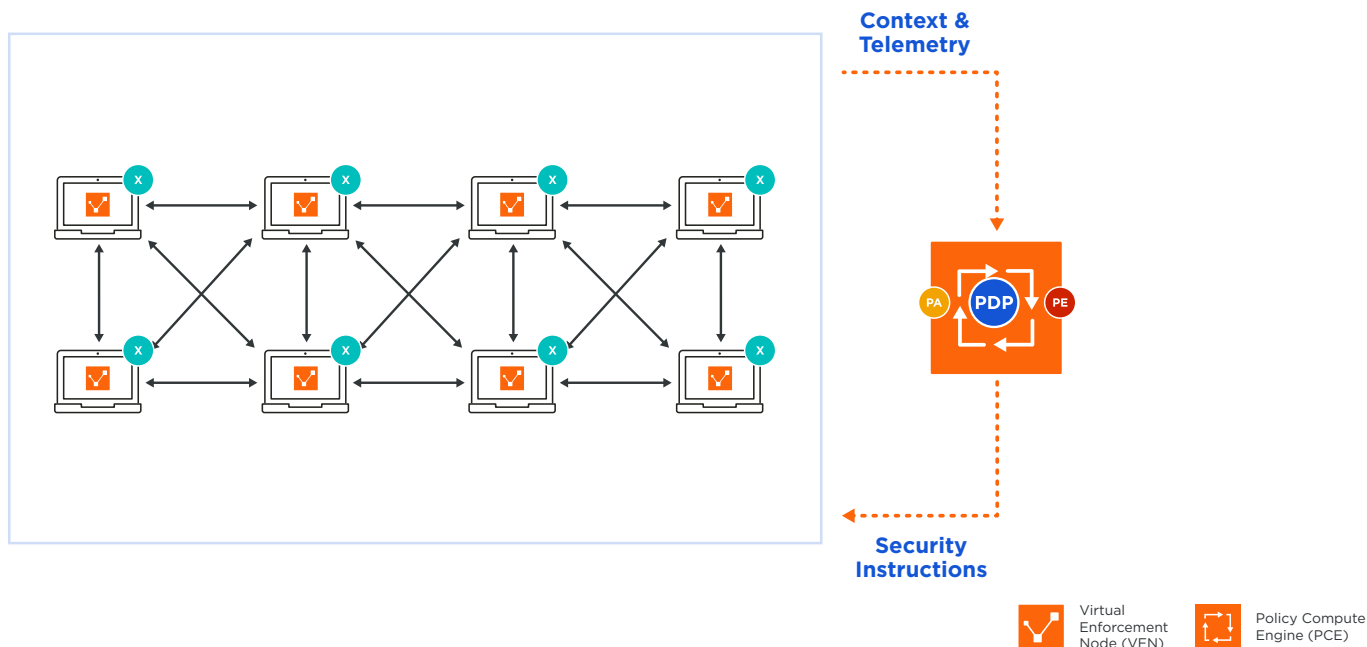
**PIP** Policy Information Point (PIP): In Illumio, the PIP is the PCE API which has native integrations with ServiceNow and other CMDBs as well as authentication, EPP, SIEM, firewalls, and NAC that provide input and policy rules used by the PE when making access decisions.

Figure 5



Figure 6 shows the mapping of Illumio Edge.

#### MAPPING ILLUMIO EDGE TO ZERO TRUST ARCHITECTURE LOGICAL COMPONENTS



**Policy Enforcement Point (PEP):** Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA.

In Illumio, the PEP is the local stateful (L3/L4) firewall already installed within the host operating system as well as user identity and machine identity. Every system is an inbound and outbound PEP.

**Policy Decision Point (PDP):** Processes the authorization request and evaluates it against the organization's access policies. The PDP is made up of the Policy Engine (PE) and Policy Administrator (PA) .

In Illumio, the PDP is the Policy Compute Engine, which implements the local policy on the host. It includes policy creation and governance. The PCE then distributes the policy to the VENs for implementation into the PEP.

Figure 6

## Conclusion

Illumio enables agencies and commands to achieve end-to-end Zero Trust via host-based micro-segmentation. The Illumio software architecture directly maps to the core logical components defined in NIST SP 800-207. A host-based micro-segmentation approach enables agencies and commands to plan and deploy Zero Trust that scales across multi-cloud and heterogeneous OS compute infrastructure. Illumio's analysis and decision (PDP) is not in line to traffic – it does not impact application performance. Since host-based micro-segmentation is decoupled from networking constructs, you do not have to re-architect your network or SDN.

## 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 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 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 (DHS) 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 Core directly meets the security capability requirements to manage assets (boundary protection and encryption), and supports the vulnerability management requirements.



**Homeland  
Security**

### 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.







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.



See what customers have to say about Illumio.

[gartner.com/reviews/market/cloud-workload-protection-platforms/vendor/illumio](https://gartner.com/reviews/market/cloud-workload-protection-platforms/vendor/illumio)

The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085, Tel (669) 800-5000, [illumio.com](https://illumio.com). Copyright © 2021 Illumio, Inc. All rights reserved. This document is protected by U.S. and international copyright and intellectual property laws. Illumio's products and services are protected by one or more U.S. and international patents listed at [illumio.com/patents](https://illumio.com/patents). Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. To review a list of Illumio's trademarks, go to [illumio.com/trademarks](https://illumio.com/trademarks). Third-party trademarks mentioned in this document are the property of their respective owners.