illumio

TECHNICAL BRIEF

Illumio Core

Quickly build your organization's cyber resilience with Zero Trust Segmentation across your clouds, data centers and endpoint devices

Innovation at a Glance

With Illumio, you can isolate ransomware, build your cyber resilience and prevent breaches from turning into cyber disasters.

- **Automated security enforcement:** Immediately enforce allow/deny-list rules.
- **Real-time view of application communications:** Easily see all your traffic flows and understand their potential risks.
- **Multi-cloud security at scale:** Continuously enforce workload security across clouds or data centers.

Architectural Overview

With Illumio Core, you can streamline your path to building Zero Trust security to defend your organization against today's growing security threats.

Illumio Core delivers industry leading micro-segmentation that provides unified visibility and allow/deny-list controls.

Illumio Core includes the following components:

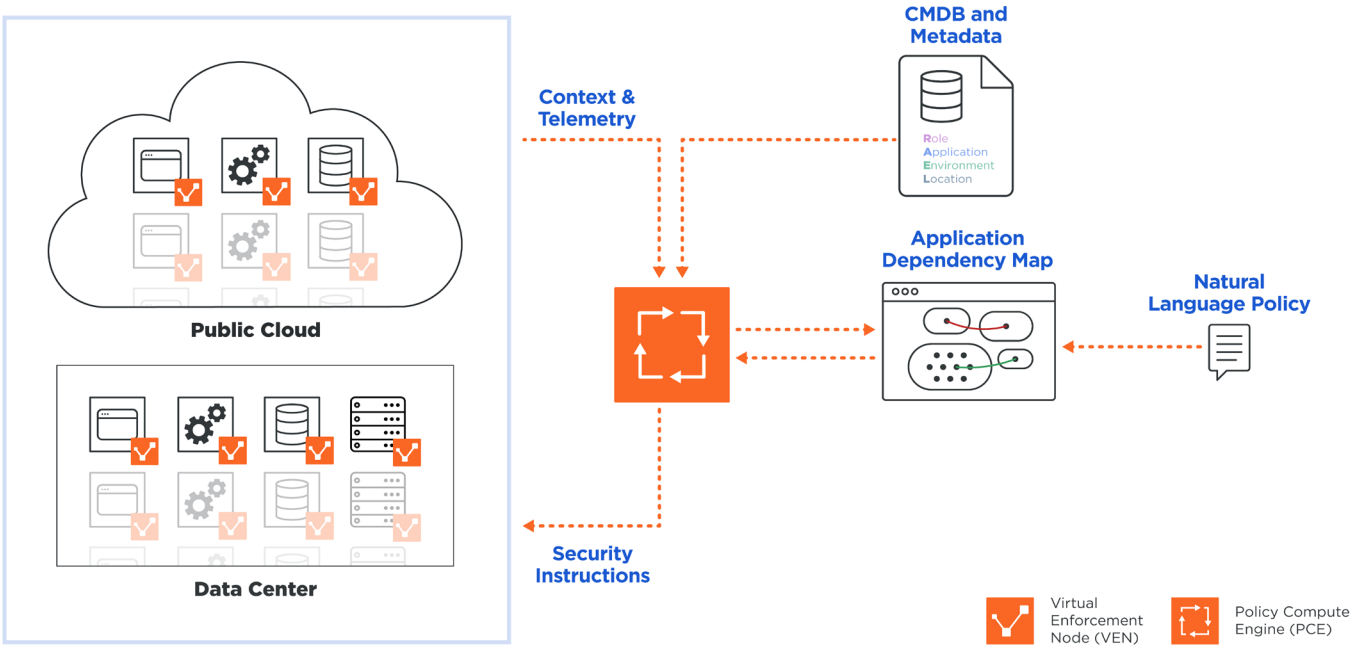
Policy Compute Engine (PCE)

The PCE is the Illumio management console and segmentation controller. It continuously collects telemetry information from the VEN, providing real-time mapping of traffic patterns and recommending optimal allow-list rules based on contextual information about the environment, workloads and processes.

Virtual Enforcement Node (VEN)

The VEN is a lightweight agent that is installed in the guest OS of a host or endpoint. It collects flow and metadata information and transmits these to the PCE. It also receives the firewall rules from the PCE to program the managed host's native stateful L3/L4 firewalls. Critically, the Illumio VEN is not inline to traffic. It does not enforce firewall rules or route traffic.

ILLUMIO CORE ARCHITECTURE



Agent-Less Visibility and Segmentation Enforcement

In environments where agents are not deployed (such as legacy systems, IoT/OT and cloud objects like AWS RDS), Illumio Core ingests flow data from networking equipment (routers, switches, load balancers), cloud object metadata, cloud native security group information and flow logs.

This combined telemetry provides a unified map of the communication flows across your digital infrastructure.

To segment, Illumio programs the ACLs (access control lists) of routers, switches and load balancers. And for cloud traffic, it recommends and programs policies to optimize native-cloud security groups.

Critical Capabilities

Illumination

Illumination delivers real-time visual insights into your application communication flows. This information helps you understand critical pathways, detect anomalous behavior, build segmentation policies and test rules before enforcing segmentation rules.

Core Services Detector

Core Services Detector uses machine learning to quickly identify security-critical infrastructure services like domain controllers and load balancers, then recommends labels and Zero Trust Segmentation policies to secure legitimate traffic.

Enforcement Boundaries

Enforcement Boundaries offer guided workflows, visualization and reporting to help organizations safely and efficiently transition from an allow/deny-list firewall rules approach to a true allow-list model — avoiding the complexity of managing the priority order of firewall rules at scale.

Policy Generator

Policy Generator uses flow history to create and recommend optimal segmentation policies for application workloads, regardless of the location or type of workload. Create policies without knowing networking constructs like IP addresses, subnets and VLANs, as well as easily keeping track of the priority order of firewall rules.

Explorer

Use Explorer to query the historical traffic database in the PCE to analyze traffic patterns. Generate reports for auditing, threat hunting, troubleshooting and creating allow-list rules.

Vulnerability Maps

Vulnerability Maps combine application dependency maps with vulnerability data from vulnerability scanning tools. Gain a detailed understanding of potential pathways for lateral movement by malware and hackers. Apply vulnerability-based segmentation to limit the spread of breaches.

SecureConnect

SecureConnect supports on-demand, 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. It is FIPS 140-2 validated.

Product Specification and Attributes	Description
VEN Operating System (OS Support for Servers)	AIX, Amazon Linux, CentOS, Debian, Oracle Linux-Red Hat Kernel, Oracle Linux-UEK Kernel, Red Hat Enterprise Linux (RHEL), Rocky Linux, SUSE Linux Enterprise Server, Scientific Linux, Solaris, Ubuntu, Windows
VEN Operating System (OS Support for Endpoints)	Windows 7 and 10, wired or wireless interfaces, domain-joined (corporate) and non-domain-joined (private) interfaces
Container Orchestration Platforms	Kubernetes, IBM Cloud Kubernetes Services (IKS), Rancher Kubernetes Engine (RKE), OpenShift
Vulnerability Maps-supported third party integrations	Qualys, Rapid 7, Tenable
Supported Internet DNS Protocols	IPv4, IPv6, FQDN
Supported 3rd Party IT/SecOps integrations	Illumio Core offers **robust APIs/plug-ins** for IT/SecOps, CMDB, CI/CD and container orchestration.

Detailed Illumio Core product information can be found on **docs.illumio.com**.

Illumio Core offers both an on-premises and cloud deployment option. Illumio provides an uptime Service Level Agreement (SLA) of 99.8% for Illumio Core Cloud. For information about the SLA, see the Illumio Master Subscription Agreement (**www.illumio.com/eula**).

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.