illumio

TECHNICAL BRIEF

Illumio Architecture

Quickly build your cyber resilience with Zero Trust Segmentation (ZTS) across your cloud, data center, and endpoint devices

Architectural Overview

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

Illumio delivers industry-leading Zero Trust Segmentation that provides unified visibility and network controls. Illumio includes the following two 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 allowlist 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.

Innovation at a glance

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

Automated security enforcement

Immediately enforce allow/denylist rules.

Real-time view of application communications

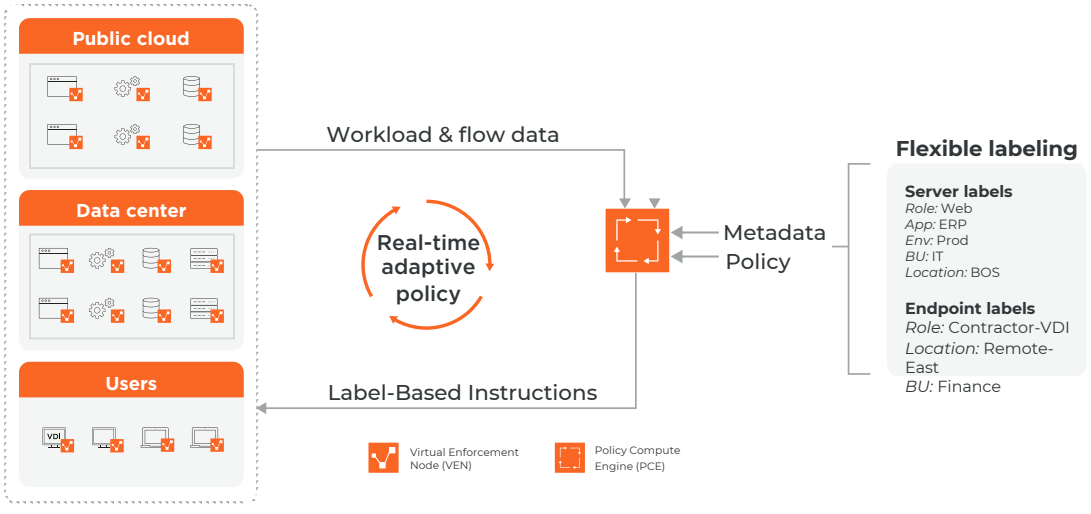
Easily see all your traffic flows and understand their potential risks.

Multi-cloud security at scale

Continuously enforce workload security across clouds or data centers.

Control endpoint traffic

Non-domain support empowers you to roll out segmentation beyond the traditional network perimeter.



Agentless Visibility and Segmentation Enforcement

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

This 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, it recommends and programs policies to optimize cloud-native security groups.

Critical Capabilities

Application dependency maps

Visualize real-time insights into application communication flows. This helps you understand critical pathways, detect anomalous behavior, build segmentation policies, and test rules before deploying them.

Allow and deny rules

Easy-to-write rules using natural language help organizations safely and efficiently progress towards ZTS while avoiding the complexity of traditional models.

Policy generator

Flow history is used to create and recommend optimal segmentation policies for workloads, regardless of the location or type. Create policies without knowing networking constructs like IP addresses, subnets, and VLANs.

Non-domain support

Illumio's segmentation is not tied to the network. Thus, policy can be applied wherever a device is located. Policy is automatically updated based on the location of the device for optimum segmentation coverage.

Vulnerability maps

Vulnerability maps combine ZTS with vulnerability data from scanning tools. Gain a detailed understanding of potential pathways for lateral movement by malware and hackers.

Workload-to-workload encryption

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.

Product Specifications

Platform support

- The Illumio VEN runs on Windows, macOS, and Linux. With broad version support, Illumio can provide coverage in virtually any environment.
- Segment agentless workloads with Illumio CloudSecure and Network Enforcement Nodes (NEN).
- Support container deployments through Illumio's containerized VEN for major orchestration platforms such as Kubernetes and OpenShift.

For an up-to-date list of supported operating systems and containers, see support.illumio.com.

Technical integration

Illumio teams with the leading software, infrastructure, and security companies to deliver integrated and interoperable solutions that support your Zero Trust strategy. Find out about our latest integrations at illumio.com/partners/tap.

Detailed Illumio product information can be found at docs.illumio.com.

Illumio offers both on-premises and cloud deployment options. Illumio provides an uptime Service Level Agreement (SLA) of 99.8% for Illumio Core, Endpoint, and Edge SaaS PCE. For information about the SLA, see the Illumio Master Subscription Agreement at illumio.com/eula.

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.