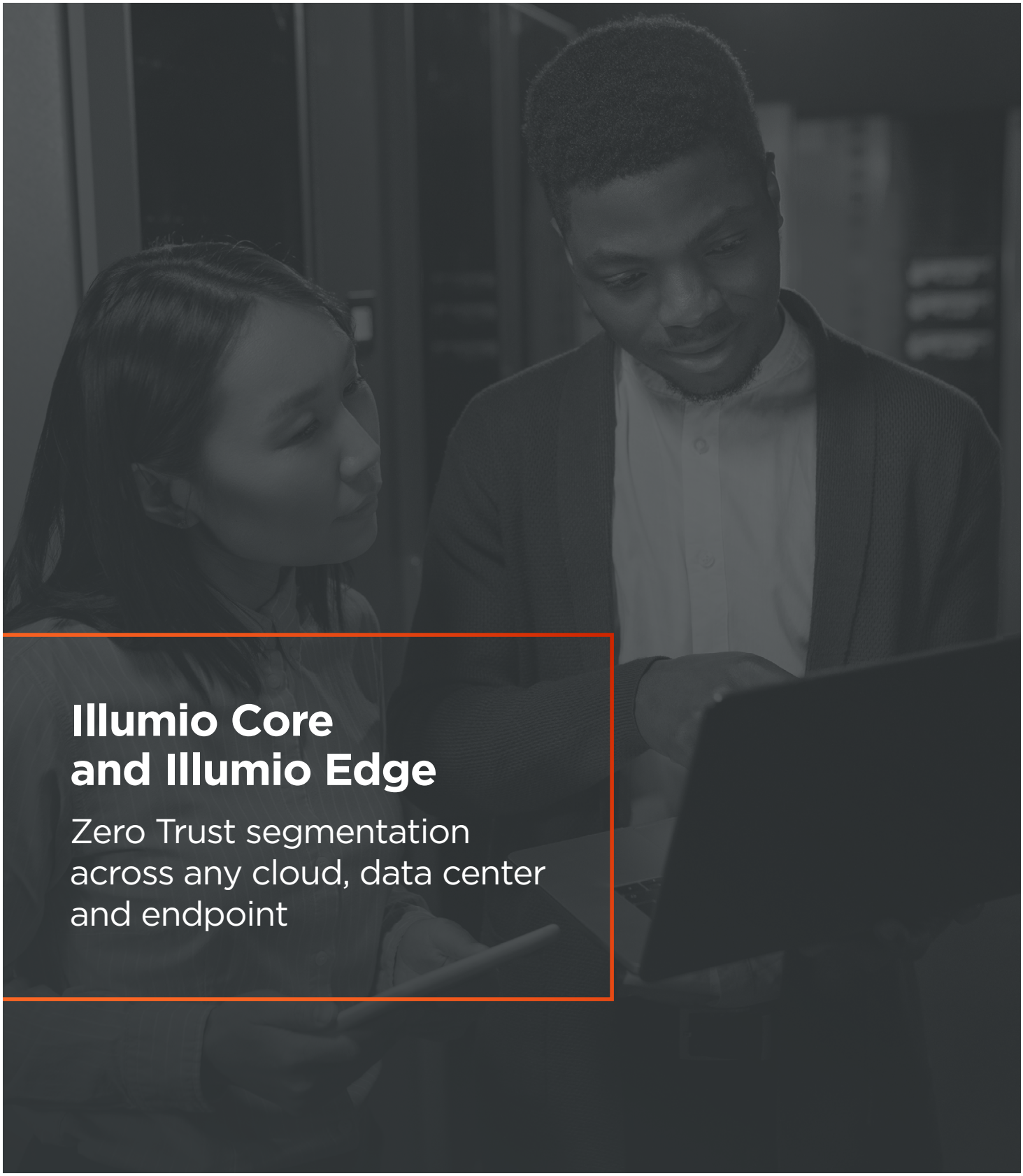
illumio

PRODUCT BRIEF



Illumio Core and Illumio Edge

Zero Trust segmentation across any cloud, data center and endpoint

Stop Lateral Movement With Modern Segmentation

As cybercrime skyrockets, organizations must focus on preventing the lateral movement of security threats across their data centers and endpoint devices.

Illumio Core and Illumio Edge prevent lateral movement, effectively stopping the spread of ransomware, viruses and cybercriminals by applying Zero Trust controls to your applications, containers, clouds, data centers and endpoints.

Illumio's approach to Zero Trust delivers comprehensive visibility into application dependencies and provides the automated segmentation needed to reduce your attack surface, contain cyberattacks and protect critical assets.

Illumio Core

Simplify and speed your path to Zero Trust segmentation in the data center

With Zero Trust segmentation in place (also known as micro-segmentation), organizations can effectively limit lateral movement in the data center, helping protect high-value assets and meet regulatory requirements.

Critically, Illumio Core helps you progressively and safely build policies to segregate and protect your data center resources without being constrained by rule ordering. This lowers costs by simplifying policy implementation and reducing disruption.

Key Benefits

Gain visibility across your data center, cloud platforms and endpoint devices.

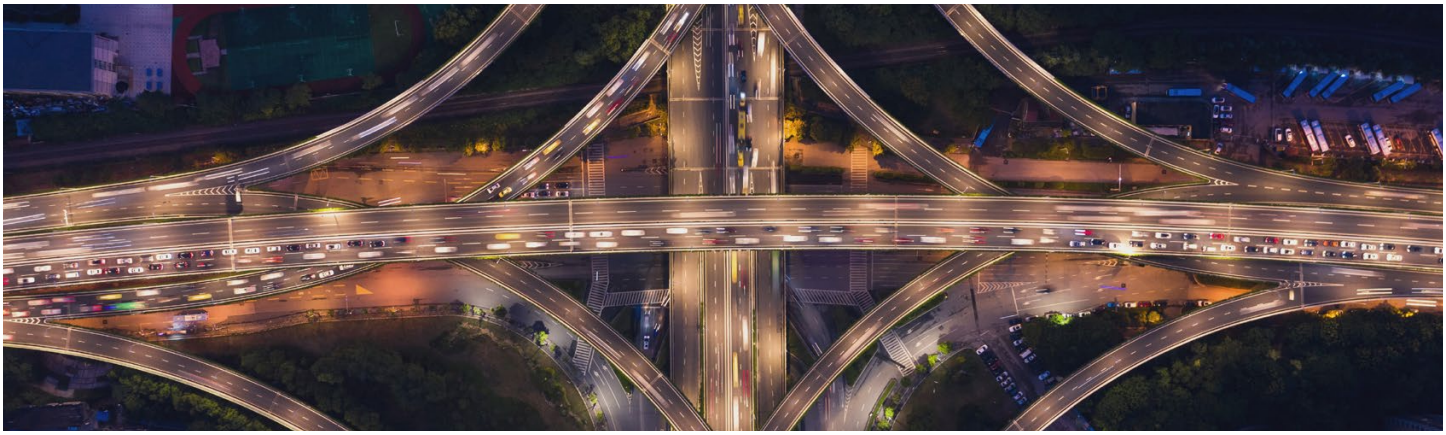
Segment in minutes and accelerate your Zero Trust initiatives with simplified policy generation and automated enforcement.

Stop ransomware and contain cyberattacks by enforcing security consistently and at scale across your data center, cloud platforms and endpoint devices.

Ensure uniform least-privilege access between endpoints and applications, whether users are connecting on a campus network or through a VPN.

Model and test policies before going into enforcement to avoid breaking applications and disrupting business operations.

Lower costs by making it easy to collaborate across network, security, risk and DevOps teams to accelerate policy deployment.



illumio

Illumio Core provides key advantages in developing your Zero Trust segmentation capabilities.

Gain Intelligent Visibility

Use a real-time application dependency map (Illumination) to visualize communications between workloads and and applications. Gain insights on these dependencies to build your segmentation policies. Security teams can use the map in "visibility mode" to test policies, ensuring enforcement won't break applications. (Figure 1)

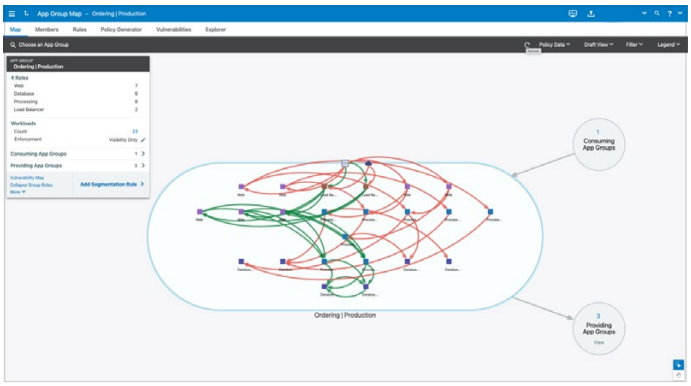


Figure 1

Simplify Policy Creation

Segment applications in minutes using an automated segmentation policy creation workflow (Illumio Policy Generator) that allows you to define the level of granularity needed. This saves critical time, accelerates security workflows, and reduces the risk of human error. (Figure 2)

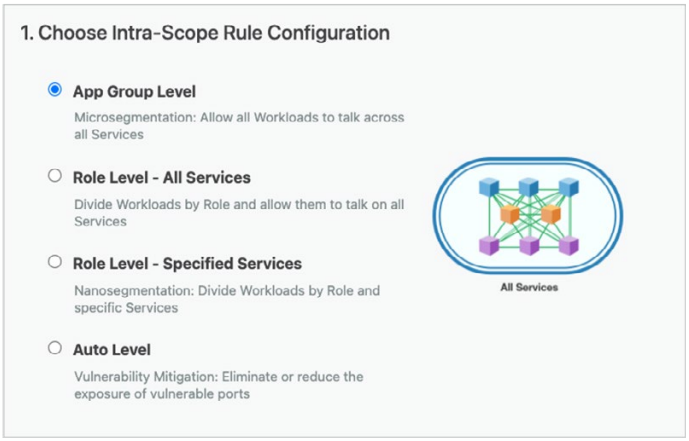


Figure 2

Build Enforcement Progressively

While creating a full list of allow-rules is the ultimate objective for Zero Trust segmentation, Illumio Enforcement Boundaries allow you to progressively build simple policies by selectively enforcing restrictions on specific workloads — free of rule-ordering complexity. This approach reduces the risk of errors and drastically cuts time to first enforcement.

Ensure Protection Across Hybrid Networks

Illumio Core supports a wide range of operating platforms in physical, virtual, cloud and container environments, providing consistent enforcement at any scale. Host-based segmentation keeps the enforcement close to the workload and adapts to changes. Integration with third-party network vendors moves the enforcement closer to the data.

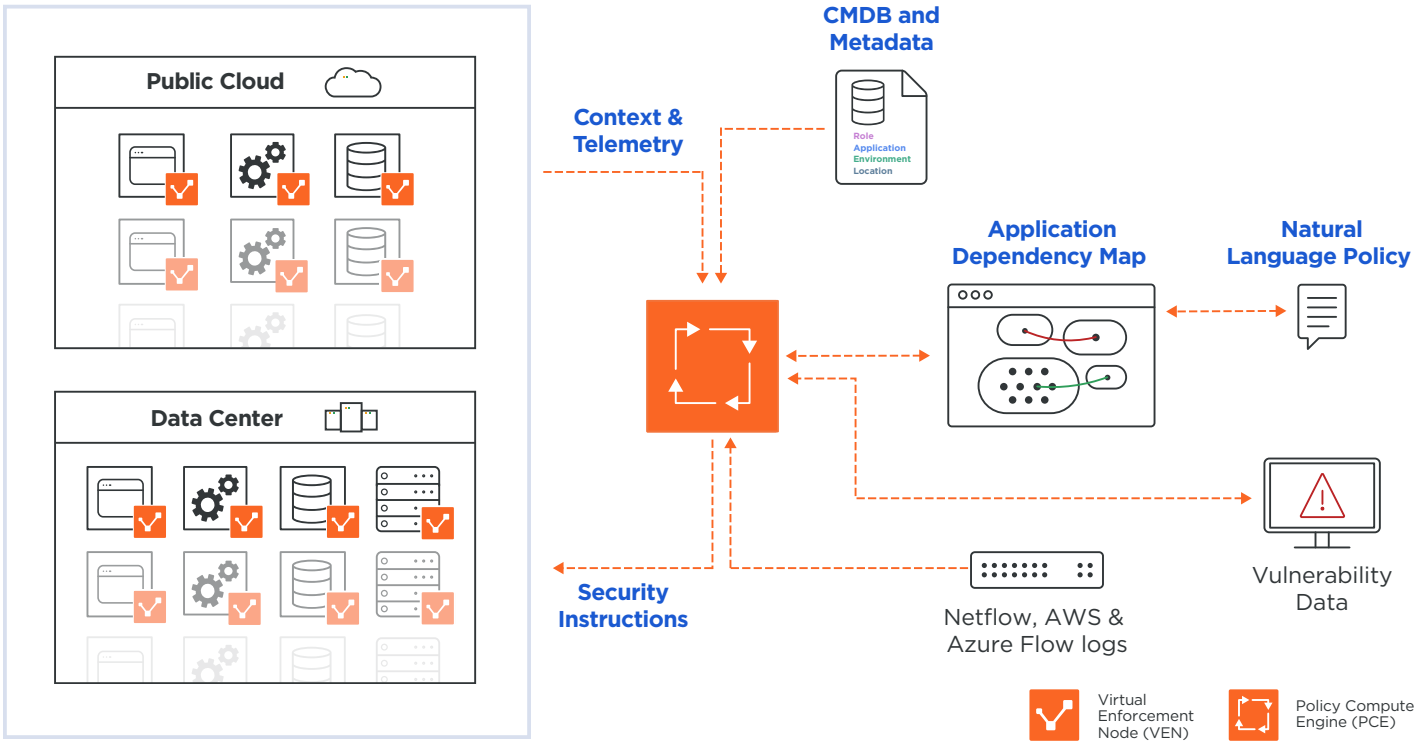
illumio

How It Works

Illumio Core is made up of two primary components:

1. **Illumio Virtual Enforcement Node (VEN):**
   The VEN runs on the workload and acts as a failsafe transceiver collecting data from the workload and passing it back to the Illumio Policy Compute Engine. It receives rules from the PCE and then pushes them to the native firewall.

2. **Illumio Policy Compute Engine (PCE):**
   The PCE uses the data from the VEN to build the application dependency map. It then automatically converts natural language policies into rules for each workload.



illumio

Illumio Core Product Information

VEN Operating System support	AIX, Amazon Linux, CentOS, Debian, Oracle Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Solaris, Ubuntu, Windows
Container orchestration platforms	Kubernetes, IBM Cloud Kubernetes, OpenShift
Supported cloud environments	Amazon Web Services, Azure, Google Cloud Platform, IBM Cloud
PCE deployment options	On-premises, SaaS, private and public cloud
Technology integrations	Palo Alto Networks Dynamic Address Groups, App for ServiceNow, App for Splunk, App for QRadar
Vulnerability mapping partners	Tenable, Rapid7, Qualys
Flow consumption	IPFIX, NetFlow, S-flow, J-flow, AWS flow logs, Azure flow logs, Text, YAML
Workload addressing	IP lists (IPv4/IPv6), FQDN
Scale	From 1 to 150,000 VENs and 750,000 workloads
Network Enforcement Node – supported platforms	Cisco Nexus 9000 series (TOR), Arista 7000 series (TOR), F5 Big IP, AVI
Visibility mode	Blocked, Potentially Blocked, Allowed
Enforcement modes	Visibility-Only, Selective Enforcement, Full Enforcement
Policy parameters	Workload ID, FQDN, IP lists, virtual services

Illumio Edge

Bring Zero Trust to your endpoint devices with uniform policy enforcement and full visibility of endpoint traffic

Illumio Edge gives IT and security teams an easy path to endpoint Zero Trust.

Contain ransomware, malware or even zero-day threats to a single laptop or other endpoint device with both inbound and outbound traffic controls. Easily enforce least-privilege access from devices to applications in your data center and cloud platforms with Zero Trust user policies.

Illumio Edge provides key advantages for preventing lateral movement from endpoint devices.

Contain Ransomware to a Single Endpoint

Use discovered traffic to author policy based on real-time network visibility. Easily prevent mass infections of zero-day attacks with rules blocking lateral movement between endpoints over common ransomware propagation protocols like SMB and RDP. (Figure 3)

Simple Zero Trust User Access

Quickly deploy identity-based group policies to limit user application access by Active Directory group and device identity. Lock down access to critical infrastructure through designated user groups and port protocols so only IT staff can access jump boxes through SSH. (Figure 4)

Gain Endpoint Traffic Visibility On or Off the Network

Visualize all observed traffic between workloads using Illumio Explorer. Help security, application, operations, compliance and audit teams search and analyze historical records for planning, auditing, reporting, and troubleshooting. (Figure 5)

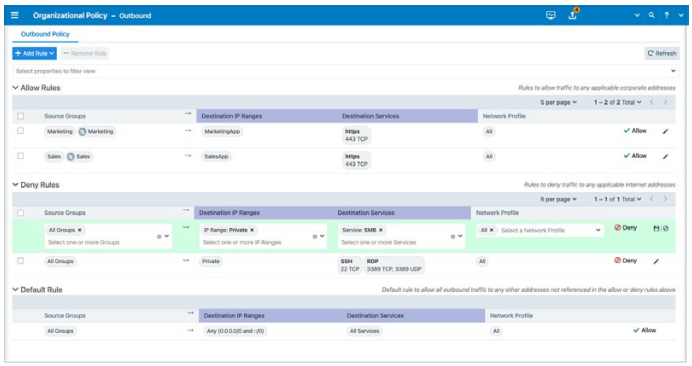


Figure 3

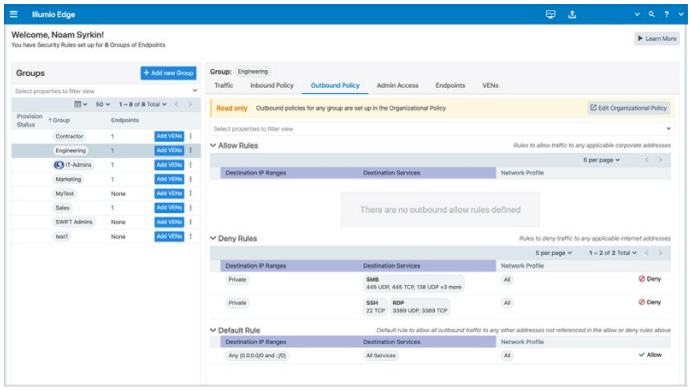


Figure 4

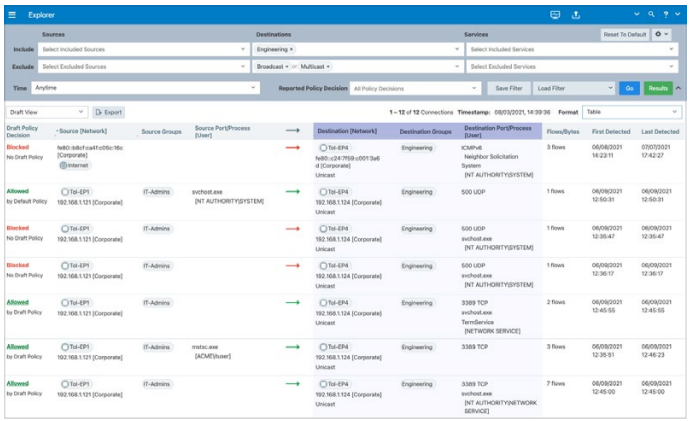


Figure 5

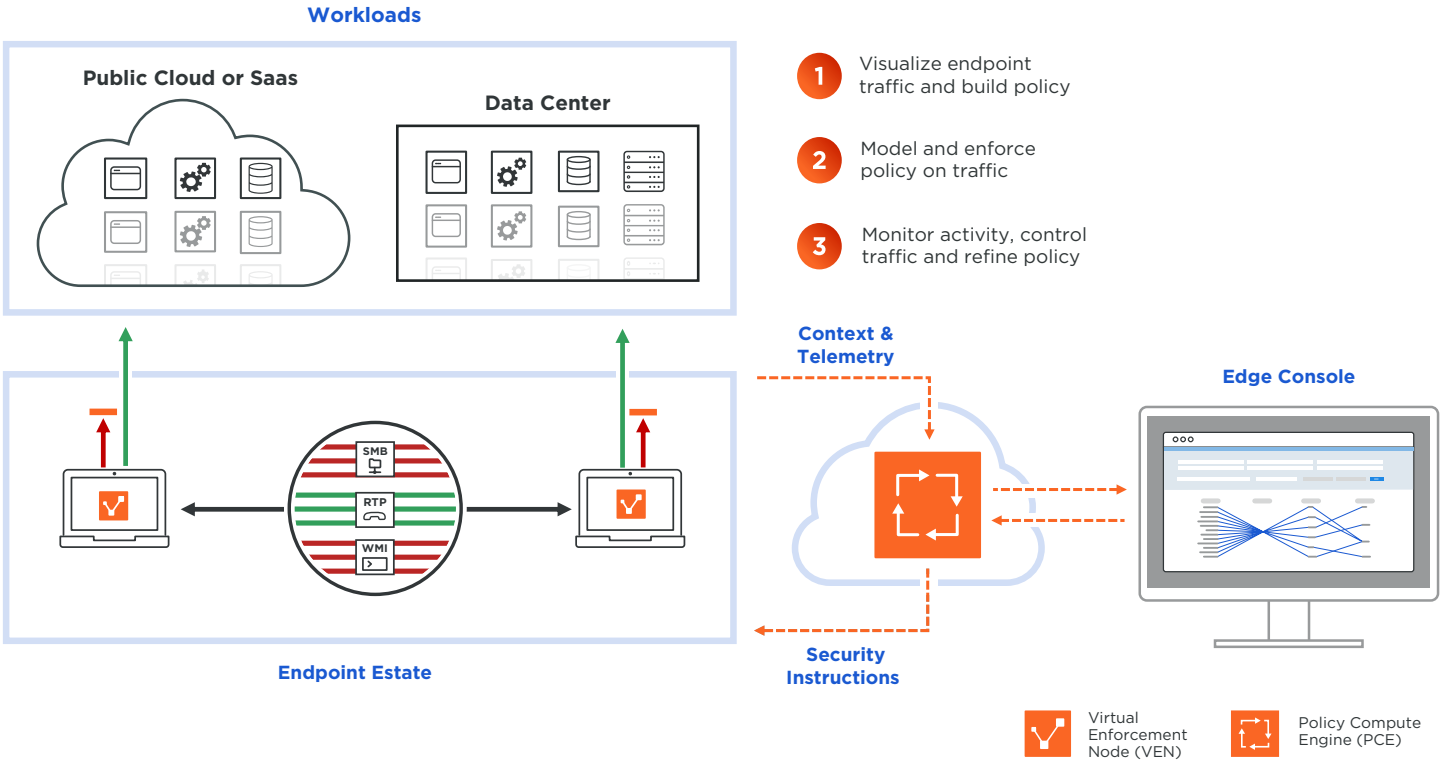
illumio

How It Works

Illumio Edge is made up of two primary components:

1. **Illumio Virtual Enforcement Node (VEN):**
   The VEN acts as a failsafe transceiver collecting telemetry from endpoint traffic and passing it back to the Illumio Policy Compute Engine. It receives rules from the PCE and then pushes them to the native firewall.

2. **Illumio Policy Compute Engine (PCE):**
   The SaaS-based PCE uses the data from the VEN to model and enforce policy. It leverages Active Directory, device identity, and fully qualified domain names (FDQNs) for simple grouping and policy creation.



illumio

Illumio Edge Product Information

VEN Operating System support	Windows 7 and 10, wired or wireless interfaces, domain-joined (corporate) and non-domain-joined (private) interfaces
PCE deployment options	SaaS
Workload addressing	IP Ranges (IPv4/IPv6), FQDN
Scale	From 1 to 50,000 VENs and 100,000 unmanaged workloads
Visibility mode	Blocked, Potentially Blocked, Allowed
Enforcement modes	Visibility-Only, Enforcement
Policy parameters	Workload ID, FQDN, IP ranges
System Requirements	Single core 1 GHz
Memory	128 MB
Disk	10 MB

Illumio provides an uptime Service Level Agreement (SLA) of 99.8% for Illumio Core and Illumio Edge. For information about the SLA, see your Illumio Purchase Order and the Illumio Master Subscription Agreement (https://www.illumio.com/eula).

Illumio, the pioneer and market leader of Zero Trust Segmentation, stops breaches from becoming cyber disasters. Illumio Core and Illumio Edge automate policy enforcement to stop cyberattacks and ransomware from spreading across applications, containers, clouds, data centers, and endpoints. By combining intelligent visibility to detect threats with security enforcement achieved in minutes, Illumio enables the world's leading organizations to strengthen their cyber resiliency and reduce risk.

Gartner peerinsights™

See what customers have to say about Illumio.