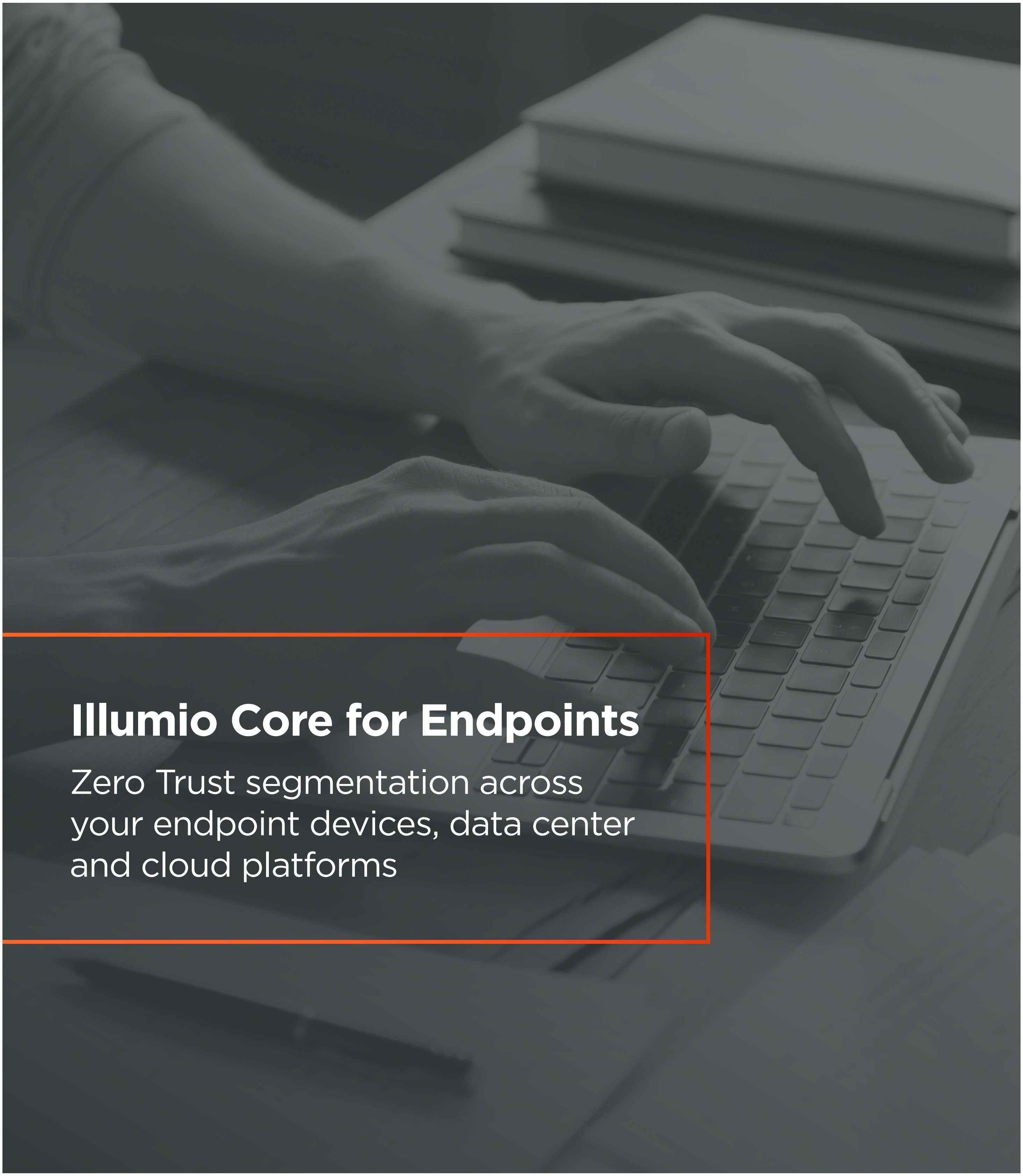
PRODUCT BRIEF



Illumio Core for Endpoints

Zero Trust segmentation across your endpoint devices, data center and cloud platforms

Illumio Core for Endpoints

Simplify and speed your path to Zero Trust segmentation

As the threat of cybercrime escalates, preventing the lateral movement of malware, viruses and cybercriminals is essential to securing your IT infrastructure.

With Zero Trust segmentation in place (also known as micro-segmentation), organizations can effectively limit the movement of cyberattacks across a network, helping protect high-value assets and meet regulatory requirements.

Illumio Core for Endpoints provides Zero Trust segmentation that works across any cloud, data center or endpoint. Critically, it helps you progressively and safely enforce segmentation without being constrained by rule ordering. This lowers costs by simplifying policy implementation and reducing disruption.

Illumio Core for Endpoints 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 your endpoints and your data center or cloud workloads. Insights into connectivity serve as the basis for building segmentation policies. (Figure 1)

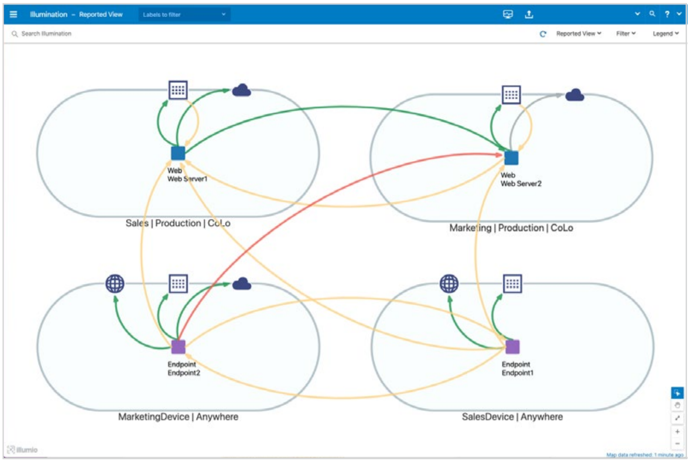


Figure 1

Key Benefits

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

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 from endpoints to any data center and cloud through Zero Trust segmentation.

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 Explorer helps security, application, operations, compliance and audit teams search and analyze historical records of all observed traffic between endpoints and workloads for planning, auditing, reporting and troubleshooting. (Figure 2)

Simplify Policy Creation

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

You can quickly deploy identity-based group policies to limit user application access by Active Directory group and device identity. For example, you can lock down access to critical infrastructure through designated user groups and port protocols so that only IT staff can access jump boxes through SSH.

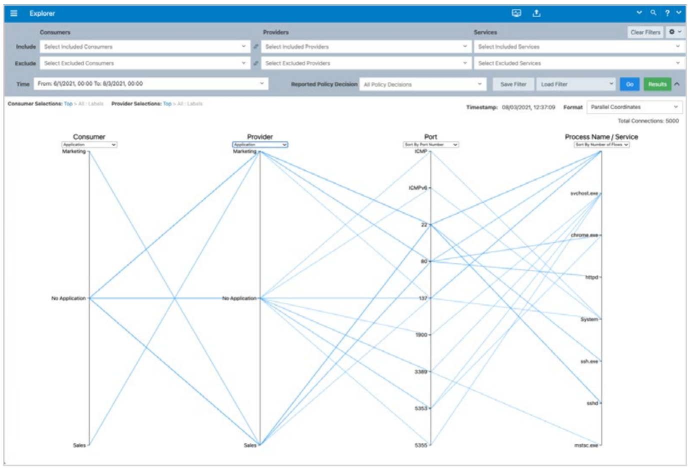
Build Enforcement Progressively

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 for Endpoints supports a wide range of operating platforms in physical, virtual, cloud, container and endpoint environments, providing consistent enforcement for the smallest to largest organizations.

Host-based segmentation keeps the enforcement close to the workload and adapts to any changes. Integration with third-party network vendors moves the enforcement closer to the data. Illumio Core for Endpoints also supports fully automated incident response, integrating with SIEM and SOAR platforms for alerting and automatic quarantine.



Explorer

	Consumers	Providers	Services
Include	Select Included Consumers	Select Included Providers	Select Included Services
Exclude	Select Excluded Consumers	Select Excluded Providers	Select Excluded Services

Time: From: 6/1/2021, 00:00 To: 8/3/2021, 00:00

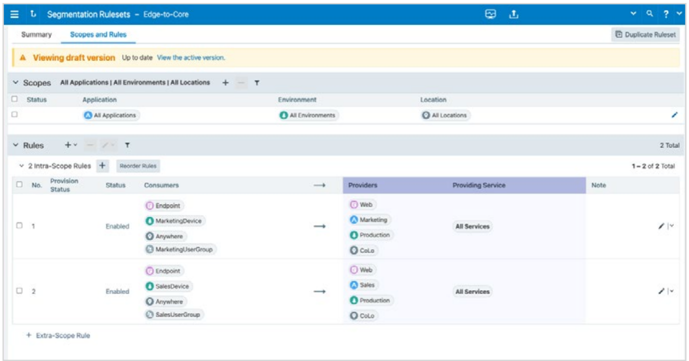
Reported Policy Decision: All Policy Decisions

Consumer Selections: Top > All : Labels Provider Selections: Top > All : Labels

Timestamp: 08/03/2021, 12:37:09 Format: Parallel Coordinates

Total Connections: 5000

Figure 2



Segmentation Rulesets – Edge-to-Core

⚠ Viewing draft version Up to date View the active version.

Scopes All Applications | All Environments | All Locations

□	Status	Application	Environment	Location
□		All Applications	All Environments	All Locations

Rules 2 Total

2 Intra-Scope Rules 1 – 2 of 2 Total

□	No.	Provision Status	Status	Consumers	→	Providers	Providing Service	Note
□	1		Enabled	Endpoint MarketingDevice Anywhere MarketingUserGroup	→	Web Marketing Production CoLo	All Services	
□	2		Enabled	Endpoint SalesDevice Anywhere SalesUserGroup	→	Web Sales Production CoLo	All Services	

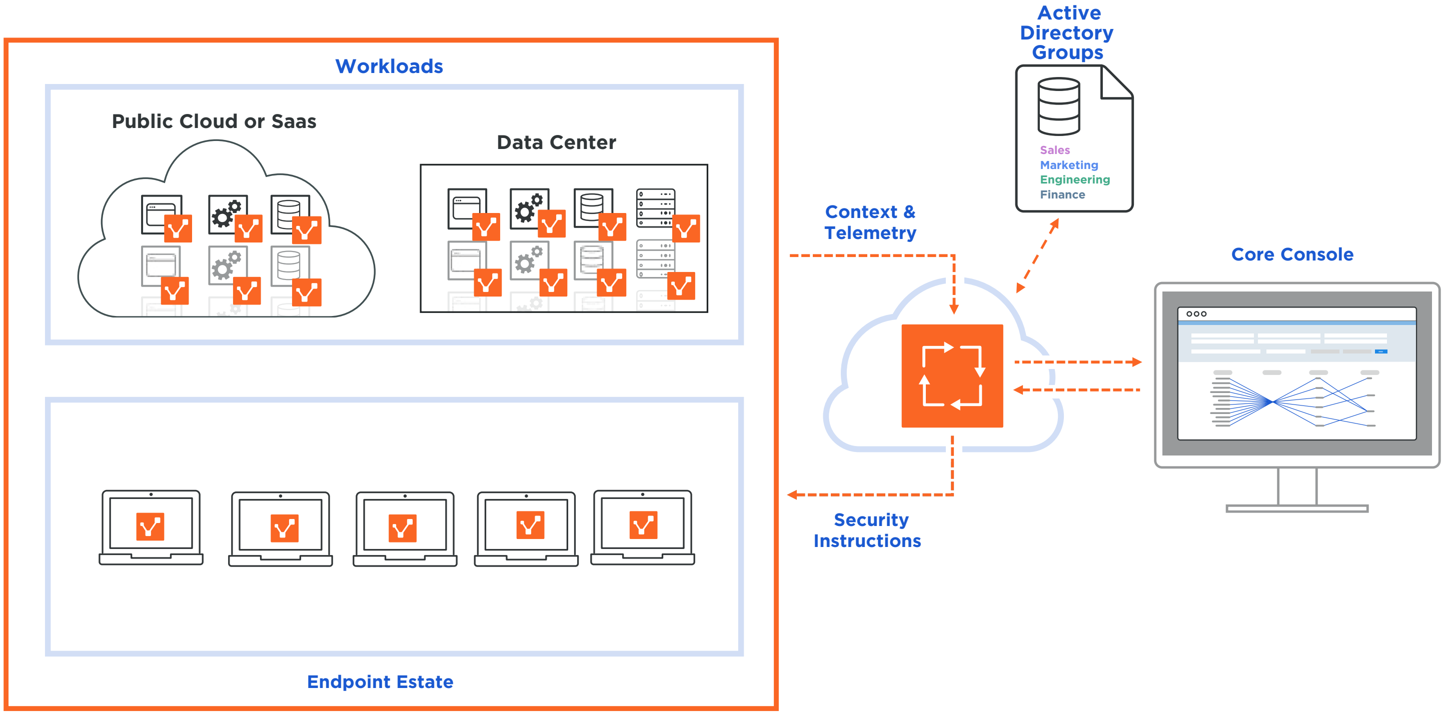
Figure 3

How It Works

Illumio Core for Endpoints is made up of two primary components:

1. Illumio Virtual Enforcement Node (VEN): The VEN acts as a fail-safe transceiver collecting the data and metadata from workloads and endpoints and passing it back to the Illumio Policy Compute Engine (PCE). 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 to rules for each workload or endpoint.



Product Information

VEN Operating System support	Server workloads: Red Hat Enterprise Linux, CentOS, Amazon Linux, AIX, Solaris, Debian, Oracle Linux, SUSE Linux Enterprise Server, Ubuntu, IBM Z, Linux, Windows Server Endpoint workloads: Windows OS, wired or wireless interfaces
Container orchestration platforms	Kubernetes, OpenShift, IBM Cloud Kubernetes Service
Supported cloud environments	Amazon Web Services, Azure, Google Cloud Platform, IBM Cloud
PCE deployment options	On-premises, SaaS, private and public cloud
Flow consumption	IPFIX, NetFlow, S-flow, J-flow, AWS flow logs, Azure flow logs, Text, YAML
Workload addressing	IP lists (IPv4/IPv6), FQDN
Technology integrations	Palo Alto Networks, App for ServiceNow, App for Splunk, App for QRadar
Vulnerability mapping partners	Tenable, Rapid7, Qualys
Switch integration	Cisco Nexus 9000 series (TOR), Arista 7000 series (TOR)
Load balancer integration	F5, AVI
Visibility mode	Blocked, Potentially Blocked, Allowed
Enforcement modes	Visibility-Only, Selective Enforcement, Full Enforcement
Policy parameters	Workload ID, FQDN, IP lists, virtual services, label groups, Active Directory groups and device ID (endpoints)

Illumio provides an uptime Service Level Agreement (SLA) of 99.8% for Illumio Core for Endpoints.
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.

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.