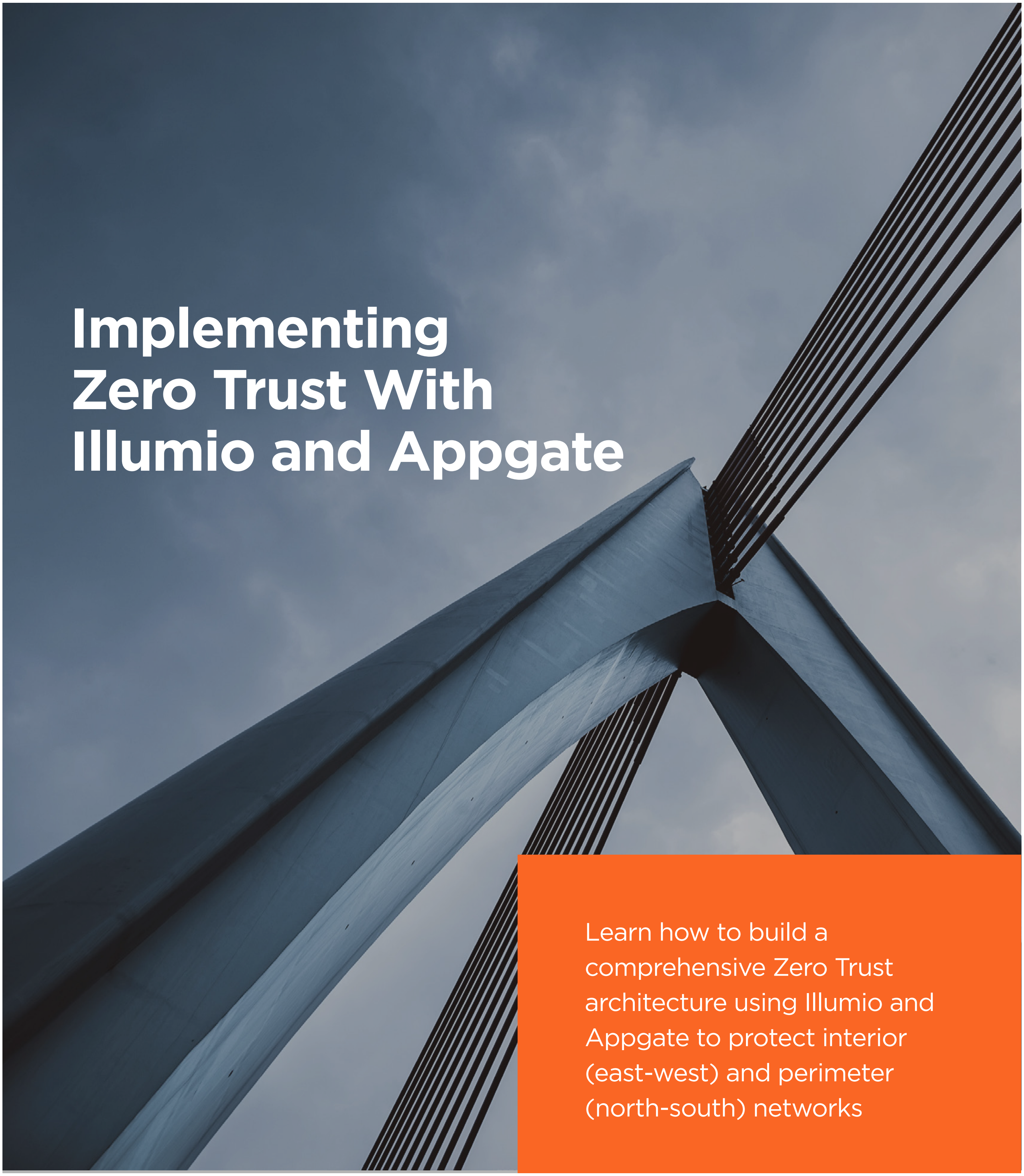
SOLUTION GUIDE



Implementing Zero Trust With Illumio and Appgate

Learn how to build a comprehensive Zero Trust architecture using Illumio and Appgate to protect interior (east-west) and perimeter (north-south) networks

Contents

Implementing Zero Trust

Your biggest challenge: Where to start?

Zero Trust is complex with many moving parts. Most organizations follow a five-pillar model to build their strategy composed of data, users, devices, workloads and networks. In this security model, organizations must apply the principle of "least privilege" to each pillar, and only authorize data sharing between them when it's absolutely necessary.

To start building Zero Trust, you have to choose which pillars to address first.

To do so, you must identify and rank the most consequential assets — other than data — that you need to protect. For most organizations that means critical workloads like database servers, application servers and web servers.

Protecting these assets requires three Zero Trust approaches:

1. **Apply Enhanced Identity Governance (EIG):** Many companies started their Zero Trust journey by deploying EIG. That is a necessary and good first step, but only one of the three controls in a strong Zero Trust architecture.
2. **Build Zero Trust network access (ZTNA) to workloads via the perimeter network (north-south traffic):** Most organizations are very aware of perimeter security. The pandemic — and the way it rapidly accelerated the remote workforce trend — has only made perimeter security an even bigger priority.
3. **Apply Zero Trust microsegmentation to workloads in the interior network (east-west traffic):** East-west security is relatively new. Most organizations are less aware of it and don't understand it very well. Yet many breaches over the last few years have made it clear that there's more to interior security than authenticating users.

As mentioned, many organizations have put EIG in place. That leaves substantial ground to cover for a complete Zero Trust program. Fortunately, you only need two additional products — Illumio Core and Appgate SDP — to build these three minimum recommended Zero Trust tactics.

These three tactics are becoming standard practice for Zero Trust security. The following chart further describes them — using definitions from the National Institute of Standards and Technology's (NIST) document SP 800-207 — and outlines the solutions you can deploy to perform each.

Zero Trust Approach	Description	Example Products
Enhanced identity governance (EIG)	Access policies are based on identity of actors and assigned attributes (device used, asset status, environmental factors). Essentially ICAM (incident, credential and access management) with endpoint security.	Okta with MobileIron MS AD with Microsoft Intune
Microsegmentation (host-based)	Uses agents to program the native firewalls in each host or endpoint to design and enforce ZT perimeters.	Illumio Core
Software defined perimeter (SDP/ZTNA infrastructure)	An SDP approach that applies an identity-centric, dynamic and continuous secure access architecture to enforce ZT. The infrastructure is cloaked so that users can only see cloud and data center resources that they're authorized to see.	Appgate SDP

Defining these three approaches is only half the equation. Now, let's look at the common vulnerabilities and security risks that a Zero Trust solution must address.

Common Vulnerabilities and Risks in Perimeter and Interior Networks

Interior Networks (East-West)

Vulnerabilities	Associated Risks
Excessive workload-to-workload interconnectivity	Attacks can rapidly spread laterally
Absence of workload segmentation barriers and lateral movement sensors	Failure to limit attacker's spread radius. Failure to deny and report spread attempts.
Non-dynamic control: Over-reliance on non-contextual metadata (workload IP addresses)	Failure to adapt to changes in context (workload migrated from DEV to PROD environment)

Perimeter Networks (North-South)

Vulnerabilities	Associated Risks
Absence of cloaked, per-user, per-app access control	Unauthorized access to east-west workloads + data
Non-dynamic control. Over-reliance on non-contextual user metadata (device IP addresses).	Failure to adapt user entitlements to user contexts (variances in user role, date, time, location)
Over-reliance on non-contextual workload metadata (workload IP addresses)	Failure to adapt user entitlements to workload context (workload migrated from DEV to PROD environment)

The vulnerabilities and risks of perimeter (north-south) and interior (east-west) traffic shares common themes:

- Over-reliance on non-contextual metadata (either workload or device IP addresses)
- Failure to dynamically adapt to changes in workload context or user entitlements

These are big issues in today's dynamic, hybrid IT environments, where changes can happen at any moment within all five Zero Trust pillars. To adapt, you must be able to quickly update policy enforcement at a moment's notice. For example, you will need to adapt your Zero Trust controls any time a workload — like a database — migrates from an on-premises data center to the cloud, or from a development environment to a production environment.

Your ability to adapt your Zero Trust architecture to changes in your environment will largely depend on the tools you use.

When designing your architecture — or when evaluating proposals from tool vendors — include these five requirements:

1. **Abstraction:** The ability to create and use workload metadata (labels) instead of IP addresses, which change frequently
2. **Flexibility:** Support for on-premises and cloud-based deployment
3. **Low Latency:** Avoidance of unnecessary data round trips to and from the cloud
4. **Integration:** Mature APIs for integration with DevOps and third-party tools
5. **Enterprise-Grade:** Role-based (RBAC) and attribute-based (ABAC) access controls for workload segmentation

Now, let's look at a Zero Trust strategy that meets these requirements and creates north-south network protection using Appgate, and east-west network protection using Illumio Core.

A Three-Step, Best Practice Approach to Zero Trust Security

Illumio Core and Appgate support a comprehensive Zero Trust approach to address key vulnerabilities and risks for today's hybrid networks

Step 1a: Install Illumio Core on the east-west network

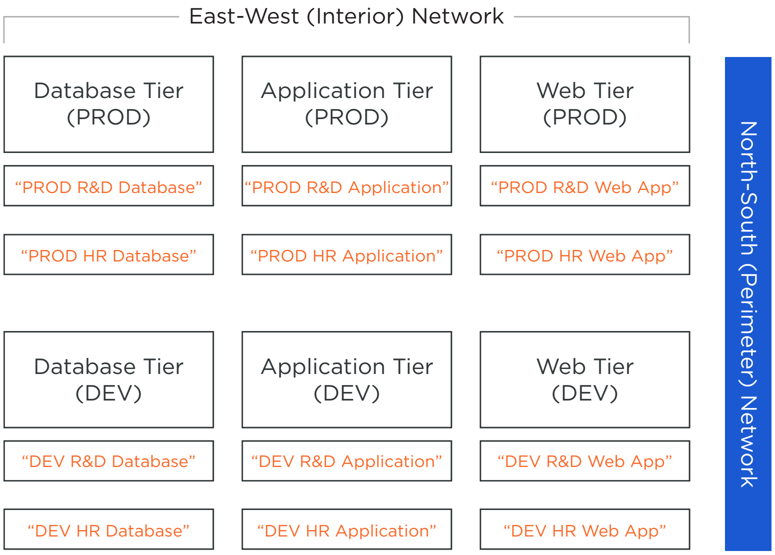
Install Illumio Core on your east-west network, and you will:

- Reveal all workloads and workload-to-workload interconnections, many of which will likely be unnecessary sources of risk.
- Easily set and enforce policies, and rapidly adapt to changes in each workload's context (e.g., a workload moving from DEV to PROD).
- Augment each workload's IP address with Illumio's four-dimensional label metadata, based on natural language. Those labels are:
  - Role: "Web Tier Application"
  - Application: "Finance Application"
  - Environment: "Production" (PROD) or "Development" (DEV)
  - Location: "Langley Data Center 1"

Appgate is uniquely designed to consume metadata like Illumio Core's workload labels, making it more dynamic than other remote access solutions.

When Illumio Core updates the workload metadata — for example when a workload moves from one location to another and its IP address changes — Appgate programmatically updates its entitlements with no disruption and ensures access policies remain unchanged.

By making use of Illumio Core's abstraction — workload labels — instead of an underlying physical network construct — an IP address — access control policies can dynamically adapt.



Step 1a in the Zero Trust Journey

Install Illumio on the East-West Network

- Reveal workloads and excessive workload-to-workload interconnections
- To enable ease of policy setting and Zero Trust policy enforcement, and to add the ability to adapt to changes in each workload's context (e.g., if a workload is migrated from DEV to PROD)
- Augment each workload IP address by assigning the following **4-dimensional Illumio Label**:

1. **Role:** "Web Tier Application"
2. **Application:** "HR Application"
3. **Environment:** "PROD or DEV"
4. **Location:** "Langley Data Center 1"

Step 1b: Use Illumio Core to implement east-west workload segmentation

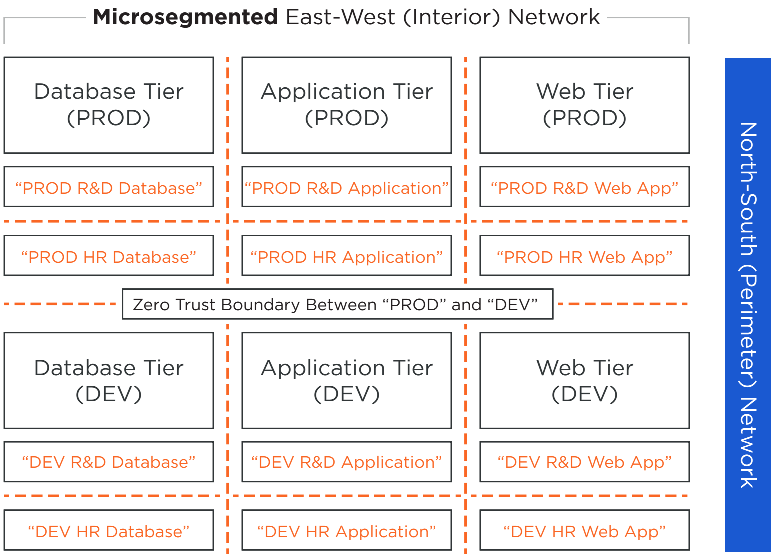
Within a few hours of installing Illumio Core, you can visualize your east-west network and begin segmenting workloads with host-based microsegmentation.

With Illumio Core, you can:

1. **Discover all workloads and visualize their flows.** Illumio Core creates a detailed map of the entire IT environment. This map gives you a simplified view of workload communications among applications, clouds, containers, data centers and endpoints.
2. **Label workloads with role, application, environment and location.** Illumio Core creates metadata that it and Appgate SDP can use to dynamically enforce policies. These labels are the foundation for much of what Illumio Core does. Illumio Core uses them to organize workloads, draw its connectivity map, and enforce security policy (instead of using failure-prone IP addresses).
3. **Create microsegmentation barriers to eliminate excess workload-to-workload connectivity and shrink the east-west attack surface.**

Illumio Core's radically simple policy creation engine builds advanced security controls and policy at the application, tier-to-tier, port and process level.

Illumio Core automatically places the policies in the right location, so you don't have to worry about rule conflicts. This makes fine-grained segmentation fast and easy. It eliminates the painful rule ordering that is common to most microsegmentation products.



Step 1b in the Zero Trust Journey

Use Illumio to implement East-West Workload Segmentation

- - - - Orange dashed lines indicate full or partial boundaries enabled by Illumio Zero Trust microsegmentation policy

Step 2: Install Appgate SDP for cloaked, north-south user-to-workload Zero Trust network access (ZTNA)

ZTNA is now the standard for secure access control — especially as cloud, remote work and edge computing trends turn the traditional security perimeter inside out. ZTNA starts from a default deny posture and then extends limited, earned trust that is continuously reevaluated.

The Appgate SDP (a software-defined perimeter) solution is a comprehensive, highly scalable, enterprise-grade solution for ZTNA trusted access. It effectively eliminates the attack surface by rendering resources invisible until the user is authenticated and authorized.

With Appgate SDP, access is conditional and contextual, based on the user's multidimensional identity profile and device posture. These dynamic, user/device-specific entitlements adjust based on risk and changing conditions. Appgate SDP simplifies policy definition and enforcement by applying a single framework to all users, devices, networks and resources.

instead of an underlying physical network construct — an IP address — access control policies can dynamically adapt.

Single Packet Authorization

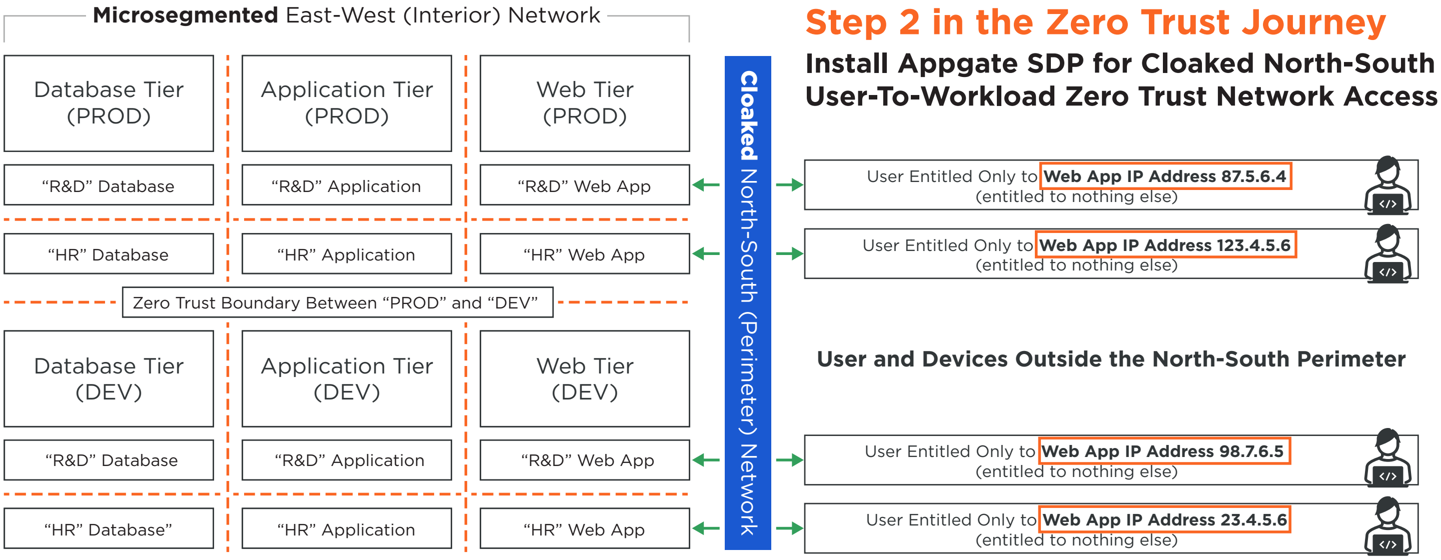
Reducing your attack surface is a critical component of ZTNA and is the first line of defense against adversaries running port scans as part of their reconnaissance campaigns. Your ZTNA solution should actively cloak your ports, making them and the resources they protect invisible.

Appgate does this with Single Packet Authorization (SPA), which uses proven cryptographic techniques to make interfacing servers invisible to unauthorized users. Only devices that have been seeded with the cryptographic key can generate a valid SPA packet and establish a network connection.

A key feature of Appgate SDP — and fundamental to any ZTNA solution — is the ability to define highly granular access using session-based micro firewalls. With Appgate, you can surgically remove access to only critical or privileged data based on the level of risk. This approach weighs factors that should be taken into consideration to make precise decisions around access control for users and devices.

Step 2 in the Zero Trust Journey

Install Appgate SDP for Cloaked North-South User-To-Workload Zero Trust Network Access

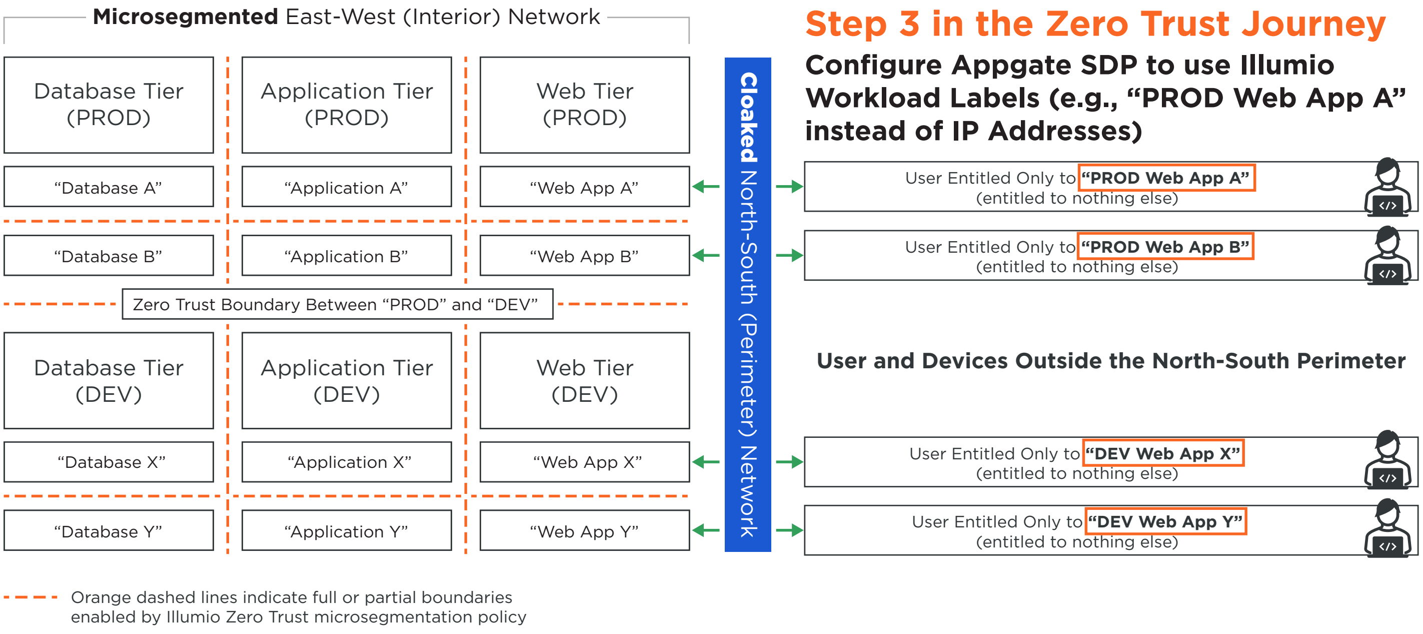

Microsegmented East-West (Interior) Network
Database Tier (PROD)
Application Tier (PROD)
Web Tier (PROD)
"R&D" Database
"R&D" Application
"R&D" Web App
"HR" Database
"HR" Application
"HR" Web App
Zero Trust Boundary Between "PROD" and "DEV"
Database Tier (DEV)
Application Tier (DEV)
Web Tier (DEV)
"R&D" Database
"R&D" Application
"R&D" Web App
"HR" Database"
"HR" Application
"HR" Web App
Cloaked North-South (Perimeter) Network
User Entitled Only to Web App IP Address 87.5.6.4 (entitled to nothing else)
User Entitled Only to Web App IP Address 123.4.5.6 (entitled to nothing else)
User and Devices Outside the North-South Perimeter
User Entitled Only to Web App IP Address 98.7.6.5 (entitled to nothing else)
User Entitled Only to Web App IP Address 23.4.5.6 (entitled to nothing else)

- - - Orange dashed lines indicate full or partial boundaries enabled by Illumio Zero Trust microsegmentation policy

Step 3: Configure Appgate SDP to utilize Illumio workload labels instead of IP addresses

As we mentioned in Step 1, Appgate can harness Illumio Core's workload labels using its "auto resolver" feature. This feature lets Appgate use metadata — the Illumio label — to dynamically adjust access policies. If something changes — whether an IP address, a port, or an environment — the auto resolver automatically adjusts entitlements.

This is especially helpful when an application moves through the CI/CD pipeline from DEV, to staging, to PROD, and changes user access at each stop. The auto resolver makes sure only the right people have access the entire time.


Microsegmented East-West (Interior) Network
Database Tier (PROD)
Application Tier (PROD)
Web Tier (PROD)
"Database A"
"Application A"
"Web App A"
"Database B"
"Application B"
"Web App B"
Zero Trust Boundary Between "PROD" and "DEV"
Database Tier (DEV)
Application Tier (DEV)
Web Tier (DEV)
"Database X"
"Application X"
"Web App X"
"Database Y"
"Application Y"
"Web App Y"
Cloaked North-South (Perimeter) Network
Step 3 in the Zero Trust Journey
Configure Appgate SDP to use Illumio Workload Labels (e.g., "PROD Web App A" instead of IP Addresses)
User Entitled Only to "PROD Web App A" (entitled to nothing else)
User Entitled Only to "PROD Web App B" (entitled to nothing else)
User and Devices Outside the North-South Perimeter
User Entitled Only to "DEV Web App X" (entitled to nothing else)
User Entitled Only to "DEV Web App Y" (entitled to nothing else)
Orange dashed lines indicate full or partial boundaries enabled by Illumio Zero Trust microsegmentation policy

Illumio and Appgate: Zero Trust Architecture for Both Perimeter and Interior Network Traffic

Zero Trust Enterprise Interior (Illumio)	Zero Trust Enterprise Perimeter (Appgate)
Software-defined, **east-west** traffic control	Software-defined, **north-south** traffic control
Dynamic, least-privileged **ingress/egress control** inside each workload on east-west network	Dynamic, least-privileged **access control** for each user and device
Fine-grained, **node-to-node communications control**	Fine-grained **access to the application front end**
Microsegmented Zero Trust **interior**	Microsegmented Zero Trust **perimeter**

With Illumio and Appgate, you can deploy a truly end-to-end Zero Trust architecture. The two platforms uniquely offer mature, highly evolved APIs that lets Illumio Core pass metadata to Appgate. This makes it possible for the two security platforms to adhere to a strict Zero Trust approach that creates dynamic, fine-grained, least-privileged access control for all traffic.

Most organizations know they need to implement a Zero Trust approach to cybersecurity — but they don't know where to begin. There's a lot of hype and misinformation out there about Zero Trust, as well as vendors with conflicting and confusing claims.

Illumio and Appgate are leading the way to help organization implement effective and efficient Zero Trust security protection. In the Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, the consulting firm ranked Illumio and Appgate as Leaders.

If you're struggling with what to do next after deploying EIG, remember that with just two products — Illumio and Appgate — you can quickly build Zero Trust security to protect both perimeter and interior traffic across your hybrid computing environments.

That's cybersecurity peace of mind.

Achieve Zero Trust Security With Illumio and Appgate

Illumio and Appgate together provide comprehensive Zero Trust security across both interior and perimeter networks. Protect and automatically keep security policies up-to-date as your hybrid IT environments continue to evolve.

Learn more about how Illumio and Appgate can help you implement your Zero Trust strategy.

Contact us today to speak with our security experts.

https://www.illumio.com/contact

During our conversation, we will:

- Discuss your current security strategy and requirements
- Help you build a Zero Trust strategy that works for you
- Show how Illumio and Appgate can help you build more comprehensive security for your organization

About Illumio

illumio

As the pioneer of Zero Trust Segmentation, Illumio prevents breaches from becoming cyber disasters. Gain real-time visibility and segmentation control to see your risks, isolate attacks and secure your data across hybrid clouds, data centers and endpoint devices.

About Appgate

appgate

Appgate is the secure access company. It's people-defined security approach provides fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments.