SOLUTION BRIEF

Illumio + Appgate for Zero Trust Security

Secure your network interior and perimeter with least-privilege access by automatically keeping security policies up to date

Organizations building a Zero Trust strategy often use the five-pillar model of data, users, devices, workloads, and networks.

This security model applies to principle of least privilege. It allows access to each of the five pillars only when and where it's necessary and authorized.

The challenge facing many organizations is how to quickly build Zero Trust security across all five pillars at the same time. They must also protect both the interior network (east-west traffic) and the perimeter network (north-south traffic).

Today's hybrid IT networks change all the time. East-west and north-south Zero Trust controls must be able to adapt and update policies in real time as changes happen.

For example, Zero Trust controls should be able to change whenever a workload, such as one from a database, migrates from an on-premises data center to the cloud or from a development to a production environment.

Before building a Zero Trust strategy, the following vulnerabilities and risks exist in each network:

Interior networks (east-west)

Vulnerabilities	Associated risks
Excessive workload-to-workload interconnectivity	Attacks quickly spread across the network
Absence of workload segmentation barriers and lateral movement sensors	Failure to limit an attacker's spread through the network Failure to deny and report attempts to spread
Static controls. Relying too much on non-contextual metadata such as 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 and data
Static controls. Relying too much on non-contextual metadata such as device IP addresses	Failure to adapt user entitlements to user contexts (variances in user role, date, time, location)
Relying too much on non-contextual metadata such as workload IP addresses	Failure to adapt user entitlements to workload context (workload migrated from DEV to PROD environment)

The solution

The Illumio Core and Appgate SDP joint solution helps you get comprehensive Zero Trust security. It secures the network perimeter and interior with Zero Trust Segmentation (ZTS) and Zero Trust Network Access (ZTNA). Illumio Core segments workloads with dynamic labelling so that a successful attack can't move through the network and gain unauthorized access to critical assets. Appgate SDP protects the network perimeter. It gives secure access to all users, no matter their device or location, through a unified policy model. The joint solution enforces least-privilege access by creating secure connections between users and resources based on verified identity and context.

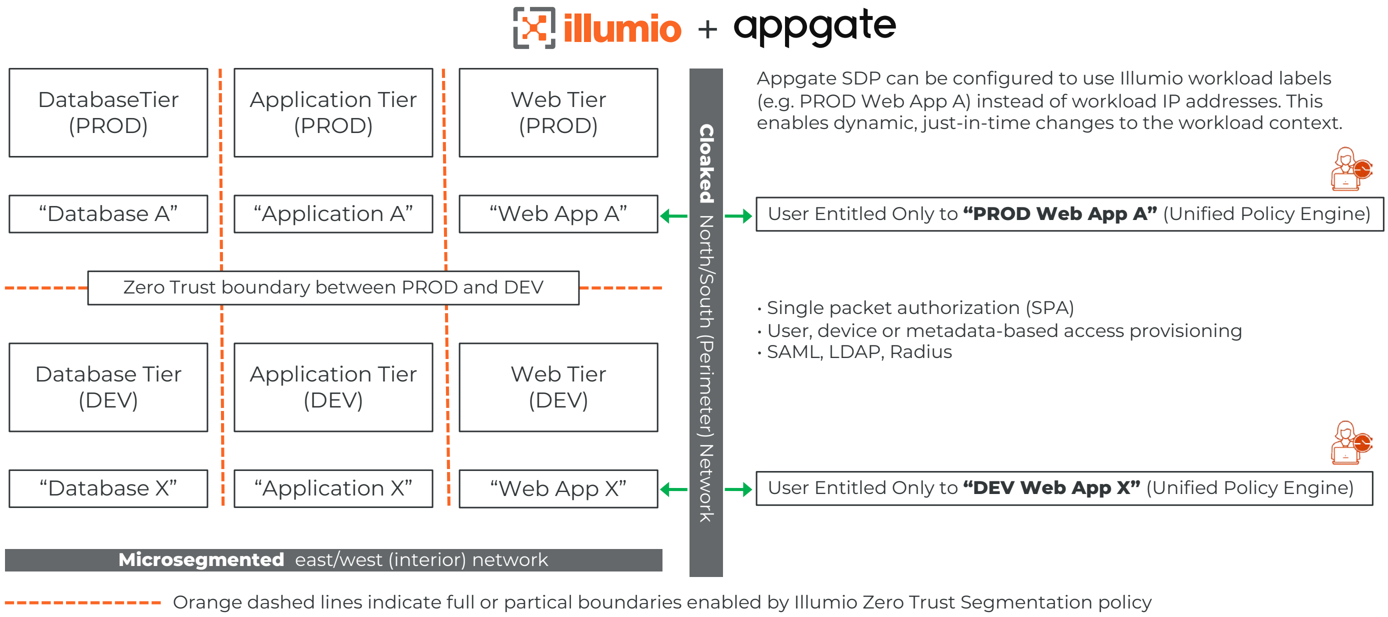
How it works

See the entire network in a few hours, and begin segmenting workloads within the day. Build Zero Trust Segmentation following these steps in as little as a few days:

1. Install Illumio Core for the east-west network. Discover all workloads and visualize their flows.
2. Label all workloads with contextual data such as role, application, environment, or location. Illumio Core and Appgate SDP will use this metadata to dynamically enforce policies.
3. Create microsegmentation barriers to get rid of excessive workload-to-workload interconnections. This will shrink the east-west attack surface.
4. Install Appgate SDP for north-south Zero Trust network access (ZTNA). Create per-user, per-session, user-to-workload access controls that are cloaked, fine-grained, and dynamic. These Zero Trust controls will shrink the north-south attack surface.
5. Set up Appgate SDP to retrieve Illumio's contextual data, including per-workload labels, with API. This will add more flexibility and fine-grained control

Integrating Illumio Core with Appgate SDP allows user-to-workload entitlement policies to dynamically adapt to changes in the workload context, such as changes to workload IP addresses.

Appgate SDP will use Illumio labels to add more information to workload IP addresses. Then, it will adapt security policy when a given workload migrates from on-premises to the cloud or from a development to a production environment.


illumio + appgate
DatabaseTier (PROD)
Application Tier (PROD)
Web Tier (PROD)
"Database A"
"Application A"
"Web App A"
Zero Trust boundary between PROD and DEV
Database Tier (DEV)
Application Tier (DEV)
Web Tier (DEV)
"Database X"
"Application X"
"Web App X"
Microsegmented east/west (interior) network
Cloaked North/South (Perimeter) Network
User Entitled Only to "PROD Web App A" (Unified Policy Engine)
User Entitled Only to "DEV Web App X" (Unified Policy Engine)

Appgate SDP can be configured to use Illumio workload labels (e.g. PROD Web App A) instead of workload IP addresses. This enables dynamic, just-in-time changes to the workload context.

- Single packet authorization (SPA)
- User, device or metadata-based access provisioning
- SAML, LDAP, Radius

Orange dashed lines indicate full or partical boundaries enabled by Illumio Zero Trust Segmentation policy

Learn more about Illumio + Appgate

Visit illumio.com or appgate.com.

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface to help organizations reduce risk and build resilience.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. It is the market leader in Universal Zero Trust Network Access (ZTNA) and online fraud protection; safeguarding organizations and government agencies worldwide.