illumio | appgate

SOLUTION BRIEF

Illumio + Appgate for Zero Trust Security

Defend both your interior and perimeter networks with least-privilege access. Automatically keep security policies up-to-date, even in today's ever-evolving hybrid IT environments.

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

In this security model, the principle of "least privilege" is applied: Access to data by each of the other four pillars is allowed only when and where it is deemed necessary and authorized.

The challenge facing most organizations is how to quickly implement Zero Trust security across all five pillars simultaneously, protecting both the interior network (East-West traffic) and the perimeter network (North-South traffic).

Given the dynamic nature of today's hybrid IT environments, East-West and North-South Zero Trust controls must be able to adapt and update policy enforcement as changes happen to one of the five pillars in real time.

For example, Zero Trust controls should have the ability to adapt (if appropriate) whenever a workload (e.g., a database) has been migrated from an on-premises data center to the cloud, and/or from a development environment to production.

Prior to implementing 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 can spread laterally, in rapid fashion
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 and 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 Solution

East-West: Zero Trust Workload Microsegmentation	Dynamic, Contextual Metadata Per Workload	North-South: Zero Trust User-To-Workload Access
Illumio Core	Illumio workload labels	Appgate SDP

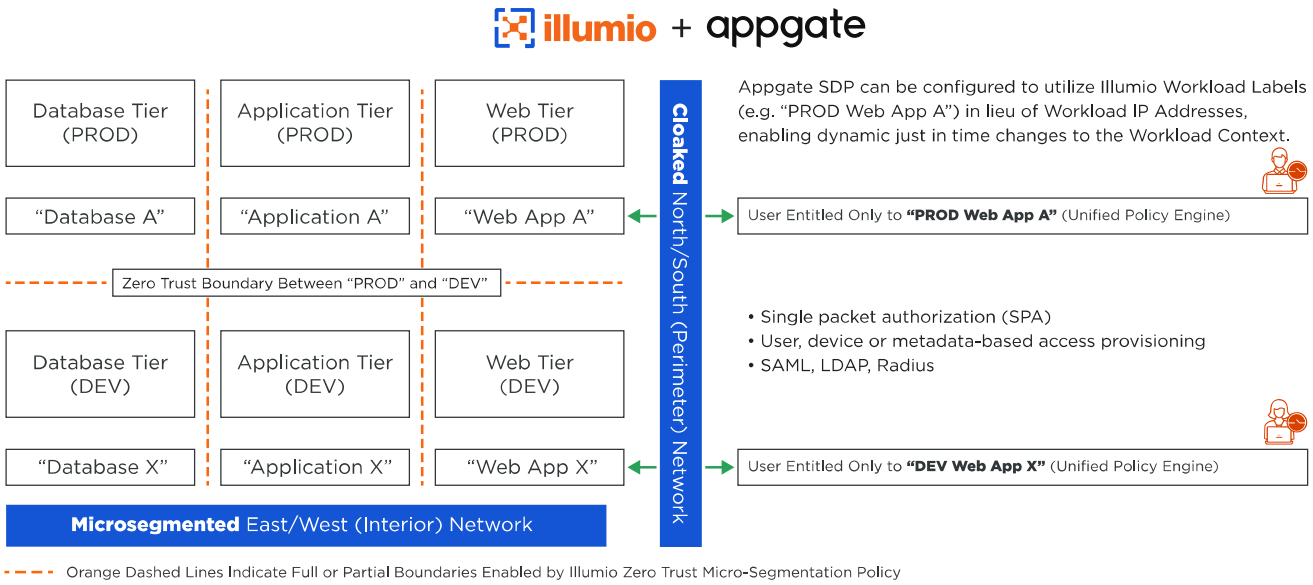
How It Works

Within a few hours, you can visualize the network and begin segmenting workloads within the day. Complete the following Zero Trust Segmentation implementation steps in as little as a couple of days:

1. Install Illumio Core for the East-West network. Discover all workloads and visualize their flows.
2. Label all workloads with contextual data (role, application, environment, location), creating metadata that will be utilized both by Illumio Core and Appgate SDP for dynamic policy enforcement.
3. Create microsegmentation barriers to eliminate excessive levels of workload-to-workload interconnectivity, thereby shrinking 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. Configure Appgate SDP to retrieve (via API) Illumio's per-workload labels (contextual metadata) for additional dynamism and fine-grained access control.

By integrating Illumio Core with Appgate SDP, the user-to-workload entitlement policies will then dynamically adapt to changes in the workload context, such as changes in workload IP addresses.

For example, using Illumio labels to augment workload IP addresses, Appgate SDP will adapt when a given workload is migrated from on-premises to the cloud or from a development environment to a production environment.



The Illumio + Appgate Zero Trust Alliance

In the Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers Q3, 2020 report, Illumio and Appgate were both named Leaders. Illumio Core and Appgate SDP together provide Zero Trust security across both interior and perimeter networks.

To learn more, please visit illumio.com or appgate.com.

About 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 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.