illumio

SOLUTION BRIEF

Illumio at the Tactical Edge

Delivering Zero Trust Segmentation during staging and deployment

Ensure mission resilience with Zero Trust

Adversaries, by definition, will always attempt to deter, disrupt, and defeat the mission. As the battlespace continues to digitalize, these attempts are becoming more and more like any other attacks against digital infrastructure.

Unlike traditional security models that often rely on perimeter defenses, Zero Trust operates on the fundamental assumption that no entity, whether internal or external, should be inherently trusted. In the face of persistent cyber threats, the key to success lies not only in prevention but also in a continuous and adaptive response that assumes adversaries are present. Adopting Zero Trust principles and technologies can help contain those attacks and limit their ability to succeed.

Securing your users, applications, and network from the inside out is the most important tactical advantage you can have against any attacker. This must be done without creating any additional complexity, load, or bandwidth demands in contested, disconnected, or degraded networks.

Secure tactical environments with Zero Trust Segmentation

Illumio's Zero Trust Segmentation platform manages security on workloads via agents deployed into modern operating systems. This software sensor enables a policy enforcement point (PEP) to each server and endpoint in an application.

Illumio enables a least-privilege policy model in which workloads allow specific access and denies all else by default. When application workloads or endpoints (the PEPs) disconnect from the Illumio Policy Compute Engine (the Policy Decision Point, or PDP), the workloads will continue to enforce policy via the most recently deployed security rules without requiring any connectivity from the PDP. Forward-deployed tactical workloads can be completely disconnected from the PDP and perform their role as the PEP.

How Illumio secures resources during staging and deployment

Take, for instance, a scenario during staging and deployment. Zero Trust is indispensable for safeguarding troops both during staging and during remote deployment.

When troops are staging a mission, their compute resources have reliable connectivity to Controllers that can be used to configure their resources' security controls. When those troops are remotely deployed, Illumio ensures that security controls which were deployed during staging remain in place, even with limited or unreliable access to resources remotely by troops. Security at every workload or endpoint will maintain the most recent policy decisions which were implemented during staging.

Illumio has accomplished this in deployments with a lightweight, persistent, and resilient footprint which requires minimum compute and bandwidth, making it suitable for environments where these are often limiting factors.

The same solution attributes are applicable to other tactical scenarios, such as building and deploying fly-away kits or pre-configuring weapons systems prior to deployment in staging areas.

When sensors are disconnected from the PDP, they continue to enforce policy based on the last instructions received.

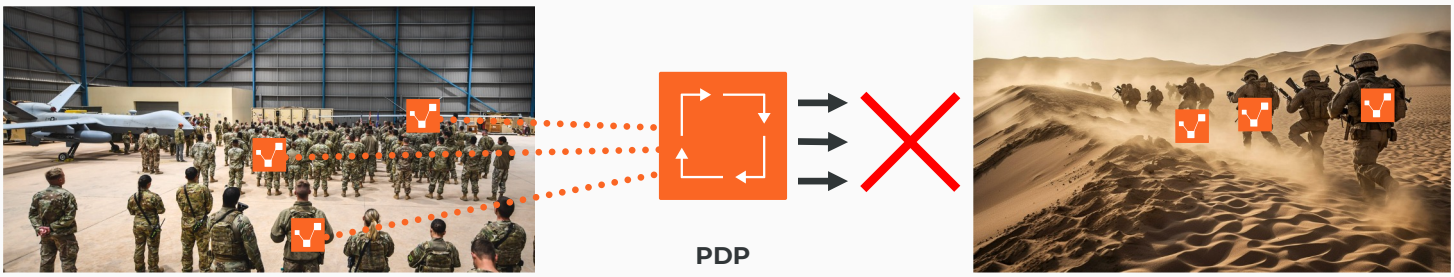
This ensures that policy is consistent even when external access is lost, whether planned or unplanned.

Policy Decision Point (PDP)

Policy Enforcement Point (PEP)

Staging Area, connected to PDP

Remotely deployed, disconnected from PDP



The adversary is already inside your network. Assuming anything different means you've already lost the battle.

Illumio enables logically grouped resources, called a ringfence, to implement least-privilege policy within or between ringfences. This can be achieved without modifying the underlying network and without having to associate the ringfence boundaries to any specific physical location or IP addressing.

Illumio ensures battlefield assets are reliably segmented whether deployed in a staging or tactical environment.

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.