TECHNICAL BRIEF

Mapping Illumio to the Department of Defense Zero Trust Reference Architecture

Illumio aligns with the architecture's seven pillars

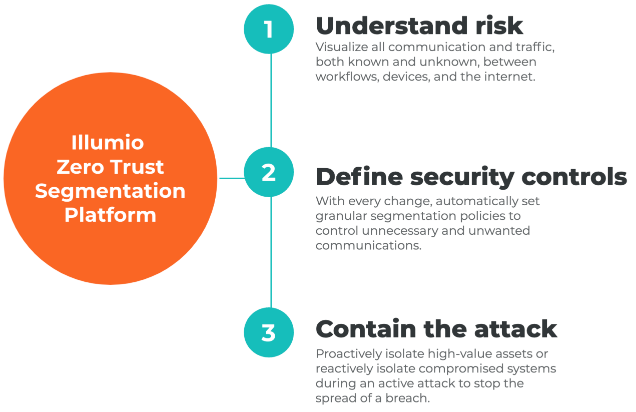
Zero Trust enabled by Illumio

The Department of Defense Zero Trust Reference Architecture, also referred to as ZTRA, requires the enforcement of seven pillars of protection for cybersecurity resources: User, Device, Application and Workload, Data, Network and Environment, Automation and Orchestration, and Visibility and Analytics. Illumio's Zero Trust Segmentation platform enables the visualization and granular enforcement of security policies across all seven of these pillars.

You can't protect what you can't see. Illumio enables the full visualization of all traffic between all workloads from an application-centric viewpoint. All application dependencies across the entire infrastructure are discovered and displayed, without relying on any security appliances deployed in the network. Illumio reveals all application traffic, between all resources, across all ports and protocols.

A breach is inevitable. While a prevention security model is still required, no solution will ever be 100 percent effective. Eventually, a failure will occur. Surviving that breach, with minimal adverse impact, is as critical as trying to prevent it. Illumio restricts the lateral propagation of traffic between all workloads, preventing a breached workload from connecting to neighboring workloads. This enables an agency to maintain operations even during an active breach.

Illumio enables application visibility by labeling resources along agency-specific definitions, rather than network-specific. These labels are then used to create a least-privilege policy model between all resources. Devices, networks, applications, workloads, and data can be ringfenced across broad segments or granular microsegments.

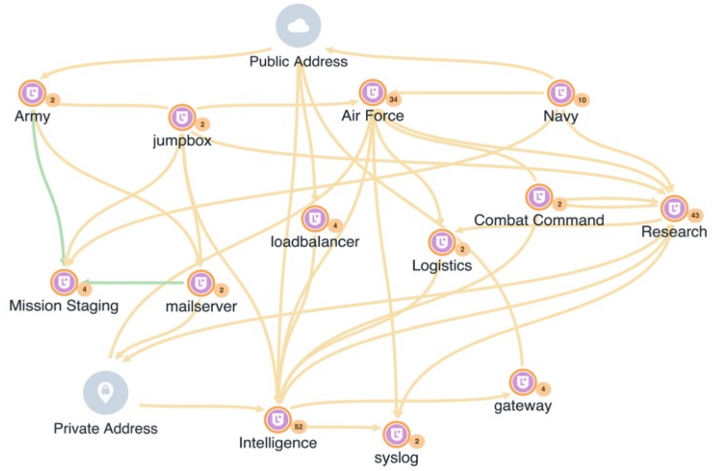


Illumio Zero Trust Segmentation Platform

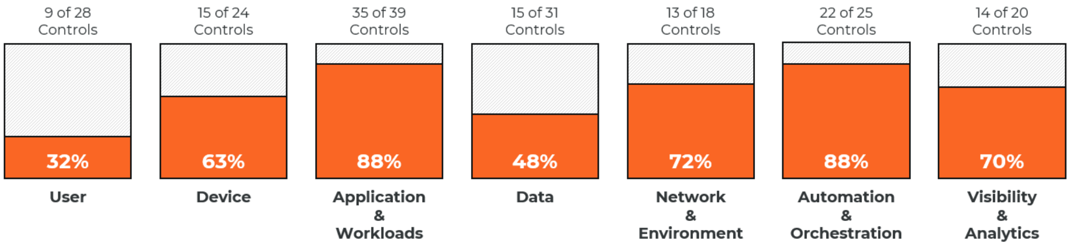
1 **Understand risk**
Visualize all communication and traffic, both known and unknown, between workflows, devices, and the internet.

2 **Define security controls**
With every change, automatically set granular segmentation policies to control unnecessary and unwanted communications.

3 **Contain the attack**
Proactively isolate high-value assets or reactively isolate compromised systems during an active attack to stop the spread of a breach.



Illumio Mapping to DoD Target and Advanced Zero Trust Security Activities



Protecting the user

Requirement: The DoD should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.

Solution: Illumio leverages identity services to enforce access to all resources. This enables the mapping of workload access directly to user or group identity.

Protecting the device

Requirement: The DoD should secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources.

Solution: Illumio enables access control to network resources based on certificates. This maps device identity to cryptographic identity, requiring any device to verify its authenticity before allowing any connection.

Protecting applications and workloads

Requirement: The DoD continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.

Solution: Illumio continuously enforces access between workloads by monitoring risk analytics in real time to protect against zero-day malware and device usage behavior that falls outside of defined baselines.

Protecting data

Requirement: The DoD should inventory, categorize, and label data, protect data at rest and in transit, and deploy mechanisms to detect and stop data exfiltration.

Solution: Illumio enables full visibility across the entire fabric and discovers dependencies between data across all workloads, encrypting all traffic in transit.

Protecting networks

Requirement: The DoD's network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles, with dynamic just-in-time and just-enough connectivity for service-specific interconnections.

Solution: Illumio's use of labels enables a human-readable approach to identifying networks along agency-specific boundaries. Illumio enables network micro-perimeters and network resources to be enforced along micro-segments at any scale.

Enabling automation and orchestration

Requirement: The DoD should automate manual security processes, orchestrating policy-based actions across the enterprise with speed and at scale.

Solution: Illumio leverages integration with SOAR and SIEM platforms to enable fully automated policy changes, eliminating the need for human intervention.

Enabling visibility and analytics

Requirement: The DoD should collect contextual details of all workloads to provide greater understanding of performance, behavior, and activity baseline across the other Zero Trust pillars.

Solution: Illumio collects all telemetry between all applications and workloads, discovering all dependencies and all network traffic, eliminating all blind spots.

Learn more at illumio.com/solutions/government

About Illumio

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.

Copyright © 2024 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.