illumio

TECHNICAL BRIEF

Mapping Illumio to the CISA Zero Trust Maturity Model

Illumio aligns with CISA's five Zero Trust pillars

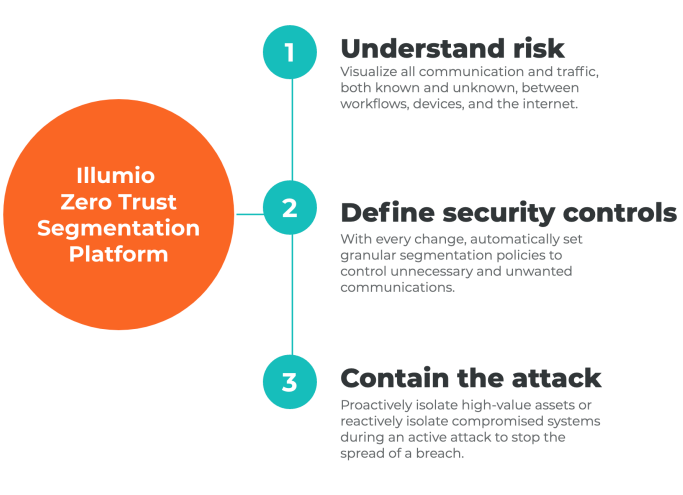
Zero Trust enabled by Illumio

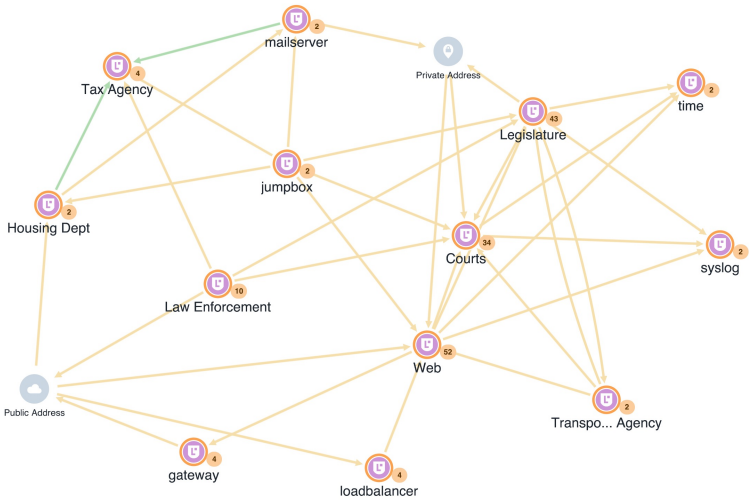
The CISA Zero Trust Maturity Model (ZTMM) requires the enforcement of five pillars of protection for cybersecurity resources: Identity, Devices, Networks, Applications and Workloads, and Data. Illumio's Zero Trust Segmentation platform enables the visualization and granular enforcement of security policies across all five 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 hybrid infrastructure — whether on-premises or in the cloud — are discovered and displayed, without relying on any security appliances deployed in the network or cloud. Illumio reveals all application traffic, between all resources, across all ports and protocols.

In the modern cybersecurity landscape, a breach is inevitable. While a prevention security model is still required, no solution will ever be completely effective. Eventually, a failure will occur. Once the first workload is breached, it needs to be contained and prevented from spreading to other workloads. Illumio enforces restrictions on the lateral propagation of traffic between workloads, at any scale, preventing a hijacked workload from connecting to neighboring workloads. This enables an agency to maintain operations even during an active breach.

Illumio uses application visibility to label resources along agency-defined boundaries. These labels are then used to create a least-privilege policy model between all resources, regardless of the underlying infrastructure. Devices, networks, applications, workloads, and data can be ringfenced across broad segments or granular microsegments. Identity is enforced via integration with identity services such as Active Directory, enabling full coverage across the CISA Zero Trust Maturity Model.





Protecting identity

Requirement: Agencies 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 at any scale. This enables the mapping of workload access directly to user or group identity, enabling the enforcement of access privileges using a least-privilege policy model.

Protecting devices

Requirement: Agencies 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 networks

Requirement: Agency network architecture consists of fully distributed ingress and egress microperimeters and extensive microsegmentation 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 microperimeters and network resources to be enforced along microsegments at any scale.

Protecting applications and workloads

Requirement: Agency 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 from external risk-exposure sources to protect against zero-day malware and device usage behavior that falls outside of defined baselines.

Protecting data

Requirement: Agencies 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 hybrid cloud architecture and discovers dependencies between data across all workloads. Illumio enables the encryption of all traffic, securing data both at rest and in transit between all resources.

Learn more at illumio.com/solutions/government

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.