illumio

INDUSTRY BRIEF

Illumio for Government

Zero Trust Segmentation (ZTS) ensures mission resilience in the public sector

The challenge

Government organizations are constantly at risk for adversary attacks, made more difficult due to the ever-increasing attack surface. This makes it imperative to assume breaches are inevitable.

The annual FBI Internet Crime Report shows that 115 government organizations were victims of ransomware over the last year. Known malware like Triton show that traditional prevention and detection technologies are no longer sufficient to stop attacks.

Preparation is a challenge. This is compounded by an inability to see the complete application and workload environment. These hybrid environments are often managed by siloed methods, resulting in significant risk.

Regardless of the threat, the mission must continue. Implementing Zero Trust breach containment strategies ensures resilience despite an adversary's best efforts. By implementing a Zero Trust strategy, governments can improve mission resilience, meet statutory and legal mandates, and build trust.

Illumio is committed to meeting stringent government security requirements

Common Criteria

FedRAMP
'In Process'

FIPS VALIDATED 140-2

Section508.gov
GSA Government-wide Section 508 Accessibility Program

The solution

Illumio delivers these benefits with Zero Trust Segmentation (ZTS). ZTS enables visibility you can trust and granular control of all lateral network traffic between workloads, whether on-premises, in the cloud, or on the endpoint.

The Illumio ZTS Platform delivers:

- **Unparalleled visibility:** Gain a complete, detailed view of all traffic flows between workloads in seconds
- **Consistent enforcement:** Implement uniform policy across hybrid environments without silos
- **Enhanced cyber resilience:** Contain and reduce the impact of breaches for uninterrupted mission execution.

How it works

Illumio ZTS segments on the host. This means no matter where a workload is located, it can be protected rapidly and at scale.

By restricting traffic movement in the data center, the cloud, and on endpoints, Illumio blocks attackers from infiltrating deeper into the network. With Illumio, government organizations can stop and contain attacks before they spread and halt the mission.

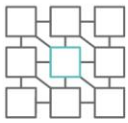
The Illumio ZTS Platform provides these key benefits:

- **ZTS in minutes:** Rapid breach containment prevents operational impacts without requiring a significant amount of time or a deep technical bench.
- **Protect legacy workloads:** Application ringfencing protects mission-critical technology, regardless of support status.
- **Proactive attack prevention:** Easily shut down high-risk ports commonly used by adversaries to spread through an environment.

Zero Trust Segmentation use cases

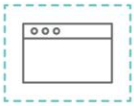
Eliminate blind spots

Visualize all communications and traffic between workloads across on-prem and cloud environments.



Prevent lateral movement

Lower risk of adversaries accessing sensitive information by controlling east-west traffic.



Ringfence high-value assets

Proactively control communications and isolate business-critical applications and environments.

Move securely to the cloud

Whether a "lift and shift" or re-architecture, visibility and protection follow for mission continuity.

Ensure continuous protection

Maintain protection in disconnected and air-gapped networks, even if access to Illumio is lost.

Control information sharing

Restrict third-party access to only allow what is necessary and wanted within the environment.

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware 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