illumio

PRODUCT BRIEF

The Illumio Zero Trust Segmentation Platform

One platform. One console. Any environment.

Breach containment. The new paradigm.

The attack surface is ever expanding

In the past two years, ransomware attacks have become increasingly pervasive, occurring every 11 seconds and affecting a staggering 76% of organizations. This highlights the significant challenge faced by CISOs and security and IT teams as environments shift from on-premises to a hyperconnected, cloud-first, hybrid landscape. The expanding attack surface brought about by digital transformation is increasing the risk for all organizations.

The sprawl of hybrid IT introduces significant gaps in the attack surface. Attackers are feasting on a landscape of multiple clouds, endpoints, data centers, containers, VMs, mainframes, production and development environments, OT and IT, and more.

The only solution that handles communication across all types of workloads

The Illumio Zero Trust Segmentation (ZTS) Platform is the only solution that handles it all: Endpoint-Endpoint, Endpoint-Server, Server-Server, as well as extensive support for cloud workloads, containers, IoT, and OT devices. Empowering organizations to be more resilient for whatever may come their way.

This innovative approach and unparalleled visibility allows us to move from the “find and fix” mindset to the “limit and contain” reality. Illumio uses the insight into traffic flows to apply the principles of Zero Trust to focus on breach containment, not just prevention and detection.

Key Benefits

See risk

Unparalleled visibility shows all communication and traffic between workloads and devices across the hybrid attack surface.

Set policy

Set granular and flexible segmentation policies that control communication between workloads and devices to only allow what is necessary and wanted.

Stop the spread

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

Protect workloads with the industry's first platform for breach containment

Unlike prevention and detection technologies, ZTS contains the spread of breaches and ransomware across the hybrid attack surface by continually visualizing how workloads and devices are communicating, creating granular policies that only allow wanted and necessary communication, and automatically isolating breaches by restricting lateral movement proactively or during an active attack. ZTS is a foundational and strategic pillar of any Zero Trust architecture.

Full attack surface coverage

The definition of the perimeter is becoming less clear as endpoints connect from various locations, server workloads are distributed between the data center and the cloud, and the number of IoT and OT devices continues to rise.

For complete coverage of the modern attack surface, Illumio not only covers traditional on-premises assets and endpoints. It can also segment and protect agentless assets like legacy systems, IoT and OT, and cloud workloads, eliminating silos and improving cyber resilience.

Critical Capabilities

Enable Zero Trust

Illumio ZTS supports all pillars of Zero Trust, protecting data, users, devices, workloads, and networks.

- Maintain continuous, risk-based verification
- Enforce least-privilege access
- Gain comprehensive security monitoring

Strengthen cyber resilience

Be prepared and prevent systems and networks from being derailed if security is compromised.

- Implement granular controls to limit attack scope
- Identify areas of high risk
- Build long-term protection

Breach containment in minutes

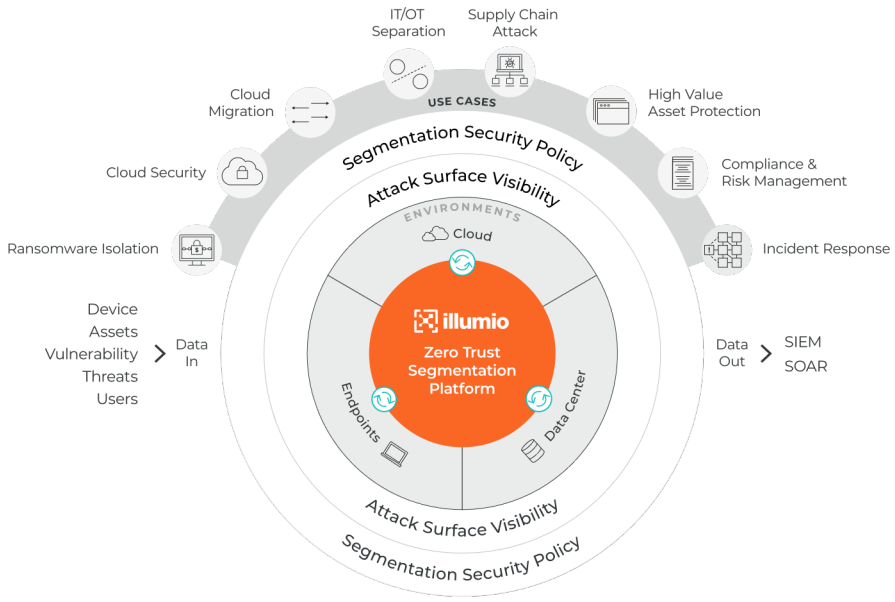
Apply Zero Trust principles to focus on containment, not just prevention and detection.

- Stop ransomware from spreading
- Quickly quarantine compromised systems
- Speed response with automated alerts

Visibility made easy

Gain a complete, detailed view of all traffic flows between workloads in seconds.

- Identify risk by assessing current traffic patterns
- Rapidly discover shadow IT
- Analyze traffic flows and patterns for policy compliance



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.