



Assume Breach. Minimize Impact. Increase Resilience.

Stop breaches and ransomware from spreading across the hybrid attack surface

Zero Trust Segmentation (ZTS) is a modern security approach that contains and minimizes the impact of breaches and ransomware.

Unlike prevention and detection technologies, ZTS contains the spread of breaches 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.

Digital transformation is dramatically expanding the attack surface, and attacks like ransomware are more pervasive than ever. In the past two years alone, 76% of organizations were attacked by ransomware, and ransomware attacks occur every 11 seconds.

The tools traditionally used for security cannot solve this new problem.

Prevention and detection tools like firewalls, EDRs, or SIEM only give surface-level visibility into traffic flows that connect the applications, systems, and devices that are communicating across IT. They were not built to contain and stop the spread of breaches.

Illumio is a Leader in microsegmentation



The Forrester New Wave™: Microsegmentation, Q1 2022

Protecting more the 2 million workloads for organizations of all sizes. from Fortune 100 to small business

servicenow









Morgan Stanley



BNP PARIBAS

DocuSign



CATHAY PACIFIC



BlueCross

Global law firm stops ransomware with Illumio

- Phishing email infiltrated unprotected endpoint and spread to SQL servers
- Incident response identified 'patient zero' via Illumio real-time workload telemetry data integrated into SIEM
- Illumio instantly isolated 12 impacted servers, stopping the spread of the breach. No data loss confirmed; only 4-hours from infiltration to remediation

READ STORY

Significant risk reduction in weeks

- Cut business risk in two weeks
- Deployed Illumio ZTS Platform to 2,000+ servers to visualize all communication and traffic between workloads
- Discovered several areas of risk such as unnecessary internet connections and open ports
- Immediately set segmentation policy to protect high-value applications and assets by only allowing necessary communication



Protecting hybrid and multi-cloud IT

- ServiceNow customers have high expectations, and client audits routinely put IT security to the test
- Illumio was identified to protect core services and domain controllers across a multi-cloud environment
- A hypervisor-based microsegmentation tool previously failed due to cost and technical complexity
- Illumio ZTS Platform provides visibility to show risk, feeds telemetry into a SIEM for investigations, and segments high-value assets to improve cyber resilience

servicenow

READ STORY



One Platform. One Console. Any Environment.

The Illumio Zero Trust Segmentation Platform is the industry's first platform for breach containment. Scalable yet easy to use, Illumio ZTS provides a consistent approach to microsegmentation across the entire hybrid attack surface — from multi-cloud to data center to remote endpoints, from IT to OT. With Illumio ZTS, organizations can quickly and easily:

See Risk

See risk by visualizing all communication and traffic between workloads and devices across the entire hybrid attack surface.

Set Policy

With every change, automatically set granular and flexible segmentation policies that control communication between workloads and devices to only allow what is necessary and wanted.

Stop the Spread

Automatically isolate compromised systems and high-value assets in minutes to stop the spread of an active attack.



Illumio Core

Segmentation for on-premises and cloud data center workloads

Illumio CloudSecure

Agentless segmentation for cloud-native workloads

Illumio Endpoint

Segmentation for end-user MacOS and Windows devices



