Illumio for Managed Service Providers

Uses Cases for Zero Trust Segmentation

Segmentation secures today's evolving threat landscape

Digital threats are evolving at an unprecedented pace. Businesses are facing cyberattacks that not only breach defenses but also propagate within networks, causing significant downtime and financial loss. Ransomware can halt entire operations, demanding exorbitant ransoms to release data.

Traditional cybersecurity approaches assume that everything within a network is trustworthy. But this leads to a reactive, not proactive, security posture. Once breached, traditional defenses offer little resistance to lateral movement. This allows attackers to escalate privileges and inflict widespread damage.

A modern cyber strategy with Zero Trust Segmentation (ZTS) at its core assumes breaches will happen and adopts a "never trust, always verify" mindset. ZTS microsegments network resources so that access is granted as needed, stopping lateral movement across the cloud, endpoint, and data center environments.

Use cases for Illumio ZTS

Visibility

Map all communication and traffic between workloads and devices with Illumio.

Illumio maps interdependencies across hybrid multi-cloud environments. This provides end-to-end visibility into how applications, workloads, and systems interact. Mapping is crucial for MSPs because it allows them to identify critical assets and build security policies that protect these connections without disrupting business functions.

Benefits of ZTS for MSPs

- ZTS offers MSPs a unified, dynamic defense against cyber threats and is the cornerstone of any robust cybersecurity strategy.
- ZTS ensures that clients' networks are resilient to both external breaches and insider threats.
- ZTS adapts to threats in real-time. This gives MSPs and their clients a sustainable, scalable security posture.

Ransomware containment

Stop and contain ransomware attacks at their source to prevent them from spreading.

Ransomware is the top cause of breaches for many industries, and attacks can occur across any sized business. Illumio is a pivotal ally for MSPs and their clients against ransomware. We help you operationalize the NIST Cybersecurity Framework (CSF) — the gold standard for strategically assessing an organization's cyber risk management.

ZTS isolates attacks at their source. This reduces ransomware's ability to move through your cloud, endpoint, and data center environments.

Containing ransomware with Illumio protects critical infrastructure and sensitive data while ensuring business continuity in the face of cyber threats.

Environmental separation

Easily separate environments to stop breaches from spreading to critical assets.

Without clear network borders, the complexity of network security grows, exposing systems to risk. With Illumio ZTS, MSPs can separate systems by building policies that automatically adapt to each change in your clients' environments. This reduces the attack surface by preventing traffic from moving between hybrid environments — without impacting operations.

ZTS can help speed up cybersecurity compliance and meet regulatory or industry mandates. These commonly share requirements based on cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Critical Security Controls, all without the complexity of touching physical networks.

Admin isolation and jump hosts

See and control administrative access.

Illumio allows you to limit admin access to only hardened, bastion jump hosts where access to critical systems is tightly regulated and monitored. This method isolates administrative tasks within a secure segment of the network. As a result, it reduces the risk of unauthorized access and lateral movement within the IT infrastructure.

IT/OT convergence

Secure the integration of cyber-physical systems.

Business transformation is driving the adoption of automation and digitalization. In many industries, there are business needs for the convergence of IT and OT. Still, any attack on either environment must be contained to maintain service delivery.

With Illumio ZTS, you can collect connectivity data from IT and OT devices to map interdependencies. It can be enriched with asset and vulnerability scanning data.

Illumio also helps you apply easy-to-understand labels based on function and risk. You can enforce policy based on least privilege and even use network switches for legacy systems.

Cyber resilience and incident response

Identify your critical risk and reduce your attack surface, limiting the ability of an attacker to move laterally.

Planning is a crucial principle of cybersecurity hygiene. We must assume breaches will happen and proactively prepare for them. MSP clients must be able to withstand and quickly rebound from cyber threats.

Illumio stops ransomware from causing a major business failure by reducing the attack surface and containing attacks at their source. This prevents ransomware from reaching critical systems and data. Illumio ZTS also limits a breach's impact, helping businesses stay resilient and preserve their reputations.

Illumio also helps you proactively reduce the attack surface by providing application dependency maps that reveal intended and unintended connectivity between applications.

The proven microsegmentation leader

Illumio was named a leader in The Forrester Wave™: Microsegmentation Solutions, Q3 2024. Illumio is a Representative Vendor in the Gartner Market Guide for Microsegmentation.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.