illumio

INDUSTRY BRIEF

Illumio: Securing Higher Education

Zero Trust Segmentation (ZTS) protects sensitive data and ensures continued operations during a breach

The challenge

The education sector is a high-value target for threat actors. In fact, CISA has reported that cyberattacks on educational institutions have risen from 400 in 2018 to more than 1,300 since then.

Threat actors breach academic resources to hijack operations via ransomware, steal student records for identify theft, and siphon intellectual property from academic research.

Many schools also use academic tools hosted in the public cloud that are accessed remotely from anywhere – often outside the network perimeter. As a result, traditional firewalls aren't enough to stop breaches. Security teams must protect individual workloads no matter where they reside.

Addressing these risks requires architecting academic network environments into two broad security segments: administrative workloads and student workloads. These, in turn, need to be protected by strong perimeter network security.

The solution

Illumio delivers these benefits with Zero Trust Segmentation (ZTS). ZTS enables granular control of all lateral network traffic between workloads, both in on-premise data centers and in the public cloud.

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 ransomware and breaches for uninterrupted operations

Key benefits of Illumio

Full network traffic visibility

Gain full visibility into all traffic between all workloads, eliminating all blind spots.

Breach containment

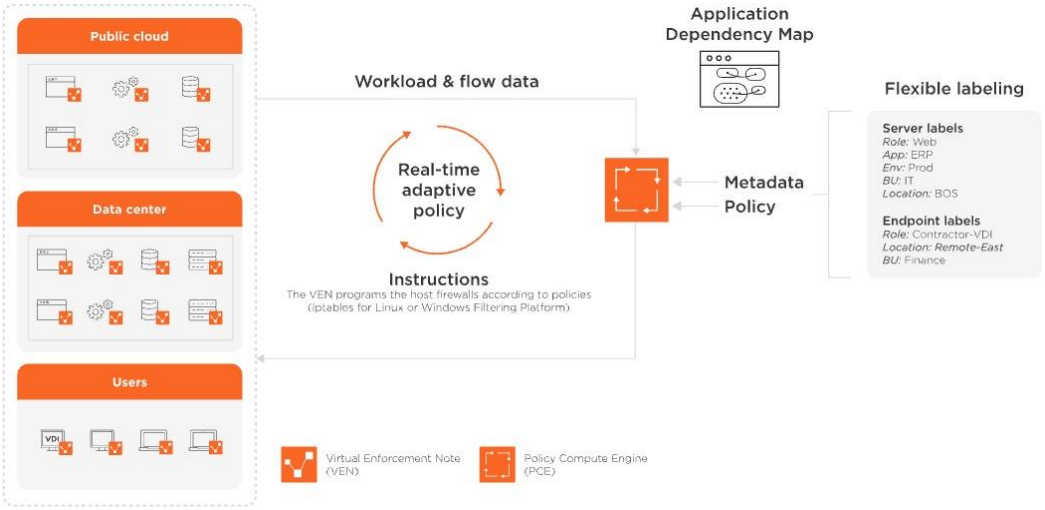
Breaches are inevitable. The Illumio ZTS Platform creates a least-privilege policy model to stop and contain breaches.

Lower cyber insurance costs

To reduce premiums, cyber insurance requires lateral segmentation between workloads. Illumio enables these segmentation requirements.

Meet Zero Trust security audits

Illumio enables granular control of traffic between all workloads, enabling a Zero Trust architecture that can meet audit requirements.



How it works

Campus networks are often treated as a transit network. The institution serves as a kind of ISP, giving students open access to the Internet. Traditionally, security is at the perimeter, limiting inbound traffic but allowing most outbound traffic.

However, this architecture doesn't consider that many threat vectors reside within the campus network, whether accidental or deliberate. Once malware infects one workload, it will often issue command-and-control traffic out to the Internet to "phone home" for instructions. Therefore, outbound traffic needs to be addressed by the security architecture just as much as inbound traffic.

Despite the most robust perimeter network security, breaches are inevitable. Illumio can secure all endpoints, limiting the risks introduced by malware trying to breach the campus network from unprotected devices.

Illumio ZTS contains breaches by isolating them at the first infected workload, enabling academic services to continue without interruption, even during an active breach.

By restricting traffic movement in the data center, the cloud, and on endpoints, Illumio blocks attackers from infiltrating deeper into the network. With Illumio ZTS, security teams can stop and contain attacks before they spread and cause significant harm.

The Illumio ZTS Platform helps institutions visualize the network and begin segmenting workloads on day one:

- **See east-west network traffic.** Discover all workloads and visualize their flows with Illumio's application dependency map.
- **Label all workloads with contextual data** (e.g., role, application, environment, location, etc.), creating metadata used by Illumio Core to identify application dependencies by owner, not by network addressing.
- **Create an allow-list policy model** where only the required traffic is allowed between workloads, blocking all else by default. This could include blocking SSH and RDP laterally between all workloads, only allowing it from central administrative hosts and eliminating excessive levels of workload-to-workload interconnectivity. This shrinks the east-west attack surface.

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.