# Illumio: Securing Elementary and Secondary Education

Zero Trust Segmentation (ZTS) contains ransomware and ensures continued operations during a breach

## The challenge

According to a 2022 U.S. Government Accountability Office report, at least eight school districts in the U.S. were breached in the 2022-2023 academic year alone, and half had to cancel classes or close completely. Breaches costed these districts $50,000 to $1 million on average.

Breaches on elementary and secondary schools can make academic resources inaccessible, halt remote learning, and put student data at risk. Schools are at increased risk of cyberattack due to a lack of cybersecurity awareness among students and staff, few security resources, and limited IT staff. These challenges make schools tempting targets for bad actors looking to extract ransom payments and steal student identities.

The most significant threat is school-provided endpoints which are often used by students and staff both on campus and at home, leaving them open to risky public networks. Schools must have visibility into traffic between all resources to create and enforce least-privilege security policies on all workloads, whether on the campus network or remote.

## The solution

With the Illumio Zero Trust Segmentation (ZTS) Platform, schools get access to:

- **Unparalleled visibility:** Visualize all traffic between workloads and devices across the entire hybrid attack surface.
- **Consistent enforcement:** Set flexible, granular segmentation policies to to only allow what is necessary and wanted.
- **Enhanced cyber resilience:** Proactively isolate high-value assets or reactively isolate compromised systems during an active attack to stop the spread of a breach.

## Key benefits of Illumio

### Full network traffic visibility

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

### Contain ransomware

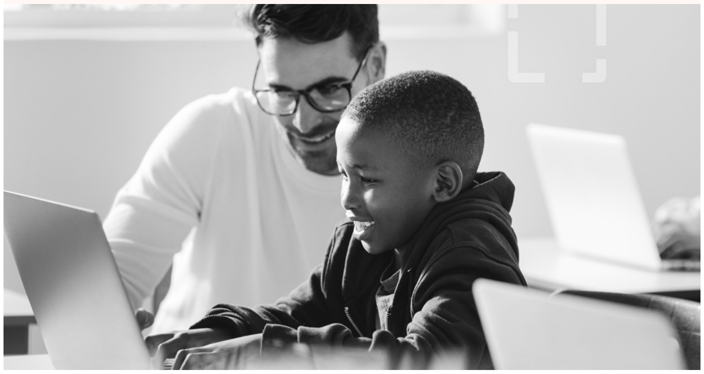
Breaches are inevitable. Illumio prevents ransomware from spreading across school resources, maintaining operations and data privacy.

### Lower recovery expenses

Restoring school compute resources from a ransomware breach can be expensive. Illumio stops lateral movement, reducing costs associated with a breach.

### Protect shared school resources

Students often take school-issued devices home, making protecting them a challenge. Illumio enforces endpoint policy regardless of where devices connect.



## How it works

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

However, this architecture doesn't address the fact that many threats reside within the campus network, whether accidental or deliberate. Once malware infects one workload, it can spread very quickly to neighboring workloads. Modern ransomware can spread faster than it can be detected, making a proactive approach to security essential.

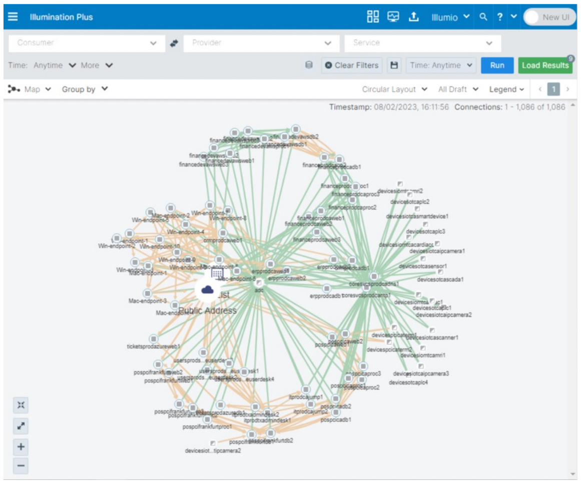
The Illumio ZTS Platform enables end-to-end visibility and the ability to make sense of that visibility to protect workloads. Illumio helps visualize traffic between all workloads, revealing application behavior. Labels can then be assigned to workloads identified by what they do rather than their IP address. This enables a metadata-driven policy model, only allowing required traffic and denying all else by default, at any scale, from hundreds to hundreds of thousands of workloads.

In addition to protecting school compute workloads, maintaining student data privacy is a high priority. The U.S. Government Accountability Office found in a 2020 report that breaches on schools leaked students' grades, bullying reports, and sensitive personal data like social security numbers – leaving students vulnerable to emotional, physical, and financial harm.

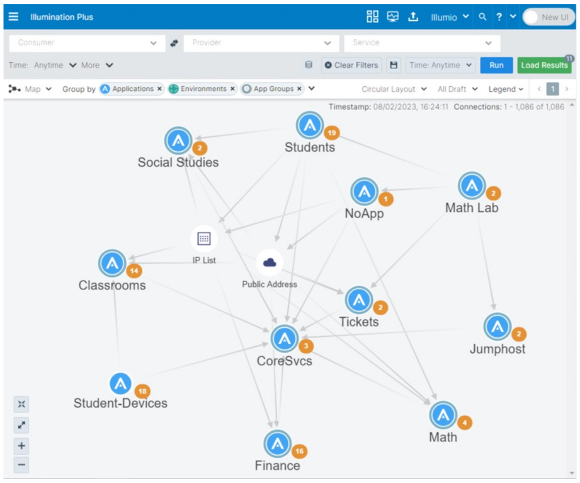
Illumio ZTS helps prevent student, staff, and school administration data from being compromised during a breach or ransomware attack. Security teams can proactively prepare for a breach by isolating high-value resources and databases. During an active attack, they can reactively isolate compromised systems to stop the spread of a breach. This enables schools to continue operations without interruption, even during an active attack or restoration process.

With Illumio ZTS, small security problems don't escalate into major cyber disasters. Schools want to focus on learning, not on paying a ransom, restoring downed systems, and scrambling to continue operations during a breach. Illumio ensures that learning continues – securely.

Visualize all traffic



Segment according to function



## 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.

Copyright © 2023 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.