illumio | netskope

SOLUTION BRIEF

Illumio + Netskope: Extend Zero Trust to Remote Access Architecture

Automatically see compromised workloads and update Netskope One remote access permissions with Illumio Zero Trust Segmentation

Securing Zero Trust enforcement points

The NIST Zero Trust Architecture lays out three primary Zero Trust enforcement points: identity, network access, and workload segmentation. Identity is implemented at the endpoint, authenticating the end user, and network access is implemented at the ZTNA boundary, historically using VPN.

Workload segmentation defines every destination workload as a dedicated trust boundary — also called microsegmentation. This means only required traffic can move laterally between workloads, denying all else by default.

If malware compromises any of these workloads, the workload needs to be quarantined from all access. Most importantly, all of this needs to happen dynamically.

Workload segmentation has historically been the most difficult to implement. Traditionally, workload security uses some type of security appliance deployed in the network, such as a firewall, IDS/IPS solution, or enforcing access via network boundaries.

But trying to solve workload-specific requirements using network-specific solutions doesn't scale — the result is broad segmentation, not microsegmentation. And any changes to workloads within those boundaries are usually invisible to the first two Zero Trust enforcement points.

If any workload gets compromised by malware and quarantined from other workloads by a workload management controller, how is this change made visible to the network access enforcement boundary?

Key benefits

Full visibility across the hybrid multi-cloud
By combining Illumio ZTS with Netskope One, organizations gain a consistent, real-time view of user-to-application and application-to-application traffic.

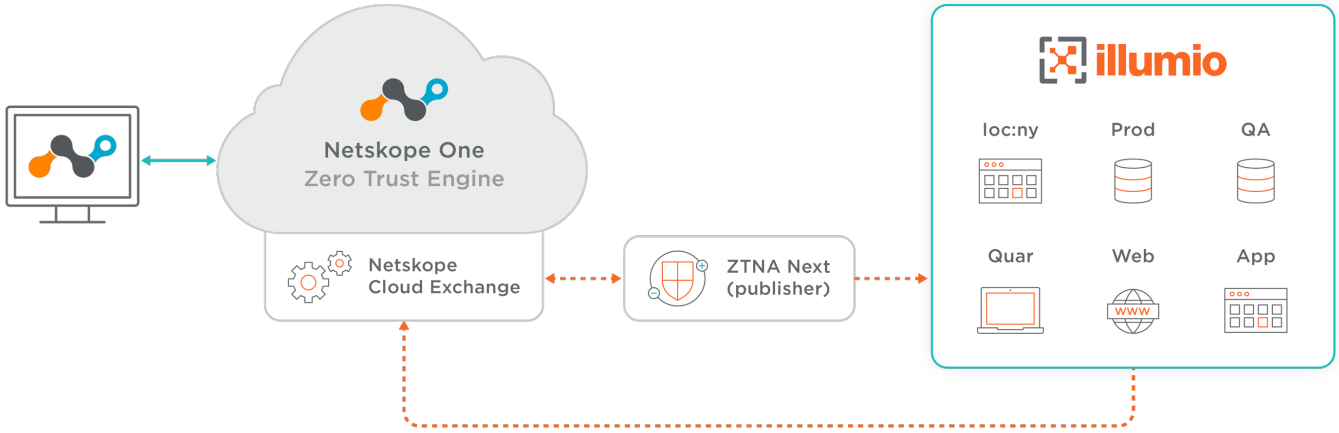
Protect users from non-compliant workloads
Combined visibility defines Netskope policy to block access between users and potentially compromised workloads or workloads in segmented environments.

Enforce dynamic ZTNA policy
Netskope's security policies automatically update user access based on metadata from Illumio, eliminating the need to rewrite rules as workload attributes change.

Secure cloud workloads with Illumio and Netskope

Illumio manages all workloads at any scale using labels, providing application-centric visibility across all hybrid, multi-cloud environments. This enables microsegmentation of every single workload, defining every workload as a dedicated trust boundary and enforcing least-privilege access between all workloads.

When integrated with Netskope One, Illumio identifies a workload compromised by malware, re-labels it as quarantined, notifies Netskope of this change. This allows Netskope to remove the quarantined workload from its remote access permissions.



Ensure a complete Zero Trust architecture

Integrating Illumio Zero Trust Segmentation with Netskope One solves two key challenges:

- **Extend visibility** from re-labeled workloads to Netskope
- **Stop lateral movement,** ensuring a small security incident doesn't become catastrophic. Illumio assumes a breach will occur and is ready to contain it anytime.

Because Illumio enforces network access directly at the workload, it remains agnostic to the underlying network. This means Illumio can extend workload enforcement at very high scale across any network.

By integrating Illumio with Netskope, you can complete your Zero Trust security architecture.

Netskope + Illumio plugin

Illumio has developed a plugin which is deployed in the Netskope Cloud Exchange Platform. This plugin polls Illumio at regular intervals for any workload which has been re-labeled as Quarantine, and if Illumio responds with such a label change, this plugin then updates Netskope of this change. In addition, if a workload is changed from QA to Production, Netskope is notified of this label change and the user loses access to that workload.

This enables Netskope to dynamically update access Policy, with full visibility into dynamic workload changes, Together, Illumio and Netskope leverage a dynamic Zero Trust solution.

Get started today

- Download Netskope Cloud Exchange.
- Find the Illumio Plugin for Threat Exchange in the Netskope Cloud Exchange Platform.

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.

About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One Platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go.