

Illumio + Netskope: Extend Zero Trust to Remote Access Architecture

See compromised workloads in real time with Illumio and automatically update Netskope One remote access permissions.

Building consistent, complete Zero Trust

The NIST Zero Trust model calls for three key enforcement points: identity (who's accessing), network access (how they get in), and workload segmentation (what they can reach).

Identity and network access are familiar territory — you authenticate users and control access at the network perimeter.

But when it comes to securing what's inside your environment, that's where workload segmentation comes in.

Workload segmentation means every workload becomes its own trust boundary. Only the traffic that should be allowed is permitted. Everything else gets blocked by default.

Most security tools weren't built for this. They rely on network boundaries and static rules.

That's fine — until a workload changes or malware sneaks in. Suddenly, you've got a blind spot.

Closing the loop

When you combine Illumio breach containment with Netskope One, you close the loop between workload security and user access dynamically and at cloud scale.

Smarter, faster Zero Trust enforcement

Static policies can't keep up with dynamic threats. Illumio and Netskope bring Zero Trust enforcement that adapts in real time — no manual rule changes required.

Here's how it works:

Key benefits

See every connection, everywhere

Get full visibility into lateral traffic across your hybrid multi-cloud. That means a real-time, consistent view of both user-to-app and app-to-app connections.

Protect users from high-risk workloads

If a workload is compromised or quarantined, Netskope policies automatically block user access. Combined visibility makes sure users never connect to workloads that shouldn't be trusted.

Zero Trust access that updates itself

Forget manual rule changes. Netskope policies adapt instantly using Illumio metadata. When workloads move, change, or get quarantined, access rules update on the fly.

- Illumio sees a compromised workload. It immediately re-labels it as quarantined.
- Netskope gets the update. The quarantined workload is removed from user access permissions with no manual rule changes or delays.
- Your Zero Trust architecture just got smarter. Threats get contained, users lose access to high-risk workloads, and your environment stays one step ahead of bad actors.

A true end-to-end Zero Trust architecture

Pairing Illumio with Netskope One closes two major security gaps: visibility and containment.

- **See what's changing, instantly.** When Illumio re-labels a workload, like marking it quarantined, Netskope gets the update in real time.
- **Stop threats before they spread.** Illumio assumes breaches will happen, so it's always ready to contain lateral movement and keep small incidents from turning into disasters.

Because Illumio enforces access directly at the workload, it doesn't matter what network you're on; it scales everywhere. Together, Illumio and Netskope give you a true end-to-end Zero Trust architecture.

Illumio + Netskope plugin

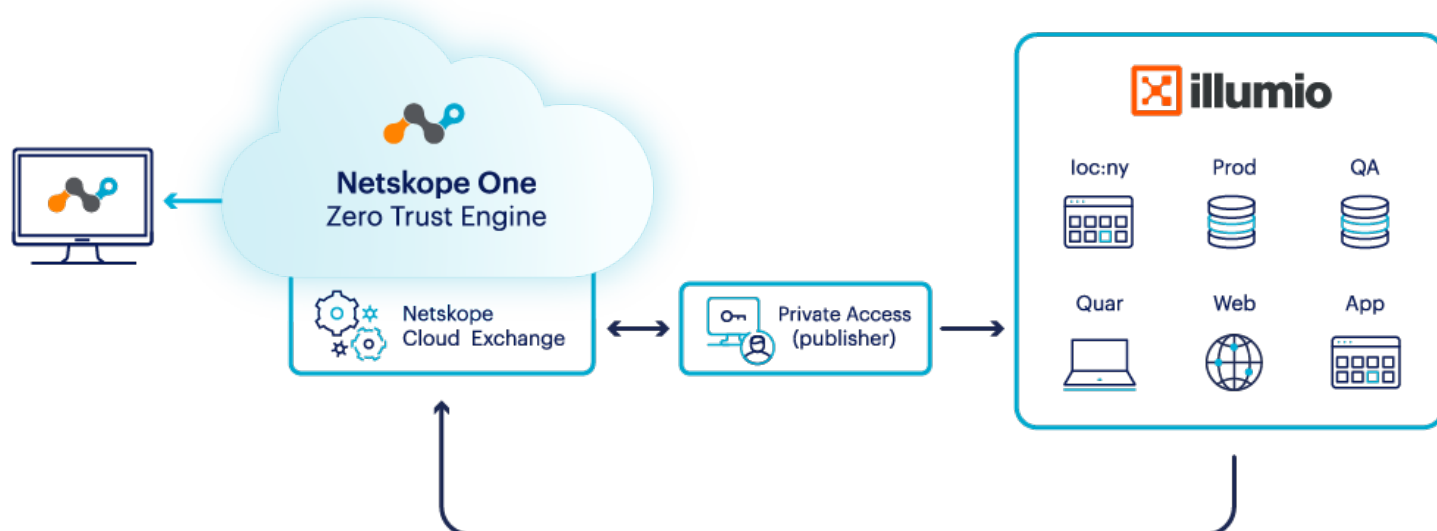
The Illumio plugin runs inside the Netskope Cloud Exchange Platform, constantly checking for changes in workload labels. If Illumio flags a workload as quarantined, Netskope instantly updates access to block it.

The same goes for other changes, such as a workload shifting from QA to production. Netskope gets the update and adjusts access automatically.

The result is dynamic policies that adapt in real time, full visibility into workload changes, and a truly living Zero Trust solution powered by Illumio and Netskope.

Get started now

- Download [Netskope Cloud Exchange](#)
- Find the [Illumio Plugin for Netskope](#)



About Illumio



Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2025 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.