illumio | netskope

SOLUTION BRIEF

Illumio + Netskope for DORA Compliance

Meet key DORA requirements with the Illumio plugin for the Netskope Cloud Exchange

Why Illumio + Netskope for DORA?

The financial sector relies on more information and communication technology (ICT) than ever, making it more vulnerable to cyberattacks and operational disruptions. The EU created the Digital Operational Resilience Act (DORA) to help financial institutions withstand, respond to, and recover from ICT-related threats.

Meeting DORA's requirements isn't just a choice anymore. It's necessary to keep trust, security, and strength in today's connected financial world.

But how can you meet these standards quickly? Illumio and Netskope have partnered to help you achieve DORA compliance with microsegmentation and ZTNA.

Meeting DORA's core pillars

DORA has five core pillars to help financial services build a strong cyber resilience framework:

- ICT risk management
- Incident reporting
- Operational resilience testing
- Third-party risk management
- Information sharing

DORA compliance includes many different rules, and no single tool can cover all of them. To make sure you meet as many rules as possible, it's important to use platforms that handle multiple areas.

By using the combined power of Illumio and Netskope, security teams can successfully meet network segmentation requirements with the Illumio plugin for Threat Exchange.

Key benefits

Full visibility across the hybrid multi-cloud

Combine Illumio Zero Trust Segmentation (ZTS) with Netskope One to get a consistent, real-time view of user-to-application and application-to-application traffic.

Protect users from non-compliant workloads

The combined visibility of Illumio and Netskope allows Netskope policies to block access to potentially compromised or segmented workloads.

Enforce dynamic ZTNA policy

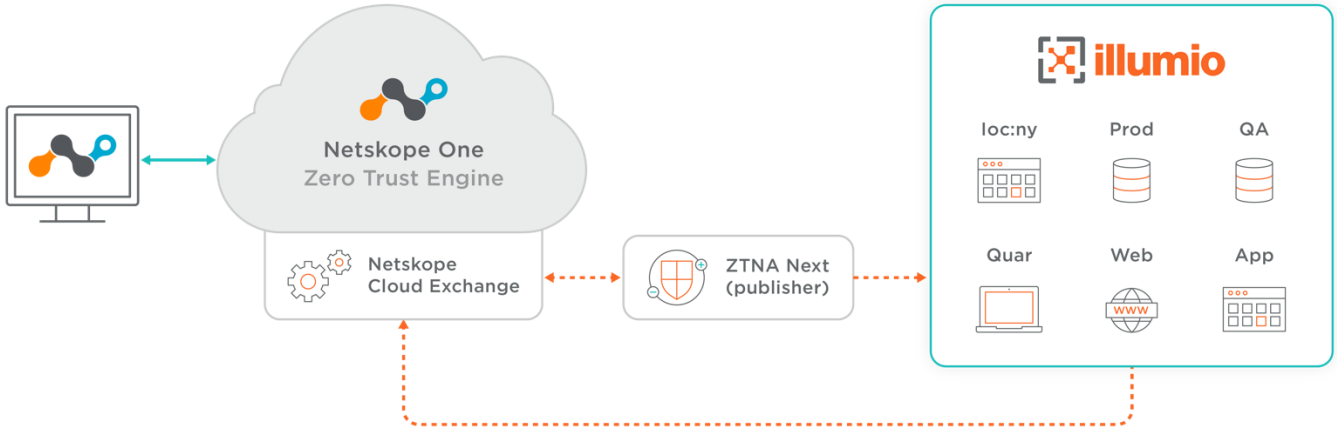
Netskope's security policies automatically update user access based on metadata from Illumio, so there's no need to rewrite rules when things change in the workload.

DORA's network segmentation requirements

Objective: Improve ICT security by reducing the risk of unauthorized access and keeping breaches within separate network sections.

Key requirements

- **Segregation and segmentation:** Build network segregation and segmentation based on the criticality, classification, and risk profile of ICT systems and networks



- **Access controls:** Use strong network access controls to make sure only approved personnel can access critical or sensitive network segments.
- **Dedicated networks:** Create separate and dedicated networks for managing critical ICT assets to stop unauthorized access.
- **Encryption:** Use encryption to secure network connections, especially when dealing with critical or sensitive data, to keep its confidentiality and integrity while in transit.

Implementation

- **Mapping and visualization:** Manage and identify vulnerabilities by mapping and visualizing network segments.
- **Risk-based approach:** Look at each systems' risk profile and importance to separate the network using the right security measures.

Benefits

- **Enhanced security:** Stop breaches from spreading and protect sensitive data.
- **Improved resilience:** Keep important systems separate to make sure they continue running during security incidents.

Illumio plugin for Threat Exchange

The Illumio plugin for the Threat Exchange module of the Netskope Cloud Exchange platform helps you meet DORA compliance requirements.

This plugin regularly checks with Illumio to see if any workload has been re-labeled as quarantined. If Illumio reports a change, the plugin updates Netskope. And if a workload is changed from quality assurance to production, Illumio informs Netskope, and the user loses access to that workload.

The Illumio plugin allows Netskope to update access rules in real time and easily keep track of workload changes.

Get started today

- Learn more about the Netskope Cloud Exchange
- Find the Illumio plugin for Threat Exchange in the Netskope Cloud Exchange Platform

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes how workloads and devices are communicating, creates granular segmentation policies which only allow necessary communication, and automatically isolates ransomware and breaches.

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.

Copyright © 2024 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.