Illumio + Check Point: Unified Policy Across the Hybrid Mesh

Share logs, rules, and labels to contain attacks between and within zones.

Hybrid mesh breaches spread

Frontier AI lets attackers find flaws, exploit them, and spread through a network in one automated run, often faster than teams can patch. Once inside, they can reach critical assets in minutes.

Hybrid networks make this harder. Firewalls guard the borders between data centers and clouds, but inside each zone, the web, app, and database tiers still talk freely. That east-west traffic is where attackers move, and perimeter controls weren't built to see it.

Two controls, one model

Check Point and Illumio close this gap together:

- Check Point guards the borders. Its firewalls stop threats in the north-south traffic that moves between zones, clouds, and the data center.
- Illumio guards what's inside. It controls east-west traffic between workloads, so an attack that gets past the firewall can't spread.

A shared set of labels ties the two together. Both platforms use the same labels in their policies, so security and firewall teams work from one view of every app.

A shared policy language

An Illumio label describes what a workload is and what it does. A rule tied to a label covers every workload with that label, in any cloud or data center. And it keeps up as workloads come and go.

Key benefits

The integration helps contain frontier AI attacks in three ways:

Write firewall rules in app terms

Use labels like App and Role. Check Point maps them to current IPs, so no one manages address lists.

Fix the riskiest paths first

Use Illumio Insights to see which Check Point rule allows each flow and rank exposures by how close they get to critical assets

Contain breaches fast

Quarantine a compromised workload while the rest of the app keeps running.

Most rules use four types of labels:

- App: the app or service, such as an online store
- Role: the job a workload does, such as web, database, or jump host
- Environment: production, staging, or development
- Location: a data center, cloud region, or site

With these labels, a firewall rule reads like a plain business rule, such as "Development can't reach Production" or "Only jump hosts can reach admin ports."

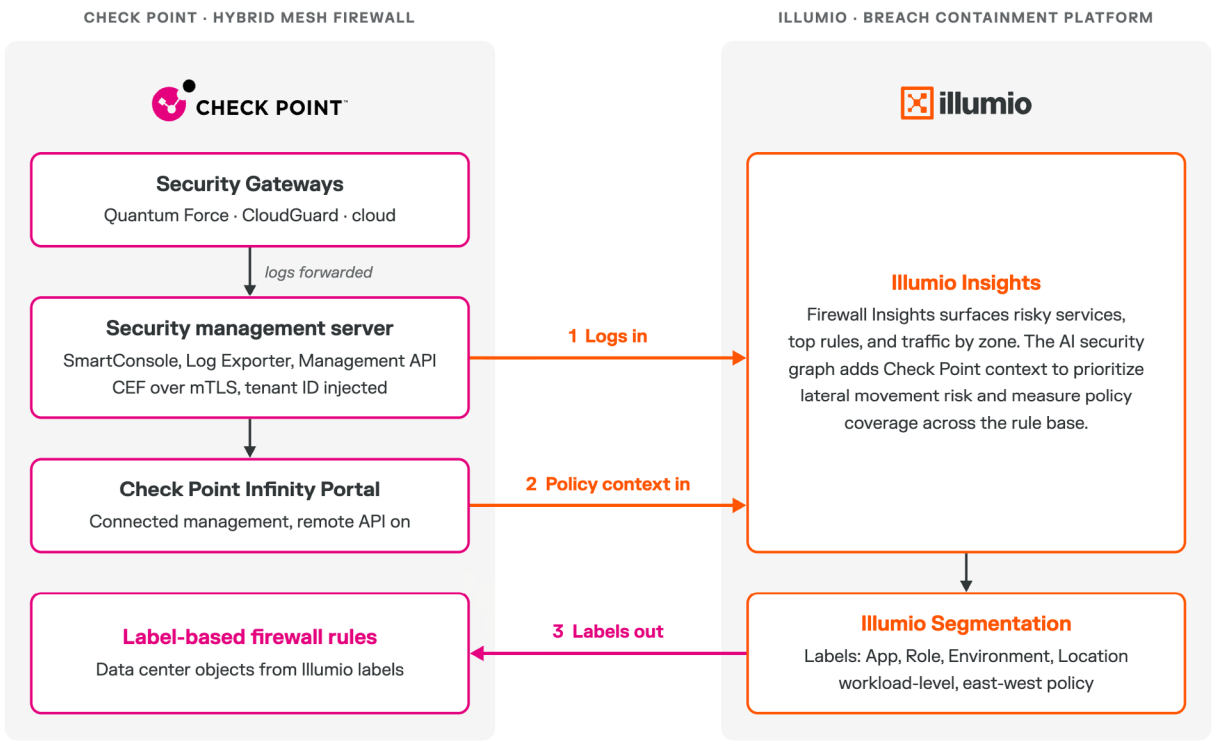


Figure 1. Illumio and Check Point integration

How the Illumio + Check Point integration works

Three data flows link the platforms: two send Check Point data into Illumio, and one sends Illumio labels to Check Point. Each platform only reads from the other, so the firewall team still writes and installs its own rules.

Flow 1: logs in

Check Point gateways forward their logs to the Security Management Server. Its Log Exporter sends logs, flows, and threat events to Illumio as common event format (CEF) over mutual transport layer security (mTLS) on transmission control protocol (TCP) 514. Illumio Insights uses this feed to show risky services, top rules, and traffic by zone.

Flow 2: policy context in

The Illumio API Connector reads the rule base, zones, policy packages, and objects through Infinity Portal. Access is read-only and starts from the customer's side. Insights uses this context to link each flow to the rule that allowed it and show policy gaps.

Flow 3: labels out

Once the firewall team adds Illumio as a Data Center Server in SmartConsole, Check Point pulls Illumio labels and their IP addresses. Rules can use each label as a source or destination, and IPs update at each policy install.

See risk and contain breaches in four steps

Once all three flows are running, teams can go from spotting a risk to containing it in four steps:

1. **See.** Firewall Insights shows Check Point traffic by risky service, rule, and zone. The AI security graph links each flow to the rule that allowed it and the workloads behind it.
2. **Prioritize.** Insights ranks exposures by lateral movement risk. Teams can start with the paths that reach critical assets.
3. **Write policy once.** Teams write Illumio Segmentation policy with labels and test it against real traffic before they turn it on. Check Point rules use the same labels.
4. **Contain.** When a workload is compromised, the team gives it a quarantine label. Illumio enforces the containment policy at the workload. The Check Point rule tied to the same label takes effect at the next policy install, and the rest of the app keeps running.

Deploy the integration

Setup takes three steps, one for each data flow. Start with the logs, since the API Connector only becomes available once a Log Exporter is active. You can set up label export at any time.

Before you begin, you'll need

- A Check Point Security Management Server on a current release, with expert-mode command-line interface (CLI) access. Every gateway must forward its logs to it.
- An Illumio Insights tenant with the owner role
- For policy context, a management server connected to Check Point Infinity Portal
- For label export, Illumio Segmentation and API credentials for Check Point to use

Step 1: send logs to Illumio

On the management server, create a key and a certificate signing request (CSR). In the Illumio Console, go to **Settings** › **Connectors** › **Check Point** and add a **Log Exporter**. Upload the CSR, then download the signed certificate, root certificate, and tenant script. Back on the server, create a **Log Exporter** target in CEF format, run the script, turn on mTLS, and restart the exporter. It shows as Active in the Illumio Console when it's working.

Step 2: add policy context

Connect the management server to Infinity Portal and turn on Remote API Access in **SmartConsole**. Create an **Infinity Portal API key for Security Management** and a **SmartConsole** admin who signs in with an API key. Then add the **Check Point Infinity Portal API Connector** in the Illumio Console, enter the values, and test the connection.

Step 3: export labels

Create Illumio API credentials that can read labels and workloads. In **SmartConsole**, add Illumio as a **Data Center Server** and import the labels your rules need. Use them as a rule's source or destination, then install policy.

Technical details

Here's what teams need to know before setting up the integration:

- **Log transport.** CEF over mTLS on TCP 514 to syslog.illum.io. Certificates are exchanged during setup, and the tenant ID travels in the CEF cs1 field.
- **Topology.** A single-domain Security Management Server. Multi-Domain Security Management isn't supported.
- **Network.** Outbound connections only, from the management server to syslog.illum.io and to Infinity Portal. No inbound rules are needed.
- **Data shared.** Illumio receives firewall logs and read-only policy data. Check Point receives labels and their IP addresses.

See it in action

Learn how Illumio and Check Point stop and contain attacks across your hybrid network.

illumio.com/partners/check-point

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 and Customer Favorite 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 © 2026 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.