Check Point and Illumio Integration

Accelerating Zero Trust with Proactive Threat Prevention, Visibility, and Microsegmentation

Hybrid cloud environments are growing fast — and so is your attack surface. Today's mix of on-premises infrastructure and multiple cloud platforms creates a web of connections that is hard to monitor, let alone secure.

Traditional network segmentation can't keep up. Workloads now move freely between data centers and cloud platforms. Without modern tools, security teams lack visibility, giving lateral threats space to move unseen across your organization.

Stopping lateral movement: key challenges

Modern infrastructure is more complex than ever. And that's reshaping the threat landscape, exposing new paths for lateral movement.

The attack surface is expanding

Every new cloud connection, workload, and user adds to the complexity — and the risk. As hybrid environments grow, so do the number of potential entry points for attackers. Security teams must defend an ever-widening perimeter where visibility is limited, and traditional defenses can't keep up. The result: more opportunities for threats to slip through and move freely across your environment.

Traditional tools are not enough

Perimeter-based security tools weren't built for today's infrastructure and can't protect against modern threats. Zero-day attacks and modern malware rely on lateral movement to spread — moving from one system to another inside the network. Legacy defenses focus on north-south traffic (data entering and leaving the environment). But most data traffic flows east-west, within and between internal systems. That means threats can spread undetected.

In manufacturing, this could mean a breach jumping from IT systems to critical operational technology (OT). In healthcare, attackers may move from administrative tools to systems that store sensitive patient data.

Limited visibility

Security teams can't protect what they can't see. In hybrid environments, traffic flows across a maze of on-premises and cloud systems. Blind spots emerge, and threats move undetected through them.

Legacy monitoring tools weren't built to track these complex pathways. Without visibility and control over east-west traffic, threats stay hidden — and uncontained.

And with no clear view of potential attack paths, security teams can't assess risk or prioritize the most vulnerable systems. The result: slower detection and response, giving attackers more time to reach critical assets.

Identifying lateral risks and dynamically blocking threats

Check Point and Illumio have joined forces to help prevent lateral movement and contain breaches with complete visibility, proactive threat prevention, and advanced microsegmentation.

By integrating the Check Point Infinity Platform with the Illumio breach containment platform, teams can quickly identify and contain lateral movement risks across hybrid and multi-cloud environments.

This combined offering brings together these Check Point products:

- Quantum Force Firewalls
- CloudGuard Network Security
- Infinity ThreatCloud AI

And AI-powered security management with:

- Illumio Segmentation
- Illumio Insights

Check Point firewalls act as key enforcement points to intercept and block malicious traffic. And Illumio provides visibility into lateral movement along with fine-grained microsegmentation that instantly contains the breach and minimizes the impact.

Our combined solution stops unwanted lateral movement, enhances visibility for security teams, protects critical assets, and enforces Zero Trust security across complex hybrid environments.

Strengthening Zero Trust

- Protect critical assets with microsegmentation that's easy to deploy — accelerating and simplifying Zero Trust.
- Unify security policy management for consistent protection across on-premises and cloud environments.
- Break down security silos with a holistic approach that improves visibility as workloads move between environments.

Preventing lateral movement

- Detect and stop attacks earlier in their lifecycle, preventing them from spreading.
- Proactively eliminate risk by identifying and closing the pathways attacker use to reach high-value assets.
- Automatically contain compromised systems with isolation boundaries that minimize the blast radius of breaches.

Advanced threat intelligence

- Combine threat intelligence from ThreatCloud AI and Illumio Insights to identify the earliest signs of new threats.
- Correlate threat indicators from many sources to uncover hidden risks that siloed tools would miss.
- Map traffic patterns and potential attack paths to focus remediation efforts where they matter most.

Protect your enterprise against tomorrow's attackers

By combining AI-driven threat prevention and microsegmentation, you can build more resilient security architectures that protect critical assets in today's ever-changing landscape. The Check Point and Illumio partnership strengthens Zero Trust security and equips enterprises to tackle both current and emerging threats across today's complex hybrid environments.

Already using Illumio? Scan or click for more information.

Already using Check Point? Scan or click for more information.

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.