Illumio for Microsoft Sentinel

Integrate Illumio data with Sentinel data lake. Detect and contain lateral movement risks through Security Copilot.

The challenge

Cybersecurity teams have long relied on a multi-layered defense — often called defense in depth, the layered security model, or the security onion. These layers span the network, applications, endpoints, and data.

To stitch them together, customers use APIs to pass security event data across systems. But those integrations are brittle, complex, and costly. Worse, they're slow to manage and still leave dangerous gaps that attackers can exploit.

The solution

With Microsoft Sentinel's cloud-native SIEM and AI-driven assistant, security teams gain unified visibility into lateral movement risks and attack paths across hybrid and multi-cloud environments.

Analysts cut through alert fatigue with prioritized insights, investigate threats with greater precision, and isolate workloads directly within Copilot. The result: faster detection, smarter response, reduced dwell time, and measurable improvements in cyber resilience executives and regulators can trust.

Illumio for Microsoft Sentinel comprises the following components, available to quickly trial and purchase on the Microsoft Security Store:

- **Illumio Insights.** AI-powered cloud detection, response, and containment.
- **Insights Agent for Security Copilot Agent.** Actionable AI-powered security advice.
- **Illumio for Microsoft Sentinel Data Lake Connector.** Publishes Illumio security data into the Sentinel data lake, which can be correlated with signals from Microsoft Defender, Entra, Purview, and other ISV partner solutions.
- **Illumio Segmentation.** Microsegmentation for every IT environment.

Key benefits

Expose lateral traffic risks

Simplify investigations across complex hybrid environments.

Detect attack paths

Turn raw traffic data into clear, useful insights to accelerate threat detection and analysis. Spot threats faster and make fast, informed response decisions.

Contain breaches with one click

Take clear, prioritized actions with AI driven guidance.

Optimized for Microsoft Sentinel

Publish security data and correlate it with other security data. Insights Agent, within Security Copilot acts as security advisor. Procure on Microsoft Security Store.

Illumio Insights and Segmentation, combined with Microsoft Sentinel and Microsoft Security Copilot, create a powerful integrated solution that changes how organizations detect and respond to cyber threats. It brings Illumio breach containment intelligence into Sentinel's cloud-native SIEM and its AI-driven assistant. Security teams get unified visibility into lateral movement risks and attack paths across hybrid and multi-cloud environments.

The power of a security graph, squared

Graphs are increasingly recognized as a critical approach to identifying and resolving threats. Microsoft and Illumio take complementary approaches to leverage the power of the graph.

Microsoft Sentinel Graph

The Sentinel Graph provides a holistic view across all layers of your IT environment with visual, entity-centric representations of security data.

It maps relationships between users, hosts, IP addresses, alerts, and incidents, connecting them into an interactive graph. This allows analysts to quickly see the scope and context of an attack, trace potential lateral movement, and uncover hidden patterns not visible in raw logs or tables.

By transforming complex data into an intuitive investigation tool, the graph helps security teams reduce both time-to-detect and time-to-respond, showing how isolated events fit into a broader attack chain.

Illumio Security Graph

The Illumio Security Graph delivers a live, visual map of communications across workloads, applications, devices, and users in hybrid environments. By continuously ingesting telemetry, it builds a dynamic graph that reveals how systems are connected, what traffic is flowing, and where risks or policy gaps may exist.

Unlike static network diagrams, it adapts instantly as environments evolve, giving security teams the visibility to spot risky dependencies, uncover high-exposure connections, and design or enforce segmentation policies with confidence.

Work easily, powerfully, and flexibly with security data

Security information is often trapped in silos across different tools and platforms, making it hard to get fast, complete answers. Illumio for Sentinel breaks down those barriers, giving security teams richer insights in two key ways.

AI-guided, no/low-code investigations

Through a Copilot interface, analysts can ask questions in plain language and instantly see the biggest risks, the potential blast radius, and prescriptive recommendations for how and where to deploy segmentation policies.

Rigorous, programmatic analysis

Practitioners can correlate data across ISV datasets to uncover more threats. With Jupyter notebooks, they can script in Python, run rules as Apache Spark jobs, and map out attack paths with precision.

Try now on the Microsoft Security Store

Preconfigured, ready to use.

https://securitymarketplace.microsoft.com/solutions?query=illumio

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.