illumio

INTEGRATION BRIEF

# Illumio App for Splunk

Leverage Illumio Zero Trust Segmentation to quickly understand your security posture and respond to incidents.

## Extend Illumio insights to SecOps

SIEM tools like Splunk are essential for Security Operations teams. They centralize and analyze data across your IT environment so you can get real-time visibility into potential threats.

Splunk's advanced correlation and alerting capabilities help teams quickly detect, investigate, and respond to incidents.

We know that you want to make your Illumio Zero Trust Segmentation (ZTS) data accessible to more teams across your organization — like the Security Operations Center (SOC) teams who rely on Splunk to monitor environments for alerts and anomalies.

With the Illumio App for Splunk, SOC teams can quickly identify potentially compromised workloads, improve decision making, speed up response times, and remain compliant — all through a single dashboard monitoring the health of all PCEs.

## How it works

Available on Splunkbase, the Illumio App for Splunk delivers out-of-the-box dashboards for security and operational insights into your Illumio-secured data center.

The Illumio Technology Add-On for Splunk (TA-Illumio) integrates Illumio Policy Compute Engine (PCE) data with Splunk's Common Information Model (CIM) for field names, event types, and tags.

With the TA-Illumio, you can easily analyze Illumio data in Splunk or other security tools in the Splunk ecosystem. Illumio extracts fields that you can in direct search. Use Splunk's query language to find information such as:

- Top outgoing and incoming connections by port, machine, or location
- Most active machines and source ports or services

## Key benefits

### Quickly identify critical threats

Get information about firewall tampering attempts and port scans to know immediately if there is suspicious activity that may show an imminent attack.

### Reduce investigation times

See all workload details, traffic events, and audit events in a single view. Reduce the amount of legwork you need to do to investigate an incident.

### Respond faster with automated actions

Quarantine suspicious workloads directly from Splunk in a single click. Use Splunk alerting to help with managing an Illumio deployment.

## Custom alerts. One-click quarantine.

The TA-Illumio provides a Splunk alert action to quarantine workloads managed by the Illumio PCE. Admins can set up a custom policy on the PCE to block all connections to and from quarantined workloads, except for SSH/RDP access from a management network.

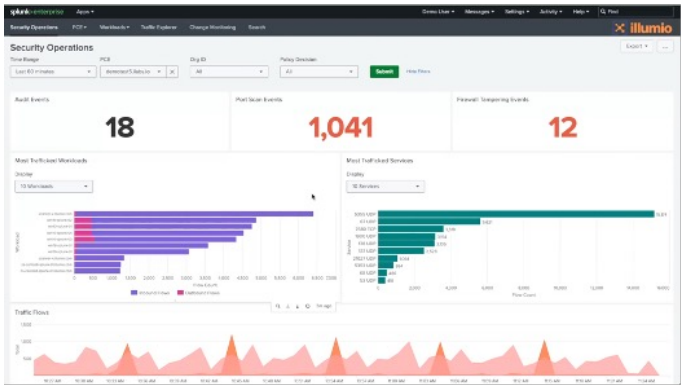
The app automatically applies the quarantine labels, triggering the PCE to recalculate and push the updated policy to workloads in seconds.

## Powerful dashboards to help turn insights into action

Intelligent visibility — insight that's easy to understand and act on — is key for organizations to secure and protect their data and infrastructure.

The Illumio App for Splunk offers dashboards to help SecOps teams detect threats, stop ransomware, and protect critical assets.

- **Security Operations Dashboard:** Gain east-west traffic visibility to identify compromised workloads and monitor the overall security state of your network. Get data on port scans, firewall tampering, and top hosts that have the most blocked or potentially blocked traffic.
- **PCE Operations Dashboard:** Monitor the health of the overall PCE cluster status, service status, per-node service status, and CPU, memory, and disk use.
- **Workload Operations Dashboard:** Monitor Illumio-managed workloads, unmanaged workloads used in Illumio policy, and offline or suspended VENs.
- **Traffic Explorer:** See traffic flows by policy decision or port distribution. View top talkers, designations, ports in use, and whether connections were blocked or allowed.
- **Change Monitoring:** Get comprehensive data logs on policy changes, including timestamps, resource types, and users.



The Illumio App for Splunk Security Operations Dashboard

## Validated by Splunk

The Illumio App and Technology Add-On for Splunk have both been certified by Splunk.

The Illumio App for Splunk provides powerful insights for security and operations teams, helping you understand your security posture and respond to cyberattacks in just a few clicks.

TA-Illumio enriches Illumio data with Common Information Model (CIM) field names, event types, and tags. This makes it easy to use Illumio data in Splunk queries or with other CIM-based apps including other apps in the Splunk ecosystem.

## Get started today

Download the Illumio App for Splunk and the Illumio Technology Add-On today.

splunk base.splunk.com

## 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.