illumio

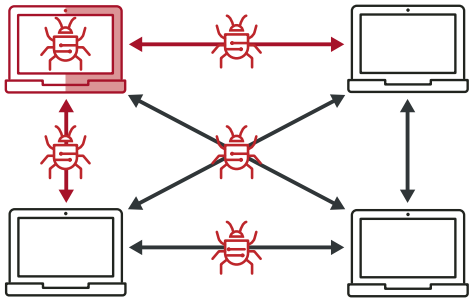
DATASHEET

Illumio Edge: Endpoint Zero Trust

Stop the spread of ransomware
at the first endpoint

Ransomware and malware are designed to target entire organizations, not just single endpoints. Attackers can move laterally to lock up whole networks in seconds or take more time to move internally while "living off the land" and target crown jewels. Either way, an isolated incident on a single endpoint can turn into a large scale breach, particularly if new ransomware has yet to be detected.

Since response should begin before detection, Illumio Edge brings Zero Trust to the endpoint, with containment by default to stop the spread of ransomware and malware at the first endpoint.



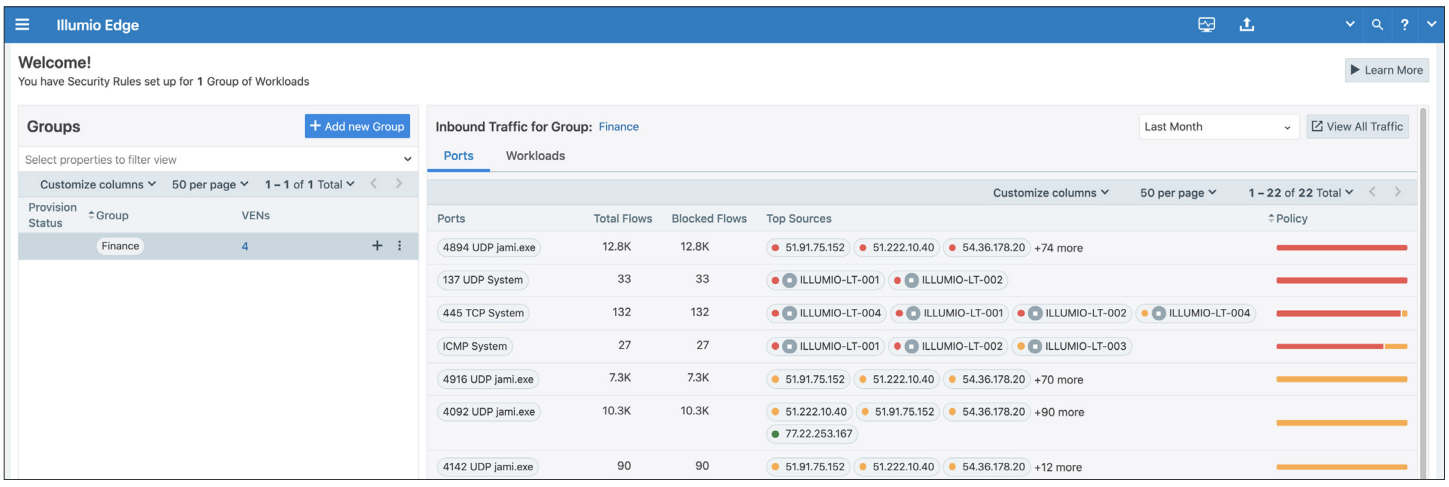
Illumio Edge:

- Makes every endpoint a Zero Trust endpoint, preventing ransomware from spreading peer to peer, even before it is detected.
- Ensures endpoints are segmented with allowlist policy that will not disrupt users or business.
- Complements endpoint security and EDR as they detect and respond to threats.
- Ensures the first endpoint infected is the last endpoint infected since ransomware cannot propagate.

Powerful ransomware protection. Invisible to users.

Illumio Edge starts with the creation of automated, risk-free allowlist policy. With policy in place, simple enforcement follows the endpoint wherever it goes – on or off the network. Not only is enforcement in place fast, it is also invisible to employees, never harms system performance, and does not trigger IT tickets.

Visibility into endpoint peer-to-peer communications allows you to further refine policies based on business needs and understand attempted ransomware propagation.



Use the Illumio Edge dashboard to monitor all active inbound services. In "test mode," you can confirm policies by reviewing potentially blocked traffic (yellow) before enforcement.

illumio

Key benefits

- **More effective ransomware and malware protection:** Preventive containment increases attack resilience and bolsters existing endpoint security postures.
- **Zero-risk Zero Trust:** Allowlisting the right business-critical applications is simple – no need for cumbersome GPOs or manual firewall rule writing.
- **Tiny footprint, vast peace of mind:** The agent (Virtual Enforcement Node) doesn't tax the host, so endpoints never slow down.
- **Easy integration with CrowdStrike:** CrowdStrike customers can activate Illumio Edge via their existing Falcon agent.

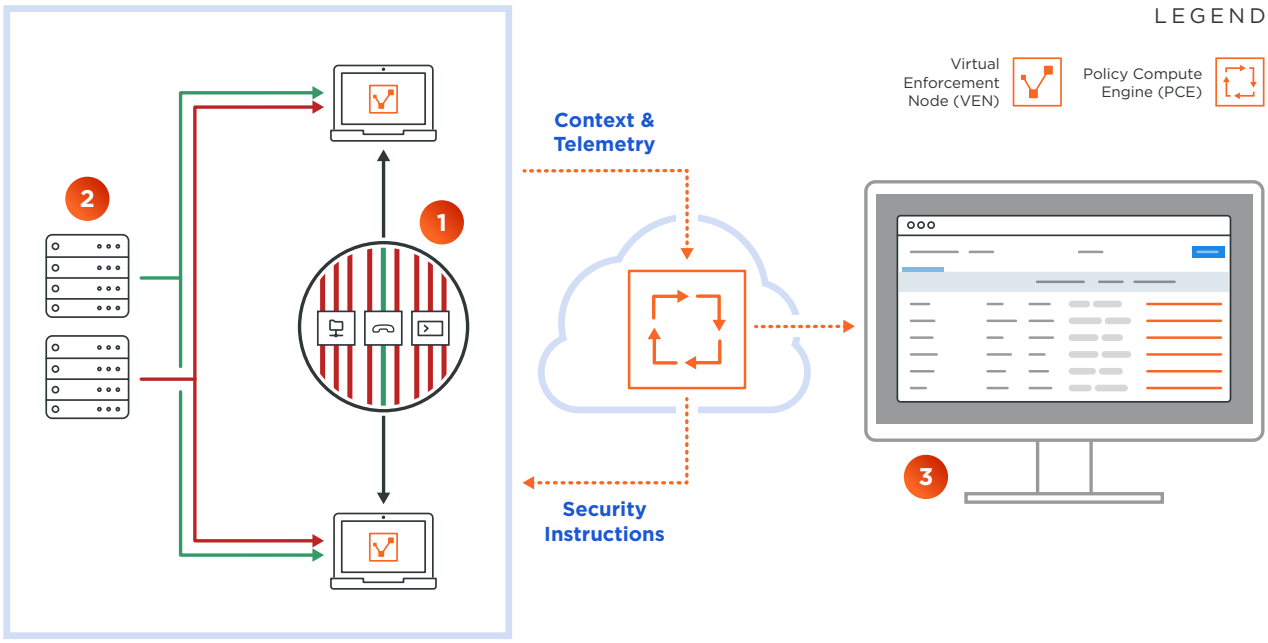
Illumio Edge blocks all unnecessary network communications to an endpoint, dramatically reducing the risk of ransomware and malware propagating laterally throughout an environment. In effect, Illumio Edge segments end-user laptops without touching the network. Gone is the cost and networking headache of deploying NAC for segmentation to prevent threats from spreading.

To do this, we program the OS firewall for enforcement, so there is no tax on the endpoint, whether CPU, memory, or network performance.

Illumio Edge provides an easy three-step approach to stopping unnecessary network communications:

1. Define authorized services
2. Fine-tune for custom applications
3. Run in test mode to ensure policy is correct, then place in enforcement and monitor blocked traffic

EDGE ARCHITECTURE



Key features

Three guided steps to Zero Trust
Follow a three-step guided workflow based on endpoint communications to get policy in place fast.

Endpoint-to-endpoint visibility
Use Explorer, an intuitive search tool, to see network traffic between endpoints to understand activity and design policy.

Blocked traffic dashboard
Use your dashboard for quick insights into any blocked inbound connections to help identify potential ransomware and avoid business interruption.

Specifications

Operating System	System Requirements	Memory	Disk
Windows 7 and 10	Single core 1 GHz	128 MB	10 MB

CrowdStrike integration

CrowdStrike customers protecting Windows laptops can activate Illumio Edge for CrowdStrike in their Falcon agent, without an Illumio VEN. To do so, customers need Falcon Prevent NGAV or Falcon Insight EDR. Additionally, customers must activate the Falcon Firewall Management module.

Core capabilities

Cloud-delivered	✔
Lightweight agent	✔
Off-network protection	✔
Complementary to EDR solutions	✔
Uses native OS firewall	✔
Distributed enforcement for massive scale with no performance impact	✔
Automated Zero Trust policy	✔
Endpoint-to-endpoint visibility	✔
No host OS overhead	✔

illumio

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any endpoint, data center or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com.