DATASHEET

Illumio Edge: Endpoint Zero Trust for Federal Agencies

Promote cyber resiliency, secure remote work, and obstruct ransomware and lateral movement attacks

The shift to remote work significantly altered and expanded the attack surface. Visibility and control at the edge is different from on-campus connections in significant ways. For starters, network visibility and control ends at the edge. An agency has no visibility and control over the remote home network an employee uses to connect to the agency's data center and cloud environments. The risk of compromising an agency-issued laptop via peer-to-peer application connections is higher if a remote worker's home network includes several internet-facing IoT devices, printers, and gaming consoles. Attackers can use any one of these devices as the entry point to compromise the agency-issued laptop.

Once compromised, that endpoint can be the beachhead for launching an aggressive ransomware attack that affects other endpoints, servers, and cloud instances in an agency's data center network. The compromised laptop could also launch malware that would move laterally across the network, targeting high value assets (HVAs) to eventually exfiltrate or manipulate classified or sensitive agency data. (Figure 1)

LATERAL MOVEMENT ATTACK WITHOUT ZERO TRUST MICRO-SEGMENTATION

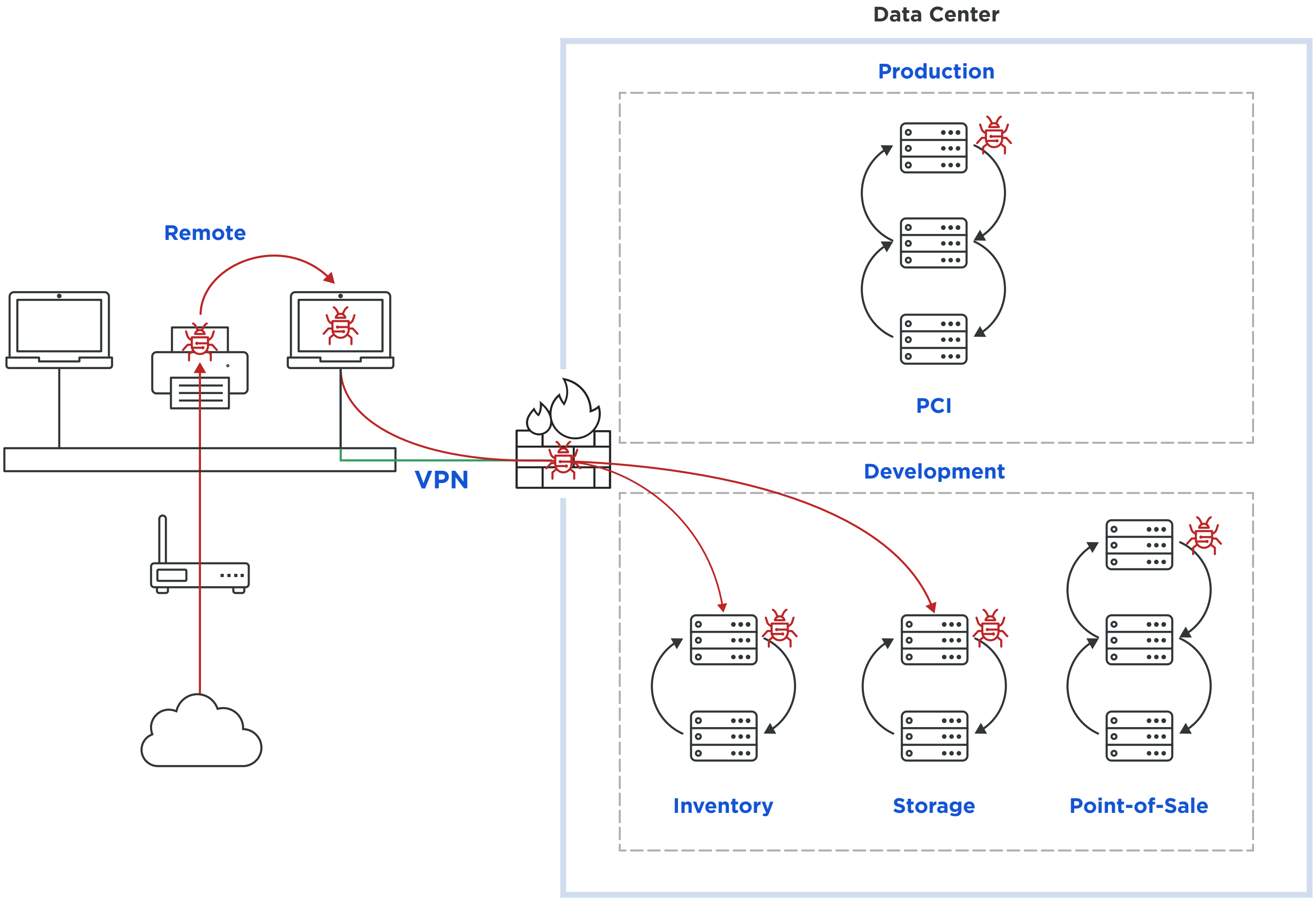


Figure 1

Zero Trust for endpoints

Concerns over one's ability to reduce the attack surface, obstruct the rapid propagation of ransomware, and constrain lateral movement attacks are driving more federal agencies and commands to accelerate their Zero Trust implementations.

Zero Trust implicitly assumes that the network and endpoints have been breached. Zero Trust at the endpoint focuses on validating and authenticating a user, device, and application, using contextual information about the behavior and environment prior to granting permission, and on giving access and allowing connections only to the resources it needs to do its job – and nothing else. Micro-segmentation is an effective foundational technique for controlling these connections.

Zero Trust is a holistic security strategy. Federal agencies have existing investments in solutions like multi-factor authentication (MFA), endpoint protection platforms (EPP), endpoint detection and response (EDR), network access control (NAC), and patch management. This combination of security tools enables Zero Trust after malware is detected or after security researchers uncover a vulnerability.

Achieving Zero Trust at endpoints requires:

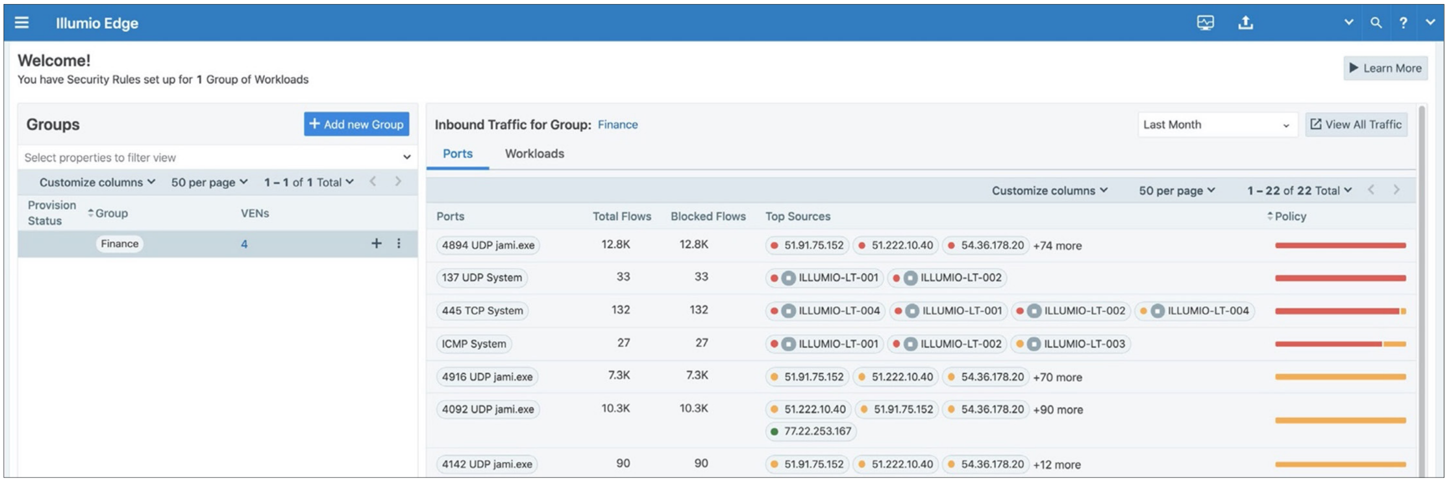
1. visibility into all the endpoints' connections and flows.
2. the capability to use this contextual information to model the allowed behavior and proactively design Zero Trust policies.

The outcome is a "containment by default" solution that obstructs the spread of ransomware and malware that takes advantage of peer-to-peer application communications. This solution is Illumio Edge.

Obstruct ransomware and lateral movement

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 identify potential security gaps in a federal employee's remote work network, understand attempted ransomware propagation and lateral movement attacks via peer-to-peer connections, and further refine policies based on business needs. (Figure 2)



Welcome!
You have Security Rules set up for 1 Group of Workloads

Groups

Provision Status	Group	VENs
	Finance	4

Ports	Total Flows	Blocked Flows	Top Sources	Policy
4894 UDP jami.exe	12.8K	12.8K	51.91.75.152 51.222.10.40 54.36.178.20 +74 more	
137 UDP System	33	33	ILLUMIO-LT-001 ILLUMIO-LT-002	
445 TCP System	132	132	ILLUMIO-LT-004 ILLUMIO-LT-001 ILLUMIO-LT-002 ILLUMIO-LT-004	
ICMP System	27	27	ILLUMIO-LT-001 ILLUMIO-LT-002 ILLUMIO-LT-003	
4916 UDP jami.exe	7.3K	7.3K	51.91.75.152 51.222.10.40 54.36.178.20 +70 more	
4092 UDP jami.exe	10.3K	10.3K	51.222.10.40 51.91.75.152 54.36.178.20 +90 more 77.22.253.167	
4142 UDP jami.exe	90	90	51.91.75.152 51.222.10.40 54.36.178.20 +12 more	

Figure 2: 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.

Key benefits

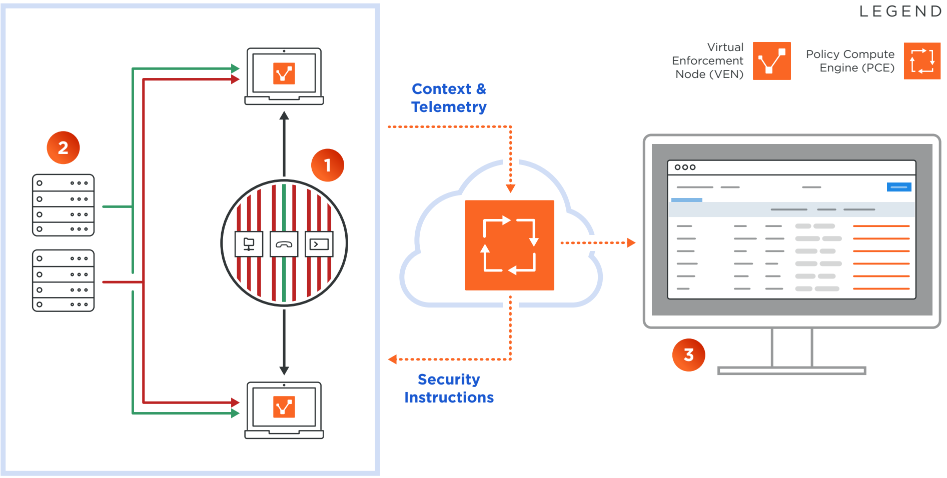
- Accelerate Zero Trust for endpoints: Proactively prevent unauthorized application connections between endpoints.
- Fast implementation: A user-friendly workflow enables authorized admins to quickly start designing and enforcing Zero Trust policies.
- More effective ransomware and lateral movement attack protection: Preventive containment increases attack resilience and bolsters existing endpoint security postures.
- Zero-risk Zero Trust: Allowlisting legitimate peer-to-peer connections, both on and off the network, 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 age.

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. (Figure 3)

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

ILLUMIO EDGE ARCHITECTURE



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

Figure 3

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 mission 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 is a cybersecurity software company enabling end-to-end Zero Trust in Defensive Cyberspace Operations. The company helps agencies, commands, and organizations achieve Zero Trust and prevent attacker lateral movement by protecting high value assets, critical applications, and workloads through real-time application dependency mapping, coupled with host-based micro-segmentation. Illumio is FIPS 140-2 validated and NIAP Common Criteria Protection Profile Certified. Illumio can be placed in multi-vendor hardware environments, using existing infrastructure to improve agencies' cybersecurity postures and effectively accomplish their missions.

Gartner peerinsights™

See what customers have to say about Illumio.
gartner.com/reviews/market/cloud-workload-protection-platforms/vendor/illumio

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085, Tel (669) 800-5000, illumio.com.

Follow us on:

illumio