illumio

PRODUCT BRIEF

Illumio Endpoint

Segmentation for end-user devices

Stop breaches from spreading across endpoints

Attackers love targeting the user

Prevent endpoints from causing a ransomware outbreak by stopping lateral movement from your most vulnerable assets.

The attack surface is expanding with users working from anywhere. These users are a prime target because they can be tricked into performing actions through social engineering, phishing, or device tempering. Traditional endpoint security solutions claim to stop breaches, but the reality is that devices still get breached.

The stats don't lie. According to ESG, 76% of organizations experienced a ransomware attack in the past 2 years. Despite these shocking stats, 47% of organizations still don't operate under an "assume breach" mindset.

Vendors are playing cat and mouse to prevent exploitation of new zero-day attacks to no avail. Endpoint security solutions need time to adapt to new attack vectors, time you don't have.

Dwell times and mean time to remediate (MTTR) mean that an attacker or malware exploit can move freely to other endpoints or into juicier targets in your data center before detection or remediation.

Segmentation prevents lateral movement – if the ports aren't open, attacks can't spread.

Illumio Endpoint provides Zero Trust Segmentation on end-user devices. Combine this with Illumio Core and Illumio CloudSecure for segmentation across the data center and cloud environments for full visibility and segmentation over all your workloads, anywhere.

Key benefits aligned to your Zero Trust journey

Visualize endpoint traffic anywhere

From home or the office, quickly assess and mitigate risk by seeing all network traffic.

Control application access

Don't allow endpoints access to the full data center – only allow defined users access to the right applications.

Secure endpoint exposure

Isolate cyberattacks to a single device – even before the attack is detected by other security tools.

Supercharge endpoint security

Stop ransomware and contain cyberattacks by enforcing security consistently at scale from endpoints to any data center and cloud through Zero Trust Segmentation.

Illumio Endpoint is a proven solution to support your defense-in-depth strategy. Stop breaches from spreading by dynamically limiting what ports are open and what IPs the endpoint can communicate with.

Complement your EPP/EDR solution by dramatically limiting the attack surface. This way, the first device that gets affected will be the last, giving your traditional security solution more time to react.

Critical Capabilities

Close the door on risky traffic

Illumio supports a wide range of operating platforms in physical, virtual, cloud, container, and endpoint environments, providing consistent enforcement for the smallest to largest organizations.

Easily reduce the risk Windows and MacOS devices pose to the network with Illumio Endpoint. Prevent mass infections of even zero-day attacks with rules blocking lateral movement from these devices over common ransomware propagation protocols like SMB and RDP.

Effortlessly block all but necessary communication to and from laptops, VDIs, and workstations based on the location of the device with Illumio Endpoint.

Say goodbye to blind spots

Use a real-time application dependency map for all traffic no matter the location. Visualize communications between endpoints and the data center or the cloud to build policy with confidence.

Build, model, and test policies before going into enforcement to avoid disrupting business operations or compromising on security.

Let only the right users in

Ensure uniform least-privilege access between endpoints and applications, whether users are in the office, connected to a VPN, or working remotely.

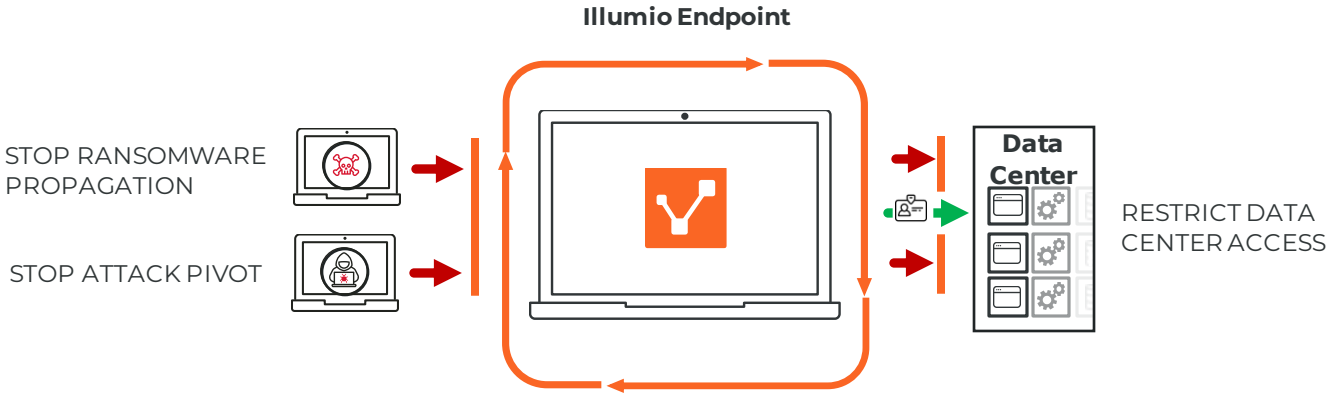
Further decrease the attack surface by rolling out identity-based policies to limit application access by Active Directory group and device identity.

For example, lock down access to critical infrastructure to select users and port protocols so only designated IT staff can access jump boxes through SSH from select devices. Or assign only select departments access to the ERP while in the office.

Enforce with zero touch to the network

Illumio provides segmentation that is not tied to the network, unlike NAC or SDN. Host-based segmentation keeps the enforcement close to the workload and adapts to any changes.

Integrating with third-party network vendors moves the enforcement closer to the data. Illumio Endpoint supports fully automated incident response, integrating with SIEM and SOAR platforms for alerting and automatic quarantine.



About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.