illumio

SOLUTION BRIEF

Illumio for Small and Midsize Businesses

Application-level visibility in minutes.
Automated policy management.
Segmentation made simple with a single console.

Your challenge: Controlling attack spread with limited IT resources and shrinking budgets

Segmentation is fast, affordable, and attack agnostic

Small and midsize businesses (SMBs) are the most targeted market segment for ransomware attacks, with 81 percent of successful ransomware operations against companies with less than 1,000 employees.

Attackers can easily breach networks, rapidly spread from system to system, compromise a massive volume of data and business processes, and ultimately demand a ransom to end their attack. Your security and IT teams must protect and manage more systems with fewer resources.

While organizations have adopted tools like Endpoint Detection and Response (EDR) to stop these attacks, they remain at risk. Breaches can spread in minutes, and tools like EDR can take hours to detect, investigate, and respond to an attack.

Legacy segmentation solutions like VLANs, ACLs, and internal firewalls require not only network re-architecture but also forklift upgrades of network equipment, often alongside significant disruption and lengthy professional services engagements.

With Illumio's agent-based segmentation, your underlying network architecture doesn't matter, saving you money by working with the equipment you already have.

Illumio provides SMBs with a fast, easy-to-use tool to gain visibility into their networks, contain breach spread with a few clicks, and segment endpoints so that attacks have nowhere to go.

Key Benefits

Instant visibility

See all the real-time traffic flows not only in and out of your network but across all the workloads and applications within it — down to the ports and processes being used.

Breach risk reduction

Meet segmentation requirements and instantly reduce the spread of breaches by cutting off all protocols used by malware to propagate.

Server and endpoint segmentation

Isolate cyberattacks to a single device to prevent attacker pivot and protect workloads that cannot have agents.

Quickly meet segmentation requirements

With fewer IT resources than their counterparts in the enterprise, more small and midsize organizations are adopting security frameworks like NIST CSF, CIS, and CMMC to establish actionable roadmaps for their security strategy — all of which have an increasing number of recommended controls around the segmentation of networks which can be quickly met with Illumio.

Additionally, cyber insurance providers are looking for solutions that will reduce restoration costs, decrease attack blast radius, and prevent re-infection. Insurance conversations now often mention segmentation as a mitigation technique that can reduce policy renewal costs.

Critical Capabilities

Instant visibility
Discover your network assets and quickly query historical traffic flows to save time troubleshooting issues. Illumio automatically creates a real-time map that shows how your systems are connecting and communicating with each other and the outside world.

Capture critical insights in as little as an hour by automatically mapping all communications across your applications and devices.

Quickly block risky ports
Don't wait to detect a breach. Organizations must contain attacks and stop them from spreading before they are detected and remediated by assuming a breach and denying all unnecessary network traffic by default.

With a few clicks, Illumio makes it fast, simple, and easy to close every instance of the pathways that breaches typically exploit — like Remote Desktop Protocol (RDP) — across your entire network. Then, Illumio can selectively allow necessary, legitimate traffic through those pathways.

Increase effectiveness of detection tools
Segmentation supports your defense-in-depth strategy by providing your existing EDR/MDR solutions enough time to adapt to new attacks by preventing the attacker from spreading to other systems.

By dramatically limiting the attack surface, the first device that gets affected will be the last, giving your traditional security solutions more time to react.

Secure endpoints by default
Easily control all traffic going between your endpoints and the connection to them. Block all but necessary communication to and from your laptops, VDIs, and workstations within hours of implementation.

Isolate cyberattacks to a single device — even before the attack is detected by other security tools. Further decrease the attack surface by rolling out identity-based policies to limit application access by Active Directory group and device identity.

Protect your critical servers and applications
Quickly apply targeted segmentation to applications and servers you can't let attackers compromise in any way by ring-fencing them and strategically blocking access from the outside world. Illumio detects server roles and automatically applies the appropriate label, then recommends specific segmentation rules according to best practices for each server type — all within a few clicks.

Segment to stop the spread of breaches

Secure your servers and endpoints in minutes.

Go to: illumio.com/solutions/SMB

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.