10 Reasons To Choose Illumio For Zero Trust Segmentation

1. Predictability

Organizations choose Illumio because of our highly predictable architecture. Our lightweight VEN is not inline to traffic, and Illumio programs the workload OS firewall. In contrast, other vendors use inline agents that are not passive, and they perform the firewall operations.

Unfortunately, this type of solution can be unpredictable if the agent fails, causing applications to break abruptly or, worse still, have no security policy at all. Illumio doesn't have these issues because our policies remain in place even when agents go offline. The workload continues to use the last known policies set to the OS workload firewall.

Illumio's endpoint offering is also very predictable. Our solution works both on and off the corporate network. Some other vendors only work on the corporate network which limits the effectiveness of providing policies endpoints such as Mac and Windows laptops and workstations.

2. End-to-end application visibility

You can't secure what you can't see. That's why you need comprehensive visibility into all workloads in all areas of your network. Illumio's end-to-end application dependency mapping provides visibility across your entire attack surface, improving your security posture and ability to prevent and respond to attacks.

Get visibility into the cloud, virtual machines, hybrid or multi-cloud environments, and on-premises data centers. This includes a wide range of platforms and environments including Windows, Linux, AIX, Solaris, Kubernetes, OpenShift, VMware, AWS, Azure, IBM, and Oracle.

With Illumio, organizations can define and enforce Zero Trust Segmentation policies that take effect everywhere: on-premises, on third-party cloud platforms, at remote locations such as home offices, and in IoT environments. For example, Illumio's integration with Cylera and Armis help extend visibility into IoT environments like medical devices.

Unlike other platforms, Illumio provides a comprehensive solution that protects most environments against ransomware and other forms of cyberattack.

3. Simplicity instead of complexity

Faster time-to-value

Other segmentation solutions often require a heavy upfront lift to set up the inventory before creating policies, costing you time and trust. Illumio makes it quick and easy for organizations to design rules, automate policies, and gain visibility — in a matter of minutes or hours. Illumio's Policy Compute Engine (PCE) and agent architecture are lightweight and very easy to deploy, allowing you to be operational in a matter of hours. Illumio's Policy Generator uses network traffic to recommend and generate microsegmentation policies for every workload and application, regardless of its location.

Flexible, multidimensional labeling

With Illumio, you can create flexible, multidimensional labels for locations, applications, or environments in addition to OS types, business units, and more. Multidimensional labeling means you can build more flexible security policies.

Quick, easy set up for groups and tags

With many microsegmentation products, setting up groups and tags to define specific segmentation policies is time-consuming, error-prone work, requiring constant trial and error to get right.
Illumio streamlines this work by integrating with next-generation firewalls such as Palo Alto Networks. We also integrate with IT Service Management tools such as ServiceNow's Configuration Management Database (CMDB) to import workload tags to provide more context to workloads.

When segmentation solutions make grouping and tagging difficult, teams often cut corners, grouping users and devices too broadly simply to get the work of assigning groups done. By simplifying this work, Illumio makes it easier to set up the precise segmentation policies that best meet your needs.

4. No time-consuming, error-prone rules ordering

Some microsegmentation platforms offer too many types of rules for enforcing microsegmentation policies: Allow, Block, Override and Reject. Because they support multiple rules, the ordering of rules matters a great deal when implementing segmentation policies.

For example, security analysts might decide to allow most traffic from an endpoint to enter a data center, but they might decide to reject some of the traffic from certain applications or at certain times. In cases like this, it's critical that security analysts get the order of rules right; otherwise, the wrong traffic will be blocked.

Rule ordering might seem straightforward with just one or two examples. But when the scope of work expands to hundreds of workloads, it becomes much more time consuming and problematic. Illumio provides a simple and straightforward model for segmentation rules. By default, all traffic is blocked. Only explicitly authorized traffic is allowed to pass through. There's never any confusion about which rules are in effect. And you no longer need to worry about packets being dropped either.

Because Illumio makes it easy to model segmentation policies, security teams can easily determine which traffic should be authorized. They explicitly allow that traffic, and Illumio blocks the rest in accordance with Zero Trust best practices. The result? As close to airtight protection a company can get for stopping the spread of cyberattacks on its networks.

5. Contain ransomware

Illumio's Enforcement Boundaries contain attackers from moving laterally across your network. This enables security architects to immediately isolate any workload or endpoint compromised in an attack. Enforcement Boundaries can be activated instantly through scripts or by manual control, isolating workloads and endpoints already infected from spreading across the organization.
Illumio also quickly and easily blocks remote desktop protocols (RDPs) and server message block protocols (SMBs) that ransomware commonly use to enter and move throughout networks.

6. Powerful visualization maps

Illumio provides visualization maps with real-time telemetry data so teams can understand critical pathways, detect anomalous behavior, build segmentation policies, and test rules before enforcing segmentation rules.

Illumio can also use application dependency maps. With the map's powerful graphical features, business leaders, application owners, and security teams can monitor real-time application usage and traffic patterns and determine which traffic should be allowed for business-critical operations. Once they understand which traffic patterns are legitimate, these teams can work together to quickly define policies that allow business-critical traffic to pass through while blocking everything else.

Illumio provides risk visibility by combining data from leading vulnerability management solutions with application dependency maps. This helps teams gain a detailed understanding of potential pathways for lateral movement by attackers, helping them to prioritize patching critical assets and create policies to block pathways.

7. Easily build, model, and test

It's much easier to build, model, and test segmentation policies with Illumio. Illumio's Policy Generator can discover and automatically suggest policies based on real-time traffic patterns. Illumio's real-time application dependency mapping provides the guidance business and security teams need for defining policies that protect the traffic legitimately needed for business. Business and security teams can model those policies, seeing alerts about the traffic that Illumio would block were the policies actually being enforced. This kind of modeling makes the work of fine-tuning policies quick and straightforward.

Because Illumio supports natural language definitions for policies, teams can divide the work of designing rules from those individuals who are implementing them. This provides checks and balances for compliance purposes, preventing one application group from overwriting rules of another group of rule designers. This also can prevent the havoc around implementing the wrong set of rules that can stop mission critical traffic from communicating. And if needed, teams can easily roll back policy changes to the previous version.

A team that can oversee these rules can put these policies in place to prevent disruption to the business, giving your business leaders and application teams peace of mind.

8. Integrations

Illumio supports a wide range of integrations, including Kubernetes, Hashicorp, IBM, Appgate, Qualys, VMware vSphere, Ansible, ArcSight, AWS, Docker, Chef,Okta, RedHat, Microsoft Azure, Puppet, ServiceNow, and Splunk. These integrations make it easier to import data for workload tagging and visibility and to coordinate Illumio enforcement actions with SIEM and SOAR playbooks and other automated workflows.

9. Expertise

At Illumio, our expertise is Zero Trust Segmentation. Illumio delivers a proven path for success with a reliable customer support and delivery model. Over 500 organizations worldwide trust Illumio for easy-to-use, fast time-to-value Zero Trust Segmentation deployments.

Illumio's platform is purpose-built to solve the problem of delivering microsegmentation solutions at scale for companies across every industry. Forrester recognized Illumio as a Leader in microsegmentation, a testament to the success of our approach.

10. Scalability

Illumio has demonstrated exceptional scalability with deployments up to 700,000 workloads. These workloads can be in the cloud, on-premises data centers, endpoints, and in hybrid environments. Illumio supports some of the largest microsegmentation installations in production anywhere, providing the most comprehensive protection available anywhere against ransomware attacks and breaches.

The Power of the Illumio Zero Trust Segmentation Platform

- Learn how to protect devices and workloads with the first platform for breach containment: www.illumio.com/products
- Read the Bishop Fox report for more results from attack emulations measuring the effectiveness of Illumio ZTS against active ransomware threats.

illumio