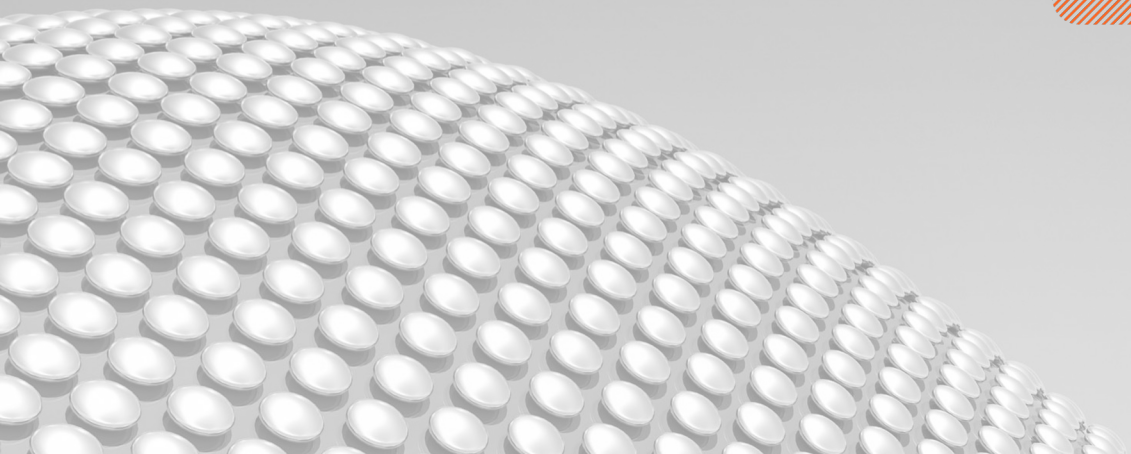
illumio

ONBOARDING GUIDE

The Zero Trust Segmentation Onboarding Guide

An essential guide to discovering how Illumio accelerates and simplifies the path to Zero Trust with Illumio Core and Illumio Endpoint.



Onboard With Confidence

Ready to get started?

Our onboarding guide is designed to be your go-to resource to support you through this change and adoption. We know a shift like this one can be complex – it requires integrating a new security product into existing systems.

Gained through practical insights from proven processes, this guide is intended to provide guidance on timelines and other considerations as you prepare to operationalize and onboard with Illumio Core. Please note that actual timelines may vary depending on your organization's specific goals and the scale of deployment.

Week 0 – 2 | **Deploy**

Welcome to Illumio!

Meet with your Illumio team and plan your deployment. Complete installing Illumio in the *Idle* enforcement state and select your segmentation path.

Week 2 – 6 | **Discover**

Discover real-time traffic flows and draft your first security policies to optimize your segmentation strategy in the *Visibility Only* enforcement state.

Week 6 – 8 | **Protect**

Transition into the *Selective Enforcement* state as an intermediary step towards full enforcement and see how a subset of your managed workloads can be protected while refining your policies.

Week 8+ | **Validate**

Implement your proven policies by moving into *Full Enforcement*. Enforce all inbound and outbound services based on Illumio's allow-list policy model, while your Illumio team prepares you to scale your segmentation strategy.

illumio

Onboarding Guide Overview

What to expect

Organized into weekly steps, our guide provides you with a structured roadmap to walk you through each stage as you deploy, write policy, and move to enforcement.

From initial setup to integrations and finding success based on your organization's needs, each week is carefully crafted to help you understand how to onboard and progress with Illumio smoothly and efficiently.

As part of your journey, you'll have access to dedicated support resources and expertise through our Customer Success, Professional Services and Technical Account Management teams who are committed to your success. Our teams will ensure personalized guidance and proactive assistance tailored to your goals every step of the way.

Week 0 – 2 | **Deploy**

Enforcement State: Idle

Step 1 Planning Kickoff

Step 2 Meet Your Champions

Step 3 Get Started with Illumio

Step 4 Choose Your Segmentation Path

Week 2 – 6 | **Discover**

Enforcement State: Visibility Only

Step 5 Making the Switch

Step 6 Visualize All Traffic Flows

Step 7 Labels, Data and Traffic Views

Week 6 – 8 | **Protect**

Enforcement State: Selective Enforcement

Step 8 Policy Writing

Step 9 Selective Enforcement and Ransomware Protection

Step 10 Application Attestation

Step 11 Prepare for Policy Review

Week 8+ | **Validate**

Enforcement State: Full Enforcement

Step 12 Preview and Refine Your Policy

Step 13 Move to Enforcement

Step 14 Operational Readiness Review

Step 15 Onwards, Together

illumio

Quick Wins with Illumio

Prioritizing Illumio Endpoint vs. Core

Deploying Illumio effectively requires a tailored approach, as priorities differ from one organization to another. Whether beginning in the data center, cloud, or on endpoints, it's vital to reflect the organization's specific needs and security landscape.

To ensure a successful deployment on your endpoints, aim for broad coverage to gain the best insights during the initial phase. Rather than concentrating on a single department, deploying an Endpoint VEN on at least one or two endpoints per business unit can enhance the overall understanding of your environment.

Deploying in the datacenter requires a clear understanding of the project goals. Options range from starting with the most critical applications or starting with a low-stakes application to gain experience first.

However, in most cases, a successful Illumio deployment hinges on a strategic, phased roll out that prioritizes outcomes. Refer to the table below for potential early wins to prioritize.

Quick Wins	Product	Details
Secure high risks ports	Core and/or Endpoint	The Ransomware Protection Dashboard keeps track of risky ports like RDP, SMB, WinRM. Leverage these actionable insights to reduce your exposure score.
Admin Access	Core and/or Endpoint	Use policy templates to setup rules for admin traffic (RDP, SSH) including jump boxes.
Ransomware kill switch	Core and/or Endpoint	Prepare to quarantine each managed workload or endpoint in minutes.
Core Services Protection	Core	Use policy templates to secure core services like a domain controller with ease.
Endpoint to Endpoint	Endpoint	Stop the unnecessary ability for peer-to-peer communication between laptops and workstations with quick exceptions for legitimate traffic.
Inbound to Endpoint	Endpoint	Eliminate inbound communication on laptops and workstations with explicit and dynamic exceptions when needed.

Weeks 0 – 2 | Deploy

Your journey starts here.

Deploying new software to production can be difficult – and taking on ownership of that process is a significant responsibility. We know from experience that the process involves many moving parts across the business, including existing toolsets, operations, and teams. Our focus for the first couple of weeks is getting you onboarded and deployed.

We'll guide you through how to map your project plan and build a rollout timeline. We'll also provide a pre-deployment checklist as a starting point to help with the planning process before walking through how to deploy and manage the Illumio Virtual Enforcement Node (VEN), a key architectural component for getting started with Illumio. With an Illumio Core SaaS deployment, Illumio hosts and manages the Policy Compute Engine (PCE) infrastructure used to provide Illumio core services.

If you need additional assistance at any point during the onboarding process, contact your Illumio Account team or visit the Illumio Support Portal for 24/7 access to resources.

What to expect

Step 1 *Planning Kickoff*: Strong project planning is the first step to success. Establish project goals with your Illumio team – your Customer Success Advisor (CSA) and Technical Account Manager (TAM) – will guide you through defining your success criteria.

Step 2 *Meet Your Champions*: Identify and align with your internal champions who will provide the mandate necessary to prioritize your Zero Trust segmentation initiative. Your Illumio team will facilitate role assignment exercises.

Step 3 *Get Started with Illumio*: Collaborate with our Professional Services (PS) team throughout the technical deployment, beginning with the installation of the Virtual Enforcement Node (VEN) software on your workloads and/or endpoints. This process will also include setting up operational integrations such as SSO, SIEM and Infrastructure Orchestration integration.

Step 4 *Choose Your Segmentation Path*: Determine the optimal segmentation strategy for your Zero Trust security journey and review our recommended approach for rule creation along with a list of starter segmentation strategies for quick wins.

Weeks 2 – 6 | Discover

Discover real-time traffic and lay the foundation with labels.

Getting the most value out of Illumio depends on the data about your environment. In the Discover phase, and over the next few weeks, we will give an overview of several topics that are important to building a strong foundation that will help you quickly deliver value from Illumio.

In the first part of the Discover phase, we will take advantage of the Illumio visibility feature to map managed workloads to existing metadata in order to develop a labeling schema that works for your security posture. Solid groundwork in this area is crucial. Policy object discovery and documentation can be challenging but is a critical step to writing effective policies.

Moving into the later part of the Discover phase, we will identify traffic patterns and create unmanaged workloads and IP lists. This will be necessary to create security policies that expand the scope of your Zero Trust architecture and accelerate your path to Zero Trust success.

What to expect

Step 5

Making the Switch: Transition from *Idle* mode to *Visibility Only* mode by migrating your VENs to start discovering and analyzing application traffic flows in Illumination, Illumio's real-time application dependency map. Our Professional Services Consultants can support your team with change management and configuration so that you can start building security policies.

Step 6

Visualize All Traffic Flows: Identify network connections and collaborate with our PS team through policy object discovery exercises to categorize and document your infrastructure where VENs are not installed.

Step 7

Labels, Data and Traffic Views: Your metadata is just as important as our security controls – take this opportunity to refine your metadata for improved visibility and segmentation. Your Illumio PS and TAM can guide you through the process of designing and implementing labels based on your metadata.

As you review your implementation plans, collaborate with your TAM to prepare for application-level traffic views, with support from your PS team in creating and implementing them.

Week 6 – 8 | Protect

Create simple policies starting with your core services.

Maximizing the value of Illumio depends on establishing a strong foundation, a task you've already accomplished in the preceding weeks. In this phase of your journey, the Illumio team will collaborate with you to write and implement policies for your core services.

For these situations where flexibility is required, Illumio Core provides the ability to enforce a set of rules that determine where segmentation rules apply by using the selective enforcement. Based on your organization's goals, our teams will provide guidance on how to apply enforcement boundaries or ransomware protection to effectively model-test Zero Trust segmentation.

The goal of the Protect phase is to apply application ring-fencing policy to reduce the attack surface through a simple and easily managed policy structure. Throughout this phase, the Illumio team will guide you through critical policy decisions for your high-value applications to ensure uptime and maximize security.

What to expect

Step 8

Policy Writing: Draft, test and review security policies. Our PS team will work with your team to implement policy for core services, environmental separation (selective enforcement), ransomware protection and application ring-fencing using best practices suited to your infrastructure size and complexity.

Step 9

Selective Enforcement and Ransomware Protection: Illumio's selective enforcement feature can perform administrative access restriction, ransomware protection or environmental boundaries. Illumio PS will help create rules and ensure a smooth implementation without service interruption to critical applications.

Step 10

Application Attestation: Your Illumio TAM can help prepare your application owners for the task of validating the application architecture so that we can properly protect your high value applications. Our Illumio PS team will help create traffic explorer filters and reports to clearly show traffic at the application level to ensure correct policy is written for your applications.

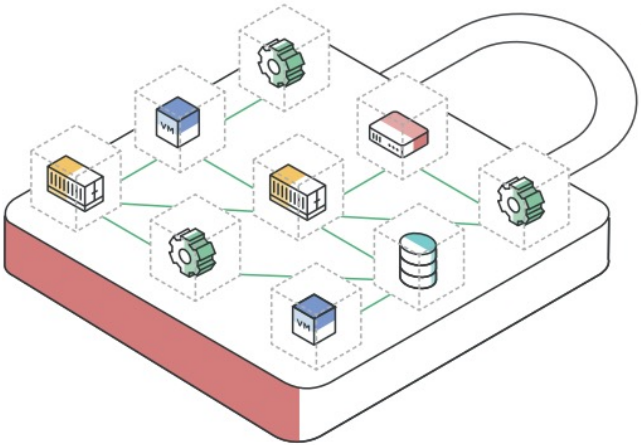
Step 11

Prepare for Policy Review: Generating reports regularly during the policy validation stage is important as it provides valuable data for sharing with application owners, managers, executives, or auditors. Your Illumio PS/TAM team can help create a validation cadence that facilitates a seamless transition into the enforcement phase for your applications via UI, API or exported documents.

Week 8+ | Validate

Take the next step in your journey toward Zero Trust.

While selective enforcement helps overcome the limitations of an allow-list model that requires a complete list of rules allowed to enable security enforcement, selective enforcement is an intermediary step. Moving workloads from selective enforcement to a true allow-list security model with full enforcement is an important goal to plan for from onboarding. Remember, a plan is essential for a successful deployment.



Step 12

Refine Your Policy: View the revised effects of your ruleset in Illumination in draft view to see the changes that will be enacted by your policy when enforced. Refine as necessary and collaborate with the Illumio team to set up a process.

Step 13

Move to Enforcement: Moving into full enforcement is on an application-by-application basis. The Illumio team ensures that enforcement is done in coordination with your change management process with a clear backout and remediation plan in place.

Step 14

Operational Readiness: Our TAM and PS teams can help you create runbooks, escalation procedures, internal ticket procedures, and monitoring integration so that your steady state operations run smoothly post-onboarding.

Onwards, Together

We understand that deploying a solution is a continuous process rather than a one-time event, and the duration can vary depending on the environment and organizational objectives. Step 15 represents more than just a conclusion to onboarding; it highlights one of our core values and commitment: onwards, together.

We believe that continuous policy refinement is an integral component of an effective security strategy. As threats evolve and networks change, it will be essential to regularly review and adjust security policies to maintain optimal protection.

The steps outlined in this onboarding guide are designed to equip you and your team with the necessary confidence to advance your Zero Trust journey with Illumio. By following these steps and collaborating with your Illumio team, you will be better equipped to realize significant yearly ROI[1] such as:

- $20M+ saved in app downtime
- Multiple cyber disasters averted annually
- Digital transformation projects accelerated

As you update your Zero Trust timeline at this stage, continue to iterate on the allow-list rules and be diligent with traffic reviews and weekly reporting. At any point in the onboarding process, contact Illumio Customer Support for additional support from our teams or visit the Illumio Support Portal for 24/7 access to resources.

We're here to help.

Get support on identifying issues, making software fixes and more.

Our Technical Support team is available online and offline 24/7 for your Illumio solution.

Visit our Support Portal >

- Open a new support case
- Email support@lllumio.com

Direct hotline support (Toll Free)

- Australia: 1 800 995 469
- France: 08 00 94 00 75
- New Zealand: 0800 369 529
- Singapore: 800 321 1271
- United Kingdom: 0800 069 8795
- United States: 1-888-631-6354

Direct hotline support (Toll)

- United States: +1-408-831-6354
- International: +1-408-831-6354

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware 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.