illumio

Onboarding Illumio 101

Introduction, Resources, and Best Practices for your Successful Deployment

Illumio Onboarding

Completed Contract

Illumio finance will confirm completed contracted with start date, license count, PCE model and support & services.

Illumio Welcome Email

- Onboarding Questionnaire
- Support Portal Account Sign Up
    - Technical Troubleshooting tickets
- Training
    - Free On-Demand training
- Community Access

Illumio Kickoff Meeting

Set up time with your customer success advisor to overview the deployment process, plan out goals & objectives, and discuss next steps & timeline for your Illumio Implementation.

PCE (Policy Compute Engine) Login and Getting Started

SaaS PCEs will have access on contract start date; On-prem PCEs will need to be build.

PCE “Org Owner” will have first access as granted by support, that contact will need to create and invite additional users to login to the PCE.

Go to the Illumio Community “Deployment” Page for videos and content on how to start deploying Illumio.

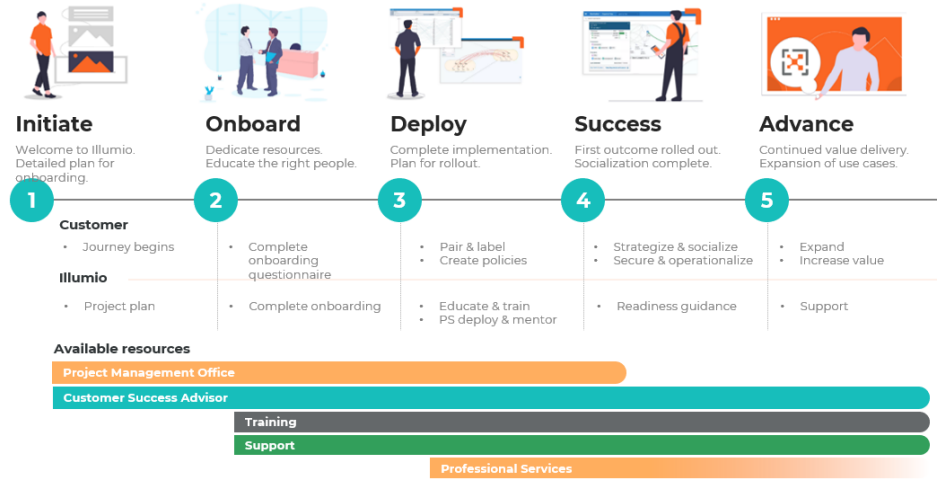
Illumio Resources

Illumio People Resources

Customer Success Advisors: Strategist that helps build deployment plans, leverage best practices and achieve business outcomes.

Professional Services: Contracted technical experts guiding agent deployment, labeling strategy, policy creation, policy enforcement, and more.

Project Management Office: Create, plan, and document your Illumio deployment.



Illumio Support Resources

Support: 24/7 access by email, phone, or opening cases - P1 critical to P4 General issues and break-fixes.

Training: On-demand or instructor lead training divided into courses, and programs ranging from basis policy admins to advanced Illumio experts.

Community: Free 24/7 guidance, access to other Illumio customers and experts, deployment guides, and best practices with updated webinars and events.

High-Level Implementation Process

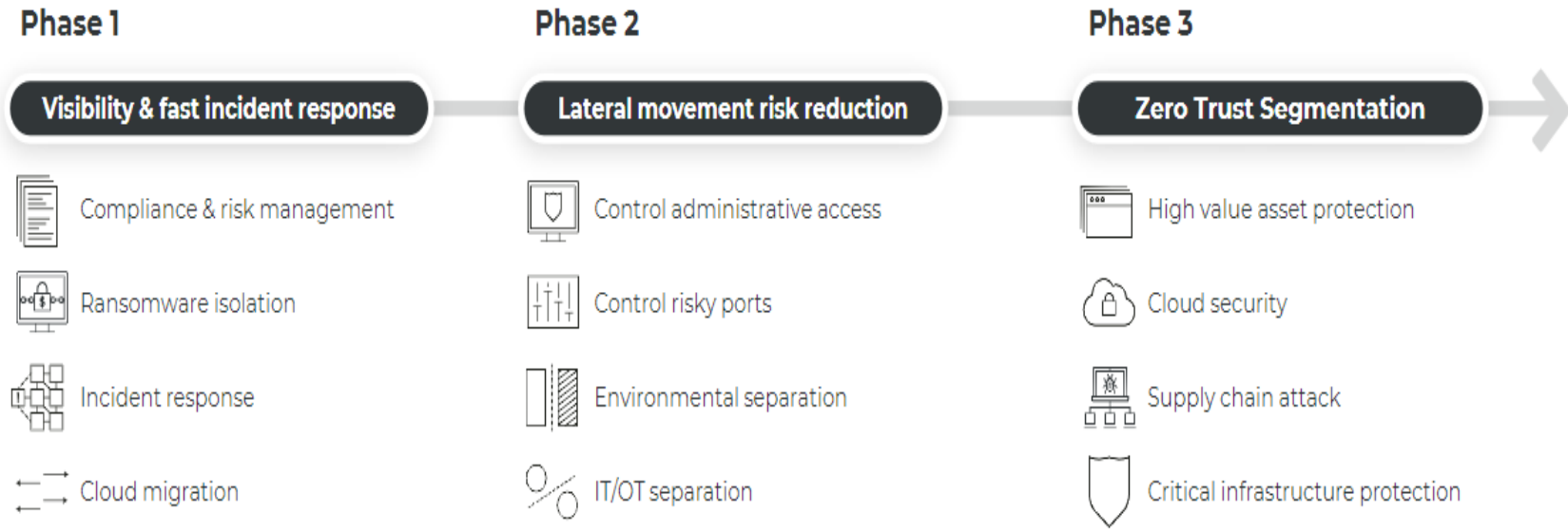
Maturity of Deployment

VEN Agent Install to Visibility: Installing VEN agents (Virtual Enforcement Nodes) to all workstations gives centralized visibility for all connections and creates a traffic map that is essential to writing and provisioning security policy.

Labeling: Use Illumio labels to identify workstations, group labels to create policies, or onboard new workloads to a policy group.

Selective Enforcement: “Deny List” policy for widespread risk reduction and general ransomware prevention. Use cases below in "Phase 2".

Full Enforcement: “Allow list” policy for micro-segmentation to protect critical assets and create a zero-trust environment.



Best Practices

1. **Start with visibility**
   - Deploy VEN's on all workload devices.
   - Collect data on existing traffic.
2. **Use selective enforcement for fast value and protection**
   - Step up your Illumio enforcement capability in phases.
3. **Utilize training and the community**
   - Illumio Training Portal
   - Knowledge Base
   - Illumio Community
4. **Document and work with stakeholders**
   - Early buy-in.
   - Establish team communication cadence.
5. **Lean on the Illumio working team**
   - Reach out to your CSA, PS, PMO or Support at any time for help.

Key Takeaways

What to do now:

1. Log in to your PCE.
2. Sign up for the support portal: https://support.illumio.com/
3. Use the community onboarding page to get started: https://community.illumio.com/s/onboarding
4. Follow high level deployment overview: https://community.illumio.com/s/deployment
5. Review best practices: https://community.illumio.com/s/best-practices
6. Complete Training: https://support.illumio.com/training/index.html
7. Deploy VEN's in visibility mode.
8. Create workload labeling scheme.
9. Write enforcement policies.
10. Enable selective enforcement.

illumio

Thank you!