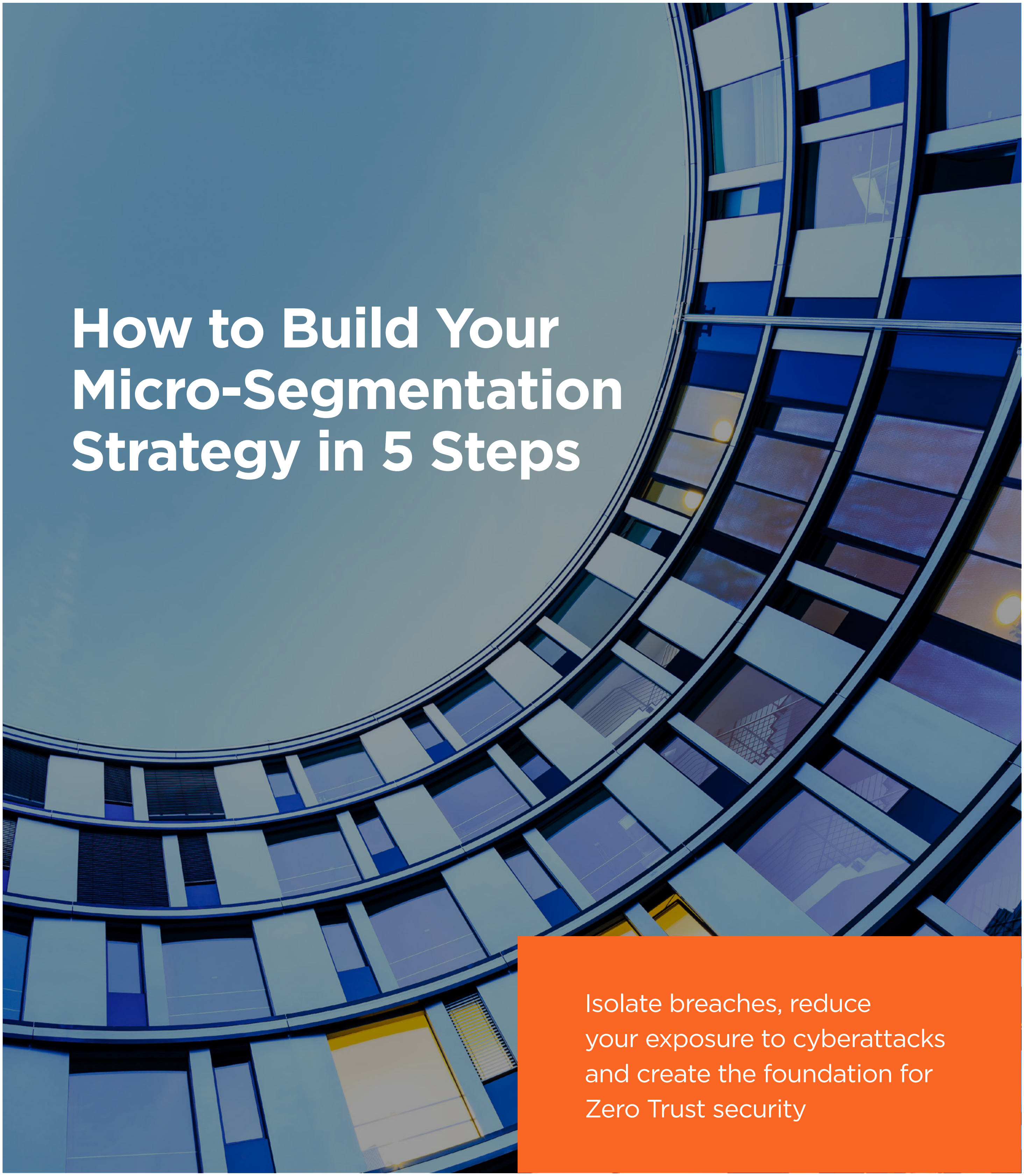
illumio

STRATEGY GUIDE



How to Build Your Micro-Segmentation Strategy in 5 Steps

Isolate breaches, reduce your exposure to cyberattacks and create the foundation for Zero Trust security

Contents

Why You Need Micro-Segmentation

Your environment has changed, and your attack surface has expanded.

In the past, you operated your own on-premises network. It was primarily composed of physical servers and corporate-owned devices. You were able to build a hardened security perimeter around this network and focus your efforts on just keeping bad actors outside of it.

Today, you operate a hybrid network. It's composed of virtual and physical servers, and corporate and employee-owned devices. Some of these devices live in your office, but many of them can now live in practically any location. You can no longer build a perfect security perimeter around this network. Breaches are now inevitable, and you need a way to prevent bad actors from moving easily inside your network.

Micro-segmentation solves this problem. It builds security inside of your network by closing pathways between your systems. When properly performed, micro-segmentation stops bad actors from gaining a foothold to spread to your high-value assets and cause significant harm.

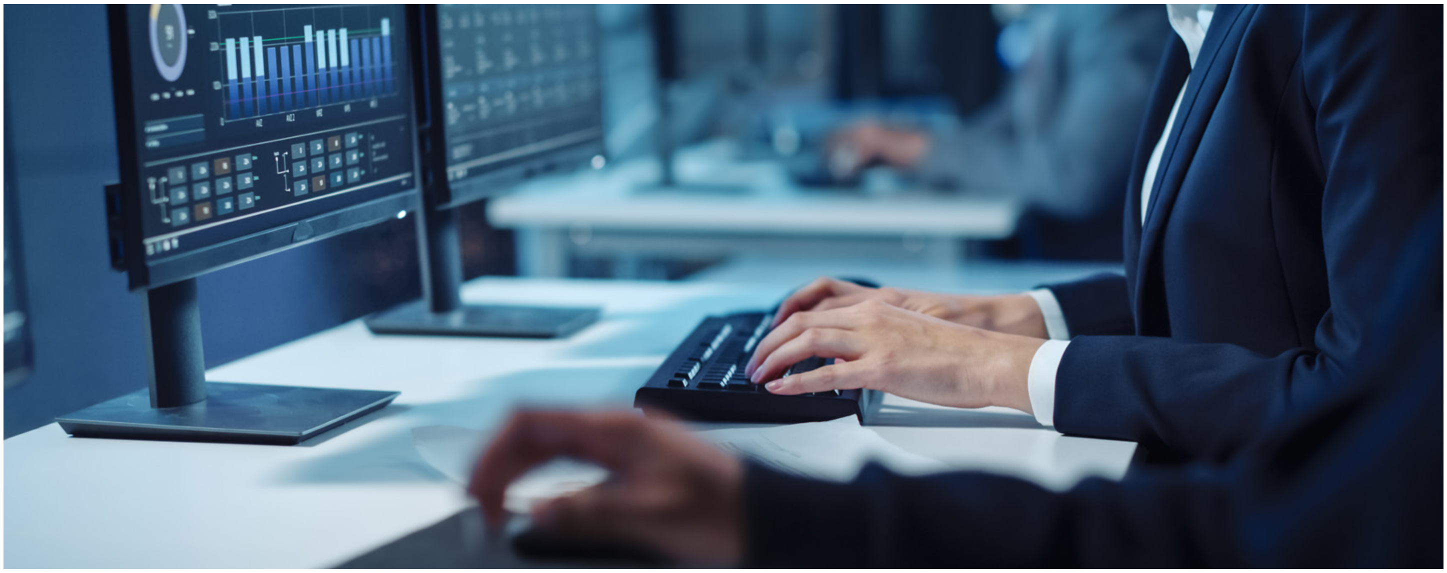
With the right micro-segmentation strategy, you will:

- **Reduce your attack surface:** You will eliminate many of the vulnerabilities inherent to modern network environments.
- **Contain breaches and damage:** You will limit how many systems and data sources a bad actor can compromise.
- **Accelerate the journey to Zero Trust:** You will build foundational pillars for most Zero Trust security strategies.
- **Achieve regulatory compliance:** You will meet security policy mandates for many regulatory frameworks.

This guide will help you build and implement the right micro-segmentation strategy.

To do so, we'll explore:

- How micro-segmentation works
- How to build an effective micro-segmentation strategy in 5 steps
- How to choose the right tool to drive your micro-segmentation project



Micro-Segmentation: What It Is and How It Works

Micro-segmentation is a simple security strategy. You create security policies that put walls around the systems in your network. These walls prevent unnecessary traffic from moving between your systems. This isolates your systems and separates them from other systems and areas within your network, limiting how far a bad actor can move through your network once they breach it.

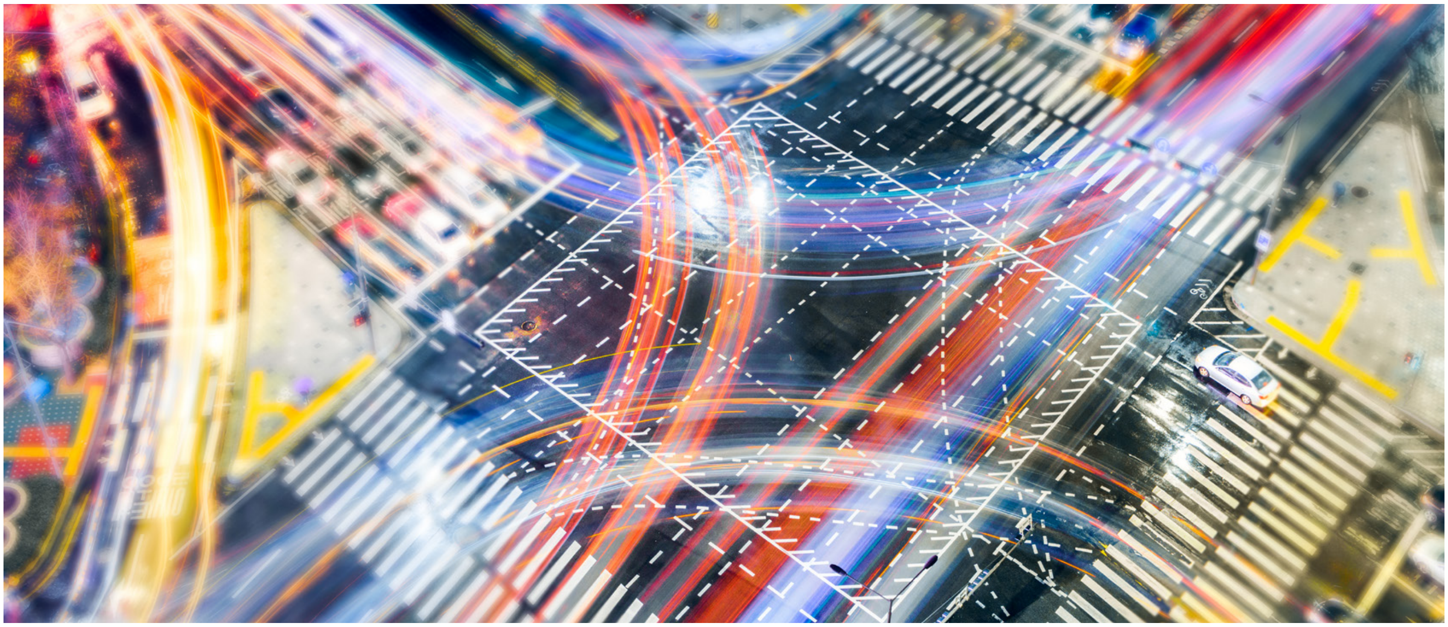
Micro-segmentation creates these walls around multiple types of systems at multiple levels of your network architecture. With the broadest segmentation, you can create a wall that separates two big areas from each other — for example, your DEV and PROD environments. With the most precise micro-segmentation, you can create a wall around an individual system — like an application, endpoint or cloud asset — that defines what other individual systems it can connect with and in what manner.

The right micro-segmentation strategy will tightly define how the systems in your environment communicate with each other. It will only allow system-to-system communications that are necessary to maintain your business operations, and it will eliminate pathways that bad actors can follow to reach your high-value assets.

However, there is no "one-size-fits-all" micro-segmentation strategy that you can implement to protect your network. Every organization has a unique:

- Network architecture
- Catalog of systems within their network
- List of high-value assets they need to protect
- Maze of pathways they must leave open to maintain operations
- Broader security strategy that micro-segmentation must support

As such, you must build a micro-segmentation strategy that's unique to your organization. To start, you must understand and begin to select which security outcomes your micro-segmentation strategy needs to deliver.



The Most Common Micro-Segmentation Scenarios

Micro-segmentation gives you a flexible strategy that can support and deliver a wide range of security results.

Your micro-segmentation strategy will likely serve more than one of these scenarios, depending on the specifics of your applications and networking environment. The most common include:

- **Securing core services:** Micro-segmentation can secure the core services — like DNS, domain controllers, NTP and LDAP — that are used by multiple workloads and systems and which are essential to your environment's operations. Application owners sometimes lack visibility into these services and struggle to work with other teams to secure them. Micro-segmentation can give you more visibility and control over how these services are being used.
- **Enforcing ransomware protection:** Micro-segmentation can improve a ransomware detection and response program. Most ransomware rapidly moves through networks by exploiting a small set of high-risk ports and protocols like RDP and SMB. Micro-segmentation can close and control these ports and protocols, which slows a ransomware attack, limits the number of systems it can compromise, and buys time for detection and response tactics.
- **Separating environments:** Micro-segmentation can separate modern environments better than traditional tools like firewalls. These tools struggle to maintain even broad segmentation in today's highly dynamic environments and introduce risk when user accounts need access between segments. Micro-segmentation gives you a simpler and more sustainable approach to separate environments and keeps them separate even as your network evolves.
- **Ring-fencing applications:** Micro-segmentation can separate your applications to keep them secure and compliant with regulatory frameworks. Traditional approaches — like firewalling or network virtualization — cannot manage today's high volume and wide variety of applications. These approaches are too complex and lack granular controls. Micro-segmentation can separate applications and workloads in the most complex environments, from data centers to OT networks.
- **Securing the cloud:** Micro-segmentation can protect public, private, multi-cloud and hybrid environments. Nearly every organization uses the cloud. Some use it to reduce costs, others to expand their reach, and others — like banks and manufacturers — use it as the core of their business. Micro-segmentation can consistently secure your cloud, no matter what architecture you deploy, no matter your use case, and no matter the stage in your cloud adoption journey.
- **Creating tier-based micro-segmentation:** Micro-segmentation can protect the highest-value asset in every system — its data. To do so, it can control the flow of traffic between a system's web, application and data layers. This effectively segregates the tiers within the system and prevents attackers from reaching critical data. This is one of the finest-grained forms of micro-segmentation but is achievable with the right strategy and tools.

How to Build Your Micro-Segmentation Strategy

To help define what your roadmap looks like, let's walk through the five steps you must follow to build and implement your micro-segmentation strategy.

5 Steps to Build an Effective Micro-Segmentation Strategy

While you can follow many different paths to build a micro-segmentation strategy, our customers have found the following five-step process effective:

1. **Identify your high-value assets**
2. **Gain visibility into communication flows**
3. **Design your strategy**
4. **Test your new policies**
5. **Segment your environment**

Let's look at each step in greater depth.

Step 1: Identify your high-value assets

First, you must set your priorities.

You cannot defend every one of your assets from every possible threat (at least not at first). Instead, you must identify which of your assets are most important to your broader security strategy and your organization's mission. Then, develop a micro-segmentation strategy to protect those assets by isolating them in your network.

Your high-value assets (HVAs) are unique to your organization. They can include data, applications, systems, services and anything else that's both digital and mission critical. If you're in retail, that might be your customer database. If you're in healthcare, that might be your medical scanner. No matter what your HVAs are, choose what you must protect first and then build your strategy around them.

Step 2: Gain visibility into communication flows

After identifying your HVAs, you must then understand how they can be accessed.

To do so, you must map the connections between your workloads, applications and devices. Then, you must combine this visibility with vulnerability scan data. Doing so will show you where your HVAs are connected, vulnerable and exposed to other systems through ports that bad actors like to travel to compromise assets.

This visibility will tell you where and how to segment your network to protect your HVAs. It will tell you which pathways lead to your HVAs, which of those pathways aren't being used and can be closed, and which pathways must remain open for legitimate traffic but must be watched closely for malicious activity.

Step 3: Design your strategy

Once you know what HVAs you must protect and how they are vulnerable, you will be ready to define a strategy that keeps those assets safe.

As mentioned before, there is no such thing as a "one-size-fits-all" micro-segmentation strategy. Instead, here are a few proven tips for developing your unique strategy:

- Select from the above micro-segmentation use cases.
- Choose different use cases for different locations in your environment.
- Apply coarse-grained segmentation to low-value locations in your environment and fine-grained micro-segmentation to your HVAs.
- When needed, use micro-segmentation as a compensating control for other vulnerability management activities — like patching — that might be lagging.

- Create a timeline to segment your network in stages. First, test your approach on low-risk areas of your environment. Then prioritize your HVAs. Finally, plan to progressively harden the rest of your environment over time.

Step 4: Test your new policies

Your micro-segmentation policies shouldn't break your business.

We've all either heard of, or been involved in, an episode where a security operator has hit the "publish" button for firewall rules, and then minutes later, the phone starts ringing because half the company is off air.

To avoid this, your micro-segmentation strategy can't block legitimate traffic that must continue to flow within your network. There are three ways to prevent this:

1. Use the visibility you developed in step two and write security policies that are sensitive to how traffic must naturally flow during normal business operations.
2. Write simple security policies that have minimal chance of creating unexpected impacts on applications when applied to production environments.
3. Run tests that show you the impact of prospective rule changes on live traffic without having to actually apply those changes.

Step 5: Segment your environment

Finally, you must distribute and enforce your micro-segmentation policies.

How you do so — and how well you can apply policies in a fast, accurate and sustainable manner across enterprise-scale networks — depends almost entirely on the micro-segmentation technology that you use.

The next section will explore why traditional tools typically fail to implement micro-segmentation strategies and how Illumio succeeds where they struggle.

Picking the Right Micro-Segmentation Technology

Most organizations should implement micro-segmentation, but they struggle to bring their strategy to life using traditional tools. Here's why those tools typically fail, and how Illumio makes micro-segmentation achievable.

Why Traditional Tools Struggle to Implement Micro-Segmentation

Most segmentation tools were not designed to create scalable, granular micro-segmentation between the systems inside of large, constantly changing networks.

Traditional network tools — like firewalls, VLANs or subnets — were designed to segment largely static networks from one another. Updated tools — like virtual firewalls or software-defined networking — are still highly manual, error prone and restricted by network constructs and IP addresses.

If you try to use these tools to create micro-segmentation within your network, you will need to install, manage and regularly update hundreds, thousands or even hundreds of thousands of individual instances of these tools. Doing so is expensive, complex, time-consuming and ultimately impossible for many organizations.

The result: When most organizations segment their networks with traditional tools, they typically expend a lot of resources just to maintain very broad segmentation. This does little to reduce their attack surface, limit the movement of bad actors, and keep them secure against modern threats.

Illumio solves these problems.

Meet Illumio: A Modern Solution for Micro-Segmentation

Illumio is a unified platform designed to create micro-segmentation within modern networks. Illumio solves the problems with traditional network tools and provides a new approach to rapidly segment networks at both broad and granular levels.

To do so, Illumio:

- **Performs host-based segmentation:** Illumio does not layer external tools over your systems. Instead, Illumio configures the native firewall controls that already exist in nearly every operating system and workload. By doing so, Illumio rapidly segments your network without touching its architecture.
- **Segments diverse environments:** Illumio creates micro-segmentation across multi-cloud, hybrid and on-premises networks. Illumio can segment workloads, endpoints and cloud assets from a single platform and apply policy to any system, including bare-metal, virtual machines, containers and more.
- **Simplifies policy management:** Illumio makes it fast and simple to apply and maintain policy across hundreds of thousands of systems. To do so, Illumio streamlines, simplifies and automates the four key stages of segmentation policy management — discovery, authoring, distribution and enforcement.
- **Maintains segmentation as networks evolve:** Illumio does not force you to re-architect your network or manually re-configure your segmentation tools every time your network changes. Instead, Illumio applies segmentation policies that automatically follow systems even as they move and change.

By taking this new approach, Illumio makes micro-segmentation achievable for organizations of any size.

How Illumio Provides Support for Comprehensive Micro-Segmentation

Illumio provides a flexible suite of features that can help you meet a wide range of micro-segmentation requirements — including each of the scenarios we previously outlined.

- **Illumio secures core services:** Illumio can quickly and easily define and enforce application policies. To do so, Illumio's Core Service Detector helps you identify and label the centrally connected services in your network. This feature looks for 51 common core services that applications depend on, pinpoints each instance of these services in your network, and then suggests an appropriate label for each.
- **Illumio enforces ransomware protection:** Illumio can create proactive and reactive ransomware defenses. Illumio's Enforcement Boundaries can block protocols on a single system, a group of systems or on all hosts that use it. This feature lets you close protocols that ransomware likes to travel through in just a few clicks, making it easy to shrink your attack surface or contain an in-progress incident in seconds.
- **Illumio creates environmental separation:** Illumio can simplify the process of writing and enforcing environmental separation policies by eliminating the need for rule ordering. Illumio can also drastically reduce the risk of misconfiguration when enforcing these policies. For example, if you need to give an administrator access to both sides of an environment, Illumio can put in place simple exceptions to your policy.
- **Illumio performs applications ring-fencing:** Illumio can quickly and easily place a secure ring-fence around any application, no matter if it lives in the data center or in the cloud. Illumio's real-time application map can show you a single application and visualize each of the workloads that compose it. From there, you can clearly see what the application connects to and which connections you can close to isolate it.
- **Illumio secures the cloud:** Illumio can automatically map, segment and secure workloads in the cloud as easily as workloads in the data center. Illumio can show you the flow of traffic between the resources in cloud applications, provide recommendations on how to segment and secure those applications, and implement those policies by configuring their native cloud security functions.
- **Illumio creates tier-based micro-segmentation:** Illumio can use the same core features to quickly and easily create any level of segmentation — from ring-fencing applications, applying tier-level separation or enforcing highly granular policy. With Illumio's Policy Generator, you can click a few buttons, select the right level of separation, and control the flow of traffic at multiple levels of any application.

Building Micro-Segmentation With Illumio

Our customers have used Illumio to implement micro-segmentation following the five steps we outlined above. Here's how Illumio helped them bring this framework to life.

- **Gain real-time visibility:** Illumio creates a comprehensive application dependency map and a real-time picture of the traffic flows in your network. With this visibility, you will see how your HVAs can be accessed, see which of those pathways you can close and which you must keep open, and — overall — see what type of segmentation to place within each area of your environment.
- **Segment at optimal levels of granularity:** Illumio lets you create a flexible strategy to implement the right segmentation in the right places. Illumio can create broad segmentation (such as separating DEV and PROD environments), fine-grained segmentation (such as segmenting small groups of systems), or nano-segmentation (such as isolating individual application tiers or workloads).

- **Test policies before deployment:** Illumio's real-time visibility shows you all traffic flows and makes it easy to accurately decide where to enforce policies. Further, Illumio can test each new policy you write and show you its impact on live traffic — without actually applying the policy — reducing the risk of making changes and helping to avoid network failures.

- **Quickly implement and maintain security:** Illumio simplifies, streamlines and automates every stage of policy management. Illumio can rapidly apply policy to tens or hundreds of thousands of systems without generating significant network strain. Further, Illumio maintains security policy and segmentation rules on your systems even as your network evolves.

Real-World Micro-Segmentation: How Illumio's Customers Build Cyber Resilience

Illumio is proven in the real world. Many of the world's largest and most innovative organizations use Illumio to segment their networks.

Our customers have implemented Illumio to create micro-segmentation within modern enterprise networks. A few recent examples include:

- An e-commerce site secured 11,000 systems in three months — and successfully passed a critical audit.
- A leading SaaS platform safeguards 40,000 systems under full DevOps automation, including policy and enforcement.
- A large custodial bank protects $1 trillion per day of financial transactions under federal regulatory scrutiny.

Illumio is used by:

- More than **15** of the **Fortune 100**
- **6** of the **10 largest global banks**
- **5** of the **leading insurance companies**
- **3** of the **5 largest enterprise SaaS companies**

"Illumio has filled a gap for which there was previously no solution. In addition to meeting compliance regulations, we have seen drastic improvements in our overall security posture."

Steffen Nagel
Head of Information Technology
Frankfurter Volksbank

"Gaining live visibility into flows between workloads down to the paths of protocols provided immediate value. The ability to use the map to easily allow-list traffic and achieve the level of segmentation needed will be a tremendous time-saver over manually programming firewall rules."

Mikael Karlsson
Head of IT Infrastructure
AFA Försäkring

"The initial attraction [to Illumio] was really the simplicity. Having the ability to span the physical and virtual and present insights in a highly resolved fashion is a game-changer."

Andrew Dell
CISO
QBE Insurance

Segment Your Network — Starting Today

Building and implementing a micro-segmentation strategy can be challenging, but Illumio can help.

- Visualize your data center and cloud — without re-architecting your network.
- Build your application map and vulnerability map.
- Shift your focus to the connections inside your perimeter.
- Apply controls and create segmentation at the endpoint level.
- Simplify, streamline and automate segmentation policy management.
- Take an agile, incremental approach that emphasizes quick wins.
- Apply policies to every component and system within a single unified platform.
- Segment hundreds of thousands of systems and millions of internal connections.
- Build a segmentation strategy that makes sense for your environment.
- We work with you to implement and maintain your micro-segmentation strategy.
- Complete most micro-segmentation projects in months, not years.

It’s Time to Achieve Micro-Segmentation With Illumio

See Illumio in action

Watch a demo of Illumio Core.

Learn more about how Illumio can help you build your micro-segmentation strategy

Contact us today to speak with our sales team. During our conversation, we will:

- Discuss your current security strategy and requirements
- Help you build a micro-segmentation strategy that works for you
- Show how Illumio can implement your strategy and improve your security