



Achieving Segmentation with Illumio

How Illumio makes segmentation
fast, simple and scalable for any
organization.

Contents

Why You Need a New Approach to Achieve Zero Trust	2
What is Zero Trust and Why Do You Need It?	2
The Role of Segmentation in Zero Trust	3
Meet Illumio: A Modern Platform for Segmentation	3
Illumio Delivers Full Flexibility in How You Segment	4
 How Illumio Builds Segmentation	 5
A Focus on East-West Traffic (Not Just North-South)	5
Host-Based Segmentation, Not Network-Based	6
Create Both 'Deny Lists' and 'Allow Lists'	6
 How Illumio Manages Segmentation Policy	 7
Policy Management Made Simple, Streamlined and Safe	7
Policy Discovery	7
Policy Authoring	8
Policy Distribution	8
Policy Enforcement	8
 How to Achieve Zero Trust With Illumio: Step-by-Step	 9
An Agile, Incremental Approach Segmentation	9
4 Steps to Quickly Build and Enforce Your Initial Segmentations	9
Maintaining, Managing and Evolving Segmentation Over Time	10
 Illumio Under the Hood	 11
A Unified Platform for Segmenting Everything	11
Your Single Source of Truth and Action	11
A Modern Platform That Builds Segmentation Fast	12
 Illumio in the Real World	 12
Case Studies: How Our Customers Build Segmentation	12
Bringing Illumio to Your Organization	16

Why You Need a New Approach to Zero Trust

While most organizations know Zero Trust can solve their biggest security challenges, they still struggle to bring this strategy to life. To help, Illumio offers a new solution.

What is Zero Trust, why do you need it?

Zero Trust is a proven approach for solving many of today's biggest security challenges.

In the past, most organizations operated their own data centers, employees used corporate devices in on-premises locations and systems were protected by hardened perimeters. The idea was that by keeping out bad actors, these practices assured an organization that all activity within its perimeter was both legitimate and safe.

Today, that approach is obsolete. IT environments now combine physical, virtual, private and public cloud systems. Employees have both corporate and personal devices that they can use anywhere and anytime.

The result: A blurring of the distinction between inside and outside the perimeter and between what's trusted and not trusted. Also, perimeter breaches have become inevitable, internal attack surfaces have become massive and flat, and bad actors have gained the ability to move easily among systems until they achieve their malicious and often illegal objectives.

All these challenges can be addressed with Zero Trust. This approach shifts an organization's focus away from preventing breaches. Instead, Zero Trust prevents harm once a bad actor has gained access.

Most current Zero Trust strategies are designed around three core concepts:

1 All entities are untrusted by default.	2 Comprehensive monitoring is maintained.	3 Least privilege access is enforced.
Don't focus on stopping breaches. Instead, assume bad actors are already in your network. Focus on stopping them from moving laterally to access your systems and steal your data.	Don't assume all movement within your network is legitimate. Instead, visualize the attempted connections in your organization. Then verify that they're legitimate <i>before</i> you let them access your systems and data.	Don't leave your organization open. Close most of your open connections. Allow systems to connect to one another only when they explicitly must do so.

The role of segmentation in Zero Trust

While implementing Zero Trust can involve many security disciplines, most strategies include segmentation as a foundational pillar. Segmentation is the process of managing how your systems communicate both with each other and with the outside world. Done effectively, segmentation can help you:

- **See and understand your risks:** Segmentation shows how your applications communicate and interact both with each other and with the internet — in real time and at scale. This can help you map the exposure and risk levels for all your applications and data. That, in turn, can help you to better prioritize your security efforts.
- **Protect your data:** Segmentation secures your applications by applying unified least privilege policies across your entire infrastructure. This limits your data's exposure to risk. It also creates baseline protections that can be continuously improved (if you so desire) by creating increasingly granular policy levels.
- **Respond quickly and effectively to changes in your environment:** Segmentation maintains your security posture and state of least privilege, even if your environment changes. It does this by combining enriched telemetry, dynamic policy and complete API coverage. Working together, these technologies can keep your environment safe — and without impacting your applications.

Despite the many benefits of segmentation, most IT architectures were developed without it, and most security tools can create only broad separation among largely static environments. Many organizations also lack internal teams with the expertise and bandwidth required to implement and maintain segmentation using traditional tools. As a result, while most organizations understand the benefits of segmentation, many still struggle to implement it.

When these organizations attempt to create granular segmentation they often spend a lot of time and effort. But they still fail to reduce their attack surface, limit the movement of bad actors and secure their data against threats.

Illumio offers a new solution that addresses many of these operational challenges. Illumio helps organizations make Zero Trust implementations faster, more scalable and more achievable.

A modern platform for segmentation

Illumio is a unified platform designed to help organizations build segmentation across workloads, endpoints and cloud services. Illumio addresses the shortcomings of more traditional tools by providing a new approach, one that rapidly segments modern IT environments down to the level of system, application, port or process.

With Illumio, you can:

- Build segmentation faster, easier and in a more scalable way than you could with more traditional tools.
- Complete most initial projects in just days or weeks, thanks to the way Illumio focuses on protecting high-value assets and quickly applying selective enforcement.
- Simplify, streamline and automate each stage of the policy management lifecycle. This, in turn, will let you implement and maintain granular, large-scale segmentation, even if you have only limited internal teams working on the project.
- Model policies before you deploy them. This helps lower the risk of disrupting business processes during your segmentation project.
- Segment your every component and system, and create a single source of truth and action for each of role involved in your segmentation.

Here are some of the key capabilities Illumio delivers for implementing Zero Trust:

Speed	Simplicity	Comprehensiveness
With Illumio, most initial segmentation projects can be completed in just days or weeks.	Illumio streamlines and automates many of the core tasks of Zero Trust, including policy management.	Illumio segments an IT environment at the macro, micro and nano level, and across any system.
Scalability	Safety	Achievability
Illumio can enforce policy across hundreds of thousands of systems – and the millions of connections between them.	Illumio runs from a single agent. It's invisible to users, produces a light load on each system and runs at low risk for application disruption.	Illumio is field-tested and proven in the real world. Our customers deliver verified segmentation at enterprise scale.

Illumio delivers full flexibility in how you segment

Another benefit of Illumio: It lets you segment your environment, building a foundation for broader Zero Trust initiatives. Because Illumio works equally well in any type of hybrid environment, it can protect organizations ranging from cloud-first startups to complex multinational corporations.

Illumio can also help you set up a reactive “containment switch” that quickly applies a restrictive set of segmentation policies. In the event of a security incident, you can simply switch on this control to stop the attack from spreading. What's more, you have the option of either locking down your network as a whole or severing your highest-risk communications, whichever is more effective.

Illumio uses a flexible and extensible toolset. That can help you drive a wide variety of segmentation projects, including:

- Blocking high-risk ports
- Isolating core services
- Separating environments
- Ring-fencing critical assets

- Securing hybrid environments
- Satisfying regulators and auditors
- Identifying and restricting outbound connections
- Managing user and administrative access
- Controlling users and endpoints by identity
- Isolating and protecting high-value applications

For the rest of this solution guide, we'll explore how Illumio can be used to build segmentation in situations where traditional tools often cannot. We'll also show you how to use Illumio to achieve Zero Trust within your own organization.

How Illumio Builds Segmentation

To correct the many shortcomings of traditional security tools, Illumio rethinks segmentation from the ground up. Illumio provides a new approach to key areas of this security strategy.

A focus on east-west traffic (not just north-south)

Traditional, perimeter security tools focus on north-south traffic — the movement of data either in and out of an organization or from users into applications.

To be sure, monitoring north-south traffic is still important. It can tell you whether bad actors have breached your organization and, if so, whether they're pulling down tools to either advance their attack or steal data from your systems.

However, monitoring north-south traffic alone will not tell you whether bad actors are actively moving inside your organization. Nor can it tell you which of your systems and data may have been compromised. This, in turn, can create gaps in your detection and response capabilities, giving bad actors plenty of time to progress. Currently, the average time needed to detect an attack is a very long 212 days. And the average time to contain a breach once it's been detected is another 75 days. That's a total time of 287 days — more than nine

months — to remediate an attack, according to the latest [IBM Cost of a Data Breach study](#).

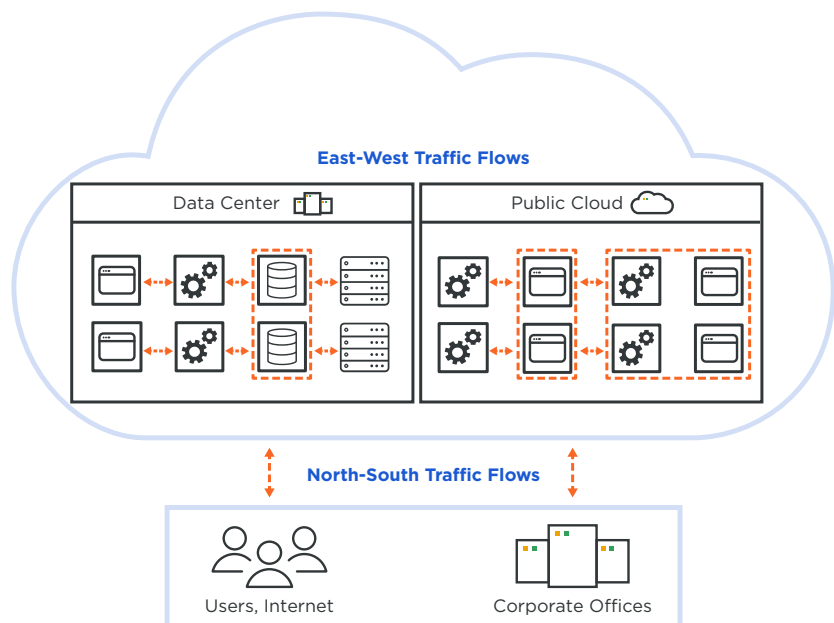
To detect attacks faster, you need to also monitor east-west traffic. That's the lateral movement of data among systems within your organization.

To monitor east-west traffic with traditional tools, you could manually install a firewall-like tool at every connection point. In practice, however, this is generally impossible. A modern organization can have hundreds of thousands of systems, along with millions of potential connections between them. There's no way to connect them all manually.

Illumio addresses this challenge by monitoring both north-south and east-west traffic. It also logs every movement or attempted movement made between your internal and outside systems — all without placing hardware between them. Illumio also logs these movements for historical reference when reacting to a breach.

75% of data center traffic is east-west

On average, every 1 MB of north-south traffic entering a data center or cloud will generate 20 MB of associated traffic east-west, workload-to-workload. This means that relying on perimeter firewalls will make you blind to the vast majority of traffic.



Host-based segmentation, not network-based

Here's another difference: Traditional security tools perform what's known as "network-based segmentation." This means they layer external tools — such as network devices, firewalls and software-defined networking tools (SDNs) — to manage policies that define how systems within your organization can communicate.

This approach was designed to segment environments that were both largely on-premises and quite stable. However, when network-based segmentation is applied to modern organizations that are distributed and constantly changing, it can create serious problems:

- You're forced to re-architect the network every time it needs to be resegmented. In today's dynamic organizations, this occurs all the time.
- You can implement only broad macro-segmentation, leaving most of the organization flat and vulnerable.
- You must untangle a complex web of VLANs, subnets, IP addresses and access control lists, all of which demand high degrees of manual effort to manage.
- You add complexity and costs to your organization's underlying infrastructure because you now require a growing stack of point solutions.

Illumio addresses these problems by taking a different approach, one known as "host-based segmentation" (also referred to by Gartner as "identity segmentation"). This means Illumio does not layer networking tools onto your computer systems. Instead, it configures the native firewall controls that already exist in operating systems and networking equipment. This approach lets you:

- Segment your environment without touching or changing its architecture.

- Apply policies to follow workloads even as they move and change.
- Visualize, orchestrate and coordinate segmentation from just a single console.

Create both 'Deny Lists' and 'Allow Lists'

Most traditional tools struggle to identify which of an organization's connections must remain open. This can make it difficult to apply the granular policies capable of providing effective security without breaking the functionality of applications.

As a result, most organizations either:

- Build policy around generic "deny lists." These block the few things the organization never wants to allow across network boundaries.

or

- Apply very broad access "allow lists." These leave open the few communications the organization always wants to allow.

or

- Attempt to use both at once.

The result: unnecessary connections between systems are left open, connections required to maintain business operations are closed, and pathways that bad actors can use to create a breach and then spread their attacks are left open.

Illumio addresses these problems by securing your organization while leaving necessary connections open. To do this, Illumio:

- Shows you all connections to or from a system. Illumio also helps you understand which connections need to remain open.
- Creates targeted enforcement boundaries that act as a more accurate "deny list." Then Illumio blocks a few specific communications while leaving the rest open.

- Creates granular “allow lists” that can default-deny every connection except the small list of connections the system absolutely needs.
- Visualizes the impact of your policies on live traffic. This helps you to anticipate the impact of blocking or allowing a connection. It also helps

you to ensure your policies are working as intended.

- Simplifies, streamlines and automates the enforcement and management of these policies. This ensures that your systems’ unnecessary connections are kept closed at all times.

How Illumio Manages Segmentation Policy

Segmentation is built by effective policy management. Illumio makes it fast, easy and safe to apply and maintain policies for organizations of all sizes.

Policy management made simple, streamlined, and safe

Most traditional security tools manage policy through manual actions that take far too much time and effort. Also, these tools typically force you to apply policy “blind,” that is, with no understanding of how the policy will impact your users and their systems. This can lead to business disruptions every time you make a change.

By contrast, with Illumio you’ll simplify, streamline and automate the four key stages of policy management: policy discovery, authoring, distribution and enforcement. Further, you can model policies and see their impact on users and systems before you enforce them. This helps prevent business disruptions and accelerates policy distribution.

Here’s how Illumio manages a segmentation policy at each of the four stages in its lifecycle:

1

Policy discovery

Because you can’t segment what you can’t see, Illumio provides all of the information you need to understand your applications, endpoints and cloud services — and to write granular, meaningful segmentation policies for each.

Illumio will help you:

- Create a comprehensive map of your applications and their contexts, including all communications and dependencies.
- Visualize and explore traffic flows across your entire environment from both macro and micro perspectives from environmental segmentation down to the workload level.
- Give application owners purpose-built views and workflows.

2**Policy
authoring**

Seeing your systems is just the start. You must also write policies to minimize your risks and secure your systems. Illumio moves seamlessly from discovering which policies you need to efficiently creating segmentation policies for your environment.

With Illumio, you will:

- Write declarative, easy-to-understand policies that get automatically translated into real-world rules.
- Organize your systems with the familiar names and labels you already know — not by their IP addresses.
- Write a policy once and then reuse it as many times as you need and on any number of systems.
- Streamline collaboration by letting application owners and teams independently complete steps of the authoring process.

3**Policy
distribution**

Once you've written a policy, you must distribute it to every system that needs it. Illumio automatically translates policies into rules that systems can understand. Then it quickly and accurately distributes those rules to as many devices as you have.

With Illumio, you will:

- Program the firewalls that already exist inside your systems – instead of deploying new third-party firewalls.
- Continuously and automatically maintain policy on systems as they swap IP addresses or otherwise change locations.
- Rapidly distribute fine-grained policy to any number of systems.
- Program non-host-based enforcement points — like load balancers, network devices, firewalls, mainframes and cloud-native systems — to apply truly unified security policies.

4**Policy
Enforcement**

Finally, you must reliably enforce the policies you distribute everywhere and at all times. Illumio rapidly enforces segmentation policies across even enterprise-scale infrastructures — and it keeps those policies in place no matter what.

With Illumio, you will:

- Maintain both application performance and security policy to protect mission-critical environments.
- Perform selective enforcement of segmentation policy anywhere in your environment.
- Accelerate enforcement with pre-application testing and visualization.

How to Achieve Zero Trust With Illumio: Step-by-Step

Illumio understands that Zero Trust security is an ongoing effort. First, Illumio can quickly build initial segmentation across modern organizations. Then it can help you maintain, refine and evolve that foundation over time.

An agile, incremental approach to Zero Trust

Most traditional security tools demand a “waterfall” approach to building Zero Trust. They force you to deliver sweeping changes to your organization in the scope of a complex, multiple-staged project. As a result, many times these projects fail to get approval. Among those that are funded, many are abandoned before completion. And the few projects that are completed fail to improve security until their very end.

Illumio takes a different, better path. It gives you an agile approach to building Zero Trust across your organization. **Illumio does this by letting you capture quick wins that dramatically improve your security within just the first few days and weeks of deployment.** From there, if you choose, Illumio can make it easy to tighten your controls, refine your segmentation and isolate more of your high-value assets.

4 steps to quickly build and enforce your initial segmentations

Using Illumio, many of the world’s largest organizations have quickly deployed segmentation:

- An e-commerce site segmented and secured 11,000 systems in just three months
- A leading SaaS platform applied and enforced policy on some 40,000 systems
- A large custodial bank that handles \$1 trillion of financial transactions daily now also protects its systems

While there is no one way to achieve Zero Trust with Illumio, many of our customers have followed a similar set of four steps to build their initial segmentations:

Step 1: Develop visibility	<p>Illumio can centralize your organizational visibility, share it with your employees and integrate it with other elements of your Zero Trust ecosystem.</p> <p>Illumio provides a real-time map of your systems, showing how they communicate. This map also reveals your risks, shows what “normal” system behavior looks like and helps you to define how to best segment your architecture.</p>
Step 2: Proactively and reactively close high-risk paths	<p>Next, Illumio can also set up two “quick wins” — a proactive and reactive set of segmentation policies — that dramatically improve your organization’s security:</p> <ol style="list-style-type: none"> 1. Proactively close, wherever possible, high-risk pathways that modern attacks like to exploit — including RDP, SMB and FTP. 2. Develop a highly restrictive set of policies you can apply instantly as a “containment switch” during an attack. This prevents the attack from spreading.

Step 3: Build fundamental Zero Trust macrosegmentation

In this step, Illumio systematically builds fundamental segmentation policies across your organization.

Most organizations will build a strong fundamental base for their Zero Trust strategy if they:

- Build environmental segmentation by, for example, separating development and production.
- Limit administrative access rights and privileges for commonly exploited applications.
- Enforce policy on core, highly-connected services such as Active Directory and Network Time Protocol.

Step 4: Implement microsegmentation to isolate high-value assets

Finally, Illumio can create granular microsegmentation that's tailored to your unique needs. For most organizations, this means building microperimeters around critical systems.

Additional activities can include:

- Securing hybrid environments
- Further ringfencing environments
- Creating policies to satisfy regulations and auditors
- Applying identity-based segmentation for both users and their endpoints

By following this timeline, you can use Illumio to quickly establish initial segmentation, secure systems across most of your organization and create a foundation for your Zero Trust security strategy.

Maintaining, managing, and evolving segmentation over time

Once you've completed your initial segmentation project, you'll have improved your fundamental security in a meaningful way. From there, you can continue to improve your security and manage your segmentation at more granular and powerful levels.

Over the long term, you can use Illumio to:

- Constantly improve your Zero Trust strategy by applying more effective application-specific enforcement and environmental segmentation.
- Detect anomalous behaviors and potential incidents by continuously visualizing and monitoring your entire environment.

- Prevent security breaches from spreading by proactively controlling any unwanted lateral movements.

Illumio can also automatically maintain your segmentation as your systems and organization evolve. Illumio makes it easy to tweak and expand your segmentation whenever your security needs change.

To do this, Illumio automatically:

- Adapts policies and recalculates rules as your organization changes.
- Scales policies and then applies them to new systems as your organization grows.
- Ensures policies follow systems as they move to new locations in your organization.

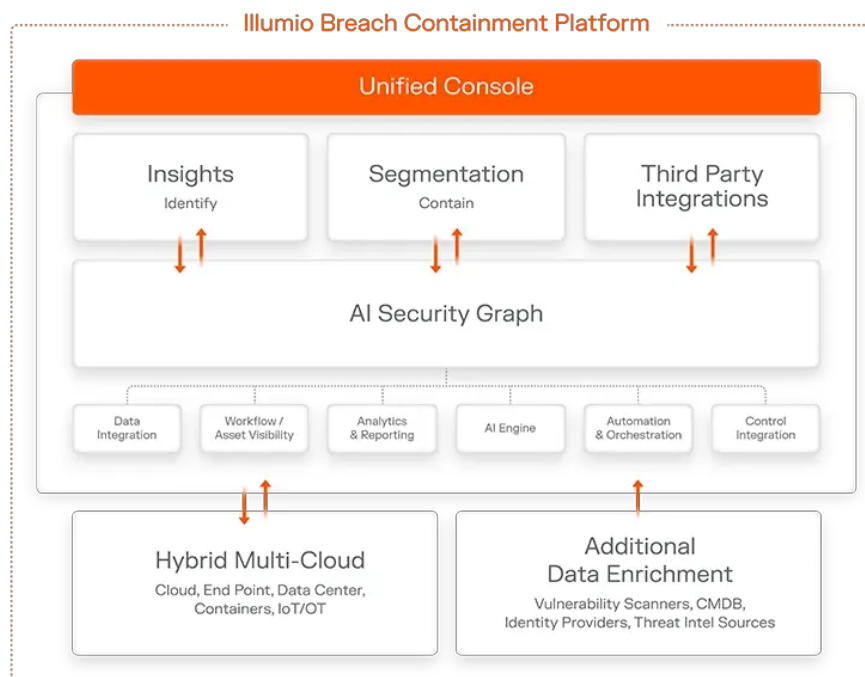
Illumio Under the Hood

Illumio was designed for building segmentation across modern organizations quickly and seamlessly. To do this, Illumio follows many best practices for modern application design and deployment.

A unified platform for segmenting everything

Most traditional security tools are point solutions, meaning they can build segmentation only within a limited set of use cases and only across a limited set of infrastructure components.

Illumio not only complements these tools but also gives you a unified platform that builds multilevel segmentation across every component of your organization. Illumio can segment multi-cloud, hybrid cloud and on-premises environments. And it can apply policy to any system, including bare metal, virtual machines, containers and cloud.



Your single source of truth and action

While segmentation is a cross-functional project, most traditional security tools generate scattered data and siloed views of the organization. They separate visibility from policy management. And they create friction between the roles involved in segmentation.

Illumio addresses these problems by creating a single source of truth for your data. Illumio gives each of your employees a single console that displays all custom views and policy management controls they'll need.

Here are some of the ways Illumio supports the cross-functional nature of segmentation:

- **Network, infrastructure, and security employees** use Illumio to translate business mandates into segmentation policies that are efficient to automate, operationalize and manage.
- **Security employees** use Illumio to create a fundamentally stronger security posture, drive faster and more accurate detection, and rapidly contain detected threats and evict attackers.
- **Leaders** use Illumio to measure risk mitigation, generate on-demand documentation of policy provisions, and track, manage and report on the overall progress of a segmentation project.

A modern platform that builds segmentation fast

Illumio follows modern application design principles to deploy quickly, run with a light load, grow with your needs and deliver value immediately.

Illumio is powered by six key technologies:

Automation	Scalability	Integrations
Performs many of the core tasks of segmentation policy creation and upkeep hands-free	Builds segmentation in organizations of any size and expands as you bring more systems online	Works out-of-the-box with other operations, security and analytics tools in a Zero Trust ecosystem
Role-based access control	Lightweight performance	Cloud-based instance
Empowers multiple roles to perform segmentation tasks without interfering with other roles	Runs in a way that's invisible to users, producing little load that could disrupt or raise the risk of business processes	Operates either on-premises or 100% in the cloud without additional infrastructure or ongoing maintenance

Illumio in the Real World


Many of the world's largest organizations use Illumio to build their segmentation strategy. And top industry analysts and service providers have recognized Illumio as a Zero Trust leader.


Case studies: how our customers build segmentation

Illumio currently delivers scalable segmentation and stronger security to:

- More than 15% of the Fortune 100
- 6 of the world's 10 largest banks
- 5 leading insurers
- 3 of the top 5 enterprise SaaS providers

Here's how some of our customers have used Illumio to achieve Zero Trust.

 CATHAY PACIFIC Leading global airline	
Challenge	Apply Zero Trust control across 3,000+ servers and 600 applications located both on premises and in Azure and AWS clouds.
Before Illumio	Wanted to improve their security by applying Zero Trust micro-segmentation and least privilege. But existing tools were slow, inefficient and unable to integrate visibility with policy management.
After Illumio	Designed and applied Illumio Segmentation across the organization in under 3 months (compared with 12 to 18 months with legacy tools).
Testimonial	<p>“Whenever we introduce new servers or applications, Illumio is part of the commissioning process. It’s proven to be easy to deploy and implement. And Illumio has helped us be more application-centric.”</p> <p>YC Chan Head of Infrastructure Engineering</p>

 QBE Global insurance leader	
Challenge	Apply segmentation across 10,000 workloads in globally distributed data centers and multi-cloud environments.
Before Illumio	Used physical firewalls and virtual firewall appliances for segmentation. But as the organization grew, this approach proved to be labor-intensive, complex and almost unmanageable.
After Illumio	Rapidly applied flexible, scalable segmentation. Now able to maintain consistent security as the organization expands and evolves.
Testimonial	<p>“Illumio enables us to roll out firewall changes much faster than before. Previously, it would be days or weeks. Now it’s minutes or hours.”</p> <p>Nick Venn Global Collaboration and Cyber-Infrastructure Manager</p>

Challenge	Apply segmentation across a globally distributed organization with both on-premises assets and hybrid and private clouds.
Before Illumio	Commissioned an external audit that recommended segmentation to achieve real-time visibility, prevent lateral movement and strengthen the risk posture across an expanding organization.
After Illumio	Reduced segmentation operational effort by 25% and segmented all high-value assets within 4 months of launching Illumio.
Testimonial	<p>“Illumio proved to be technically superior, not just in terms of what it offers, but also its functionality and how it works. It was the most mature solution that actually delivers on its promises in a way that’s stable and consistent.”</p> <p>Jacqueline Teo Chief Digital Officer</p>

Bringing Illumio to Your Organization

The Illumio advantage is clear. When organizations use traditional tools, their segmentation projects rarely make it past the planning stage. But with Illumio, you can complete initial projects in just days or weeks. Then you can easily maintain and evolve your Zero Trust strategy as your organization grows.

- **Learn more about Illumio technology:** Contain threats and strengthen your security posture with the world's first and leading [breach containment platform](#).
- **See Illumio in action:** Schedule a [consultation](#) with one of our security experts.

About Illumio



Illumio is the leader in breach and ransomware containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by the Illumio AI Security Graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters. Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.