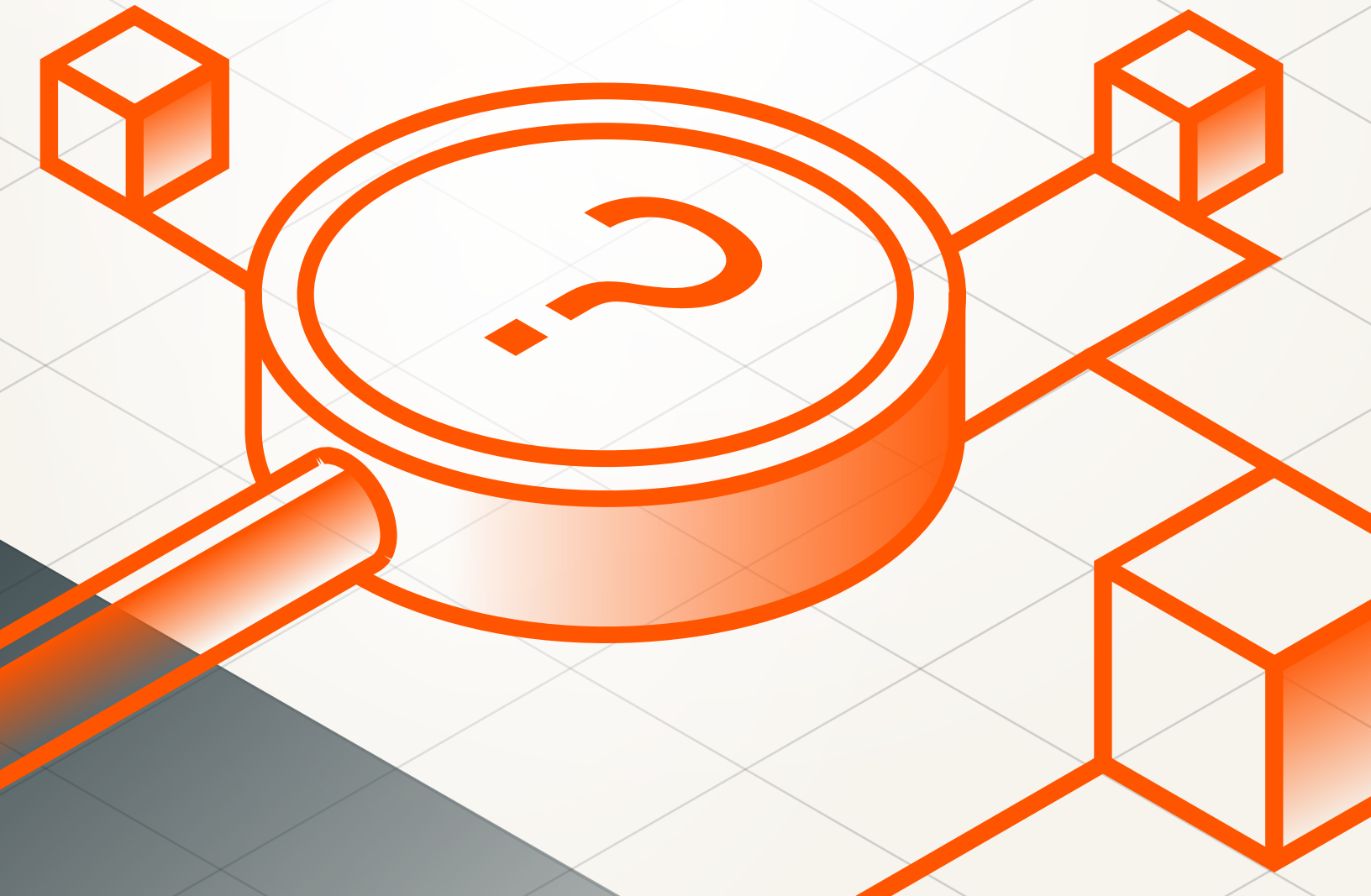
illumio

5 Questions to Ask Before Buying a Segmentation Solution

How to avoid hidden risk and choose a segmentation solution that holds up



Contents

INTRODUCTION

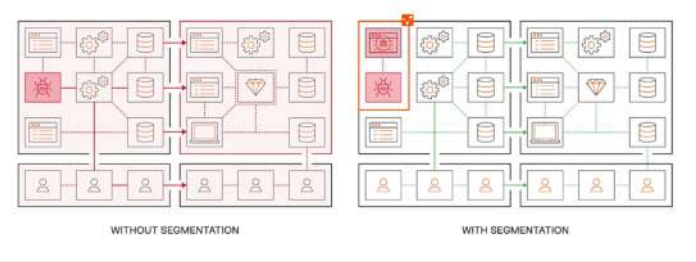
In late 2013, one of the most consequential cyberattacks in U.S. history unfolded against Target Corporation.

Hackers quietly walked in through the network's front door using credentials stolen from a third-party vendor. Once inside, they moved laterally until they had deployed malware on point-of-sale systems in more than 2,000 stores.

Ultimately, they stole credit and debit card data of more than 40 million customers and personal information for another 70 million.[1]

What made the breach so damaging was just how easily attackers navigated through the network. A compromised vendor account became the catalyst for massive lateral movement. The network trusted connections far too broadly and didn't constrain attacker movement once they were inside.

This pattern — seemingly small access turning into major loss — is a theme in breach reports decade after decade. And it's precisely what modern segmentation is built to prevent.



Segmentation is supposed to limit how far attackers can go once they're inside the network. But not all tools are built the same.

Some concentrate too much control in a single place. Others enforce policies without enough visibility or context. And many oversimplify deployment in ways that quietly open the door to new risk.

This e-book outlines the five key questions every buyer should ask when assessing segmentation vendors and how Illumio delivers segmentation that's simple without compromise.

[1] U.S. Senate Committee on Commerce, Science, and Transportation. "A 'Kill Chain' Analysis of the 2013 Target Data Breach." March 2014.

90%

of organizations faced attacks involving lateral movement in the past year.[2]

QUESTION 1

Who's really in control of your network?

Every segmentation vendor promises control. The real question: where does that control live?

Many platforms rely on centralized components to manage policy across the environment. These systems often require full administrative access. They initiate inbound connections to workloads using protocols such as remote procedure call (RPC), Windows Remote Management (WinRM), and Secure Shell (SSH).

At first glance, this design seems efficient. But it places a large amount of power in a single location. That concentration is exactly what attackers look for once they get inside a network.

Breach investigations show a consistent pattern. After initial access, attackers search for privileged control paths they can use to expand and move laterally.

If a segmentation platform relies on a central controller, that controller becomes an escalation point. Compromise it, and attackers gain leverage far beyond one system.

This is why understanding a solution's architecture matters more than a features list.

Zero Trust assumes compromise by design. No single system should hold enough privilege to weaken enforcement.

Some segmentation tools break that principle. They assume the controller will remain secure, available, and untouched.

Illumio is different — built from the ground up for Zero Trust.

Enforcement lives with each workload, not a central appliance. Workloads pull policies instead of receiving pushes from the control plane.

The platform never initiates inbound connections or needs admin credentials. If part of the environment is compromised, enforcement continues elsewhere. Control remains distributed.

Segmentation should limit what an attacker can do after gaining access. It should never increase their reach. If one compromise gives control over many systems, that's failure, not containment.

[2] Illumio. "The 2025 Global Detection and Response Report." October 2025.

QUESTION 2

Can you actually see what you're segmenting?

Segmentation without visibility turns into guesswork. Guesswork gives attackers room to move.

Many segmentation solutions promote automated policy creation based on observed traffic. But what they often miss is context.

Seeing two systems talk doesn't explain why they're talking. And it doesn't show how often that happens or what risk it creates if misused.

Attackers rely on this gap. When policies are built on traffic that teams don't fully understand, segmentation can keep dangerous paths open instead of closing them.

This puts security teams in a bind. Without clear insight into dependencies and traffic flows, they face hard choices, such as:

- Approving rules without full confidence that they'll work — and won't break anything
- Delaying enforcement to avoid risk
- Avoiding changes altogether to protect production systems

None of these approaches works at scale.

Illumio solves this problem with real-time visibility into how workloads communicate across data center, cloud, endpoint, and hybrid environments. Teams can see live flows, understand dependencies, and spot connections that no longer serve a clear purpose.

This level of visibility removes friction from enforcement. Teams are no longer forced to approve rules blindly, delay enforcement out of caution, or avoid changes to protect production systems.

With Illumio, visibility directly informs policy design. Teams can test segmentation rules before enforcing them and confirm how changes will affect applications.

Policies are based on how the environment actually behaves, not assumptions or static diagrams.

The impact becomes clear during incidents. When something breaks, teams don't have to rush to figure out what's connected. They already have the answers.

38%

of network traffic lacks enough context to support confident investigation and response.[3]

[3] Illumio. "The 2025 Global Detection and Response Report." October 2025.

QUESTION 3

Is the solution truly simple or just skipping critical steps?

Simplicity matters in cybersecurity. Teams want tools that are intuitive and easy to use.

But the wrong kind of simplicity can create real risk.

Some segmentation solutions speed up deployment by skipping agents, reducing context, or flattening policy models. That approach can shorten setup time, but it also strips away structure. Over time, that missing structure makes segmentation harder to manage.

Without strong labels, clear versioning, or audit history, policies become fragile. Even small changes can feel risky. Teams hesitate to act because they're unsure what might break.

What feels simple at the start often turns into operational debt a few months later.

Real simplicity comes from smart design, not from leaving critical capabilities out. It comes from policy models that grow with the environment instead of ones that work only when nothing changes.

It also comes from the ability to test changes, confirm behavior, and adjust safely as applications evolve and architectures shift.

Illumio is built with this kind of simplicity in mind.

Policies use clear labels instead of fragile IP rules. Teams can test changes before enforcement. Policy history is preserved, so teams always know what changed and why.

"Illumio was **simple to deploy**, didn't require any big investments in hardware, and is **really easy to manage**. We were in full enforcement of 90 to 95 percent of our estate within six months."

Fredrik Olandersson
Network Administrator, NIBE

This approach supports fast deployment without giving up long-term control.

Security teams don't need fewer steps if those steps are the ones that prevent outages and mistakes. A simple solution should never come at the cost of security.

QUESTION 4

Does the architecture actually align with Zero Trust?

Zero Trust is often described as a strategy or a framework. Architecture is what makes it real.

Zero Trust relies on a few core principles. Trust is never assumed. Privilege is kept to a minimum. Access is enforced as close to the resource as possible.

Segmentation plays a key role in enforcing those principles, but only when it follows the same rules.

Some tools claim to support Zero Trust while still relying on broad inbound access or centralized enforcement. Others make policy behavior hard to verify or offer limited audit visibility. These designs depend on trust that the system will always behave as expected.

That approach is fundamentally at odds with the Zero Trust model.

Illumio enforces segmentation locally using native operating system controls.

Every enforcement decision is logged. Policies continue to work even when connectivity is limited or parts of the environment are under stress. Enforcement doesn't depend on a constantly available, privileged controller.

This design keeps segmentation aligned with Zero Trust principles during normal operations and during incidents.

For organizations adopting Zero Trust to meet regulatory, operational, or board-level expectations, these details matter. Architecture determines whether Zero Trust stays theoretical or works when conditions are least predictable.

QUESTION 5

Is a lower price quietly increasing your risk?

Cost matters in every security decision. But in segmentation, the lowest upfront price can lead to higher cost over time.

Lower-cost tools tend to give up important capabilities. Visibility may be limited. Enforcement may not scale. Policy controls may lack flexibility.

These gaps don't always appear right away, but they surface as environments grow.

When that happens, teams find workarounds. They add more tools, create manual steps, and approve exceptions to keep systems running.

Complexity increases, and risk grows along with it. The early savings fade quickly.

Industry data shows that breach impact is shaped by how far an attack can spread and how long it takes to contain it. Segmentation plays a direct role in both.

> "A Zero Trust posture was a necessity for HGC, and Illumio accelerated us on that journey. **This has given us peace of mind — and you can't put a price on that.**"
>
> **Jacqueline Teo**, Chief Digital Officer
> HGC Global Communications

The wrong design allows attackers to move freely; the right one limits damage.

Illumio may not always be the lowest-cost option. That's intentional. Customers choose Illumio because it supports robust segmentation across hybrid cloud environments. Illumio aligns with Zero Trust goals and stays effective as your infrastructure changes.

It's critical to remember that the true cost of segmentation isn't the license. It's whether the architecture can reduce attacker movement when it matters most.

CONCLUSION

Why leading organizations choose Illumio for segmentation

Choosing a segmentation platform is a long-term decision.

It shapes how security teams control risk, respond to incidents, and scale protection as environments change. That's why architecture, depth, and experience matter.

Illumio is widely recognized as the industry leader in segmentation.

Illumio Segmentation is the first platform purpose-built to deliver modern segmentation across hybrid, multi-cloud, and on-premises environments. That focus shows up in both the platform's design and its maturity.

Illumio delivers segmentation as a complete platform. It combines deep, real-time visibility into workload communications with distributed enforcement that aligns with Zero Trust principles.

Policies are enforced locally, without introducing privileged access paths or centralized points of failure. The result: segmentation that remains effective during outages, incidents, and infrastructure change.

This approach is why Illumio is trusted across critical industries, global enterprises, and public and private sector organizations.

Segmentation simplified

Smarter segmentation

Illumio Segmentation combines real-time telemetry with AI to recommend policies instantly and accelerate security decision-making.

Works wherever you do

Consistent, automated segmentation for all workloads across clouds, endpoints, and data centers. Segmentation that scales with you.

Zero Trust, built in

Segmentation is a pillar of Zero Trust. Enforce least-privilege access and eliminate implicit trust across your hybrid multi-cloud environment.

Security industry analysts consistently validate Illumio Segmentation leadership. They cite its completeness, scalability, and strength in Zero Trust enforcement:

- Forrester named Illumio a Leader in The Forrester Wave™: Microsegmentation Solutions, Q3 2024
- Gartner named Illumio a Customers' Choice in the 2026 Gartner® Peer Insights™ Voice of the Customer for Network Security Microsegmentation

Customers choose Illumio because it works at enterprise scale and holds up under real-world pressure.

For organizations that need segmentation to work in real environments under real pressure, Illumio offers the most proven and complete foundation for building long-term breach containment.

Security graphs collect detailed information about systems and user behaviors. If not handled carefully, this raises privacy

Try Illumio Segmentation today.

Get started with a free trial.

illumio.com/try-illumio-segmentation