illumio

EBOOK

Simplifying Segmentation

The Missing Layer in a Broken Security Model

Contents

From prevention to resilience: a security reset

If we want resilience, we must abandon the assumptions that got us here.

For years, cybersecurity relied on prevention, trust, and the illusion of a stable perimeter. That world is gone. The threats are faster. The environments are more complex. And the connections we depend on — cloud workloads, SaaS apps, remote users, partner systems — shift by the minute.

Attackers don't smash through walls anymore. They walk through trusted paths, hide in normal traffic, and move laterally long before anyone notices. AI and automation have only widened the gap, giving adversaries more speed, more precision, and more chances to exploit the cracks in our defenses.

The hard truth is this: breaches are inevitable. What happens next is not.

Resilience is now the measure that matters: the ability to absorb an intrusion, contain its reach, and keep the business running even when something goes wrong.

That's why segmentation is so critical. It removes the freedom that attackers rely on. It limits their movement. It turns sprawling, hybrid environments into contained, predictable ones. And it gives security teams control at a moment when control is slipping away.

The old assumptions failed us. Resilience — driven by segmentation — is how we move forward.

The expanding attack surface

The threat landscape will keep evolving with faster automation, deeper supply-chain risks, and attackers who exploit every trusted connection. But the exact nature of the threat matters less than the reality behind it: once attackers get in, they move fast. Segmentation is what stops that movement and keeps a breach from becoming a disaster.

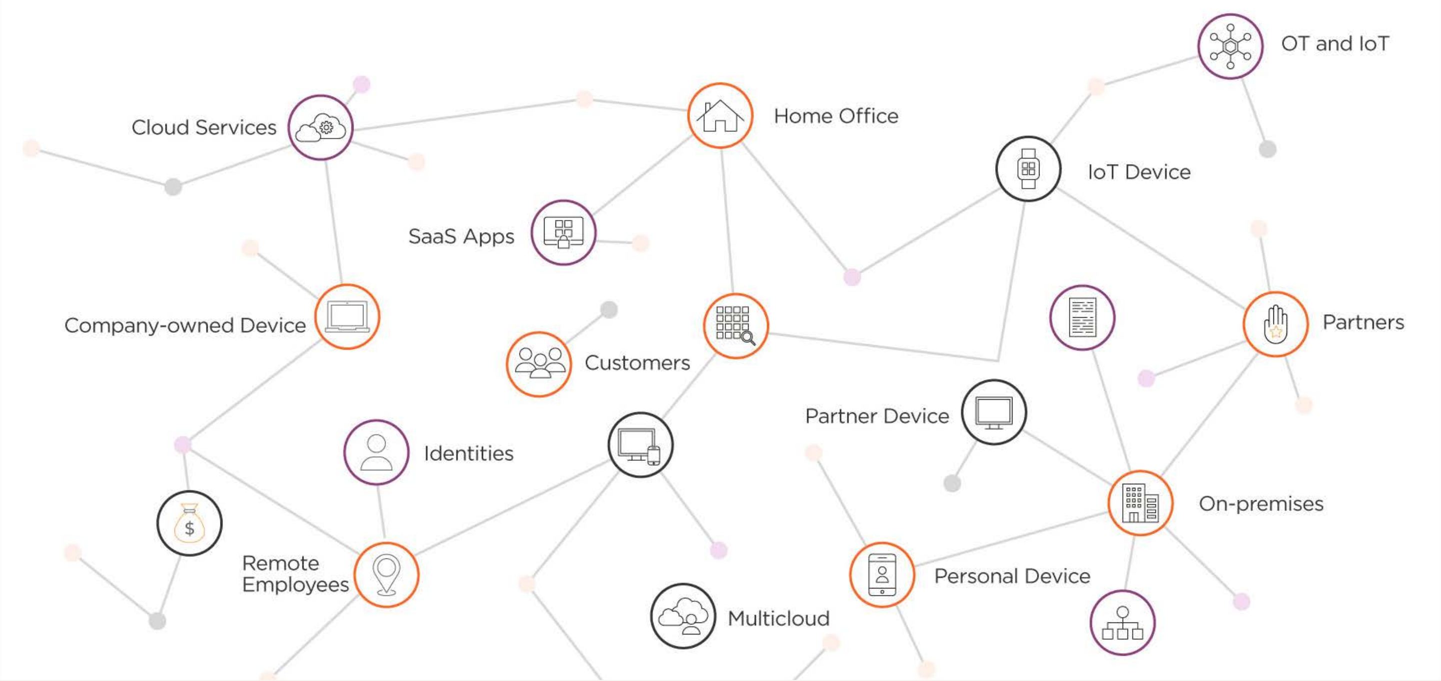


Figure 1: Every connection expands the attack surface — and the paths attackers exploit

All businesses are at risk

Big or small, every organization faces the same reality: attackers move faster than traditional defenses can respond. Breaches keep rising even as security budgets grow. Smaller teams feel this pressure most. Limited staff and aging tools make it hard to keep pace.

The core issue isn't awareness. It's architecture. Defenders need an approach that limits the blast radius of any breach and keeps the business running, no matter its size.

Welcome to the Breach Containment Era

Security today demands a shift: reducing risks and containing threats before they spread. By limiting the reach of breaches, organizations can minimize damage, even in the face of evolving attacks. This requires not just better tools but a fundamental change in strategy.

Resilience starts with Zero Trust. Segmentation makes it real.

Real resilience begins with Zero Trust. This model never assumes safety. It verifies every user, device, and action before granting access — no matter where they originate.

But Zero Trust is more than stronger authentication. To work in practice, it needs a way to limit how far an attacker can move if they break in. That's where segmentation comes in.

Why segmentation matters for Zero Trust

Segmentation divides your environment into controlled zones so attackers can't roam freely. It limits access to only what systems and people need, reducing the impact of any breach. Even if attackers gain a foothold, segmentation stops them from moving laterally and keeps damage contained.

Microsegmentation: the modern approach

Microsegmentation takes this further by creating small, secure compartments across workloads, applications, and cloud environments. Policies adapt to identity, behavior, and context, not broad, static network rules.

If one segment is breached, the rest stay protected. Think of it like a submarine: each watertight compartment isolates damage so the vessel stays afloat (see Figure 2). Microsegmentation works the same way, stopping threats before they can reach critical systems or data.

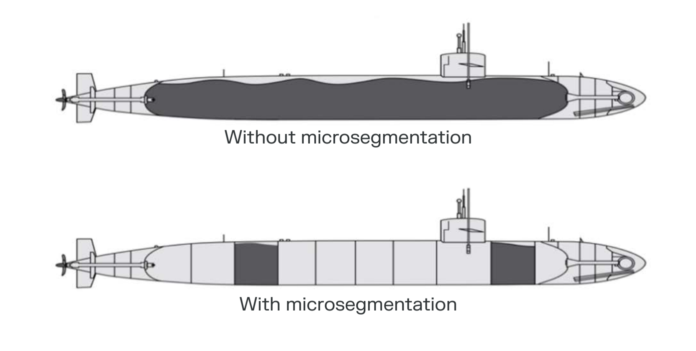


Figure 2: Microsegmentation acts like a submarine's watertight compartments, isolating threats to prevent widespread damage.

What makes this combination essential?

- **Limits the impact of breaches.** Segmentation and microsegmentation block lateral movement, containing attacks before they escalate.
- **Enhances operational resilience.** Even during an incident, critical systems can continue running because threats are isolated.
- **Simplifies regulatory compliance.** Zero Trust and segmentation map cleanly to frameworks like GDPR and DORA, helping teams meet strict requirements.
- **Adapts as threats evolve.** This model scales across on-premises, cloud, and hybrid environments, giving organizations a future-ready foundation.

What modern organizations need to stay secure

Modern environments move fast. Cloud workloads spin up and down. Users connect from anywhere. Applications talk across data centers, clouds, and continents. To stay secure, organizations need controls that can keep pace.

Here's what today's security demands:

- **Visibility everywhere.** You can't protect what you can't see — across on-prem, cloud, and hybrid systems.
- **Adaptive controls.** Policies must follow workloads, users, and applications as they move, not rely on static network boundaries.
- **Containment by default.** If an attacker gets in, the blast radius must stay small. Lateral movement cannot be an option.
- **Consistency across platforms.** One policy model, everywhere — not a different rule set for every cloud or data center.
- **Simple, fast deployment.** Security that takes months to configure isn't security. Teams need quick wins and low operational overhead.
- **Zero Trust alignment.** Modern security must support a "never trust, always verify" model and enforce least privilege at scale.

Why other segmentation methods fall short

When organizations first consider segmentation, they often turn to tools they already know: VLANs, firewalls, or cloud-native controls. But these traditional methods weren't built for today's sprawling, hybrid environments.

VLANs
VLANs rely on physical boundaries and manual configuration. They work well in static, on-premises environments but quickly break down in the cloud. Every change to workloads or network design demands reconfiguration, creating complexity, slowing operations, and leaving room for human error. In fast-moving hybrid infrastructures, VLANs simply can't keep up.

Firewalls
Firewalls are designed for perimeter defense, not internal containment. They protect the edge but offer limited visibility once an attacker gets inside. Managing hundreds of firewall rules across hybrid environments leads to policy sprawl, blind spots, and costly maintenance. And since firewalls lack workload-level context, they can't effectively prevent lateral movement.

Cloud-native security controls
Each cloud provider offers its own security tools, but they're siloed and inconsistent across platforms. That fragmentation makes unified policy enforcement nearly impossible.

What's secure in one cloud might be wide open in another. As a result, organizations end up juggling multiple cloud-native control sets that don't communicate or scale together and alignment is questionable.

Why microsegmentation is different

Unlike traditional tools tied to physical networks or static IPs, microsegmentation uses identity, behavior, and context to control how workloads communicate. It creates a unified security model that works the same way in data centers, clouds, and containerized environments.

This workload-first approach offers far more agility and accuracy, making policies easier to manage and far harder for attackers to bypass.

Top microsegmentation use cases

Microsegmentation applies simple, consistent policies across modern environments to limit risk and stop threats from spreading. These are the top ways teams put it to work.

Asset mapping and visibility
See your assets, workloads, and traffic flows clearly and in real time. This level of visibility helps you improve security policies and cut down on risks across your network.

Cloud workload migration
Keep your workloads secure every step of the way — before, during, and after migration. Use consistent policies to protect hybrid and multi-cloud environments with ease.

Critical asset protection
Protect your most important assets, like customer data and intellectual property, by setting up secure zones. These zones limit access and lower the risk of attacks.

Environmental separation
Keep production, testing, and development environments separate to avoid mixing them, reduce risks, and follow regulations.

Incident response and recovery
When a breach happens, segmentation helps you act fast—stop the spread, isolate affected systems, and recover quickly.

IT/OT convergence
Connect IT and OT securely by protecting important operational systems and reducing weaknesses in critical infrastructure.

Ransomware containment
Stop ransomware in its tracks. By segmenting systems and protecting important assets, you can block its spread and recover faster.

Vulnerability risk reduction
Protect vulnerable systems before attackers can reach them. Isolate these systems and fix security gaps to keep threats away.

From strategy to deployment: your microsegmentation roadmap

Done right, microsegmentation delivers powerful protection. But success doesn't happen by accident. It requires a clear strategy and a structured, step-by-step deployment.

The next two sections outline both. First, we'll explore how to build a strong microsegmentation program. Then we'll explain how to put that program into action across your environment.

Part I: A blueprint for effective microsegmentation

Microsegmentation isn't a one-time fix. It's an ongoing process. Building it well requires the right strategy, the right teams, and the right level of visibility. These best practices help you reduce risk, enforce policies, and contain threats at every stage.

1. GET EXECUTIVE BUY-IN

Microsegmentation succeeds when the business sees it as more than an IT project. You need leadership support to remove roadblocks, secure resources, and make segmentation part of daily operations, not an afterthought.

Overcoming executive skepticism
Executives often hesitate to support microsegmentation because it seems disruptive, complex, or hard to measure. The key is to reframe it as a business enabler, not a technical project. Start by showing the real risks inside your environment: open high-risk ports, unknown traffic flows, and critical systems exposed to lateral movement. Concrete data makes the threat tangible.

Next, highlight quick, low-impact wins like securing core services or ring-fencing a high-value application. Early results build confidence and reduce concerns about downtime. Tie the program to broader priorities — Zero Trust, resilience, cloud readiness, compliance — so leaders see segmentation as part of an existing roadmap, not a new one.

Finally, present a phased, low-risk plan that begins in idle mode and moves to enforcement only after policies are tested. A clear path forward eases skepticism and sets the stage for the cross-team collaboration and visibility work that comes next.

Quantifying the ROI
Show leaders how microsegmentation supports the outcomes they care about most:

- Reducing breach impact
- Improving regulatory alignment
- Protecting revenue-generating systems
- Strengthening business continuity

When executives understand that segmentation is essential for Zero Trust and resilience, they're far more likely to champion it across the organization.

We'll take a closer look at ROI reporting in “Showing the Impact: Measuring and Reporting ROI” (page 14).

2. COLLABORATE ACROSS TEAMS

Segmentation touches every part of the environment, so cross-team alignment is essential. Engage application owners, network teams, SOC analysts, and platform engineers early.

Shared results
This collaboration ensures:

- Policies match how applications actually work
- Deployments avoid downtime
- Changes move smoothly through development, testing, and production
- Security teams don't operate in a silo

When teams design policies together, friction decreases, and deployment speeds up.

Breaking down silos
Segmentation choices ripple through every layer of the environment. That means teams with different goals need a shared understanding of what success looks like. Start by aligning on the business outcomes — stronger resilience, fewer blind spots, and reduced lateral movement — rather than on technical details. This gives security, networking, and application teams a common target.

Hold short, focused working sessions where teams review real traffic flows together. Seeing actual dependencies builds trust and reduces friction. That's especially true when policy decisions affect application performance. Create clear owners for each step — discovery, testing, enforcement — so responsibilities don't blur or stall.

And by all means, avoid top-down mandates. Instead, bring teams into the design process early. Show how segmentation protects their systems, reduces firefighting, and cuts operational risk. When each group sees its role in the outcome, collaboration becomes easier, and deployment moves faster.

3. FIND YOUR BLIND SPOTS AND REDUCE RISK

You can't protect what you can't see — and most organizations have more blind spots than they realize. Use deep visibility to uncover hidden dependencies, risky services, and unnecessary pathways that attackers can use for lateral movement.

Key steps:

- **Map real-time traffic**. Use AI tools to detect blind spots and weak links.
- **Identify and close high-risk ports**. Lock down commonly exploited services such as RDP and SMB.
- **Block unnecessary connections**. Stop lateral movement early to shrink the attack surface.
- **Enforce security policies**. Apply least-privilege access to workloads and services automatically.
- **Audit and block unneeded traffic**. Retire old health checks, unused services, and forgotten dependencies.

4. DETERMINE CORE SERVICES THAT NEED TO BE PROTECTED

Some services are the backbone of your environment, and attackers know it. DNS, NTP, and LDAP are high-value targets because compromising them provides broad access and operational disruption:

- **Directory and identity systems**. These help enforce Zero Trust and must be protected from lateral movement.
- **Time and name resolution services**. Attackers can hijack these to redirect traffic or mask malicious activity.

Locking down core services prevents attackers from using them as stepping stones deeper into your environment.

5. PRIORITIZE CRITICAL APPLICATIONS

Not all assets carry the same risk. High-value applications — payment systems, customer databases, healthcare platforms, industrial control systems — deserve extra protection.
Good ring-fencing delivers:

- Stronger protection against ransomware and targeted intrusions
- Reduced access to sensitive data
- Clearer compliance boundaries for audits and regulators

Start by identifying the applications that would cause the greatest damage if compromised. They could be tied to revenue, customer trust, safety, or regulatory exposure.

Work with application owners to map dependencies, understand business impact, and surface any hidden connections that need protection. Prioritize apps based on a mix of factors. How sensitive is the data? How essential is the service to daily operations? How often is it targeted? And how much downtime can the business tolerate?

Once identified, ringfence the applications with strict access controls, workload-level visibility, and clear deny rules. This keeps your most valuable systems safe — even when the rest of the environment changes.

6. DECIDE WHICH ENVIRONMENTS SHOULD BE SEPARATED

Different environments serve different purposes — and mixing them increases risk.

Segmentation keeps production, testing, and development separate so misconfigurations, experiments, or unvetted code never spill into live systems. To get this right, map the flow of each environment and understand how teams use them day to day.

Dev/Test → Prod separation
Keep development and testing environments isolated from production. This prevents unfinished code, debug tools, or permissive access settings from affecting critical systems. Even a small mistake in dev can cause major disruption if the environments overlap.

Compliance-driven zones
Create dedicated segments for regulated workloads (PCI, HIPAA, FedRAMP, etc.). This reduces audit scope, simplifies assessments, and lowers the cost and effort required to stay compliant.

IT/OT
Operational technology systems often can't tolerate downtime or patching windows. Keeping them isolated from IT environments reduces the chance that an IT-borne threat jumps into industrial networks.

Cloud environment boundaries
Segment between cloud accounts, VPCs, subscriptions, and regions. Treat each as its own trust zone and avoid relying on cloud-native defaults alone.

7. OUTLINE A PHASED APPROACH

A phased rollout lowers risk and keeps your environment stable. Microsegmentation changes how workloads communicate; so enforcing policies too quickly can disrupt applications or critical services. Starting small gives you the chance to observe real behavior, validate assumptions, and adjust policies before they affect production.

We'll cover the specifics in "Part II: Bringing your blueprint to life" (page 10), but here is a high-level view.

Begin in idle mode
Watch traffic without blocking anything. This creates an accurate picture of how applications interact and prevents surprises. Idle mode is where you uncover undocumented dependencies, legacy services, and unexpected connections.

Test policies in controlled groups
Move a small set of applications or workloads into a test segment. Validate that performance stays stable and workflows continue to function. This is also where teams catch rules that look good on paper but don't match real-world behavior.

Enforce gradually
Transition workloads into enforcement one group at a time. Start with low-risk applications to build confidence, then move up to critical workloads as visibility improves. Each successful wave builds trust across teams.

Review after each phase
Use what you learn — missed dependencies, outdated rules, excessive permissions — to refine policies for the next group. This prevents old mistakes from repeating as deployment scales.

8. USE LABELS AND AUTOMATION TO MAP YOUR ENVIRONMENT

Labels and automation make microsegmentation easier to scale. Instead of managing policies workload by workload, labels let you group systems by what they do — their function, location, environment, or sensitivity. This creates policies that follow workloads automatically, even as they move across clouds or change over time.

Group by role and purpose
Label workloads based on what they support — web, app, database, identity, payments. This ensures policies reflect real application architecture, not IP addresses.

Include environment and location context
Add labels for dev, test, and prod environments, along with region, cloud account, or data center. This keeps boundaries clear and prevents accidental crossover.

Map sensitivity and risk
Use labels to identify critical assets, regulated workloads, or high-risk systems. This makes it easy to apply stronger controls where they're needed most.

Part II: Bringing your blueprint to life

You now have the blueprint. The next step is putting it into action.

Microsegmentation has a reputation for being slow and complex. In reality, today's tools make it far easier. AI speeds up discovery, labeling, and risk analysis. At the same time, modern interfaces simplify policy design.

With a gradual rollout, teams can strengthen security without causing downtime. A phased, step-by-step approach keeps the transition smooth and reduces the impact on your environment.

PHASE 1: INITIAL SETUP

A strong deployment starts with simple preparation. This phase helps you install the platform, align your teams, and get your environment ready for visibility.

Deploy and configure the system in idle mode
Start by installing the platform and running it in idle or visibility-only mode. This lets you see real traffic flows without blocking anything. Idle mode also helps you find hidden dependencies, legacy services, and unexpected connections before you start enforcing rules.

Add operational tools and prepare your infrastructure for a smooth deployment
Connect the platform to the systems you already use. These include identity providers, CMDBs, cloud accounts, logging tools, and asset inventories. Make sure that:

- Agents or sensors are deployed where needed
- Firewall rules allow the right communication
- Service accounts have the right permissions

Laying this groundwork early keeps the rest of the rollout smooth.

Provide training on the use of assessment and configuration tools
Give teams hands-on time with the tools they will use most. Show them how to review traffic, read dependency maps, and preview policy changes. Walk through visibility dashboards, labeling workflows, and rule validation. This early training builds confidence and reduces mistakes once enforcement begins.

PHASE 2: DISCOVERY

The discovery phase gives you a full picture of your environment before you enforce any rules. It helps you understand what you have, how it communicates, and where the biggest risks live.

Find every asset
Start by discovering all network assets across on-premises systems, clouds, and containers. A complete inventory prevents blind spots and ensures nothing is left unmanaged.

Bring in data from supporting tools
Integrate information from CMDBs, vulnerability scanners, and asset inventories. This adds important context — such as ownership, patch status, and risk level — that will shape your segmentation plan.

Use auto-labeling to create a structured map
Run auto-labeling to group workloads by role, environment, location, and sensitivity. Labels create a clear structure and make it easier to design accurate policies later.

Map connectivity across your hybrid environment
Review how applications and services actually talk to one another. This reveals real traffic flows, hidden dependencies, and legacy paths that may need cleanup.

Use AI to identify high-risk ports
Use AI assistance to highlight ports and services that attackers commonly target. This helps you spot weak points early and decide where to focus your first segmentation efforts.

PHASE 3: SEGMENTATION

This phase turns your visibility and mapping work into real protection. The goal is simple: limit how far an attacker can move by controlling how workloads communicate.

Block high-risk and unused ports
Close ports and services that attackers commonly target, such as RDP, SMB, Telnet, and outdated protocols. Remove unused ports to shrink your attack surface and reduce unnecessary exposure.

Implement environmental separation
Keep development, testing, and production apart. Clear boundaries prevent accidental crossover, reduce misconfigurations, and keep changes in one environment from affecting another.

Secure core services
Protect DNS, NTP, LDAP, and identity systems. These services support everything else in your environment, so restricting access to them cuts off key paths for lateral movement.

Segment critical assets into individual protect surfaces
Identify high-value applications — payment systems, databases, healthcare systems, OT controllers — and isolate them behind strict policies. This limits access to only what each system needs and prevents attackers from reaching sensitive data.

Separate other environments
Create segmentation boundaries for cloud accounts, VPCs, regions, data centers, and container platforms. Treat each as its own trust zone so risk stays contained even as the environment grows.

PHASE 4: INTEGRATION

In this phase, you connect segmentation with the rest of your security ecosystem. These integrations strengthen detection, speed up response, and add the context you need for accurate policies.

Configure connections to SIEM and SOAR systems
Send segmentation events, alerts, and policy changes to your SIEM or SOAR. This gives your security teams better visibility and allows automated playbooks to respond faster when something looks suspicious.

Enable status exchange with your ZTNA system
Connect segmentation with your Zero Trust Network Access tools. Sharing status information helps ensure that access decisions reflect what is happening on the workload itself, not just the user.

Import data from your vulnerability scanner
Bring in scanner results to add risk context. This helps you see which workloads are vulnerable, misconfigured, or running outdated software — and lets you focus segmentation controls where they matter most.

Import data from an OT asset scanner
For environments with operational technology, connect an OT asset scanner. This identifies sensitive controllers, sensors, and industrial systems so you can protect them with stronger policies and keep IT threats from spreading into OT networks.

PHASE 5: VALIDATION

Once your initial policies are in place, you need to confirm that they match how your applications actually work.

Accurate policies depend on real traffic, not assumptions, old documentation, or guesswork. Validating traffic before enforcement prevents outages, avoids breaking application flows, and helps teams trust the process. It also uncovers hidden dependencies that could create blind spots or open the door to lateral movement.

Ports and protocols
Verify which ports are actually in use. Many applications do not match vendor documentation, and old dependencies linger long after they're needed. Traffic validation helps remove outdated or overly permissive rules.

Application dependencies
Look for unexpected east–west connections between services. These often reveal hardcoded IPs, legacy batch jobs, scheduled tasks, or unapproved data transfers.

Service behavior over time
Review traffic patterns across multiple business cycles. Some dependencies only appear during end-of-month jobs, patch windows, backups, or peak demand.

Environment crossover
Confirm that dev/test workloads aren't quietly calling production services. It's a common issue that creates unnecessary exposure and makes troubleshooting harder.

How to validate effectively
Validating real traffic helps you build accurate, least-privilege policies. It reduces risk, prevents surprises, and keeps segmentation from disrupting critical systems.

Here's how to do it well:

- Use observed traffic as the source of truth. Compare expected flows to real flows and close anything that isn't required.
- Partner with application owners. Validate findings with the people who run the apps to avoid accidental disruption.
- Simulate policies before enforcing them. Use "what if" analysis or preview modes to catch issues early.
- Iterate. Treat validation as an ongoing process, not a single event. Environments evolve, and policies should evolve with them.

PHASE 6: MONITORING

Once enforcement is in place, you need to make sure segmentation continues to work as your environment changes. Continuous monitoring helps you spot issues early, understand new patterns in your systems, and respond before threats spread.

Real-time reporting turns segmentation from a static control into a dynamic defense that adapts as your infrastructure evolves.

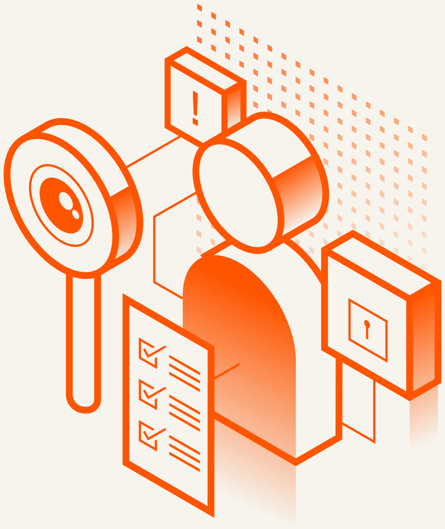
Use data from your SIEM and SOAR tools
Send segmentation events and alerts into your existing security workflow. Automation speeds detection and response, reducing the time attackers have to move.

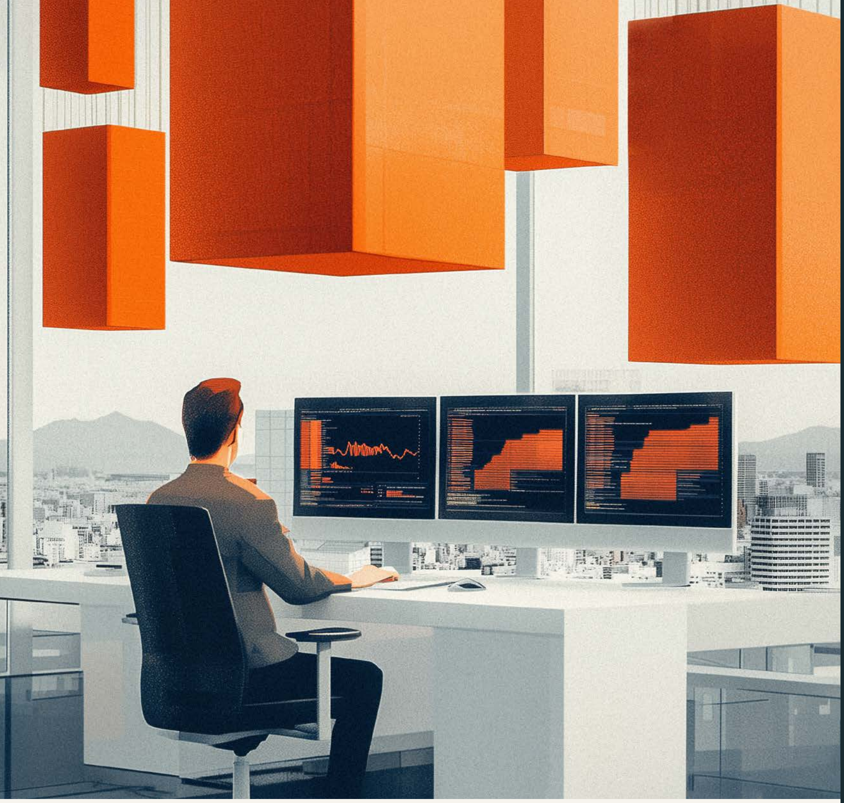
Identify unusual traffic patterns
Look for sudden spikes in east–west traffic or unexpected connections between workloads. These patterns often signal lateral movement.

Detect anomalous connections
Watch for unauthorized access attempts, especially toward identity systems or high-value apps. Connections from unfamiliar sources or attempts to bypass policies are strong signs of intrusion.

Use real-time risk insights
Combine segmentation data with asset and vulnerability details to see where your exposure is highest. Use these insights to find misconfigurations, risky services, or workloads behaving outside their normal patterns.

Enable automated alerts
Set alerts for new communication paths, traffic to protected assets, or activity that crosses environment boundaries. Automated notifications help teams respond before problems grow.





PHASE 7 (AND BEYOND): REFINEMENT

After enforcement begins, your policies need to evolve with your environment. Microsegmentation gets stronger over time as you learn how applications behave and how traffic flows change.

A refine-as-you-go approach prevents overly restrictive policies, reduces disruption, and creates steady progress toward least-privilege access. Most important, it keeps your controls aligned with the business as it grows and changes.

Start broad to keep systems stable. Then narrow access as confidence grows and your understanding deepens.

Tighten access gradually
Begin with permissive rules to keep systems stable. As you learn which connections are required, restrict unnecessary pathways and lock down sensitive workloads.

Validate policies under real conditions
Test during peak hours, batch jobs, and maintenance windows. This reveals dependencies that appear only under stress — and prevents issues later.

Adapt to change
Applications evolve, teams re-architect systems, and cloud environments shift. Review policies on a regular basis to ensure they still match how the environment works today, not how it worked six months ago.

Use feedback loops
Build a cadence with application owners and operations teams. Review proposed changes, unexpected traffic, and new dependencies together to keep policies accurate.

Professional services: when to bring in the experts

Professional services can accelerate your microsegmentation journey and help you avoid missteps. You may not need them for every deployment. But the right partners at the right moments can make a major difference.

When a professional services partner can add real value:

When you need dedicated support
Bring in experts if your team is stretched thin or if you want to move faster without risking downtime. They can help set up the platform, validate early decisions, and keep the rollout smooth.

When you want a trusted advisor
If you're unsure how to prioritize applications, handle dependencies, or map protect surfaces, a services partner can guide the process. Their experience helps you avoid common pitfalls.

When strategy matters as much as execution
Use professional services when you need high-level planning — such as aligning segmentation with Zero Trust, preparing for audits, or designing a long-term roadmap that fits your business goals.

When proven expertise reduces risk
Complex environments, legacy systems, and hybrid architectures can introduce hidden challenges. Professional services provide best practices, hands-on coaching, and battle-tested methods that keep your deployment safe and predictable.

Showing the impact: measuring and reporting ROI

Once segmentation is planned and underway, leaders want to know what it delivers. ROI helps answer that. It shows the financial return on your security investment, reduces uncertainty, and helps teams make smarter budget decisions.

The formula is simple:

ROI = (Total Benefits – Investments) / Investments or ROI = Net Benefits / Investments

A clear ROI case helps:

- **Justify spending**. Show the financial return on security investments.
- **Compare options**. Evaluate different solutions to choose the best one.
- **Prioritize resources**. Focus budgets where they deliver the most impact.
- **Inform decisions**. Equip leaders with data to drive smarter choices.

But ROI is just part of the story. When combined with a broader Zero Trust strategy, the impact of microsegmentation grows. It doesn't just save money. It reduces breach costs, prevents regulatory fines, and minimizes downtime. The result? A more secure, resilient business with measurable financial gains.

Segmentation adds value in several clear ways, starting with the following core benefits.

Cost savings

Downtime is expensive. A breach can shut down systems, halt productivity, and force IT teams into emergency mode. Every minute spent containing an attack drains resources. Segmentation limits the blast radius of a breach, keeping disruptions small and short-lived. The outcome? Lower costs, fewer interruptions, and long-term savings.

Risk reduction

Segmentation is security at its core. It blocks attackers by restricting their access. But the benefits go beyond that. Strong segmentation also protects against:

- Fines and other penalties
- Lawsuits
- Reputational damage

By limiting exposure, organizations safeguard their operations, data, and revenue.

Operational efficiency

Clear security boundaries make IT environments easier to manage. Instead of navigating a complex, high-risk network, IT teams get control. Segmentation helps:

- Respond to incidents faster
- Optimize resources
- Scale infrastructure without added risk

In a fast-moving world, segmentation improves agility, helping teams stay ahead of threats and work more efficiently.

Quantifying the benefits

How do you measure segmentation's impact? Break it down into three key categories:

- **Direct costs**. Security tools, infrastructure, and labor.
- **Indirect costs**. Hidden inefficiencies like delays and admin burdens.
- **Risk exposure**. Financial risks from compliance issues and breaches.

Assigning dollar values — based on your own data or industry benchmarks — helps build a strong business case for segmentation.

Showcase your wins

Security is a journey. Track and celebrate improvements such as faster response times, fewer vulnerabilities, and stronger resilience. Highlighting progress keeps teams motivated and supports ongoing investment.

ebay

Lessons from a digital giant: how eBay does segmentation

eBay's microsegmentation strategy flipped the script on traditional security, moving the online e-commerce giant from a reactive "whack-a-mole" game to proactive control.

It all starts with visibility. Real-time traffic mapping exposes hidden risks, unneeded communication paths, and misconfigurations. This sets the stage for better decisions.

The company used a step-by-step approach to roll out microsegmentation. It began in observation mode, slowly enforced policies, and built confidence without causing disruptions.

Automation and dynamic labeling are key to making this work. Workloads are grouped by role and app so that policies adjust as the environment changes. Blocking outdated or unused traffic, like old health checks, reduces clutter, and strengthens defenses. Teams across security, networking, and app development work together to align goals and ensure a smooth process.

Critical systems, like DNS and domain controllers, are protected first. By segmenting these critical assets, eBay can stop breaches and safeguard the core of its operations. Regular refinements and proactive reporting help catch anomalies early to stay ahead of threats.

For eBay, it's more than segmentation. It's a masterclass in modern, scalable security.

Read the customer story **here**.

Next steps

Microsegmentation is no longer a complex, high-risk project. With the right strategy, clear visibility, and a phased rollout, it becomes a practical way to strengthen resilience and contain threats before they spread. Every step — from discovery to refinement — helps reduce your attack surface and give your security teams more control.

If you're ready to turn segmentation into a core part of your Zero Trust strategy, Illumio Segmentation makes it faster, safer, and easier to deploy at scale.

Learn how Illumio can help you contain threats and protect what matters most.

Learn more at:
illumio.com/illumio-segmentation.