ZERO. Networks

BUYER'S GUIDE

The Law Firm Buyer's Guide for Evaluating Microsegmentation Solutions

Table of Contents

3 Introduction

5 Challenges with Legacy Microsegmentation for Law Firms

7 Key Differentiators of Modern Microsegmentation

10 Checklist: What to Look for When Selecting a Microsegmentation Solution for Your Law Firm

12 About Zero: Simple to Deploy, Powerful in Action

Research Note:

The data in this buyer's guide cited from ViB Tech is exclusive information from a ViB Tech survey of information technology and cybersecurity professionals, primarily from North America.

Read the full, all-industry report here »

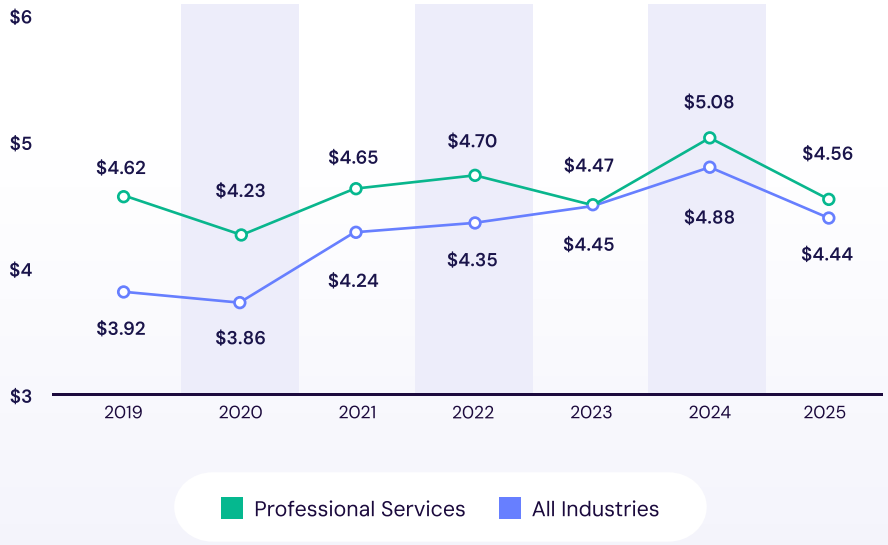
ZERO. Networks

Introduction

While network security has become a strategic imperative across all industries, law firms face uniquely interconnected pressures: escalating cyber threats, heightened regulatory and underwriter scrutiny, and uncompromising client expectations. While the global average cost of a data breach in the professional services sector – a category encompassing law firms – dipped to $4.56 million in 2025, it still exceeds the cross-industry average by more than $100,000.[1] What's more, the average cost of a data breach for the U.S. hit a record high of $10.22 million, driven in part by an accelerating trend of higher regulatory fines. Meanwhile, more than half of law firm clients say they have concerns about cybersecurity breaches; nearly 40% would consider firing a firm following a breach.[2]

Global average total cost of a data breach

Measured in USD millions. IBM, Cost of a Data Breach Report 2019, 2021, 2022, 2024, and 2025



Law firms maintain access to sensitive client data – and attackers know it. An uptick in ransomware attacks targeting law firms led the FBI to issue an alert in 2025 urging more robust identity-based controls.[3] These threats are amplified by the industry's reliance on outsourced IT services – 8 in 10 law firms outsource some or all of their IT management, making it easier for attackers to carry out targeted social engineering campaigns and exploit third-party access vulnerabilities.[4]

As law firms navigate an evolving risk landscape, a new era of compliance is taking shape, too. Nearly 90% of law firms currently have cybersecurity insurance, but they report rising premiums and increasingly stringent requirements.[5] This comes alongside a patchwork of data protection laws, state bar rules, industry risk assessments and audits, and ABA Model rules – all of which mandate robust security strategies. Complying with every cybersecurity requirement individually isn't only impractical, it also fails to deliver the comprehensive protection clients need for true peace of mind.

1 IBM, Cost of a Data Breach Report 2025
2 Integris, Law Firm Cybersecurity Report 2025
3 FBI Notification, Silent Ransomware Group Targeting Law Firms, April 2025
4 Tabush Group, 2024 Law Firm Survey
5 Tabush Group, 2024 Law Firm Survey

It's time for law firms to embrace a more comprehensive approach to cybersecurity – instantly containing every threat so attacks never turn into reputational disasters or operational disruptions.

Fortunately, security teams understand the urgent need to evolve their strategies – cybersecurity ranks as law firms' #1 IT priority.[6] And rather than relying on the same old network security measures, legal industry cyber professionals are turning to strategies that immediately thwart ransomware, mitigate identity-based attacks, and safeguard critical systems and data.

Ninety percent of security leaders are turning to Zero Trust to improve their organization's overall security posture, with 75% of them using the 7 Pillar Zero Trust Model as their guide map.[7] And, as ransomware attacks double,[8] microsegmentation has been hailed by MITRE, Gartner, the NSA, Dark Reading, Forbes, and CSO Online as the most promising solution for building a cyber resilient architecture that blocks ransomware, halts lateral movement, and satisfies zero trust guidelines.

Security leaders are embracing Zero Trust

90% consider Zero Trust very important or extremely important for improving overall security posture.

75% say the 7-pillar Zero Trust model suggested by the NSA is largely optimal for realizing Zero Trust security outcomes.

ViB Survey of IT & Security Professionals: The Role of Network Segmentation in Zero Trust Architectures

Unlike traditional network segmentation strategies – which involve dividing a large network into smaller subnetworks, or segments – microsegmentation is a much more granular and robust process of isolating all clients, workloads, applications, virtual machines, and operating systems into isolated segments with individual security perimeters. The microsegmentation market itself is projected to grow from $8.17 billion in 2025 to $41.24 billion by 2034, indicating a significant shift towards more effective solutions that address these challenges.[9]

According to data from *The Role of Network Segmentation in Zero Trust Architecture: A Survey of IT & Security Professionals* by ViB Tech, 92% of security leaders said ransomware was a top three cybersecurity concern. As a result, 95% say microsegmentation is key to cyber defense.[10] However, only 5% of those surveyed who have implemented traditional microsegmentation are satisfied with their results.[11]

Why? Because legacy microsegmentation solutions require lengthy, complex, and costly implementations – involving time-intensive, ongoing tasks such as manual labeling, tagging, and grouping – that still leave chunks of the network exposed.

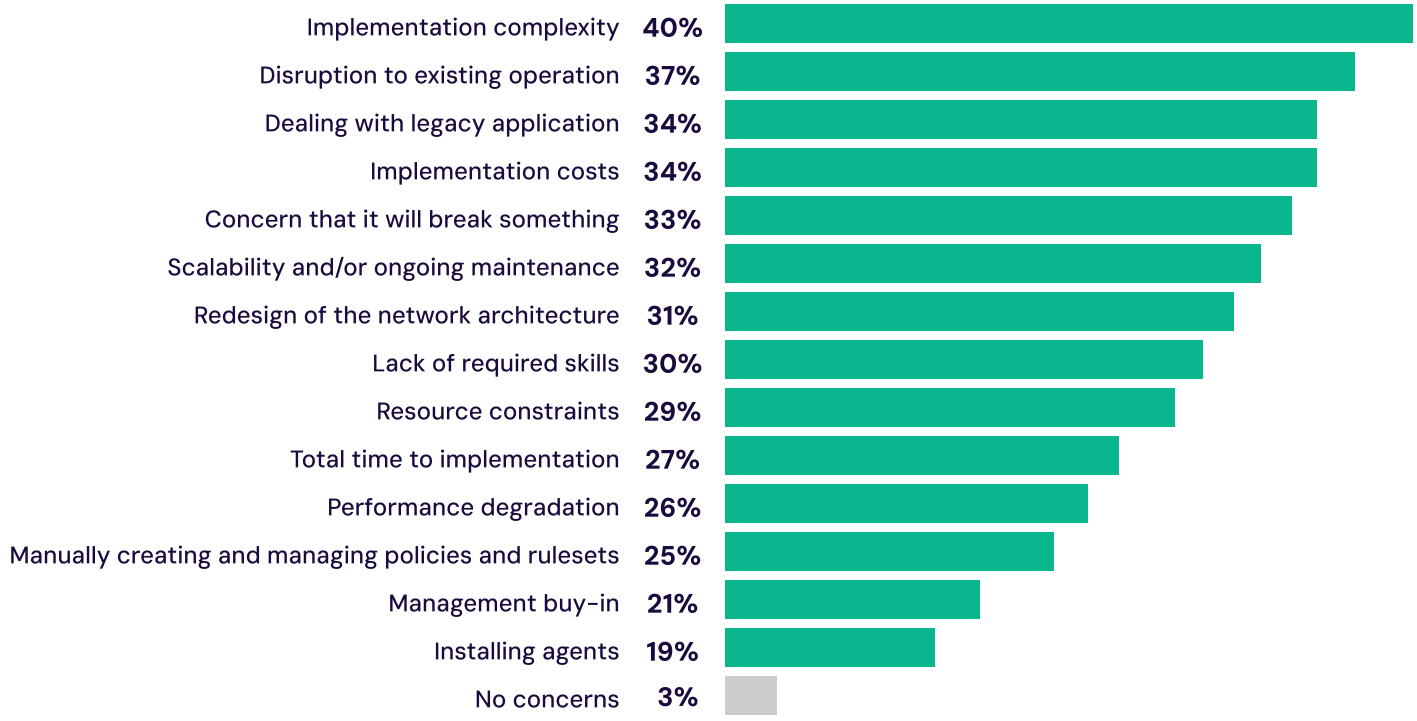
6 Tabush Group, 2024 Law Firm Survey
7 ViB Tech, The Role of Network Segmentation in Zero Trust Architectures
8 Vanson Bourne, The State of Microsegmentation 2023
9 Exactitude Consultancy, Microsegmentation Market Outlook 2025-2034
10 Enterprise Management Associates, The Maturing Microsegmentation Market
11 ViB Tech, The Role of Network Segmentation in Zero Trust Architectures

Challenges with Legacy Microsegmentation for Law Firms

Traditionally, microsegmentation implementations have been complex, resource-intensive, and disruptive.

Legacy microsegmentation solutions are often complex to deploy, difficult to scale, and disruptive to business operations. These implementations typically demand extensive manual configuration, straining internal resources, and delaying time-to-value. For law firms with limited IT staff bandwidth, the manual effort alone makes legacy microsegmentation a non-viable option, despite understanding the value of comprehensive network segmentation. When asked about key concerns with implementing microsegmentation, 40% of security leaders pointed to implementation complexity followed by disruption to existing operations (37%) and dealing with legacy applications (34%).[12]

Key concerns about implementing microsegmentation



ViB Survey of IT & Security Professionals: The Role of Network Segmentation in Zero Trust Architectures

Additionally, maintaining legacy systems can be resource-heavy, as they may not integrate well with modern security protocols, leading to inefficiencies and potential performance declines.[1]

12 ViB Tech, The Role of Network Segmentation in Zero Trust Architectures
13 Exactitude Consultancy, Microsegmentation Market Outlook 2025-2034
14 Brightflag, Hourly Rates in Am Law 100 Firms

Operational downtime transcends lost billable hours

The fear of operational downtime during microsegmentation implementation poses a significant concern as reconfiguring network architectures and security policies can disrupt operations if not managed carefully. In the legal sector, operational disruptions most directly translate to lost billable hours – just one hour of downtime could spell hundreds of thousands in lost billable hours for top law firms.[14] With this context, it's little wonder why law firms are concerned about embracing complex and potentially disruptive microsegmentation implementations.

While the financial impact of downtime is staggering, these disruptions can have consequences in law firms that extend well beyond cost. Reputational threats resulting from operational disruptions looms large as law firm clients expect precision, transparency, and availability. And in time-sensitive contexts, legal teams can't afford to accept inaccessible systems or data.

To stay competitive and resilient, law firms need solutions that align with uptime requirements, minimize performance impact, and protect critical infrastructure – without impacting business operations.

Law firms face considerably complex implementations with legacy tech stacks

Integrating with legacy systems poses challenges, and the granular nature of microsegmentation increases the risk of misconfigurations that could block legitimate traffic and cause service interruptions. Many law firms still rely on outdated or disconnected systems; even as the average law firm increases technology spending by nearly 10%, persistent security gaps remain uncovered, with investments primarily geared toward AI-enabled efficiency tools.[15]

To overcome the challenge of implementing microsegmentation in an environment marked by significant legacy tech, organizations often adopt a phased implementation approach, starting with non-critical segments and investing in thorough testing and monitoring to minimize disruptions. Though this approach can safeguard operations, the extended timeline inherent in phased implementation means parts of the network remain exposed longer, thereby compounding the risk of vulnerabilities over time. For law firms already facing accelerated cyberattacks, that prolonged risk exposure can spell disaster.

Even after implementation, there are hurdles: ongoing management, scalability roadblocks, and more

Complex, Manual Policy Management

Creating and maintaining asset tags and granular security policies can be time-consuming and prone to errors. As the number of microsegments increases, updating policies becomes increasingly complex, raising the risk of misconfigurations that could disrupt operations or create security vulnerabilities.

Scalability Challenges

Manual approaches often struggle to keep pace with organizational growth and network complexity. The sheer volume of policies can overwhelm administrators, making it difficult to adapt to rapid changes in network topology or application deployments.

Drain on Resources

Manually maintaining policies demands significant resources, increasing operational costs and creating bottlenecks in implementing necessary changes.

Risk of Human Error

The complexity of managing numerous policies raises the likelihood of mistakes, which can create security gaps or unintended access restrictions.

Lack of Agility

Manual processes can hinder quick responses to changing business needs, resulting in outdated policies and heightening law firms' existing reluctance to make necessary updates.

To mitigate these issues, organizations are increasingly adopting automated solutions to streamline policy management and enhance scalability.

15 Thomson Reuters, 2026 Report on the State of the US Legal Market

Key Differentiators of Modern Microsegmentation

Resilient network architecture that enables operational continuity is essential for law firms seeking to enhance their cybersecurity posture. By leveraging modern microsegmentation, businesses can create secure micro-perimeters around every asset, significantly reducing the attack surface and containing threats. Additionally, the implementation of just-in-time access and automated policy management ensures rapid incident response and third-party risk management – even for law firms managing environments heavy with legacy technology – ultimately fortifying defenses against cyber incidents while maintaining seamless operations.

Resilient network architecture that enables operational continuity

Modern microsegmentation is a key strategy for enhancing an organization's ability to withstand, respond to, and recover from cyber incidents – without the disruption of legacy implementations. Here's how:

Contain Threats Immediately: Microsegmentation creates isolated security zones around critical assets. This greatly reduces the blast radius of an attack by blocking lateral movement and preventing ransomware.

Enable MFA, Reduce Your Attack Surface: Modern microsegmentation should include a just-in-time MFA component. Applying MFA at the port level allows organizations to extend MFA protection to a wide range of assets, including clients, servers, legacy applications, databases, and OT/IoT devices that were previously difficult to secure. This approach not only prevents lateral movement when credentials are compromised but also reduces the attack surface by limiting access points and securing privileged ports and protocols.

Rapid Threat Response: A modern microsegmentation solution should offer rapid incident response, capable of thwarting attacks within 24 hours while maintaining network operations. For example, at Zero, our platform learns 90% of network activities in 24 hours, creating and applying security policies to host-based firewalls and implementing MFA for remote admin protocols.

Seamless Integration: Law firms managing complex, hybrid environments can easily secure sprawling infrastructures – including legacy tech – with modern microsegmentation solutions that integrate effortlessly with existing systems, mitigating the risk of downtime and leaving typical network usage patterns unaffected.

CASE STUDY

CRAVATH

CRAVATH, SWAINE & MOORE LLP

See how Cravath, Swaine & Moore LLP, evolved beyond firewalls and admin account tiering to build a layered, dynamic defense, shifting the law firm from reactive security to a prevent-and-protect model.



Fast-tracking compliance and insurance requirements

Modern microsegmentation solutions offer a game-changing approach to network security with their rapid deployment capabilities, segmenting over 90% of networks within 90 days and delivering immediate "day 2" benefits. Law firms can quickly enhance their security posture, streamline GDPR, CCPA, and CPRA compliance, meet ABA Model and State Bar Rules, significantly improve audit scores, and consistently pass penetration tests. Moreover, these solutions provide an accelerated path to satisfying cyber insurance requirements – now, and in the future.

Nearly 90% of law firms have cyber insurance today; 75% of organizations now assess segmentation posture during underwriting, offering lower premiums to organizations with higher segmentation maturity. [16] [17] As demands evolve, modern microsegmentation streamlines compliance today while positioning law firms to seamlessly target changing regulatory requirements – without straining resources.

As regulatory demands evolve and insurance requirements grow stricter, legal organizations can fortify their defenses and easily demonstrate robust security practices to auditors and clients alike by implementing modern microsegmentation. Here's how modern microsegmentation fast-tracks compliance and insurance requirements:

Compliance-Ready Architecture

- Streamlines alignment with multiple regulatory requirements
- Allows organizations to quickly adapt to various regulatory frameworks
- Helps improve security scores and overall security posture in a short timeframe

Comprehensive Coverage

- Segments all assets, including IT and OT systems, both on-premises and in the cloud
- Creates secure micro-perimeters around individual workloads, applications, and data
- Addresses compliance requirements across diverse environments

Enhanced Visibility and Control

- Provides detailed insights into network traffic patterns and asset communication
- Enables quick detection of anomalies and potential threats
- Supports compliance requirements for monitoring and reporting

Continuous Compliance Maintenance

- Provides ongoing monitoring and adjustment of security policies
- Helps manufacturing organizations maintain compliance over time, not just during initial implementation

Automated Policy Creation

- Learns network behavior and automatically generates security policies within the implementation period
- Continuously refines and adapts policies to ever-growing and changing networks – incorporating and protecting new assets and removing decommissioned ones
- Reduces human error and the need for manual policy creation and management
- Ensures policies align with compliance requirements from the start

Regulations, Industry Standards, and Insurance Requirements

ABA Model Rule 1.6(c)

A lawyer shall make reasonable efforts to prevent the inadvertant or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client

Data Protection Laws

CCPA and CRPA, GDPR, New York SHIELD Act, Massachusetts 201 CMR 17.00

Risk Assessments, Audits & Standards

NIST CSF, ISO/IEC 27001, NIST 800-207

Cyber Insurance Requirements

MFA, Network Segmentation, Least Privilege Access, Incident Response Plan, Third-Party Access Control

State Bar Rules

Rules on competence and confidentiality plus recent opinions (Florida) emphasize the importance of cybersecurity

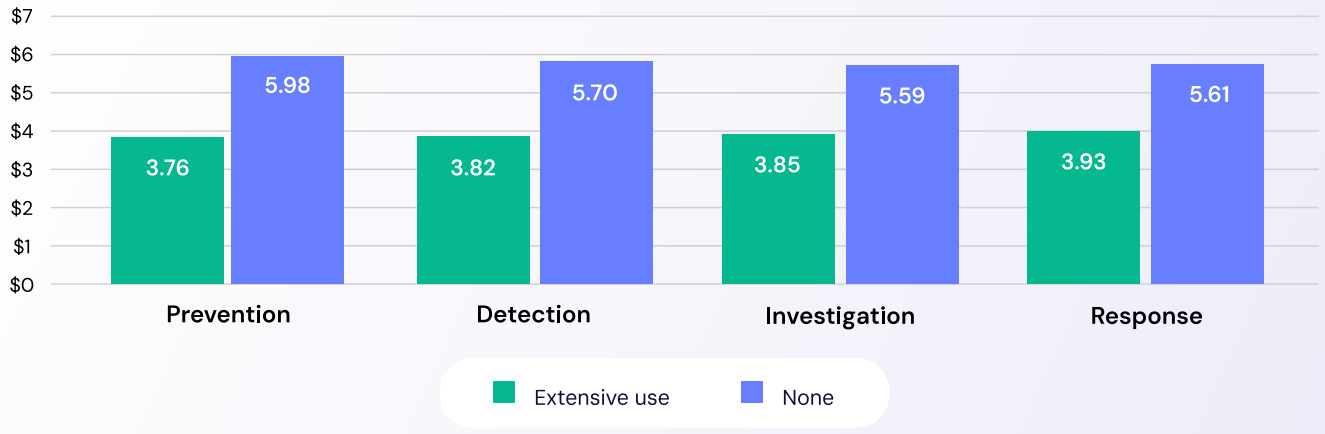
16 Tabush Group, 2024 Law Firm Survey
17 Segmentation Impact Study 2025

Automation: Cut down on implementation timelines and manual work, ongoing management costs, and legacy tech headaches

Automation is a crucial component of modern microsegmentation solutions, reimagining both implementations and ongoing management of network security – areas that rank among security leaders' top concerns.[18] By leveraging automation, organizations can significantly reduce the time and effort required for initial setup, eliminating manual work associated with tagging, policy creation, and asset grouping. For security teams grappling with significant legacy tech and minimal resources, an automated microsegmentation solution shoulders the burden of dynamically securing complex environments. This streamlined approach accelerates deployment, minimizes human error, and offers substantial long-term advantages. Automated microsegmentation solutions enable seamless scalability, automatically applying appropriate policies to new assets, freeing up IT resources, and ensuring consistent security measures across expanding environments. The impact on cost-effectiveness is striking, with the average enterprise saving 86% on costs compared to legacy microsegmentation.[19]

If we zoom out and look at the state of network security as a whole, organizations that leveraged AI and automation across their security strategy see $1.9M less in breach costs on average.[20] By adopting accurate, automated microsegmentation, organizations can significantly strengthen their security posture while also achieving considerable cost savings in the event of a breach.

Cost of a data breach based on where AI and automation are deployed in security operations



From the organizations that reported extensive use of AI and automation, measured in USD millions (IBM, Cost of a Data Breach Report 2024)

CASE STUDY

Learn how a leading class action law firm passed a pen test in hours:

- Discovered all network assets in a click
- Automated tagging, grouping, and policy creation
- Secured privileged access with network-layer MFA



18 ViB Tech, The Role of Network Segmentation in Zero Trust Architectures
19 Enterprise Strategy Group, Technical Validation: The Zero Networks Platform
20 IBM, Cost of a Data Breach Report 2025

CHECKLIST

What to Look for When Selecting a Microsegmentation Solution for Your Law Firm

It can be difficult to evaluate the difference between one microsegmentation solution and the next. This is because many vendors will throw around the latest buzzwords and make claims that are hard to assess. In reality, not all microsegmentation solutions live up to this hype.

What should legal industry security leaders look for when evaluating potential vendors? To answer that question, we've created the following guide.

For a microsegmentation project to truly succeed, it should meet the following criteria:

- [ ] **Is it easy to use?**
  In the past, microsegmentation was legendary for its difficulty and complexity. This is because manually segmenting a network that contains thousands, or even tens of thousands, of elements is virtually impossible. A modern solution must be much, much simpler to implement; ideally based on a set-it-and-forget-it approach that automates the entire process.

- [ ] **Is it effective?**
  There are a lot of bells and whistles out there – shiny, clickable maps, color-coded statuses, and seemingly unlimited external integrations. It's important to get focused. You don't want to just look at a map of your network and piece together a few policies that protect your high-value assets. Instead, you want to protect every asset and eradicate lateral movement. A modern solution should be able to segment 85% of your network – or more.

- [ ] **Does it require any additional resources?**
  Today's security teams are stretched thin. A good microsegmentation solution does not incur the need for additional headcount or hours spent manually creating and managing policies.

- [ ] **Will it start working quickly?**
  Historically, deploying a microsegmentation solution meant agents and painstakingly complicated configurations. But legal CISOs and security teams need to show quick wins, and fast deployment cycles are no longer optional. This means a good solution promises fast deployment, no agents, and no lengthy configurations.

Does it offer heterogeneous segmentation?

Today's segmentation solutions often force you to decide between sequestering users, clients, or servers. A modern approach should do it all – taking a heterogeneous approach to asset segmentation. In addition, it should offer a single point of control, both in cloud and on-premises environments.

Is it IT/OT agnostic?

Typically, OT environments require a separate approach to segmentation. For a microsegmentation solution to truly succeed in today's world, it should cover both OT and traditional IT environments.

Are there any single points of failure?

The old adage "you're only as strong as your weakest link" no longer applies. An effective solution will have no single point of failure, to make sure availability is close to 100%.

Are there hidden costs associated with it?

A good microsegmentation solution should have no hidden costs. This is because a properly segmented network should lead to simplified network security operations, as well as reduced spending on routers, and/or ACL-based segmentation.

Does it offer 'continuous segmentation'?

Modern law firms' networks are dynamic, which means there's no time to discover everything in your environment – by the time you do, it has changed. Therefore, your microsegmentation solution of choice should automatically and continuously observe network access to identify the network permissions necessary for day-to-day activity.

Does it integrate with existing infrastructure?

A good microsegmentation solution should be engineered to ensure easy integration with existing IT infrastructure. This will guarantee that typical network usage patterns remain unaffected.

About Zero:
Simple to Deploy, Powerful in Action.

Zero Networks protects law firms of all sizes with our flagship automated microsegmentation solution that works at scale, and with the click of a button, without agents or painstaking manual rule creation. Zero blocks ransomware and completely stops lateral movement, all without interrupting normal network traffic. Our modern microsegmentation solution is award-winning, validated by trusted analysts, and deployed across many different verticals, including law, healthcare, finance, and manufacturing.

We wrote this guide to help cybersecurity leaders in the legal industry make sense of the often-confusing landscape of network segmentation solutions. Not all microsegmentation solutions are created equal, and choosing one that falls short is likely to end up being a futile effort, particularly at scale. However, when it's done right, microsegmentation can help your law firm stay safe and run smoothly.

We are proud to offer the first truly automated microsegmentation designed to work effortlessly at scale, with no additional operational effort.

Here's how we do it:

Is it easy to use?

An easy, scalable implementation

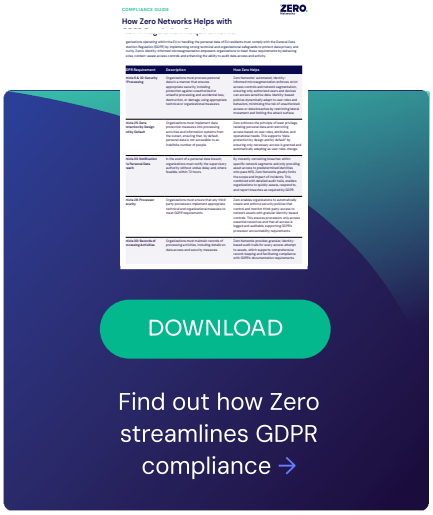
With Zero, tagging, grouping, and policy creation and maintenance are automated and incredibly accurate, eliminating manual processes that are error-prone and time consuming. Additionally, Zero's agentless architecture deploys in minutes by leveraging the native, host-based firewalls. In the case of OT devices, the ACL or switch is used instead to control traffic and enforce least privilege access.

Is it effective?

Automatically segment every asset on prem and in the cloud in days, not years

Zero makes it easy to block ransomware and ensure operational resilience with zero trust architecture. It's simple to deploy and powerful in action – we make it easy to segment the majority of your assets in 30 days, and our implementation is flexible, allowing customers to segment their network all at once or in batches.

Zero also provides compliance-ready architecture, enabling law firms to demonstrate segmentation across their entire network, easily meeting and exceeding compliance and insurance requirements.



Does it require any additional resources?

Save time, save costs, save sanity

Because it's so easy to implement, our modern microsegmentation solution does not incur the need for additional work or extra headcount to manage and maintain, freeing up IT resources to work on other projects.

In fact, Zero saves the average enterprise 87% on OpEx costs when compared with traditional firewall segmentation and 75% when compared to legacy microsegmentation tools.

Will it start working quickly?

Speedy deployment

Not only is Zero easy to deploy, but it also works fast. With us, you can segment your whole network, down to each individual machine, in a matter of minutes. It's basically microsegmentation at the click of a button.

Does it offer holistic segmentation?

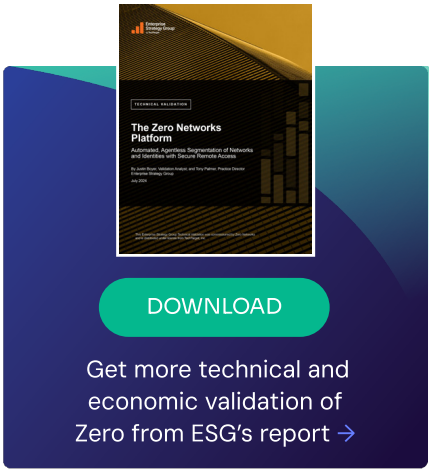
Designed for the modern network

Zero doesn't make you choose between segmenting users, clients, or servers. You can segment anything and everything with one platform. Plus, you'll have one point of control for everything, whether it's on-prem or in the cloud. Adding new assets or users to your network? Zero automatically identifies, learns, and segments them.

Is it IT/OT agnostic?

Works in both OT and IT environments

Our solution is OT/IT agnostic: it's configured to work in both types of environments – critical for today's modern manufacturing network infrastructures.



Are there any single points of failure?

Eliminates points of weakness

Zero prevents 99% of attacks from spreading and causing damage by taking every single machine and putting it in its own segment. This leaves no room for an attack to succeed — if there's a breach, there's no way for it to spread.

Are there hidden costs associated with it?

Cost-effective

Our solution is a software-defined microsegmentation solution that reduces the need for spending on other security solutions such as internal firewalls and NACs

Does it offer 'continuous segmentation'?

Requires no manual monitoring

Zero keeps itself up to date by automatically monitoring network access and identifying which permissions are necessary.

Does it integrate with existing infrastructure?

Plays nice with existing infrastructure

Zero's solution integrates easily with existing infrastructure and any host-based firewall. With Zero deployed, typical network usage patterns remain unaffected.

Bonus: Untethered to hardware

Finally, Zero's modern microsegmentation solution removes hardware from the segmentation equation — you can move and change any router, firewall, or network security appliance without having to migrate your segmentation policies to the new hardware.

See it for yourself

Try Zero

ZERO. Networks