FADDOM

# Your Checklist for Success

## Everything You Need to Know About MicroSegmentation

If you still rely on perimeter controls to protect your data center, you probably already know that your security solution is in need of an update. In this white paper, we will look at:

- Why network segmentation through VLANs or traditional firewalls is insufficient for today's hybrid and dynamic environments
- The trend of adopting micro-segmentation as a popular alternative
- The use cases for micro-segmentation
- Micro-segmentation for compliance and risk reduction
- How to avoid under and over-segmenting your network
- Using visibility as a foundational first step

The micro-segmentation market is projected to reach

**$3,032 Million** **by 2027,** a CAGR of 24.9% during the forecast period.

# The Limitations of Traditional Security Controls in Today's Data Center

Modern enterprises are totally different beasts from the way that businesses worked even a decade ago. Historically, security focused on perimeter controls that guarded traffic North-South, in and out of the data center. The rise in cloud-computing, reliance on third-party vendors and software, and DevOps style agile development practices have increased the amount of traffic that moves inside the data center, East-West. Most estimates put internal traffic at around 80% of all communications, which means that security needs to follow suit.

Some businesses are using traditional security controls to beat this modern-day problem, relying on VLANs, and enforcing communication through firewalls and ACLs. At first glance, this may seem like a great idea. After all, with VLANs you do not need any updates to your infrastructure or tools. Right? Wrong! Here are the main problems with using this approach.

**Manual Configuration:** Network and application changes are a lot of work when you need to make every configuration manually.

**Resource-Heavy:** Your engineers will need to configure switches and connect servers, all to prepare the network for the VLANs. Application teams will also need to allocate resources to building code, discovering infrastructure and preparing any other applications that will be affected by the change. You will also need to submit firewall change requests and involve firewall governance teams.

**Time-Intensive and Slow:** This process will take many months, and that's assuming you have a good map of your environment to begin with. When DevOps pipelines are being used, this is just not good enough.

**Maintenance Costs:** With two teams and a whole lot of resources and downtime, you can expect a hit to your bottom line.

**Customer Experience:** Once you're ready to start creating security policy for this new VLAN, you'll have to warn customers of down-time while you reconfigure applications, IP addresses, and integrations.

Perhaps you could look beyond these start-up costs to time and resources, if the solution itself was effective once you got it up and running. Unfortunately, VLANs are a limited technology at best. Which brings us to the most important bullet point:

**Limited Ability to Secure:** VLANs do not extend their security to the cloud, or to modern systems such as containers. This technology also doesn't provide any visibility whatsoever, which means you can't be certain that you are securing the right applications, workloads, or communications. This is true for your own peace of mind, but also for compliance and governance.

## Enter MicroSegmentation

In contrast, the best micro-segmentation was built for modern day environments, including cloud and container technology. It doesn't involve manual configuration or heavy resource-needs, and it shows quick time to implement and see value from. Here are the top four benefits you can expect to see when adopting micro-segmentation as your security technology of choice.

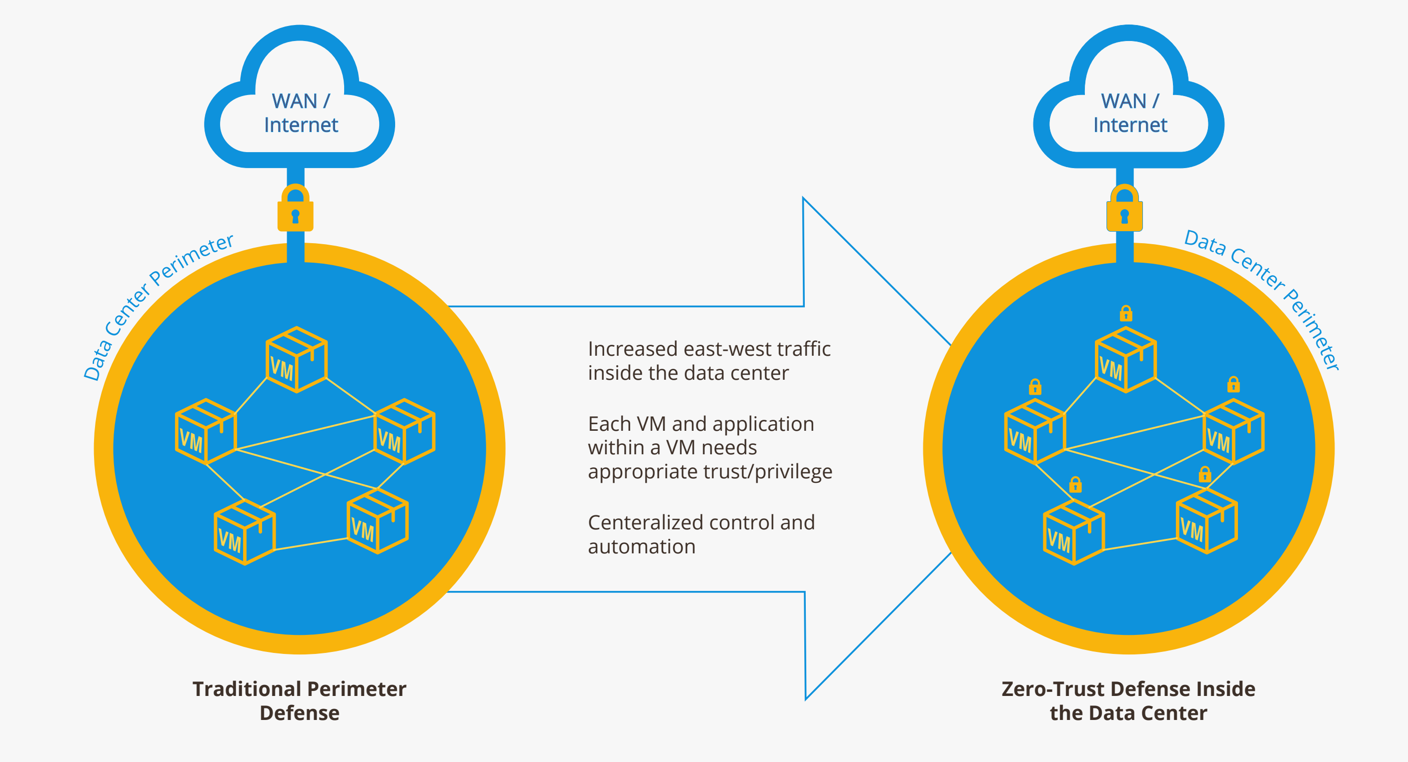
## Risk Reduction

Hybrid-cloud environments in particular, greatly increase your businesses attack surface. Application activity in this kind of heterogeneous environment needs tight controls.

Micro-segmentation is known to support businesses in working towards creating a zero-trust model. Zero-trust, coined by Forrester in 2010 is a security method where users, data, applications and workloads are given the access they need – and no more. The principle of 'assume access' means that you assume an attacker has already made it through your external perimeter. How are you going to ensure that they get no further?

By creating segments inside your network, you can reduce the attack surface substantially. Even if a breach was to occur, the attacker could only move within that specific segment, and nowhere else. One good example that is a common starting point for businesses implementing micro-segmentation technology is to create segments for your Production and Development Environments, known as environment segmentation.

Here's a graphic that can help to explain how zero-trust defence works.


WAN / Internet
Data Center Perimeter
VM
Traditional Perimeter Defense
Increased east-west traffic inside the data center
Each VM and application within a VM needs appropriate trust/privilege
Centeralized control and automation
WAN / Internet
Data Center Perimeter
VM
Zero-Trust Defense Inside the Data Center

## Stopping Lateral Movement

Once a breach has made its way through your perimeter, traditional security controls are not enough to limit their reach. In fact, there is nothing to stop attackers from making what's known as lateral movement, East-West inside your data center, escalating credentials or permissions to make it to sensitive data or critical assets.

In many cases, organizations would not even know that there is anything amiss. As we discussed, up to 80% of all communications and traffic happen inside the data center, giving attackers plenty of opportunities to blend in with the crowd.

## Achieving Compliance

Compliance is big business in today's threat landscape, and any business that deals with customer data needs to be aware of the regulations that pertain to their organization. For financial organizations that would be PCI-DSS, for healthcare, it's HIPAA, and for general customer interaction, EU businesses need to be aware of GDPR, and organizations in the US should brush up on CCPA, to begin with.

No matter which regulations you're bound by, protecting personal information is number one on the list. This usually involves your company working out what is 'in scope' and then keeping it separate, or segmented, from the rest of your data center. Micro-segmentation is perfect for this use case, and with the right visibility, you can simply isolate the applications and workloads that carry this sensitive information, and ensure that it is protected in case of an attack. While incidents do happen, and it's impossible to be prepared for everything, you can rest assured that you have done your part to protect your customers and your business reputation, and have an audit trail to provide to regulators to prove this compliance.

## Securing Digital 'Crown Jewels'

The benefit of micro-segmentation as opposed to other controls is its platform-independence and its granularity. This means that specific sensitive assets or 'crown jewels' can be protected with as much enforcement as you would like, keeping your most valuable applications and data secure, even in case of a live breach. See our sidebar on over-segmenting your environments for more information on doing this in a smart way, without losing flexibility.

## The Risks of Under and Over Segmenting your Network

Micro-segmentation technology needs to be implemented with a smart balance. The tighter the segments, the more secure they will be, but this will have a direct impact on flexibility and adaptability for your business. If however, you create coarser micro-segmentation policy to ensure you have more freedom, the attack surface could well be too large to ensure that you have adequately reduced risk.

It's a tough problem to solve. Over-segmentation could have an adverse effect on your business processes, and in fact, according to Gartner "more than 70% of segmentation projects will have their initial design rearchitected because of over-segmentation." On the other side of the coin, under-segmentation could leave you open to attack.

In this reality, many micro-segmentation projects fail, making it more important than ever that you begin with strong visibility into your entire infrastructure, so you are sure you have a full grasp of the balance that you need.

## Security Starts with Visibility

Micro-segmentation is a powerful technology, and is worthy of all the hype that's surrounding its entry into the cyber-security market. However, before you get started seeing the value to compliance, risk reduction, and general security posture, you need to start with an accurate picture of your entire environment from end to end. After all, how can you secure what you can't see?

Visibility technology is not all created equally, and the wrong choice could leave you with gaps or blind spots. In turn, this could create under or over segmentation of your projects, or lead to a dangerously wide attack surface that leaves you open to unnecessary risk. Here are the top features to look out for when choosing a visibility platform:

### Platform independent

Visibility only works if you can see everything. Some vendors give cloud coverage, while others work on premises. Integrating disparate solutions adds complexity and hassle. Don't accept less than one map that shows you everything from legacy infrastructure through to container systems and cloud, and works with all operating systems and platforms.

### Agentless

Agents and credentials will slow you down, no matter what your provider says. Wire data as opposed to machine data provides all the accuracy you need, with zero impact on performance, and much faster time to implementation and value.

### Application Dependencies

Native cloud solutions will visualize applications and servers, but won't show you the dependencies and communications. When planning a complex project like micro-segmentation, you need to be able to see, at a glance, the impact of any policies. Application dependencies to a granular level are essential, alerting you to issues such as blocked ports.

### Accurate and Real-time

Continuous scanning is a must-have, providing a real-time view of your data center instead of remaining reliant on scheduled scanning which happens during 'off' hours. Continuous scanning gives you an accurate view of what's happening in your real-life setting, not a snapshot of a specific time of day.

### Intuitive

Many vendors provide complex lists of data that are difficult for even the tech-savvy to understand. In contrast, look for a partner who provides a clear, easy to read map. This should be easy to share to business stakeholders, and customizable for the information you want to filter and see. The easier it is to use, the easier it will be to get buy in when you're ready to build policy.

# About Faddom

Faddom creates interactive, real-time maps of your entire IT ecosystem, offering granular detail. Our solution is completely platform-agnostic and has limitless use-cases. Uniquely, Faddom works without credentials, firewalls, or agents. With network discovery based on real traffic, you gain ultimate visibility of all dependencies and communications. Use this to efficiently assess costs, discover a hybrid ecosystem, or model workloads for migration.

Our platform is easy to deploy, highly scalable, and can be integrated with all of your current tools and products seamlessly. Whether you are primarily on the cloud, utilize hybrid or multi-cloud environments, or reside on-premises, Faddom can

be used to discover, plan, and maintain the most comprehensive real-time map for your application ecosystems. You can easily configure your map to manage IT assets by business context, prioritizing the right alerts and, more importantly, keeping your business running smoothly.

Contact us at
**info@Faddom.com**
to see a live demo.