Guardicore

THE DEFINITIVE GUIDE TO CHOOSING A MICRO-SEGMENTATION SOLUTION

HOW TO CHOOSE THE RIGHT SOLUTION FOR TODAY'S AGILE BUSINESS WORLD

WHITE PAPER

INTRODUCTION

Today's IT environments are getting more complex and dynamic, making isolating communication flows through micro-segmentation essential. Micro-segmentation gives your business granular workload-based security and unparalleled process-level visibility over your operations. It also reduces the risk of attack and improves governance over your entire IT stack.

Moreover, having a full understanding of your infrastructure puts you in a better position to achieve regulatory compliance, and has immense strategic value. It allows your company to safely innovate through cloud technologies and build flexible yet secure rules-based policy into every element of your architecture.

As micro-segmentation grows in popularity, there are a number of options to choose from for your security operations, from the vendors themselves to the tools and processes they offer.

Let's break it down. What are the essential elements to consider before you make your choice, and what are the must-haves for micro-segmentation in order to make it simple to truly reap the rewards?

This guide focuses on:

- Visibility through application discovery and dependency mapping
- Ensuring your solution is platform-agnostic
- Setting up simple policy management and workflows
- Using Layer 7 insight to avoid under-segmentation
- Including threat detection and breach response
- Avoiding the trap of "all or nothing" micro-segmentation

VISIBILITY THROUGH APPLICATION DISCOVERY AND DEPENDENCY MAPPING

Creating a micro-segmentation plan needs to start with understanding your environment. That entails granular visibility of your environment and all the connections and communications contained therein.

The challenge

Legacy and virtual firewalls or older micro-segmentation solutions lack process-level visibility or the ability to look at data contextually. No visibility at a granular application level makes it impossible to identify and map out segmentations for applications, workloads, or users. You will constantly be slowed down by the fact that you can't easily see the difference between sanctioned and unsanctioned behaviors or assess application dependencies.

Moreover, legacy firewall appliances are also complex, inflexible, and expensive. The costs are huge, from the huge upfront time and money involved in firewalls and hardware to the downstream costs of project management, labor, maintenance, and the very real risk of prolonged asset exposure due to lengthy implementation times.

Traditional network visibility, or manual mapping, also does not work. Data collection and manually mapping processes take time and effort, doesn't result in the level of detail required, and is increasingly difficult and error-prone in today's large data center and hybrid cloud environments. Moreover, with tens of thousands of workloads and hundreds of thousands of assets to consider, manual mapping is truly an unsustainable practice.

What's more, even process-level visibility becomes irrelevant if you don't have access to a real-time view. Even a detailed static snapshot of your application can't accurately display the dynamic nature of today's environments.

The solution

Table stakes for any micro-segmentation solution should be application visibility and dependency mapping at scale, across all environments and infrastructures. The right solution provides context within its mapping process, making analysis and segmentation seamless, quick to implement, and efficient.

With a live map of all the components in your application, from services and ports to communications and underlying processes, you get a real-time view of your architecture. At that point, you can use the solution to import relevant metadata to automatically generate asset labels.

Another automated feature to look for is the ability for the solution to suggest segmentation rules based on observing real-time behavior, adapting as necessary. With this powerful combination of granular visibility and automation, the hard work is taken out of your hands.

Visualization and automation requirements checklist:

- ❑ Real-time, granular application, process-level, workload, and user visibility
- ❑ Dependency mapping across all environments and infrastructures
- ❑ Auto-generated asset labels based on metadata
- ❑ AI-suggested segmentation rules based on real-time behavior

ENSURING YOUR WORKLOAD MICRO-SEGMENTATION IS PLATFORM-AGNOSTIC

Keeping your security procedures independent of any particular platform is essential if you are running a multi-cloud or hybrid environment. The benefits of using a combination of public and private cloud options or SaaS solutions are growing. Businesses increasingly use a mix of servers, virtual machines, and new cloud technology, such as containers. With this broad range of solutions, it can be difficult to understand who is responsible for security measures and how to deploy security everywhere.

The challenge

While the cloud-related benefits of being able to auto-scale and add mobility and flexibility are powerful, native cloud security controls are limited. Each cloud vendor offers its own limited native point tools dedicated to its architecture alone, which may not be aligned to your unique challenges. Managing a series of these cloud-native security tools is a challenge that dramatically increases the time to configure policies.

In addition, there is a lack of visibility into what's happening across all clouds at the same time (not to mention what's going on on-prem). This leads to error-prone security operations and textual logs, or snapshot maps which aren't enough to complete a comprehensive segmentation project.

Dynamic policy setting can also be a struggle, even if you are only using one cloud platform. As workloads scale up or down, security controls may not be updated or modified adequately. It can be difficult to understand who has responsibility for important security decisions, or who should stay on top of updates or patches. Without application layer visibility and using a model of shared security alone, blind spots are inevitable.

The solution

Employing a single platform-agnostic solution for security and micro-segmentation, including enforcement up to Layer 7, vastly reduces complexity. You can take advantage of cross-platform opportunities without adding risk into your environment.

Being able to deploy one solution that works across the entire IT stack doesn't just allow you to implement micro-segmentation effectively. This approach is also significantly quicker and easier to track and manage than multiple disparate security protocols. It also provides a targeted focus and tailored platform-agnostic solution for your specific business goals and security requirements, including supporting a zero trust architecture and compliance requirements.

Why choose software-based segmentation vs. cloud-native security?

- ❑ Cross-platform visibility
- ❑ Faster time-to-policy
- ❑ Stronger security
- ❑ Breach detection and response
- ❑ Easily adjustable permissions
- ❑ Granular controls
- ❑ Zero trust architecture and compliance support

Ensuring your solution is platform-agnostic and deploying micro-segmentation by workload means that as workloads move across varied and dynamic environments, security protocols stay aligned and persistent right alongside. Your IT security team doesn't have to manage multiple policies or SLAs. What's more, breach detection and response can be enforced wherever an issue may occur.

SETTING UP SIMPLE POLICY MANAGEMENT AND WORKFLOWS

Your policy engine is what the success of your micro-segmentation solution will hinge on. It's essential that your provider keeps it simple. Anyone in your company should be able to understand and manage policy creation.

The challenge

Many solutions lack a simple and straightforward UI that is logical from the first stage in the process to the execution of your full segmentation plan. Be wary if the solution you are looking at can't provide:

- Detailed impact of your rules and policy before they are applied to traffic.
- Visibility through the entire process, from a blank page through to mapping and application dependencies all the way to setting the rules themselves and seeing the benefits in action.
- Built-in automated policy suggestions that show product expertise and make the process seamless end-to-end.

Well-crafted policy creation won't make you give up on flexibility to ensure security. Many point solutions include limited "allow-only" rule sets. In order to set up an effective security posture for your environment, you need to be able to enforce global deny rules that take priority over all other rule sets. In this way, you can create unauthorized actions like stopping a workload with a particular label from accessing the internet.

For areas like compliance and regulatory assessments for PCI or HIPAA, for example, enforcing global deny rules makes your security professional's workload a whole lot easier. At the same time as establishing this type of "macro-segmentation" rules, you should also be able to create explicit granular policy through micro-segmentation for the same application segments.

The solution

Before you select your solution, ensure that your choice is flexible enough to meet your security and business needs. You want to be able to view and govern your environment exactly the way you choose.

Policy management features and capabilities checklist:

- ❑ Flexibility to set custom, compliance-based rules
- ❑ Dynamic labeling as workflows scale up or down
- ❑ Multiple workloads can share labels and policy
- ❑ Segmentation policies can be converted to blocking
- ❑ Blocking policies don't affect legitimate traffic
- ❑ No disruption to business-critical process
- ❑ Policy engine can proactively limit lateral movement

Examples of micro-segmentation options include:

- Type of environment (such as development or production)
- Regulatory sensitivity (PCI, HIPAA, etc.)
- Application (HR, CRM, domain controller, billing, etc.)
- Tier or role (database, application server, web server, etc.)
- Process (hosts, ports, etc.)

Once this is established, your policy engine must allow for dynamic provision and adaptability when changes occur. From workflows that auto-scale to services that expand or contract, IT environments are never static and are increasingly dynamic. If your policy engine doesn't adapt, micro-segmentation cannot occur.

GUARDICORE MICRO-SEGMENTATION:
Stronger Security, Greater Agility, and Savings

Large European Bank

10,000 assets segmented, 10x faster, zero downtime

"Guardicore helped us implement tight network segmentation across on-premises and cloud environments. With Guardicore we are effectively protecting our critical assets and applications."

Vice President,
Information Security

Cogna Group

Migrating data center to the cloud in two weeks

"[Guardicore's micro-segmentation] is about monitoring the access context to allow only authorized users to access each server and each communication channel between machines. This is the kind of control we must have today."

Alex Amorim,
Information Security Manager

The HoneyBaked Ham Company

Securing 45 applications without interruption in six weeks

"[With Guardicore] I get real visibility and can actually see who's connecting to what applications and servers. I have better and more control to segment, AND it's cheaper? This is a no brainer."

David E. Stennett,
Senior Infrastructure Engineer

USING LAYER 7 INSIGHT TO AVOID UNDER-SEGMENTATION

Rather than try to limit dynamic workloads, the right solution should simply make them safer from the outset.

The challenge

Traditional network segmentation is not enough for today's diverse ecosystem. Old-fashioned security procedures require keeping your IT environment as simple as possible, encouraging you to shy away from new opportunities as they come with unknown risk.

While network segmentation focuses on managing a complex environment, micro-segmentation looks at optimal security. With micro-segmentation, visibility and tight workload-based segmentation means the risk is always under control, allowing you to embrace agility and innovation without compromising on security.

In order for this to work, your business needs to ensure that it isn't under-segmenting. That means managing communication flows all the way to Layer 7.

Port hijacking has become a common threat, with breaches known to take over an allowed port for data exfiltration. Layer 4 approaches, which focus only on the transport layer, are the equivalent of a bank that doesn't employ guards once you get past the front door.

Although this might have been sufficient in the past, it's becoming increasingly easy for attackers to gain access through your perimeter and from there, wherever they want to go. If your solution only segments or protects up to Layer 4, you are not limiting the attack surface area. The more dynamic an infrastructure is and the more workloads interact and communicate across different segments, the more dangerous this security weakness becomes.

The solution

A powerful micro-segmentation approach will do the same for your data center as you would expect for your perimeter security, which you would never protect with less than a Layer 7 firewall. Segmenting and enforcing up to the application layer for your data center means that you are delivering strong security against lateral movement by open ports and protocols, stopping attacks before they get out of control. You are also blocking or allowing traffic by both source and destination processes on all your OS, rather than simply by servers and ports alone.

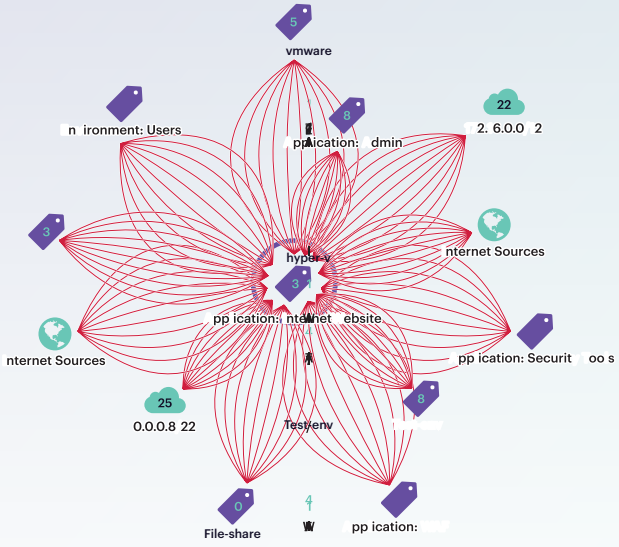
FIND OUT HOW YOU CAN REDUCE YOUR ATTACK SURFACE

Sign up for a no-software, zero-touch Attack Surface Reduction analysis and receive:

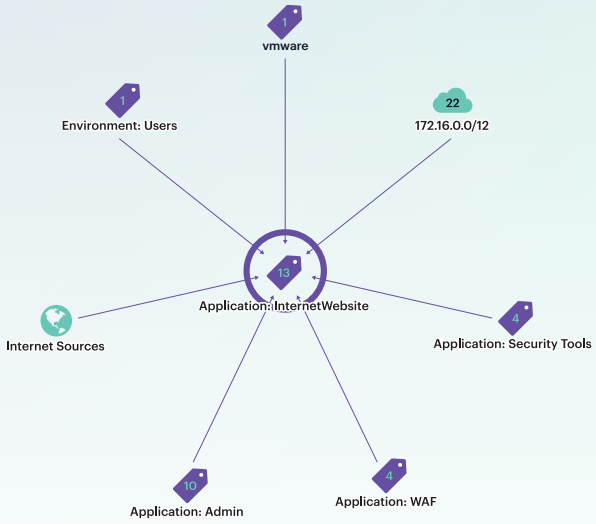
- An analysis of the attack surface of your critical applications before and after micro-segmentation.
- A clear understanding of the level of risk reduction segmentation brings.
- Communication path maps based on your own unique environment.
- A numeric score demonstrating the level of risk reduction.
- Reduction of communications paths to critical applications assets by port.
- A general explanation of attack surfaces, risk reduction, and methodology used.

A real-life report showed that a business' critical application had 3.5M possible connections, but only 120 were truly necessary. Closing all connections but the 120 required would result in a **99.93% risk reduction!**

Request report



Before segmentation



After segmentation

INCLUDING THREAT DETECTION AND BREACH RESPONSE TO STRENGTHEN SECURITY POSTURE

A comprehensive security solution needs to include features that go beyond micro-segmentation, including the ability to note when a threat appears or a breach has occurred and to stop attackers in their tracks, before they can do any major damage.

The challenge

By segmenting application components, you gain the automatic benefit of isolating breaches to your environment. This stops attackers before they increase their threat or make lateral moves.

A powerful micro-segmentation solution should be able to do more, though, integrating with security tools that offer preventative measures to stop attacks in the first place. Reputation analysis allows you to detect a breach immediately. Threat response features can then isolate and fix problems in real-time, without affecting genuine communication flows, even within the same segment.

The solution

The right micro-segmentation solution won't just contain a breach to one area. It will also put you in the best position in advance to stop a breach in its tracks, as well as create an improved security posture behind the scenes for your entire organization.

To incorporate strong security tools with your micro-segmentation solution, your solution must access data from multiple attack vectors and assess policy violations and anomalies in real time. Your solution should recognize and alert you to attempted or successful breaches. It must also actively block any attempts to use compromised assets as launch points for lateral movement.

Unauthorized communications or non-compliant traffic of any kind needs to be immediately detected. It can then be contained and analyzed in order to speed up the investigation process and use the data to prevent future breaches.

Breach detection and analysis capabilities should reveal:

- ❑ Non-compliant traffic
- ❑ Unauthorized communications
- ❑ Blocked or attempted breaches
- ❑ Compromised assets
- ❑ User credentials
- ❑ Attack methods
- ❑ Propagation tactics of the intruder

AVOIDING THE TRAP OF "ALL OR NOTHING" SEGMENTATION

The road to micro-segmentation doesn't have to feel like an uphill journey, and it doesn't need to be disruptive for your company, either. In fact, it works best if it's done slowly, in stages. Look for a provider that wants to help you take it step by step.

The right company should create an implementation plan for you that starts with visibility. This allows you to get a clear understanding of your needs before you even think about what rules or segmentation policy you want to create. This stage should give you a granular understanding of your IT architecture, including network flows and orchestration details from all of your platforms and workloads. The result should be a visual map of the relationships between your applications across on-prem, hybrid, and cloud environments.

Next, identify critical assets, which are usually high risk or high value infrastructure. Embrace the inherent simplicity of creating workflows and build flexible policies which are tailored to your unique environment, including enforcement up to Layer 7. Micro-segmentation of individual applications can begin to show you the benefit of your approach, shrinking the security perimeter substantially with just one line of policy.

Gradually increase the areas and applications you micro-segment, seeing the benefits spread throughout the organization. Don't forget to utilize underlying breach detection and resolution features for a holistic, all in one solution.

CONSIDERING MICRO-SEGMENTATION AS A WHOLE

While the benefits of micro-segmentation are simple and straightforward, starting the process can be difficult. Leverage the expertise of a company with a great track record and take advantage of the best tools and services on the market to make a success of your implementation.

Remember that implementing the right micro-segmentation solution is a multi-stage process, from visualization and mapping through building workflows and policies for segmentation all the way to breach detection and response. It's time to cost-effectively simplify the process of isolating, finding, and resolving threats in real-time, strengthening your security posture as a whole.

PROTECT WHAT MATTERS MOST WITH GUARDICORE MICRO-SEGMENTATION

Request your risk reduction analysis today:

www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.

Guardicore