Guardicore

THE ATTACK SURFACE REDUCTION REPORT

HOW TO SHOW THE ECONOMIC VALUE OF SEGMENTATION AT-A-GLANCE

WHITE PAPER

INTRODUCTION

The Guardicore Attack Surface Reduction Report is about understanding — at-a-glance — the results that risk reduction through software-based segmentation would have in your environment. No software installation is needed to calculate how much you can shrink your attack surface with Guardicore, there is zero impact to your network, and we don't ask for any commitment.

Sound too good to be true? Want to know how it works — and why it's important?

Let's start at the beginning...

THE CHALLENGES OF A FLAT NETWORK

Whether you're new or a veteran to the network security world, the terms "segmentation" and "micro-segmentation" likely ring a bell. However, if you're still using legacy firewall VLANs for segmentation, the ringing you hear is probably from alarm bells as you hesitate to start yet another long, tedious, and complex project.

That said, segmentation truly is the way to go. A flat network is a ticking time bomb waiting for an intruder with the right tools (e.g., passwords, tokens, exploits) to leverage just one non-monitored communication path to penetrate the network. Once they're in, able to move laterally inside your network from asset to asset, the situation will be almost impossible to control. In most cases, you won't even know data exfiltration or other issues resulting from compromise have occurred until it's too late.

With each server added, service subscribed to, or third-party contractor engaged with (support service for a specialized application, for example), your attack surface grows. With each open port, you've opened a new way for attackers to get into your organization's network as well.

Luckily, Guardicore Centra's software-based segmentation enables enterprises to reap the benefits of risk reduction while also supporting agile DevOps and rapid application deployment. The solution delivers optimal security at a faster speed with greater security efficacy and a far lower total cost of ownership than traditional methods.

Yet demonstrating the economic value of segmentation to management can be challenging. How do you convince them it's necessary to invest in such a solution?

What damage can result from a single compromised asset?

Attackers can:

- Probe and profile the environment around the asset
- Seek out higher-value targets
- Attempt to blend lateral movement in with legitimate application and network activity

The outcome can be extreme:

- Disrupted business continuity
- Loss of sensitive data or intellectual property
- Damage to brand reputation
- High costs to company (an average of $8.19M[1] — yikes!)

[1] IBM Security: Cost of a Data Breach Report 2019 – United States

THE VALUE OF NETWORK SEGMENTATION, I.E., "I'LL BELIEVE IT WHEN I SEE IT"

Even if you know the company's network like the back of your hand, it can still be difficult to grasp the scope of an attack surface and its associated risks. It's even more murky when you are the CFO or CEO, with less insight into how assets communicate with each other.

The idea to create the Guardicore Attack Surface Reduction Report actually came from one of our prospects (now a customer) who was facing this exact issue. The company's security team said to us, "We are sold; we know this is the solution and product we need. Now we need to convince our CFO..."

Well, having our own CFO at Guardicore we knew exactly what they meant. Our CFO is a super busy, budget-oriented guy who is driven by tangible facts. He would want to see an answer — backed by hard data — to the question: Why segmentation and why now?

Reduce the attack surface even as IT infrastructure grows and diversifies

Shrinking the attack surface using micro-segmentation solutions enables security teams to defend against the risks of compromised assets. The granular policies that can be created with a micro-segmentation tool slow or block attackers' efforts to move laterally by:

- Segmenting applications from each other
- Segmenting the tiers within an application
- Creating a clear security boundary around assets with specific compliance or regulatory requirements
- Enforcing general corporate security policies and best practices throughout the infrastructure
- Applying the principle of least privilege more broadly throughout the infrastructure

Guardicore Centra brings visibility

- Automatically discover applications and flows
- Visualize process-to-process communications
- Create contextual maps
- Make understanding activity and creating policies simple

HOW VISIBILITY LEADS TO UNDERSTANDING NETWORK RISK

Imagine someone could show you all the paths an attacker could use to access your critical assets — even the ways you didn't know existed. That big blur of interconnectivity that was previously an abstract concept suddenly becomes clear and the picture is eye-opening. That's how Guardicore's powerful Attack Surface Reduction Report tool works.

With no required software installation and zero impact to your environment, the tool provides detailed maps that allow you to clearly see — for one of your own critical applications — the communication paths before and after a segmentation policy is deployed. In other words, you get a clear picture of the application's attack surface before and after segmentation.

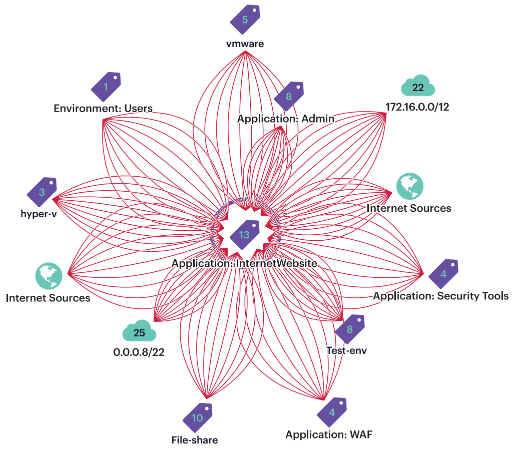
The visual representation and analysis included in the report provides the simple, quantifiable data points any decision maker looks for before approving an investment. Stakeholders can quickly compare the two views and see the resulting risk reduction percentage. This allows you to demonstrate to them, at a glance, why network segmentation is essential to reducing your organization's overall attack surface.

HOW DO YOU SEE YOUR APPLICATION'S ATTACK SURFACE?

By mapping all the potential communication paths to your critical application, the Attack Surface Reduction Report allows you to see your application's entire attack surface. We're not just showing you some random network or lab environment — we're using your network.

Leveraging Guardicore Centra's unmatched visibility features and based on the netstat-type data **we receive from you**, we provide you with a detailed analysis that is relevant to your unique environment. With the report in hand, you can instantly quantify the impact of micro-segmentation on your security posture.

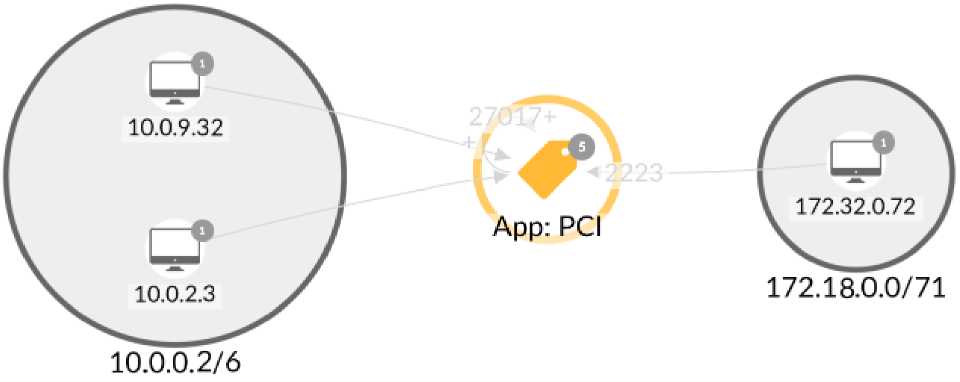
Take, for example, the application mapped out below, which is subject to PCI DSS compliance. There's no doubt about it being critical to the organization's business continuity, compliance, and reputation.



The majority of the organizations with which Guardicore runs the Attack Surface Reduction report have seen **risk reductions in the high 90 percents.**

You can see an image that every stakeholder in the company — be they security engineer, application owner, or CFO — immediately understands. This is the attack surface of the application. Approximately 100,000 communication paths combine to create the significant attack surface of this sensitive application (in a relatively small network of under 100 servers).

This next image represents the allowed connections only after software-defined segmentation is deployed — the servers allowed by policy to communicate with the application.



From 100,000, we have shrunk the attack surface of this application significantly by implementing a micro-segmentation policy and closing all but the 30 connections required. In fact, **the company achieves risk reduction of 99%**!

It's a simple fact: you can't protect what you can't see. Once you can see it, however, you can easily use a software-based segmentation solution like Guardicore Centra to rectify the situation, regardless of whether the application resides on-premises or in the cloud. As a result, the majority of the organizations with which we have run the Attack Surface Reduction Report have seen risk reductions in the high 90s.

FROM 3M CONNECTIONS TO 600: A REAL-LIFE EXAMPLE OF NETWORK RISK REDUCTION

Instant value from the Guardicore Attack Surface Reduction Report:

- **User of the Report:** Large business with a network of more than 30,000 assets.
- **Focus of the Report:** A custom application on which the entire company relied (a compromise would equal loss of hundreds of thousands of dollars per hour).
- **Current environment:** More than 3M possible communication paths to the application.
- **After segmentation:** Only about 600 communication paths were needed.
- **Solution:** After viewing the Attack Surface Reduction Report, management quickly understood the way that risk reduction could easily be accomplished with the Guardicore Centra micro-segmentation solution.

NOT ALL PORTS ARE CREATED EQUAL

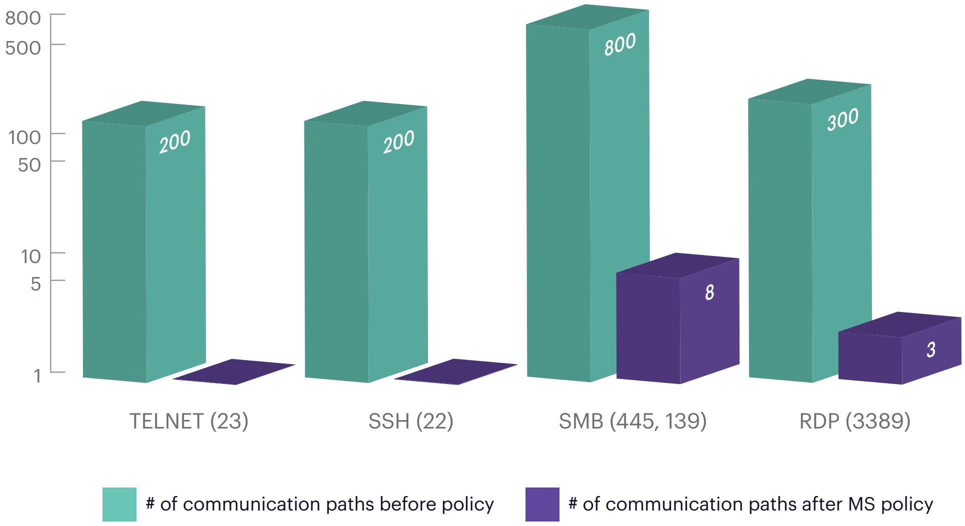
Some ports are more prone to be used during lateral movement. This is why, depending on the data we receive, we also provide a breakdown of the communications paths to the application per port.

SSH, SMB, RDP, and TELNET ports are prone to be used for lateral movement.

For example, think about ports that allow simple code execution (e.g., SSH), ports with many known vulnerabilities (e.g., SMB), or ports that are used by not-secure applications (e.g., Telnet). In other words, ports with increased levels of exposure introduce bigger risks than other ports.

Here, as well, we supply the breakdown before and after the micro-segmentation policy has been implemented.

Number of Communication Paths to App Assets by Port



HOW DOES GUARDICORE CREATE THE CUSTOMIZED ATTACK SURFACE REDUCTION REPORT?

As mentioned previously, the creation of the report is nearly a zero-touch situation. To generate the report, we analyze network data received from the application's servers. This data can be collected a few different ways. You can:

- Run an **open-source script**
- Run a SCCM script
- Utilize a NetFlow file
- Utilize a PCAP file containing packet network data
- Deploy Guardicore agents (for customers already in a PoC)

It is important to note that, in all but the fifth option listed above, we do not require any installation. All of these are completely controlled and run by the team for whom we are writing the report.

No connection is established by Guardicore at any point to the environment/servers. The data is collected and sent to an output.tar.gz file, for example, when running the open source script. It will only be available to Guardicore once it has been sent to us.

The safety of your data is of the highest priority. We do not share or use the data sent to us for anything other than the analysis and the report we provide.

"[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,
HoneyBaked Ham Company

...ESTD THE 1957...
HONEY BAKED
Ham CO

LEARN MORE

Ready to find out for yourself how your business could benefit by radically reducing risk through segmentation? Contact us today to discuss your own attack surface reduction analysis or read more about the process at **www.guardicore.com.**

DISCOVER HOW YOU COULD SLASH RISK IN YOUR ENVIRONMENT

Request your custom report:

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