Guardicore

RETHINK FIREWALLS

THE COMPELLING ECONOMIC CASE FOR SOFTWARE-BASED SEGMENTATION

WHITE PAPER

EXECUTIVE SUMMARY

Why are IT and security teams still relying on legacy firewalls to do internal network segmentation? As policy-protected applications and segments proliferate, physical firewall appliances are too complex, inflexible and just plain ineffective in today's increasingly dynamic hybrid-cloud environments. And above all, far more expensive than teams may realize. Forget the huge upfront cost of firewalls and hardware — think about all the downstream costs of project management, labor, maintenance, and the very real risk of prolonged asset exposure due to lengthy implementation times. If enterprises are to reap the benefits of agile DevOps, rapid application deployment and the cloud, there simply has to be a better way to secure assets through segmentation. And there is: software-based segmentation. It's easier, faster, more effective and — as this paper will clearly demonstrate — delivers optimal security at a far lower total cost of ownership than traditional methods.

INTRODUCTION

As the first line of defense against outside intrusion, firewalls have been without question a boon to the evolution of the internet. However, as data breaches proliferated, organizations realized they had to do something to mitigate threats inside their networks and data centers. This led to the concept of segmentation — the creation of restricted "zones" for groups of applications in the network environment. This has typically taken the form of virtual local area networks or VLANs, partitioned and secured by the same firewall technology that enforces north-south traffic at the perimeter. The combination of firewalls and VLANs has long been the default solution for network and data center segmentation.

Today, however, three converging forces are driving demand for more granular segments, and more of them. Agile DevOps and rapid delivery models put a premium on accelerated deployment of applications into production, requiring more secure zones with more precise policies. As organizations flock to the cloud and hybrid infrastructures, applications are often migrating among different environments, increasing inter-segment traffic. And the rapid proliferation of applications is creating an ever-larger attack surface for hackers to target.

FIREWALLS FOR SEGMENTATION: PAST THEIR PRIME

In this scenario, reliance on VLANs and firewalls for segmentation purposes has become unsustainable. From a purely technical perspective, the configuration of multiple VLAN and firewall installations to keep pace with the expansion of applications is a complex and cumbersome process. It is also labor intensive, diverting too many team members from higher priority security projects. Time to deployment is another issue, raising the risk of prolonged asset exposure and vulnerability. And above all, it is extremely expensive, not only in the upfront cost of firewalls and new hardware to support additional traffic, but also in the ongoing management, modifications, and maintenance of installations.

Simply put, traditional network segmentation approaches have hit a wall. In particular, as organizations seek to take advantage of dynamic cloud and hybrid environments, reliance on internal firewalling for security limits their agility, speed to policy creation and enforcement, and ability to scale their operations. The need for a modern, streamlined, less costly and more effective segmentation alternatives to legacy firewalls has never been more urgent. Enter software-based segmentation.

The need for a modern, streamlined, less costly and more effective segmentation alternative to legacy firewalls has never been more urgent.

FEELING THE PAIN — THE SOUL-CRUSHING, COSTLY TASK OF MANAGING FIREWALLS

Before delving into the advantages of software-based segmentation, it's useful to contrast it with the status quo. As an enterprise grows, so do the number of applications and the amount of data traffic, driving demand for additional network segments and more complex security policies. If you rely on firewall-protected VLANs, each new one deployed needs to be added to every switch trunk port through which inter-segment traffic flows. An IP subnetwork needs to be created for every new VLAN as well. A sub-interface must also be created for the firewall. Firewall policies then need to be created. Each of these changes usually requires approvals, maintenance windows, and the possibility of downtime, which means increased risk of network disruption.

Adding VLANs and firewalls entails a painful, multi-step process involving as many as five teams, separately responsible for switching, routing, firewall implementation, ESX servers, and security policy creation. All of this adds to the length of implementation, subjects the organization to prolonged risk, and drives up costs for software, hardware and labor. Moreover, from the engineer's perspective, this is high-risk, low-reward work — a lot of pain for very little gain, diverting time and resources from other high-priority risk management activity. Unfortunately, few of the steps in the process of change management within the firewalled VLAN environment lend themselves to automation.

FINDING THE CURE — SOFTWARE-BASED SEGMENTATION IN THREE EASY STEPS

Legacy perimeter firewall technology simply was never intended for the more precise, bandwidth-constrained demands of granular internal segmentation. Software-based segmentation has emerged in recent years as a viable, faster, more effective and lower-cost alternative to meet the demand for more and tighter network segments in today's dynamic environments. Core to the implementation of software-based segmentation is the concept of a "distributed firewall" that is much more agile and easier to manage than a traditional network firewall appliance.

Software-based segmentation makes possible as much as 10 or even 20 times faster deployment compared to traditional firewalling, with fewer people needed and virtually no downtime or disruption.

A leading example of a software-based segmentation solution is the Guardicore Centra platform. Compared to the lengthy, costly and complex process of VLAN-firewall implementation, software-based segmentation with Guardicore Centra involves just three steps:

1. **Identify and label assets:** A major drag on the traditional firewalling process is a lack of visibility into the assets that need to be secured. The Guardicore solution includes a visualization capability that enables operators to identify and label all the applications running throughout an organization's infrastructure.

2. **Visualize and group by label:** With visibility attained, operators can then organize applications into logical groups based on their labels and map the dependencies among them.

3. **Create policies:** Operators can then create policies that dictate which applications are allowed to communicate with each other based on actual flows. Applications and workflows are now effectively segmented from each other within the environment.

Software-based segmentation makes possible as much as 10 or even 20 times faster deployment compared to traditional firewalling, with fewer people needed and virtually no downtime or disruption. Moreover, once you've started the visualization and software segmentation process, you can easily divide your network further or add different policies based on labels, automate processes, address security incidents, and make swift changes in response to business or regulatory requirements.

DISTRIBUTED FIREWALL ADVANTAGES

Resides at the workload level with L7 context

Can be deployed anywhere (bare metal, VM, cloud, containers, etc.)

Security from the first to the last hop (vs. choke point of network firewalls)

Ideal for controlling east-west traffic

Dynamic security that moves with the workload

No device/ hardware to manage (security as a service)

Security decoupled from network infrastructure

WANT TO SEE HOW MUCH YOU CAN SAVE ON FIREWALLS?

Get your Firewall Savings Report:

www.guardicore.com/firewall-cost-calculator

CASE STUDY:
LARGE FOOD PROCESSOR SEES 85% SAVINGS ON SEGMENTATION

A major US pork products processor needed to segment 45 applications with an average of five servers per application, deployed at two locations. The company's goal was to eliminate its flat networks, with minimal service disruption, and have policies in place as quickly as possible.

After a review of alternatives, the company chose Guardicore's software-based segmentation solution. Though speed and simplicity of implementation played into the decision, the decisive factor was an analysis showing a savings of more than $900,000 or 85% over a 3-year period compared to securing VLANs with a leading firewall supplier. Specifically:

- The cost of licensing Guardicore Centra was 55% lower than the cost of hardware for a VLAN-firewall implementation.
- The cost of labor, based on an assumption of $2,000 per week, was a full 93% lower with Guardicore than a VLAN project with far longer duration.

In addition, Guardicore met the customer's need for fast policy implementation — securing 45 applications without interruption in just 6 weeks.

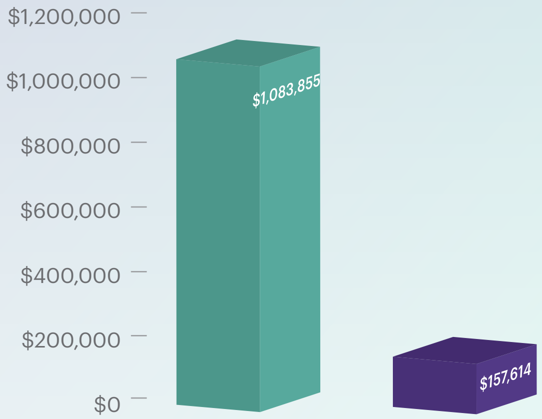
Firewall TCO*

$1,083,855

Guardicore TCO*

$157,614

⬇-$926,241



* Cost over a 3-year period

Guardicore Cost of Work*

$17,214

⬇-$579,796

Guardicore Cost of Licenses/Support*

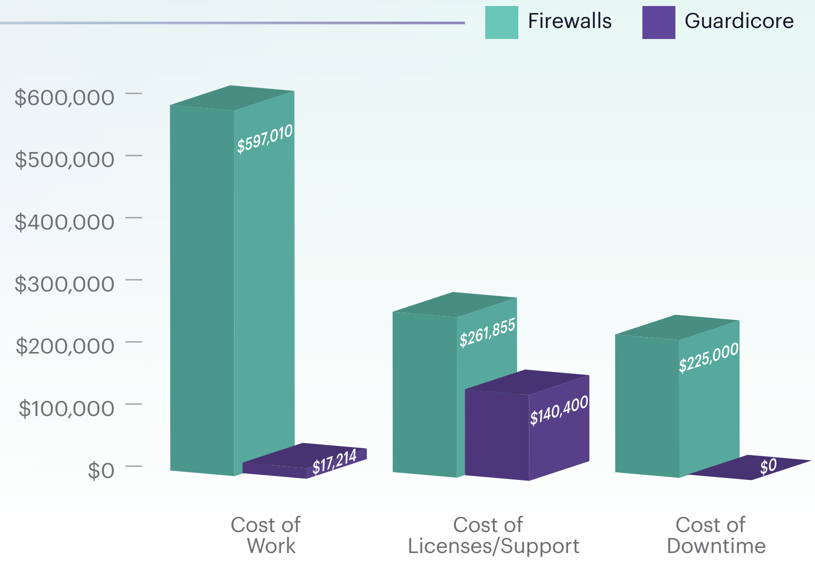
$140,400

⬇-$121,455

Guardicore Cost of Downtime*

$0

⬇-$255,000



WHAT IT ALL MEANS

Software-based segmentation delivers three key advantages over traditional firewall methods:

More effective risk reduction: By enabling rapid segmentation of applications at a very granular level, software-based segmentation results in a vastly reduced attack surface. Leveraging zero trust principles, which require strict authentication of any user, device or application attempting to access a network asset, software-based segmentation thwarts the lateral movement of threats within the data center or network environment. This further mitigates the impact of data breaches, rendering attackers unable to take over any processes even if they have successfully broken through perimeter defenses. It also allows enterprises to more quickly achieve compliance with regulations calling for the distinct isolation of critical, sensitive applications from general network traffic.

Velocity to optimal security posture: In short, software-based segmentations makes you more secure, more quickly. This enables security teams to keep up with the pace of agile DevOps application deployment and ensure that every application in production is secured. It also means that fewer resources — technical or human — are tied up in segmentation projects for lengthy periods. Teams can move on.

Dramatically lower total cost of ownership: This is the real bottom line, and probably the most significant advantage to the people signing off on the project. Software-based segmentation can be achieved with far less capital expenditure (CapEx) for a software solution compared to purchasing firewall appliances and additional hardware. It also results in far lower operating expenses (OpEx) over time in the form of labor and resource savings for ongoing maintenance and management.

By these measures alone, in a side-by-side, apples-to-apples comparison between software-based segmentation and a firewall solution for 10 application segments, the Guardicore approach was shown to deliver a potential 81% total savings, amounting to over $1 million.

Of course, though you can expect to see measurable savings in the first week of deployment, total cost of ownership (TCO) means more than just the upfront purchase price or ongoing out-of-pocket. Though the price tags may not be readily apparent, software-based segmentation produces substantial savings by virtually eliminating downtime and service disruption. Further, enterprises will avoid financial losses resulting from data breaches, as well as penalties for non-compliance. And they greatly reduce the risk of reputation damage and loss of business in the wake of a breach. IT teams and resources can be redeployed away from firewall change management and toward more productive projects. All these cost factors contribute to a lower TCO and a stronger bottom line.

CASE STUDY:
LARGE GLOBAL BANK, FACING COMPLIANCE SANCTIONS, TURNS TO GUARDICORE

Following an audit uncovering security risks in its flat networks, and faced with a body of new regulations requiring stricter segmentation, a major European financial institution initiated a segmentation project using VLANs and firewall rules. This project was taking significant time, requiring multiple stakeholders and teams, causing production downtimes and policy ambiguities. As a result, the bank was paying fines for non-compliance, in addition to unsustainably high implementation costs.

The IT team quickly looked into alternative solutions and was impressed with the level of automation Guardicore could bring to bear on its security operations. The bank deployed Guardicore Centra across multiple regions and IT infrastructure types. The project took less than three months — 10 times faster than initially estimated with traditional segmentation methods. The bank not only upgraded its security posture, but also fulfilled the compliance requirements for more than 10,000 assets. The rapid deployment resulted in accelerated risk reduction, along with dramatic cost and internal resource savings.

Large Global Bank

Project target:

Dev/Prod/UAT separation

Project scope:

1. Restrict traffic between production and non-production environments
2. App ring-fencing readiness

Legacy Segmentation

✗ Extremely slow progress

✗ Audit failures, fines, and production errors

✗ Production outages due to application downtime

Time: 2 years with Firewalls/VLANs

Guardicore Impact

✓ 10,000 non-compliant assets segmented

✓ Zero application downtime

✓ 10x faster implementation savings compliance costs

✓ Reduced manual effort with DevOps

Time: 6 Months
People: 3 Architects

CONCLUSION: ADD IT ALL UP

Firewalls aren't obsolete. They certainly have a role to play in securing the network perimeter. But in today's dynamic environments, the perimeter has become a somewhat amorphous concept. To achieve agility, organizations need to be able to secure their digital assets at the process level. And for that purpose, firewalls are not only ill-suited, but actually stand in the way of growth. Attempting granular segmentation with firewalls is a drain on resources — human, technical, and financial.

To achieve agility, organizations need to be able to secure their digital assets at the process level. And for that purpose, firewalls are not only ill-suited, but actually stand in the way of growth.

Software-based segmentation has been shown to greatly reduce risk, speed time-to-value, and deliver optimal security at a dramatically lower TCO than traditional approaches — which translates to a higher and faster ROI. This is not a futuristic vision — software-based segmentation has arrived, and is delivering these benefits to organizations across a wide range of sectors right now.

A STUDY IN IT EVOLUTION

The history of technology is one of constant improvement, simplification and falling costs. Segmentation is no exception.

Consider the example of storage, which in barely two decades evolved from floppy disks to flash drives, then network attached (NAS) and finally cloud storage. Or compute runtime, which evolved from servers to virtual machines, cloud computing to containers, and ultimately to serverless computing. In each case the key drivers were cost savings and increased flexibility. And of course, rapid advancements in technology made it possible.

The evolution of segmentation from physical firewall appliances to distributed firewalls, abstracted from the network, is similar. And the drivers are the same: reduced cost and increased flexibility (which translates to velocity of deployment), while at the same time steadily improving the effectiveness of security policies with a more granular zero trust approach.

It's time for IT teams to embrace a new model for security by segmentation, as they clearly have in other technology sectors. The physical firewall for segmentation is headed the way of the floppy disk.

WANT TO SEE HOW MUCH YOU CAN SAVE ON FIREWALLS?

Get your Firewall Savings Report:

www.guardicore.com/firewall-cost-calculator

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