Akamai

WHITE PAPER

# Rethink Firewalls

## The compelling economic case for software-based segmentation

# Executive summary

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

# Introduction

Today, we see three converging forces driving demand for a more granular means of segmenting networks and individual assets. First, agile DevOps and other rapid delivery models are putting a premium on accelerated deployment of applications into production. Inevitably, this requires creating more secure zones with more precise policies. Second, as organizations migrate to the cloud and adopt hybrid IT infrastructures, their applications are often migrating among different environments, which increases inter-segment traffic throughout their network. And third, the rapid proliferation of applications due to agile development is creating an ever-increasing attack surface for hackers to target.

# Firewalls for segmentation: past their prime

Given these conditions, a strict reliance on VLANs and firewalls for segmentation purposes is becoming unsustainable. From a purely technical perspective, the configuration of multiple VLAN and firewall installations in a way that keeps pace with application development is both complex and cumbersome. 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 to implement, not only due to the upfront cost of firewalls and new hardware to support additional traffic, but also due to associated costs from the ongoing management, modifications, and maintenance of installations.

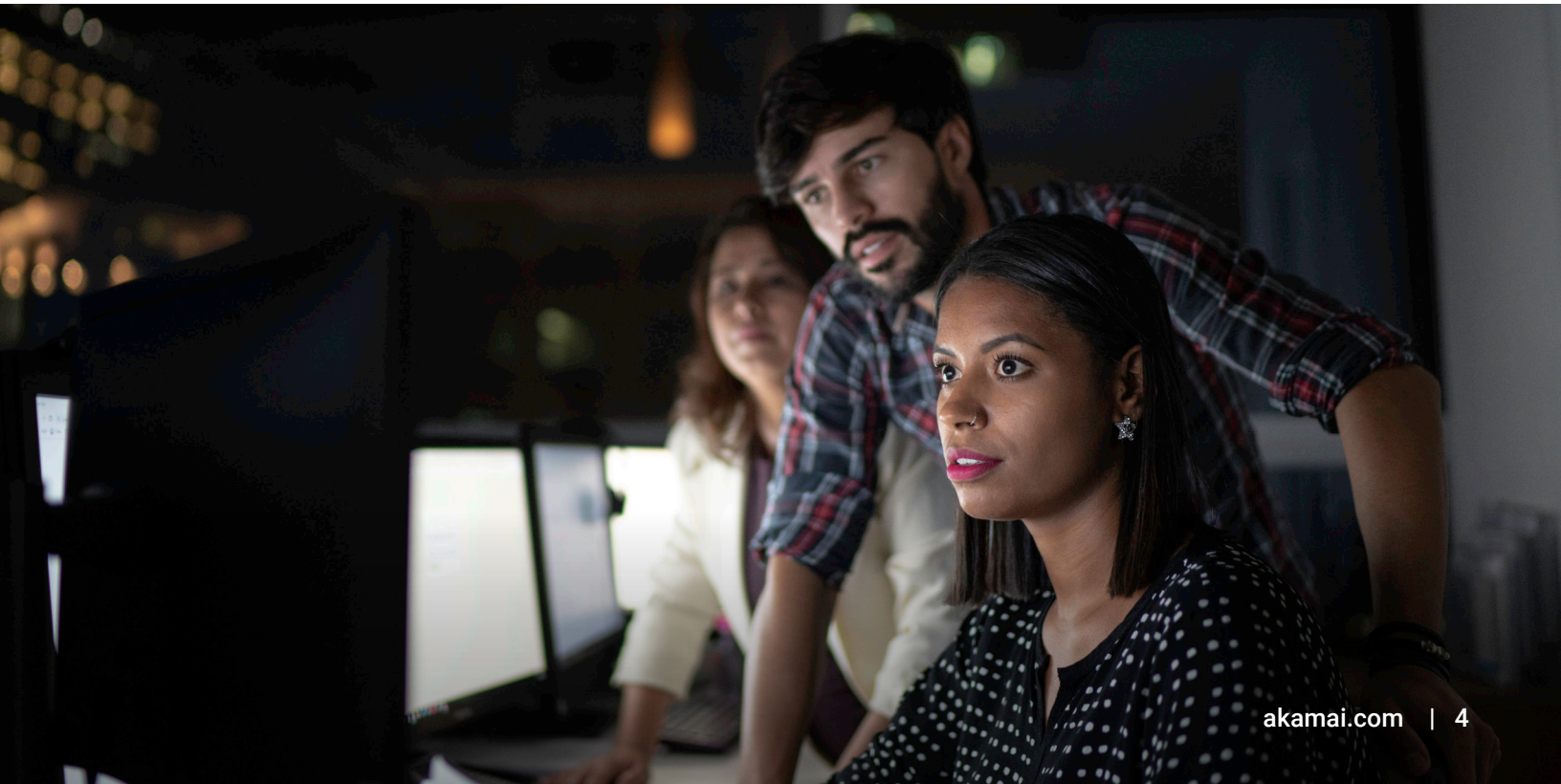
Simply put, traditional network segmentation approaches have hit a wall. In particular, as organizations seek to take advantage of dynamic cloud and hybrid environments, reliance on internal firewalling for security limits their agility, speed to policy creation and enforcement, and ability to securely scale their operations. The need for a modern, streamlined, less costly, and ultimately more effective segmentation alternative 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 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 associated 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, ESXi servers, and security policy creation. All 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.

An industry-leading example of a software-based segmentation solution is Akamai Guardicore Segmentation. Compared to the lengthy, costly, and complex process of VLAN firewall implementation, our software-based segmentation solution involves just three steps:

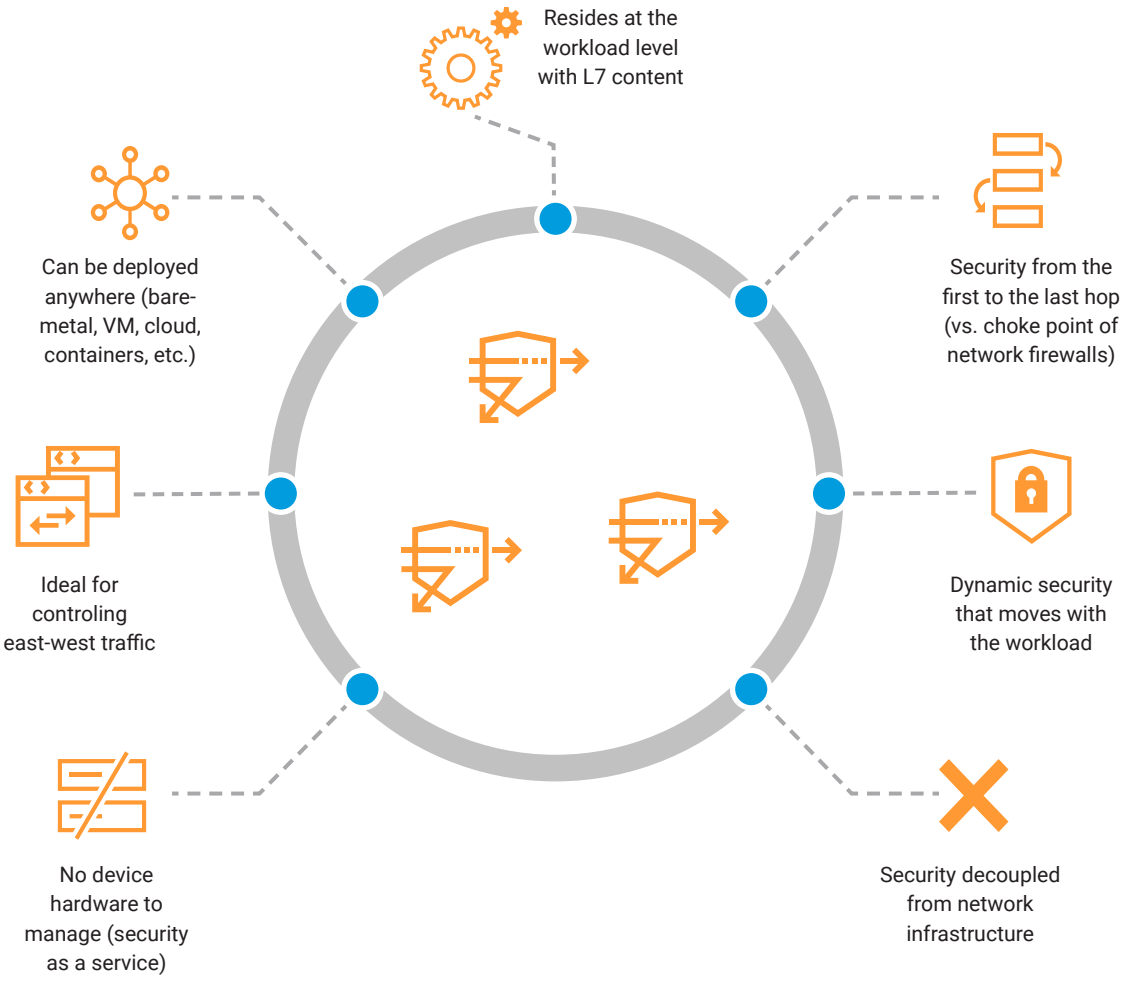
1. **Identify and label assets:** A major roadblock encountered during the traditional firewalling process is a lack of visibility into the assets that need to be secured. Akamai Guardicore Segmentation includes a visualization capability that enables operators to identify and label all the applications and their dependencies running throughout an organization's infrastructure.

2. **Visualize and group by label:** With contextual visibility attained, operators can then organize applications into logical groups based on their labels and map the dependencies among them. Our labeling process is very flexible, and allows you to group applications based on your own business context, using terminology you're already familiar with.

3. **Create policies:** Operators can then create granular security policies that dictate which applications are allowed to communicate with each other based on actual observed flows. Pre-built policy templates for common use cases simplify the process even further. Now, applications and workflows are effectively segmented from each other regardless of where they are within the environment.

Software-based segmentation is 10 or even 20 times faster to deploy compared to traditional firewalling, with fewer people needed, and virtually no downtime or disruption. Moreover, once you've started the visualization and 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



# Case study: Large food processor sees 85% savings on segmentation

A major U.S. 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 Akamai'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 three-year period, compared to securing VLANs with a leading firewall supplier. Specifically:

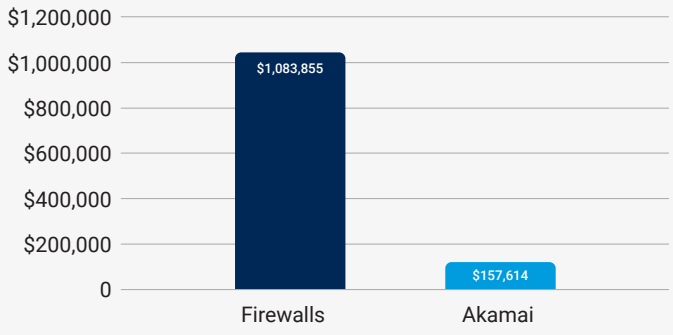
- The cost of licensing Akamai Guardicore Segmentation was 55% lower than the cost of hardware for a VLAN-firewall implementation.
- The cost of labor, based on an assumption of $2,000 per week, was a full 93% lower with Akamai than for a VLAN project with far longer duration.

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

**Firewall TCO***
**$1,083,855**

**Akamai TCO***
**$157,614**
-$926,241

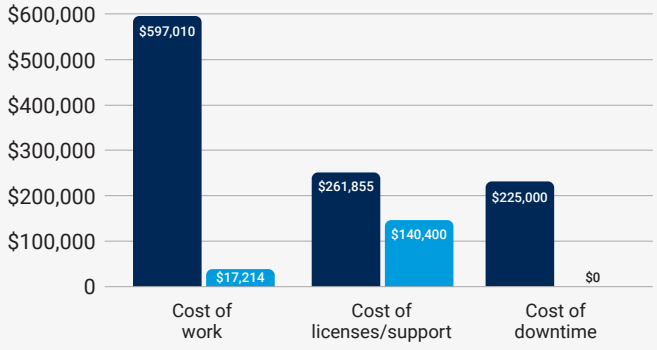
* Cost over a 3-year period




**Akamai cost of work***
**$17,214**
-$579,796

**Akamai cost of licenses/support***
**$140,400**
-$121,455

**Akamai 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 segmentation makes you more secure, more quickly enabling security teams to keep up with the pace of agile DevOps application deployment and ensure that every application in production is properly secured. It also means that fewer resources — technical or human — are tied up in segmentation projects for lengthy periods. Teams can focus their time on other important initiatives.

**Dramatically lower total cost of ownership:** This is the real bottom line, and probably the most significant advantage from a business perspective. 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.

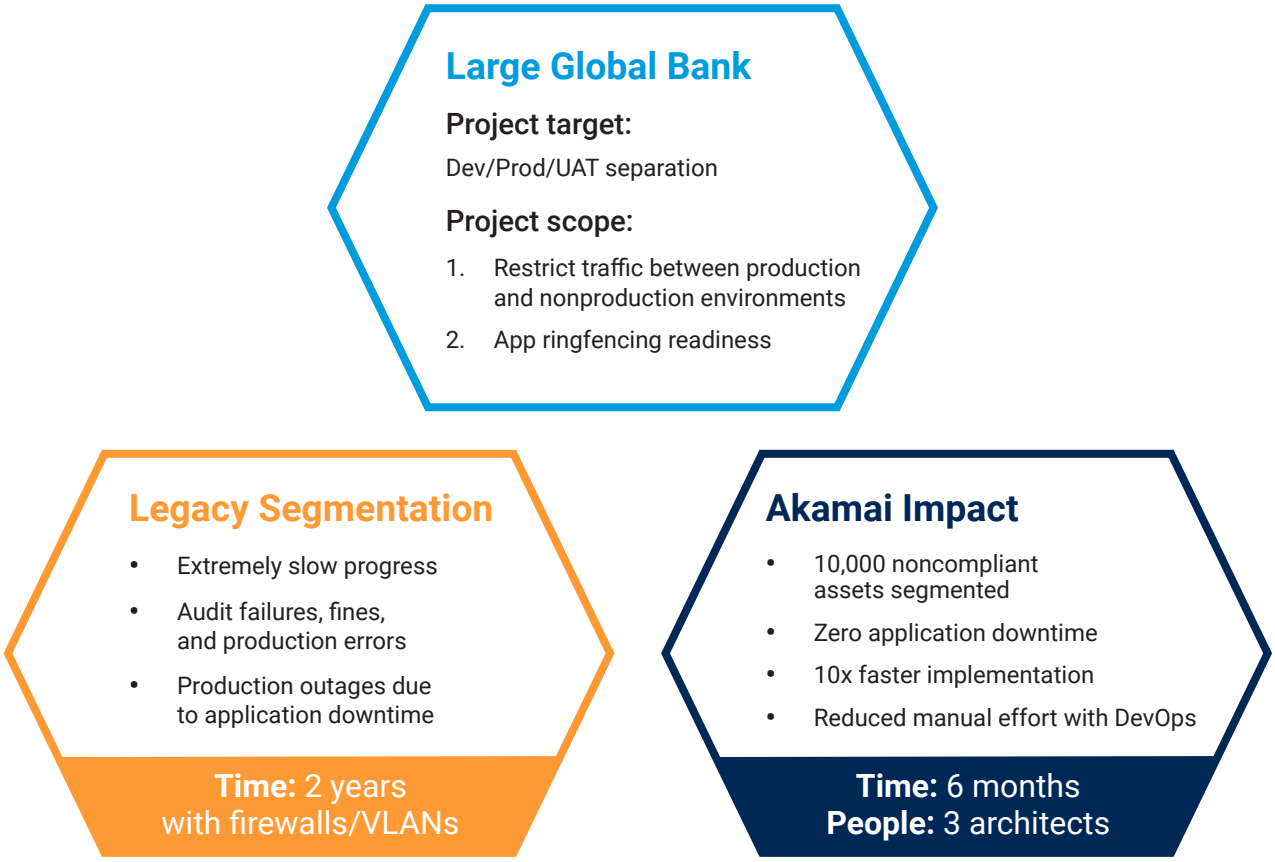
By these measures alone, in a side-by-side comparison between software-based segmentation and a firewall solution for 10 application segments, the Akamai approach was shown to deliver a potential 85% total savings, amounting close to $1 million.

Of course, though one can expect to see measurable savings in the first week of deployment, the total cost of ownership (TCO) means much more than just the upfront purchase price or ongoing out-of-pocket costs. Though the full 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 noncompliance. 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 for those who opt for a software-based segmentation solution.

# Case study: Large global bank, facing compliance sanctions, turns to Akamai Guardicore Segmentation

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 noncompliance, in addition to unsustainably high implementation costs.

The IT team quickly looked into alternative solutions and was impressed with the level of automation Akamai could bring to bear on its security operations. The bank deployed Akamai Guardicore Segmentation 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.



# 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 the necessary balance between security and agility, organizations need to be able to secure their digital assets not just at the L4 network level, but at the L7 application level — specifically, individual processes. And for that purpose, firewalls are not only ill-suited, but they actually stand in the way of progress. Attempting granular segmentation with firewalls is a massive drain on resources — human, technical, and financial.

When compared to firewalls, software-based segmentation has been shown to greatly reduce security risk and overall time to value at a dramatically lower TCO than traditional approaches — which translates to a greater ROI achieved faster. This is not a futuristic vision — software-based segmentation has arrived, and it 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 storage (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 software-based distributed firewalls, abstracted from the network, is similar. And the underlying 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 approach that supports Zero Trust.

It's time for network and security teams to embrace a new model for securing with 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 our solution in action?
## Request a demo today: akamai.com/guardicore