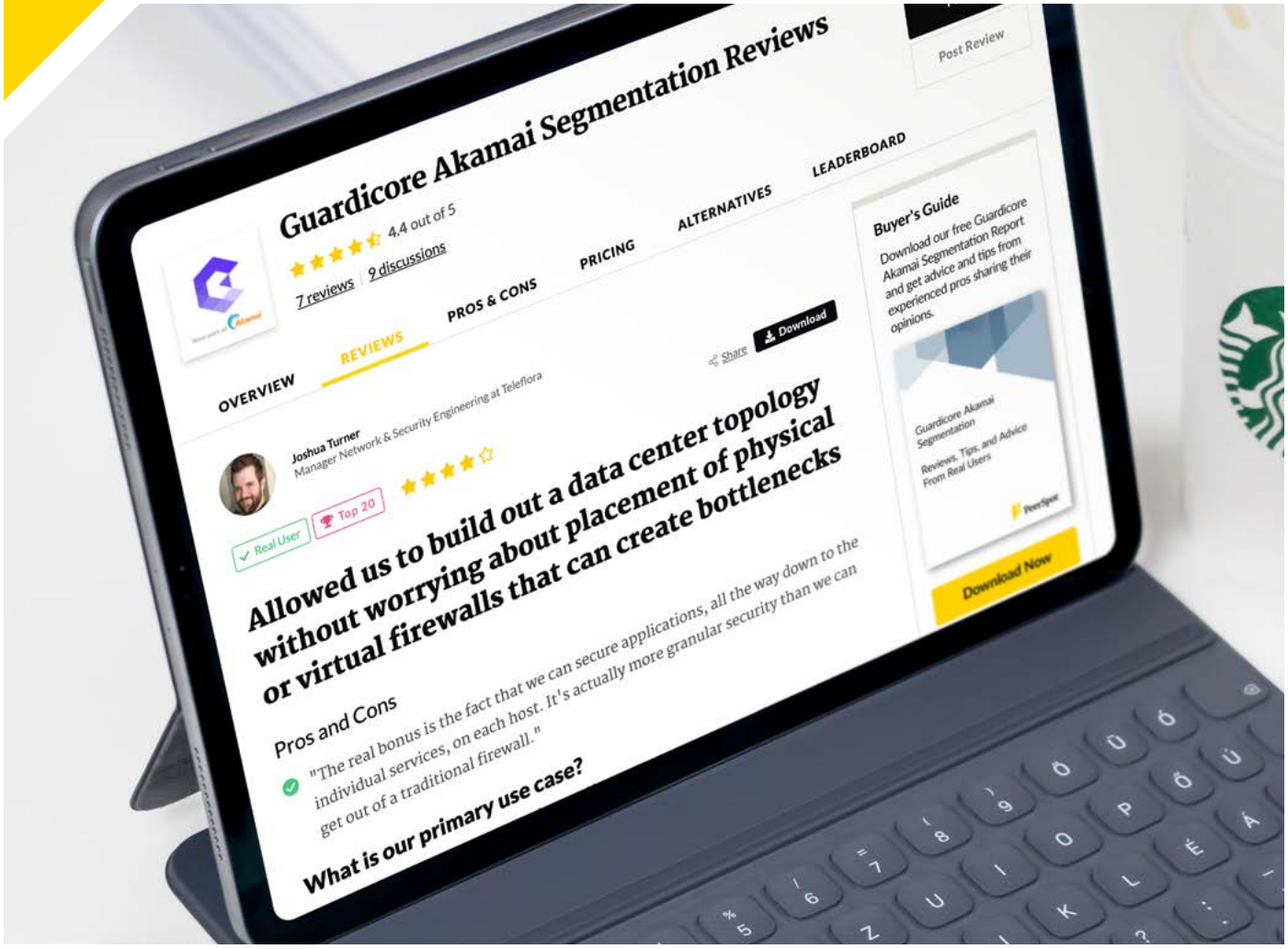
PeerPaper™ Report 2022

Based on real user reviews of Guardicore Akamai Segmentation

Getting to Effective Zero Trust Network Segmentation



PeerSpot

CSO FROM IDG

Contents

Introduction

Zero Trust network segmentation is the creation of zones in data centers and cloud environments to isolate workloads from one another for added security. This allows system administrators to control network traffic between the workloads with the purpose of reducing the networking attack surface and better containing breaches. Regulatory compliance improves at the same time. Zero Trust network segmentation policies can be formulated according to environment type, regulatory scope, application, and infrastructure tier.

An emerging security best practice, Zero Trust network segmentation offers several advantages over network segmentation and application segmentation, separating security controls from infrastructure. This allows organizations to extend visibility and protection anywhere a threat is anticipated, an essential capability for those adopting cloud services and other options that make traditional perimeter security obsolete.

This extended visibility makes it easier to discern sanctioned activity from unsanctioned. The increased visibility allows for the discovery and visualization of applications, workloads, and network flows. With Zero Trust network segmentation, the organization can more easily apply the principle of least privilege in these environments, building a stronger defense position. Figure 1 shows the difference between a traditional network segment and Zero Trust network segmentation.

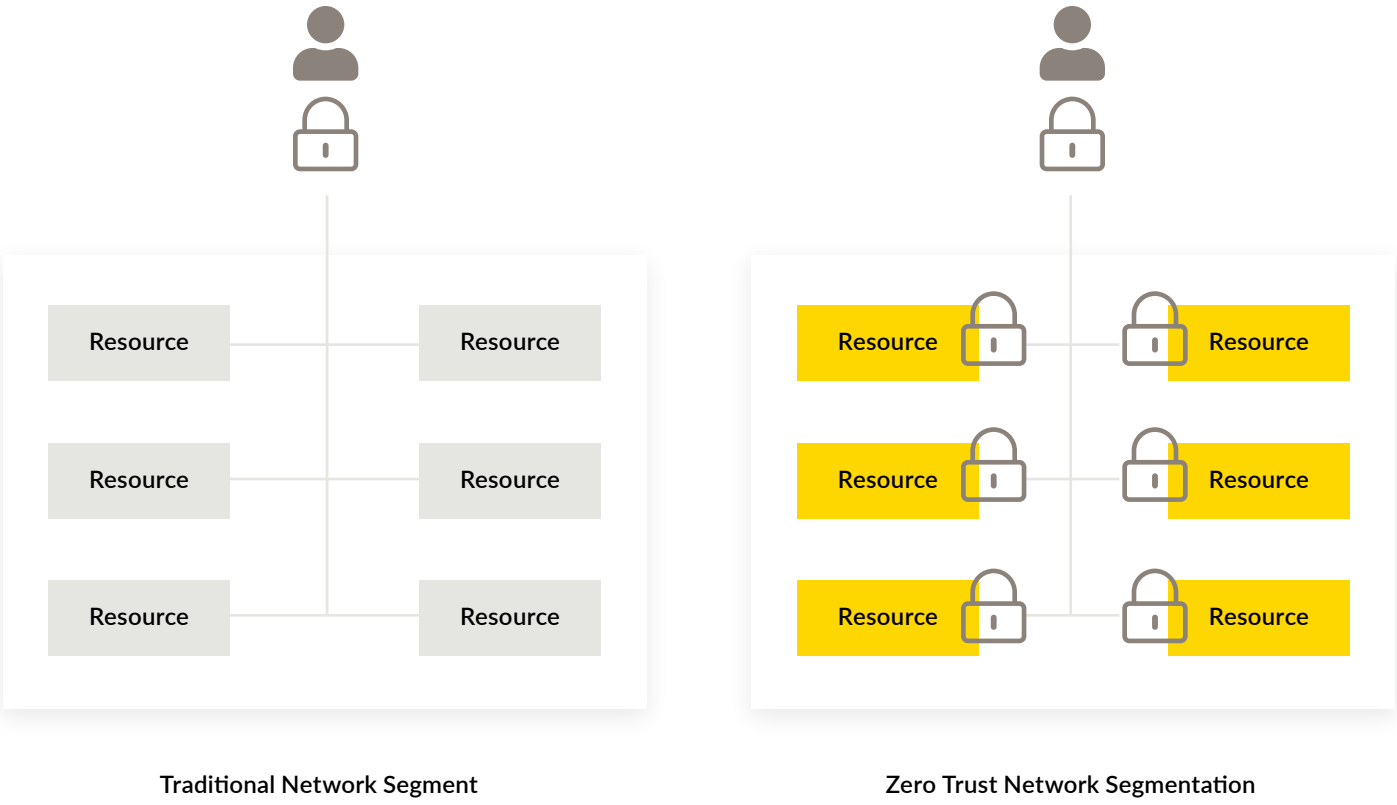


Figure 1 – Contrasting a traditional network segment with a Zero Trust segmented network.

The right Zero Trust network segmentation solution will be one that enables versatility in security policy and security operations, according to PeerSpot members who use Guardicore Akamai Segmentation. The solution must be granular in nature, offering strong visibility and threat intelligence capabilities. The solution should contribute to efficient operations – being easy to deploy and manage, with support for Zero Trust network segmentation across a broad range of computing and network environments.

Versatility in Security Policy and Operations

As the adoption of cloud infrastructure and containers increases, the value of traditional perimeter-focused security wanes, yielding to a growing need for visibility into lateral movement among data center and cloud assets. Zero Trust network segmentation and its inherent granularity offer several benefits in this scenario. As a Network and Security Engineer at the small tech company CS-Novidy put it, Guardicore's deception features provide a rich telemetry of lured origins and are a "great resource for any active defense strategy."

Prevent Lateral Movement

Zero Trust network segmentation isolates workloads and reduces attack surfaces, making it more difficult for attackers to move laterally across networks. A Senior Network Security Engineer at a tech services company with over 50 employees spoke to this issue when he explained that Guardicore provides visibility of the entire data center and helps stop lateral movement of attacks.

A Network & Security Engineering Manager at Teleflora, a retailer with over 500 employees, uses the tool to segregate the company's various environments: staging, production, QA, and applications. He said, "We are essentially replacing our traditional, internal firewalls and depending completely on Guardicore to secure all of our applications."

> **"...Guardicore provides visibility of the entire data center and helps stop lateral movement of attacks."**
>
> Read review »

Visibility

Visibility is a vital aspect of effective Zero Trust network segmentation solutions. Security teams use Zero Trust network segmentation to enhance discovery, enabling the organization to achieve more extensive line of sight into the workings of their environments. This deeper insight offers a more comprehensive view and understanding of activity. The resulting clarity better enables security teams to discern good from bad activity and to visualize and address potential gaps and threats.

The CTO at a consumer goods company with more than 500 employees considers visibility of processes and connections to be Centra's most valuable feature. He said, "Guardicore gives us a view of each connection that exists on each server. Using this, we can identify things like unused connections, or processes that are using too much in terms of resources." This knowledge provides his team with the opportunity to block such connections and in turn, improve server performance.

The product offers good visibility of what is going on in the network and the connections that the servers are making, said a Cybersecurity Coordinator at MONEX, a financial services firm with over 1,000 employees. At MONEX, Guardicore Akamai Segmentation has been useful in Zero Trust network segmentation of principal payment applications like SWIFT. He revealed, "It has even provided good information about some of the connections that I am making in and out of the system. So, we are able to correct some behaviors and kill some applications that are suspicious to the infrastructure."

> **"...we are able to correct some behaviors and kill some applications that are suspicious to the infrastructure."**
>
> Read review »

"It's actually more granular security than we can get out of a traditional firewall."

Read review »

Granularity

In tandem with deeper insights, Zero Trust network segmentation provides the ability to manage with greater effectiveness by applying more granular controls. The added detail and control are indispensable, as many organizations are adopting cloud services and new deployment options. To this point, the Teleflora network manager explained that Guardicore has allowed his company to secure older applications on a granular basis. "The real bonus is the fact that we can secure applications, all the way down to the individual services, on each host," he said. "It's actually more granular security than we can get out of a traditional firewall."

Generates alerts in real time

Monitoring and Alerts

Zero Trust network segmentation allows organizations to generate alerts in real time when policy violations are detected. The technology then blocks attempts at using compromised assets for lateral movement. Security teams need a solution that can detect applications that are behaving inappropriately and distinguish between misconfigurations and potential attacks. For the MONEX Cybersecurity Coordinator, getting alerts about suspicious behaviors on systems enabled his team to address threats immediately. He identified this as one of the main benefits of the product.

"From day one, you get threat intelligence. It will immediately block active threats, which has been useful."

Read review »

Threat Intelligence

The ability to monitor activity at a granular level and systematically gather data is a "must-have" as organizations aim to better understand their gaps and where and how threats might occur. An Infrastructure Analyst/Developer at a university with over 1,000 employees identified the overview of the firewall as Guardicore Akamai Segmentation's most valuable feature.

Specifically, as he said, "It provides something that we don't normally have. Normally, we have an external firewall and a firewall to machines, but we don't have an overview of all the traffic. We don't have any way of aggregating it to look at it more easily. Guardicore Akamai Segmentation is a visual tool where we can view this, but we also can delve down into logs and look at what is happening more easily." He then added, "From day one, you get threat intelligence. It will immediately block active threats, which has been useful."

Stops lateral movement of attacks

Internal/External Protection

Protecting assets from unauthorized internal or external access is one of the most important elements of a Zero Trust network segmentation solution. The consumer goods CTO noted that his company has a data center with approximately 200 servers running Nutanix. "We wanted to protect these servers from both internal and external attacks," he said. "By implementing Guardicore Akamai Segmentation, it has given us defense against attacks from the outside, as well as those that originate from inside of the organization."

Ease of Deployment and Management

A Zero Trust network segmentation solution should be easy to deploy and manage. Even if a solution delivers the desired features and functions, it is not optimal if it adds to administrative overhead. Speaking to this concern, a Corporate Operations Manager at Strathclyde business school, an educational organization with over 1,000 employees, remarked, "Guardicore Akamai Segmentation is much better than our previous solution, which was a bit of a nightmare to administer and look after. In that respect, this solution is much better, as there is less chance of things going wrong."

Easy to Install and Manage

"It's very easy to install," said the MONEX Cybersecurity Coordinator. It does not have any problems with other applications. With ease of installation, he added, "It does not take you a long time to build rules or have control of your agents."

Ease of management also factored into Strathclyde's Corporate Operations Manager's views on his solution. He shared, "We like the centralized management of the firewalls. Until we installed Guardicore Akamai Segmentation, we managed all our firewalls individually, so making changes was complicated, difficult, and time-consuming." The univer-

"In terms of agility, Guardicore Akamai Segmentation is massively easier to control and manage."

Read review »

sity Infrastructure Analyst concurred, observing, "In terms of agility, Guardicore Akamai Segmentation is massively easier to control and manage."

Ease of segmentation is a related quality sought after by system users. As the consumer goods CTO put it, "Its approach to implementing segmentation was very simple and straightforward. You can basically use it out-of-the-box." In particular, their use of Guardicore Akamai Segmentation's AI-powered segmentation functionality enables them to keep the time required to design segmentation to a minimum.

He then commented, "It gives us a large number of views and without that, you cannot design the system properly. The AI helps because it shows you what you need to do. Without the AI, either you will not be able to implement the system, or it will take a long time and be very difficult. For us, using this feature saved us a couple of months in implementation time."

"It is pretty simple overall to get a template and apply segmentation," said the university Infrastructure Analyst. He added, "You still need to think about how to apply it yourself to suit your needs, but it provides all the tools useful for that as well. The maps are useful. Using the templates to create rules gives you an easy start, then you can go in and refine it to suit your processes. Also, the Guardicore staff has been very helpful in helping us walk through the process and get what we needed out of the software."

The AI saves months in implementation time

Reduced the number of human resources

> "It is very quick to secure applications and systems. You can get an agent installed very quickly."
>
> Read review »

Speed to Results

PeerSpot members emphasized the importance of getting fast results with a Zero Trust network segmentation solution. For example, the MONEX Cybersecurity Coordinator shared, "It has results the next day after you install the agents, because now the agents report to the cloud. You have visibility right away of what is going on in your system that next day after you installed the agent."

He elaborated, saying, "If you installed 100 agents today, then tomorrow they will start reporting to the cloud. Also, you would have visibility regarding what is going on in those machines: Where are they communicating? What processes are being communicated? What are the available reports?"

The university Infrastructure Analyst offered additional examples of speed to results, saying, "It is very quick to secure applications and systems. You can get an agent installed very quickly. We started with 149 agents and will be adding another 100 agents over the next few weeks, as we move on to securing desktops as well as servers." In his experience, he can get results as soon as he has his aggregators up. "You can get them in a day," he revealed.

> "Guardicore Akamai Segmentation saves time when completing a segmentation project versus a traditional toolset."
>
> Read review »

Saves Time

A Zero Trust network segmentation that is easy to use should help save time in network management. This was the case for the Operations Manager at Strathclyde. He said, "Guardicore Akamai Segmentation saves a lot of time, approximately three to six months." The solution has reduced the number of human resources he needs to deploy security solutions. He went on to say, "We have two people working on segmentation rules as well as some agents taking care of the infrastructure. Before Guardicore Akamai Segmentation, we would have needed at least one more person."

The university Infrastructure Analyst similarly noted, "Guardicore Akamai Segmentation saves time when completing a segmentation project versus a traditional toolset. Since we already have a solution in place, we have a fitted process of removing the old segmentation and adding the new. However, you can run them in tandem so that is always a benefit; you can do it over time rather than as one big bang."

Support for a Broad Range of Environments

Networks and IT infrastructure tend to be heterogeneous and complex. As a result, it makes a great deal of sense for a Zero Trust network segmentation solution to support a wide variety of environments. A solution should be platform and location agnostic, able to support public and private clouds as well as legacy environments.

Virtual Machine (VM) support is also critical for success. In this use case, the university Infrastructure Analyst related, "We

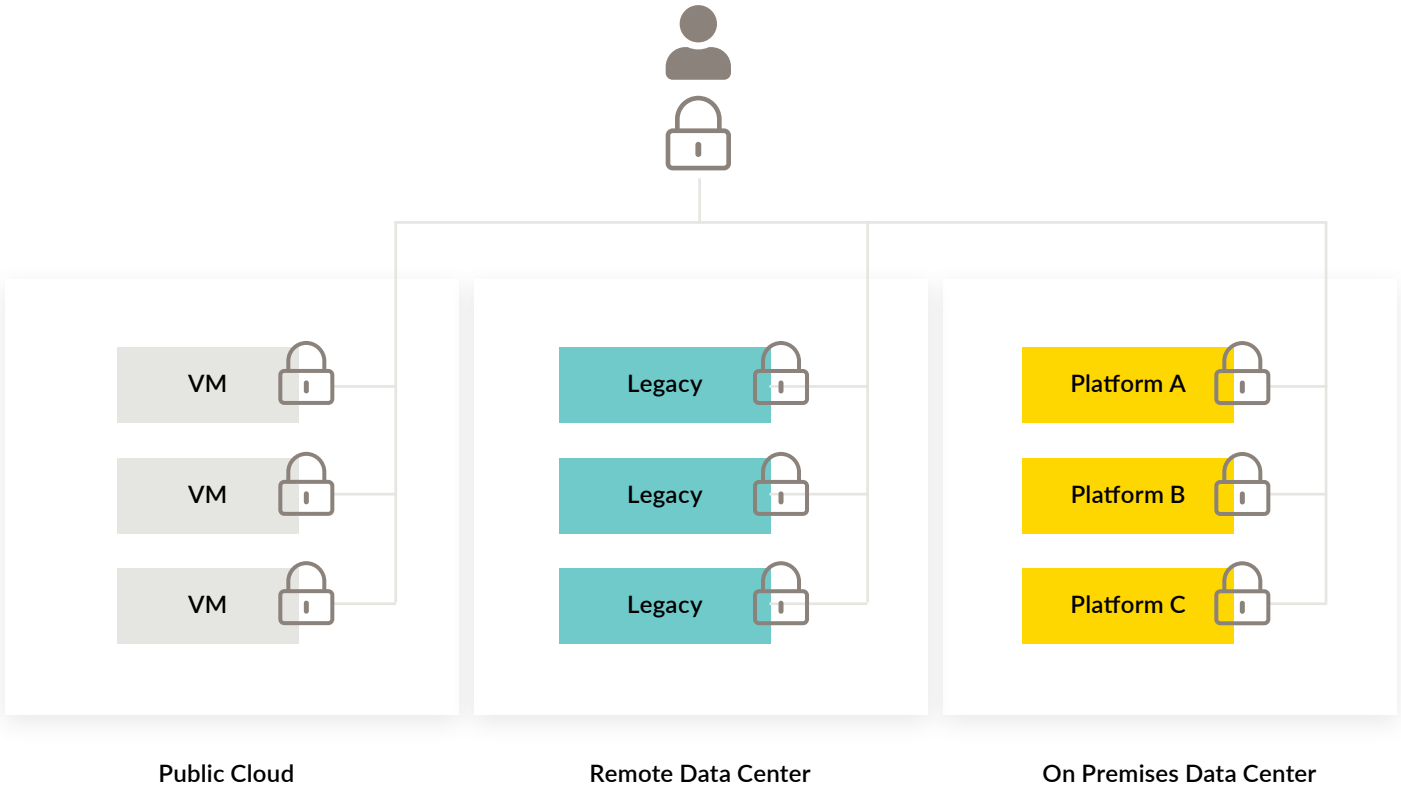


Figure 2 – Some of the diverse platforms and location requirements that must be supported by a Zero Trust network segmentation solution.

installed aggregated agents with help from the Guardicore staff who were very helpful. We installed agents on a lot of virtual machines. It wasn't really complex; it seemed pretty straightforward." Figure 2 depicts the level of variety that a Zero Trust network segmentation solution needs to support.

Public/Private Cloud

Workloads today often span public and private clouds, so Zero Trust network segmentation will ideally adapt easily to this pattern. The tech services Senior Network Security Engineer found this to be true with Guardicore Akamai Segmentation. He said, "This particular product has a deployment model both in public and private clouds and on-prem-

ises." His company is offering it to their customers, leading him to comment, "We have an advantage with this product in offering it 'both ways' on cloud and on-premises to meet the client's needs."

> "We have an advantage with this product in offering it 'both ways' on cloud and on-premises to meet the client's needs."
>
> Read review »

Legacy Environments

Cloud excitement aside, many legacy environments are here for the long term. They, too, need Zero Trust network segmentation, Strathclyde's Corporate Operations Manager found. He said, "We are planning to have the solution help cover legacy or end-of-support operating systems, like Win2003, AIX, Solaris, or RHEL, but we haven't done that yet." The consumer goods CTO shared this view. He said, "It is a benefit that Guardicore supports legacy operating systems, and I have used it with such servers."

It could be on the cloud, on-prem, or virtual

Platform Agnostic

"It does not have a dependency on a specific platform," said the MONEX Cybersecurity Coordinator. "It could be on the cloud, on-prem, or virtual. It works with most of the operating systems." The university Infrastructure Analyst had a comparable experience. He said, "The range of platforms and operating systems that the solution covers is good. It covers most of our operating systems, if not all. I don't think we have found anything so far that we have struggled to cover with it. We have been quite happy in that regard. Guardicore Akamai Segmentation is far superior in terms of

using local firewalls on its own." The consumer goods CTO simply said, "Guardicore supports the operating systems that we require. Primarily, it covers our Microsoft platform, but we have some Linux systems as well. We also used it to protect our SAP HANA database."

Location Agnostic

A Zero Trust network segmentation solution should also not "care" about where it's operating. The Teleflora network manager said it best when he commented, "The most valuable feature of this solution is the fact that it's pretty much agnostic to location. Right now, we have an on-prem data center that we manage, but if we start to migrate into different cloud locations or multiple different clouds, we can manage all the security between all of the servers and applications, through one platform. That's a future, forward-looking bonus of it."

He then shared that Guardicore Akamai Segmentation has allowed his company to build out an entire new data center topology without having to worry so much about where they place physical or virtual firewalls that can create bottlenecks. He said, "We can focus more on building a really fast and responsive network topology. Security devices, things like a traditional firewall, can often be a bandwidth or throughput bottleneck. But with Guardicore, since the firewall is running on every single server individually, and they're working together, you can just build a really big, fast, redundant network and not have to worry so much about those security bottlenecks."

> **"The range of platforms and operating systems that the solution covers is good. It covers most of our operating systems, if not all."**
>
> **Read review »**

Conclusion

As Zero Trust network segmentation becomes a standard security countermeasure, network managers and their counterparts in cybersecurity need solutions that deliver along multiple dimensions. As PeerSpot members who use Guardicore Akamai Segmentation discussed in their reviews, the right solution will be one that is easy to install and manage. It must save time and offer quick results. The solution needs to provide granular capabilities, along with threat intelligence and robust visibility into the network. And, it has to support Zero Trust network segmentation across multiple platforms, including legacy systems, public and private cloud and more. Equipped with a Zero Trust network segmentation solution that meets these criteria, network and security managers can efficiently defend digital assets against attackers who might otherwise be able to move laterally across the network.

About PeerSpot

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. PeerSpot provides technology professionals with a community platform to share information about enterprise solutions.

PeerSpot is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.peerspot.com

About Guardicore

Guardicore, now part of Akamai Technologies, delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation.