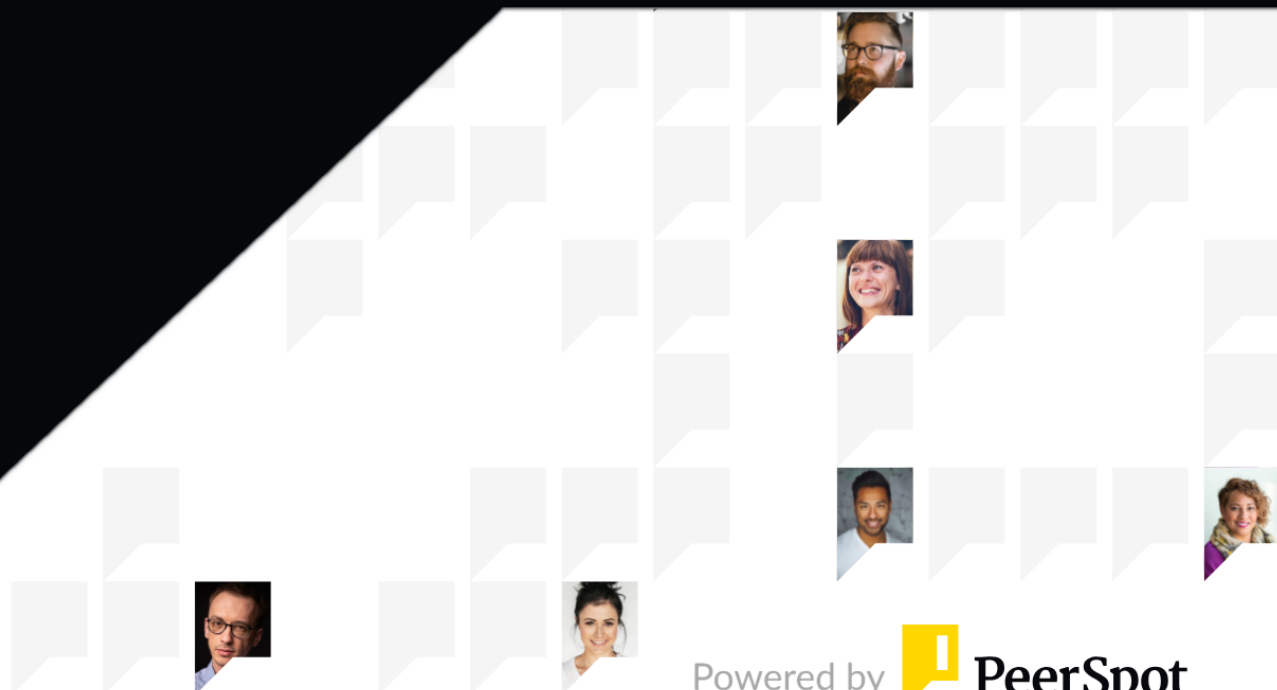




Akamai Guardicore Segmentation

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 27

Customer Service and Support..... 28 - 29

Other Advice..... 30 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Akamai Guardicore Segmentation

Akamai Guardicore Segmentation

Recap

Akamai Guardicore Segmentation offers extensive visibility and micro-segmentation capabilities, integrating seamlessly with diverse environments to enhance security measures. Organizations benefit from its platform agnosticism and centralized firewall management, maximizing protection and operational efficiency.

Known for its detailed network visibility, Akamai Guardicore Segmentation streamlines security operations across different platforms. It facilitates ease of policy creation and allows for effective segmentation, even of legacy systems. With advanced threat intelligence and real-time traffic monitoring, organizations optimize security and compliance, reducing attack surfaces through precise process and port control. This capability extends to seamless operation in environments like Kubernetes and data centers, implementing Zero Trust security models and server-to-server segmentation.

What are the key features?

- **Extensive visibility:** Offers comprehensive insight across network environments.
- **Platform agnosticism:** Operates effectively on multiple platforms.
- **Micro-segmentation:** Enables detailed control over network traffic.
- **Centralized management:** Simplifies firewall administration and monitoring.
- **Threat intelligence:** Incorporates AI for dynamic threat assessment.

What benefits or ROI should organizations seek?

- **Enhanced security:** Reduces attack surfaces and prevents lateral movements.
- **Operational efficiency:** Streamlines policy creation and enforcement.
- **Integration flexibility:** Aligns with diverse systems for seamless deployment.
- **Compliance achievement:** Supports adherence to industry standards.

In sectors like banking and financial services, Akamai Guardicore Segmentation is crucial for implementing Zero Trust models and enhancing server-to-server segmentation. These industries utilize its capabilities to replace traditional firewalls and manage complex environments, boosting security through application dependency mapping and optimized east-west traffic control.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Akamai Guardicore Segmentation is a very effective solution for organizations looking to strengthen their zero-trust security model, especially in complex hybrid environments.”



Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

- ✓ “After implementing Akamai Guardicore Segmentation, I can say that for most customers with whom we implement Guardicore, we see once we do micro-segmentation for an application that the possible connections that can be established on that application usually drop by 80%.”



Avner Nahum

Cybersecurity Consultant at a tech consulting company with 51-200 employees

- ✓ “Akamai Guardicore Segmentation is the tool that makes me sleeping well every day.”



Fernando Ortega

CISO at Paschoalotto

- ✓ “Akamai Guardicore Segmentation has impacted my organization positively because we find it difficult to remove the legacy systems, so it was very important to segment them from the rest of the network to protect them and protect the rest of our network.”



Ken Bauer

Senior Security Analyst at a retailer with 5,001-10,000 employees

- ✓ “It has significantly lowered our overall security risk and made our security much better.”



KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

- ✓ “The impact of Akamai Guardicore Segmentation is very important because it reduced risk for my corporation and organization.”



Irton Medina

Cybersecurity at Embraer

- ✓ “No one has asked for more, so I find the technical support in my region is pretty good.”



Verified user

Works at a wholesaler/distributor with 51-200 employees

What users had to say about valuable features:

“I usually recommend Akamai Guardicore Segmentation for larger companies, as we started to work with Guardicore before the acquisition and then moved to distribute Akamai. Akamai Guardicore Segmentation is not a simple solution for the Italian market because we are suffering from nanism; the majority of our companies have under 1,000 employees. Akamai Guardicore Segmentation is enterprise software, but they are pretty good in that area.

Regarding their interface, I cannot answer on technical issues or aspects because I am the sales manager, and here we show the characteristics of the software, but we do not make any demonstration of the product because we are a distributor..”

Verified user

[Read full review](#) 

Works at a wholesaler/distributor with 51-200 employees

“The best features of Akamai Guardicore Segmentation are maps and network logs. I think the analysis of logs and hits in Akamai Guardicore Segmentation is fantastic.

“The impact of Akamai Guardicore Segmentation is very important because it reduced risk for my corporation and organization. It is very important.

“Akamai Guardicore Segmentation reduced risk because it blocked malicious ransomware and uninspected traffic. I appreciate this. It is very good.

“Akamai Guardicore Segmentation reduces risk, and the configuration is very easy, among other things..”

Irton Medina

Cybersecurity at Embracon

[Read full review](#) 

“Akamai Guardicore Segmentation is very intuitive. If you're used to firewalls, you're also used to this product because it has the same look and feel.

“Automation is a nice feature that not many customers are using. Companies can set up automation so that if they see something that's not good, it can be automatically remediated. That's a feature that many customers would like.

“The visibility feature is actually where this technology is much better than firewalls. With firewalls you make policy, but you don't know why you're making the policy because you need to ask somebody about what kind of policy they need. With Akamai Guardicore Segmentation, you can actually see what's going on and you can make your policy without asking any application owner what to make. You're actually accepting a policy instead of building a policy..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“One of the best features of Akamai Guardicore Segmentation is its real-time visibility and visualization capabilities. It provides a detailed map of all east-west traffic, which is very helpful for both security and troubleshooting. Another key feature is application dependency mapping, which visually shows the communication flows between servers. This helps in understanding the complex environments and designing accurate segmentation policies.

“The granular micro-segmentation capability is also very powerful. We can create a policy based on labels such as application, environment, or role, allowing only required communication and blocking everything else, which significantly reduces the lateral movement risk.

“Additionally, the agent-based deployment is lightweight and works well across hybrid environments, including on-premises and cloud, making it flexible and easy to scale. Overall, the combination of visibility, visualization, and fine-grained control makes it a very effective micro-segmentation solution..”

Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

“More than twenty ring-fences implemented with Akamai Guardicore Segmentation have produced significant results with a three-hundred-sixty-degree vision of all the network traffic including the biggest system that we hold today.

“The best feature Akamai Guardicore Segmentation offers is great threat intelligence. Threat intelligence stands out to me as a best feature of Akamai Guardicore Segmentation because you are ready, for example, for ransomware attacks and lateral movements. I am very happy with the solution.

“In addition to threat intelligence, I have other ring-fences also. The way that Akamai Guardicore Segmentation holds the segmentation in the simplest way, giving the best visibility, is really the best thing for me.

“Akamai Guardicore Segmentation has positively impacted my organization by improving security because it increased the perimeters and the breaks in small perimeters and also giving me visibility over three hundred sixty degrees over the network.

“Since implementing Akamai Guardicore Segmentation, I have seen specific outcomes such as reducing incidents because only the tight traffic is really allowed, so you reduce the possibilities of issues and also increase the security..”

Fernando Ortega

CISO at Paschoalotto

[Read full review](#) 

Besides the visibility that I have mentioned about my use case with Akamai Guardicore Segmentation, we can also create rules. If we think that one specific namespace should not communicate with another namespace, we are able to create rules on Guardicore to avoid that communication, or not necessarily only from one namespace to the other, but from one specific port from the source to one specific port to the target, so we can also build those types of rules, and that really helps improve security for customers.

In general, I would say that the best features that Akamai Guardicore Segmentation offers include visibility and the ability to have Layer 7 visibility, which means that we are not only looking for source IPs and ports and target source target IPs and ports, but we are also looking for services. We are able to see even the service that we can create rules for, allowing from server A one specific service to communicate with server B, but if some other service tries to do that communication, it will be blocked, making that a great feature of Guardicore segmentation. There is also the deception model they have, which is the Honeypot model. Once we have one rule that is blocked for some specific ports, we can intercept an insider threat that tries to do RDP to one server that should not happen. With the deception model, that communication is blocked, and the insider is sent to a Honeypot server where they think they have established that communication and may try to add some script there. Guardicore adds logs and creates an incident, so we can see what that communication has done and how someone tried to compromise the environment.

“After implementing Akamai Guardicore Segmentation, I can say that for most customers with whom we implement Guardicore, we see once we do micro-segmentation for an application that the connection—possible connections that can be established on that application—usually drops by 80%. If we map out the proper communications that one application should have and create rules to apply the proper blocking, we see one application that could have a hundred thousand different types of communications, and after micro-segmentation, it can have only twenty thousand, thereby significantly increasing the security posture.

“In day-to-day operations, we usually don't have any impact, which is the idea of Guardicore. Once we have the rules in place, we only allow the communication that is supposed to happen. This is why we increase the security posture, but we don't

impact applications usability and anything else. For day-to-day operation and risk management, as I have mentioned, we typically reduce the communications that we can have with a specific application, so if a customer's environment is compromised, usually we can guarantee that with Guardicore segmentation, if we have the proper rules in place, other applications will not be compromised, and the communication will stay only inside that specific application. .”

Avner Nahum

Cybersecurity Consultant at a tech consulting company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

As I mentioned, being a consultant and my company being a partner with Guardicore, we decided to go with Guardicore after evaluating options such as Illumio, which we found to be less robust compared to Guardicore.

Avner Nahum

Cybersecurity Consultant at a tech consulting company with 51-200 employees

[Read full review](#) 

“I think it is hard to say if it is the best option on the market at the moment because I do not know a lot of alternatives in that area. They appear to be the kind of solution that stands out; even though Guardicore is not as famous as CyberArk, they are pretty known for what they do..”

Verified user

Works at a wholesaler/distributor with 51-200 employees

[Read full review](#) 

“Illumio is the biggest competitor. They are not using a kernel module. Akamai Guardicore Segmentation has much better visibility and has a more firewall style look and feel in how you use the product compared to Illumio..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“Akamai is much better than other solutions, such as ColorTokens and Illumio. It is more user-friendly and has more features. In fact, Illumio is actually implementing a lot of the features that Guardicore has had for years..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“This product did not replace a similar system. Also, I did not require human resources for this same task. Our company is approximately 70 years old and our network started very small. As the company grew, we maintained the same flat network that included both the data center and the users. When I looked at it, I considered two solutions for separating them. The first was the traditional firewall and a physical LAN, whereas the second approach was using Guardicore. I felt that this was the easier approach..”

Ehud Huminer

CTO at a consumer goods company with 501-1,000 employees

[Read full review](#) 

“We generally used internal firewalls on individual servers with no solution, in terms of overseeing all the firewalls.

In terms of agility, Guardicore Centra is massively easier to control and manage. The security is good. With just the network logs, you get a better view of any active threats rather than in normal firewalls where you may not find out until sometimes after the fact. You can get notified as well..”

Verified user

Infrastructure Analyst/Developer at a university with 1,001-5,000 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Akamai Guardicore Segmentation is very flexible. You don't need to change anything in the network because it's not a network thing. That's the nicest thing..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“We get an added layer of protection and user analytics that we can give to our directors in the company, so they can be more confident that things are being managed correctly..”

Verified user

Corporate Operations Manager at University of Strathclyde

[Read full review](#) 

“It has saved us a lot of time. We can secure around 500 systems. We are not growing in personnel. So, with our current personnel, I have been able to secure all the systems.

Guardicore Centra has reduced the number of human resources needed to deploy security solutions. We have two people working on segmentation rules as well as some agents taking care of the infrastructure. Before Guardicore Centra, we would have needed at least one more person..”

Jose Luis Guzman

Cybersecurity Coordinator at MONEX

[Read full review](#) 

“I know the ROI is going to be there because I know what the future's going to look like. The only reason we haven't seen as much as we possibly could have is all on us moving slowly. It's not anything to do with Guardicore. I'm really hopeful for the future with them. But right now we've only really secured a handful of applications. That's all gone really well, but we definitely have not realized its full potential. We've got a lot of older applications and it takes time to get people to agree to rebuild the server and put the agent on it.

We're trying to shift all of our servers. Instead of applying it in place, we're actually trying to go through a process of rebuilding all of our servers. During that process we'll move an application from an old server to a new one, put the agent on it, put it in the new network, and then it will be a Guardicore protected area. That's a slow process that we have imposed on ourselves. I see the light at the end of the tunnel. I think it's going to be a great solution but we are far from the end of the road with realizing all the benefits. That's just a result of taking our time and the plan that we created for ourselves..”

Joshua Turner

Manager Network & Security Engineering at Teleflora

[Read full review](#) 

“We do have ROI. First, one client found theft of data that alone justified to the client the cost. They invested heavily, well over a \$100,000 in Guardicore. That was a big purchase with an extensive setup. That discovery led to court cases. Guardicore provided evidence that they required. It was invaluable.

The second, in terms of the ROI, was for clients using Guardicore for the first time. We showed clients what occurs during patch updates, Windows updates, anti-virus updates, etc. Guardicore shows the traffic. You see your anti-virus going through the updates. Some clients they thought they were being attacked until we showed them that these are the patch monitoring servers.

For many years, clients set up updates. They do change control. They set Guardicore up, they check the lock, and they assume its all done. Guardicore shows them that it was done. The clients have proof that their applications will be filtered appropriately.

In terms of the return on investment, it was an invaluable tool to demonstrate that the client's internal practices will be implemented automatically. That blew away a lot of clients the first time they saw it. .”

Fidel Deforte

Solutions Architect at Alturna-Tech

[Read full review](#) 

Use Case

“We were using Akamai Guardicore Segmentation for micro-segmentation with Zero Trust. It's a process-level segmentation that functions just like a firewall..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“My main use case for Akamai Guardicore Segmentation is for big micro-segmentation at my company. A specific example of how I use micro-segmentation with Akamai Guardicore Segmentation in my company is the segmentation of big broadcast domains, where with this I could segregate the front end, the back end, backup networks, and out-of-band networks for administration. I have many cases with jumper services also, so many cases that we could mention working with Akamai Guardicore Segmentation..”

Fernando Ortega

CISO at Paschoalotto

[Read full review](#) 

“Our main use case for Akamai Guardicore Segmentation is to implement micro-segmentation and Zero Trust security across hybrid environments, including both on-premises and cloud workloads. We primarily use it to gain visibility into east-west traffic to control the communication between application and servers, which helps in reducing the risk of lateral movement in case of security breach. Additionally, we use it for application dependency mapping to understand how workloads interact, creating granular segmentation policies based on application, environment, and role, improving compliance posture, especially for banking and financial customers. Overall, it helps us to move from traditional perimeter-based security to more workload-level security approach..”

Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

My main use case for Akamai Guardicore Segmentation is related to Kubernetes instrumentation and visibility, although it is difficult to specify a main use case. When I work with Kubernetes, it is a very dynamic environment where we have pods that are going up and down all the time, and most of the customers don't have visibility about how those pods communicate between themselves or what type of service they consume outside.

By doing instrumentation in Kubernetes, which I have done already, even in OpenShift for on-premise environments and also on Azure, we are able to see all the pods that go up and down and all the communication that they establish inside the pod and outside the Kubernetes environment. .”

Avner Nahum

Cybersecurity Consultant at a tech consulting company with 51-200 employees

[Read full review](#) 

“I usually recommend Akamai Guardicore Segmentation for larger companies, as we started to work with Guardicore before the acquisition and then moved to distribute Akamai. Akamai Guardicore Segmentation is not a simple solution for the Italian market because we are suffering from nanism; the majority of our companies have under 1,000 employees. Akamai Guardicore Segmentation is enterprise software, but they are pretty good in that area.

It is more suitable for bigger companies. The reasons are not solely about pricing; it is also about the knowledge of the security manager in companies across Italy. For example, a small company with 500 employees might have a limited budget for cybersecurity and typically does not consider micro-segmentation as a primary solution. They may manage cybersecurity issues effectively with their existing LAN setup until they grow larger and face more complexity, which is why micro-segmentation becomes necessary. However, in Italy, it is not as well-known as in other markets due to the customer base..”

Verified user

Works at a wholesaler/distributor with 51-200 employees

[Read full review](#) 

“I use Akamai Guardicore Segmentation to block lateral movement of malicious software like ransomware. This is very important to protect my business and my corporation.

“I create labels for any assets to create rule sets in Guardicore Center with the configuration.

“The logs and network logs provide visibility that is very important for my business and my corporate entity. We use microsegmentation by environment. I do segmentation for production, homologation, and development. It is very important.

“Today, I have segmentation for Kubernetes in Guardicore, but I have problems with Guardicore with segmentation for Kubernetes because it is connected to SaaS. This is very important because we have projects starting in Kubernetes in my enterprise.

“Akamai Guardicore Segmentation is deployed in my organization on a hybrid cloud because 99% is on a private cloud computer..”

Irton Medina

Cybersecurity at Embracon

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“At the moment, I have no issues with documentation, integration with third-party solutions, or the initial setup; everything is pretty good, although you can always do more..”

Verified user

[Read full review](#) 

Works at a wholesaler/distributor with 51-200 employees

“Akamai Guardicore Segmentation's deployment is smooth. The deployment team promised us that the implementation would be completed in three weeks, but the product was available within two weeks. .”

Matthias Kropf

[Read full review](#) 

Senior Expert Enterprise Architecture at a manufacturing company with 10,001+ employees

“I would rate my experience with the initial setup an eight out of ten, with ten being easy.

It was pretty straightforward. It didn't take too long to deploy. And it was roughly done within an hour. So implementation isn't overly complex..”

Uday Varma

[Read full review](#) 

Solution Architect at a tech services company with 1,001-5,000 employees

“The initial setup is pretty straightforward.

The only thing that matters is that the customers have a strong plan, a good strategy, and a high-level and low-level design. The most exhausting part will be labeling all of your systems. And if the customer in this situation has around 1000 servers, that may be time-consuming..”

Verified user

[Read full review](#) 

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

“Guardicore Centra's setup was straightforward and I would rate it a seven out of ten. The tool's setup is straightforward as long as you identify the servers and establish the right processes. The tool came with an installation guide and setup took about four to five hours to complete. The deployment depends on the solution size and if the POC is small, the setup is easier and quicker. If you plan for enterprise-wide deployment, then you need to do capacity sizing and planning..”

Verified user[Read full review](#) 

Specialist Master - Cyber Risk at a consultancy with 10,001+ employees

“I would rate my experience with the initial setup a seven out of ten, where one is difficult and ten is easy to set up.

The technical setup was easy. It becomes more challenging when you start labeling the assets and doing the ring-fencing. You have to go deep into the architecture of the network, the application, and whatever. That’s more difficult, but in the end, it’s easier than doing classic segmentation with a firewall.

The data architecture took one week, but the segmentation logic took months. We are not finished. We started in April, and we are not finished. So, like almost half a year.

We start to define the ring for the ring fences, and then we start with a part of the network with the test environment. We test and then go. The last will be the production. We label the assets, then start a monitoring period to see the data traffic between the assets. Then we go into an alerting phase and finally to a block period..”

Verified user[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

Customer Service and Support

“We have not contacted technical support, But the Akamai person was extremely well-read on the subject, and there was almost nothing he couldn't answer during the proof of concept project..”

Verified user

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

[Read full review](#) 

“I did deal with technical support directly. It was good. I was the guy who was calling them. It was never just a call. They tried to understand the problem and the construct and came up with a solution that would assist us. .”

Vishal Chaudhary

Senior Principal Consultant Cloud/DevOps/ML/Kubernetes at Opticca

[Read full review](#) 

“Their support is pretty good. I haven't had to use them that frequently, so I'm not sure about their response times, but when they come and set your stuff up, everything seems pretty good from that end. I would assume the support after that would be similar..”

Verified user

Information Security Engineering Consultant at a university with 1,001-5,000 employees

[Read full review](#) 

“The technical support has been excellent. It is probably one of the best customer services provided by any company. They are helpful, reactive to problems, and constantly work to enable us to do what we want to do..”

Verified user

[Read full review](#) 

Corporate Operations Manager at University of Strathclyde

“It has very robust technical support. We have three or four people with whom we talk on a biweekly or monthly basis. They are very good. They take care of us. If we have any problems with the tools or rules, they are supportive..”

Jose Luis Guzman

[Read full review](#) 

Cybersecurity Coordinator at MONEX

“The response time should be better. Sometimes it’s good, but sometimes it could be better. You have a problem, you need an answer, and then you have to wait. Sometimes they do not talk with an administrator who knows anything about Guardicore. When my colleagues call support, I think my colleagues are experts. And then the support starts with really easy questions. That’s not funny.

So, I want them to be more skilled, like, more educated on the matter..”

Verified user

[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

Other Advice

“I work with the segmentation aspect of Akamai Guardicore Segmentation. Akamai Guardicore Segmentation has much better visibility and has a more firewall style look and feel in how you use the product. I would rate this review an 8 overall..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“My advice for others looking into using Akamai Guardicore Segmentation is that it gives visibility, security, and really does the right segmentation of your broadcast domains, improving not only security but visibility that you really need for your business. Akamai Guardicore Segmentation is the tool that makes me sleeping well every day, and I would rate it a ten on a scale of one to ten..”

Fernando Ortega

CISO at Paschoalotto

[Read full review](#) 

“My advice for others looking into using Akamai Guardicore Segmentation is that visibility is crucial. If you are not seeing your network clearly, your job is challenging. Visibility is the main word in Akamai Guardicore Segmentation. Our company has a business relationship with [Akamai](#) as we are a partner or reseller. I rate this product a ten out of ten..”

Verified user

Especialista em segurança da informação at a tech consulting company with 11-50 employees

[Read full review](#) 

“Since I started using Akamai Guardicore Segmentation, we have not had any situations that demonstrate specific results or metrics such as fewer incidents or improved compliance.

“My advice to others looking into using Akamai Guardicore Segmentation is to work with professional services during setup because it is not intuitive at the beginning and to take the administrator course to understand the [Reveal](#) Maps, as the Reveal Maps are the most useful way to control the segmentation.

“I give this product a rating of 8..”

Ken Bauer

Senior Security Analyst at a retailer with 5,001-10,000 employees

[Read full review](#) 

With usability, I find that Guardicore is a pretty easy solution to use and pretty straightforward. For integrations, they have lots of different integrations. One cool integration that I have already done is with the Tenable solution, from where we are able to get not only assets information but also assets with high exploitable vulnerabilities. With Guardicore working with labels, we can create a rule that whenever we have an asset with a high exploitable vulnerability, we can block

some specific type of communication inside the environment. That integration is one of the coolest I have done, but Guardicore has a lot of different integrations that I know about. As for reporting, Guardicore doesn't have nice reporting inside the solution itself, while it gives lots of different APIs where we can pull the data and build external reports, such as on Power BI. In my company, we have done that, but the reporting is not native from the solution; we have to use APIs for those types of reports.

My advice for others looking into using Akamai Guardicore Segmentation is to think about labeling. You should have labels for your entire environment regarding applications, which means having a good [CMDB](#). You don't need to have a full [CMDB](#), but you should at least build one with information about servers and which applications those servers are members of and what roles they play in the applications, so with that, you will be able to extract the best from the solution. I would rate this product an 8 out of 10. .”

Avner Nahum

Cybersecurity Consultant at a tech consulting company with 51-200 employees

[Read full review](#) 

“In one of our banking customer environments, we used Akamai Guardicore Segmentation to segment the critical application tiers such as web, application, and database servers. Initially, we enabled visibility mode to understand the east-west traffic and identify all communication flows between workloads. During this phase, we discovered several unnecessary open communications, especially between application and database layers. Based on this, we created granular segmentation policies to allow only required ports and protocols and blocked all other unnecessary traffic. For example, only specific application servers were allowed to communicate with the database servers on required ports while all other lateral movement paths were restricted.

“One additional point I would highlight is that with Akamai Guardicore Segmentation, we do not just use it for static segmentation, but also for

continuous monitoring and policy optimization. Even after the initial deployment, we regularly review the traffic patterns and update the policies based on application changes. This is very important in dynamic environments such as banking, where new service integrations are frequently introduced. Another key aspect is that we use it as a part of a broader zero-trust strategy, integrating it with other security solutions such as [WAF](#) and secure web gateways to create a layered defense approach. Also, from an operational perspective, it has helped us to reduce the dependency on traditional network-based segmentation, making security more application-aware and flexible, especially in hybrid and cloud environments.

“The visualization feature in Akamai Guardicore Segmentation has been extremely helpful for our daily operations, especially in troubleshooting and policy design. From a troubleshooting perspective, it gives us a clear, real-time view of communication flows between workloads. Instead of checking logs manually, we can quickly identify where traffic is being allowed or blocked. This significantly reduces the time required to identify issues. For policy design, the visualization helps us to understand the application dependencies before enforcing any rules. This ensures we do not accidentally block legitimate traffic, which is very critical in banking environments. It also helps in identifying unnecessary or suspicious communication paths, validating policies after implementation, and collaborating with application teams, since the visual maps are easy to understand even for non-security teams. Overall, it makes both troubleshooting faster and policy creation more accurate, reducing the operational effort and minimizing the business impact.

“Based on our experience with Akamai Guardicore Segmentation, we have seen a noticeable improvement in both troubleshooting and policy validation timelines. Earlier, troubleshooting east-west communication issues used to take around two to four hours since we had to rely on manual log analysis and multiple tools. With Guardicore visualization, we can now identify the issue within twenty to thirty-five minutes, which is roughly around sixty-five percent to eighty-five percent reduction in troubleshooting time. For policy validation, it previously took several hours to a full day, especially when coordinating with application teams. Now with the clear dependency mapping and real-time visibility, we are able to validate policies within thirty-five to sixty-five minutes, improving efficiency by around

fifty-five percent to seventy-five percent. Additionally, incident response time improved by fifty-five percent, policy deployment errors reduced significantly due to better visibility, and faster onboarding of newer applications since dependencies are clearly mapped. Overall, these improvements have helped our team become more efficient, proactive, and accurate in operations.

“My main advice for anyone considering Akamai Guardicore Segmentation is to start with the visibility mode before enforcing any policies. Understanding application dependencies and traffic flow is very important to avoid unintended disruptions. Also, involve application and infrastructure teams early in the process since accurate segmentation depends on knowing how applications communicate. I recommend taking a phased approach by starting with monitoring and mapping, identifying the required versus unnecessary traffic, and gradually enforcing the policies. Additionally, keep policies simple and structured initially and refine them over time as you gain more visibility. Overall, if implemented properly, it is a very effective solution for achieving zero-trust and reducing lateral movement risks.

“Akamai Guardicore Segmentation is a very effective solution for organizations looking to strengthen their zero-trust security model, especially in complex hybrid environments. What stands out the most is its ability to provide deep visibility and control over east-west traffic, which is something traditional security solutions often lack. While there are areas for improvement such as policy management simplicity and automation, the core capabilities are very strong and deliver real value in terms of security, operational efficiency, and compliance. From my experience, when implemented with the right approach, it can significantly enhance an organization’s overall security posture and reduce lateral movement risk. I would rate this product an eight out of ten..”

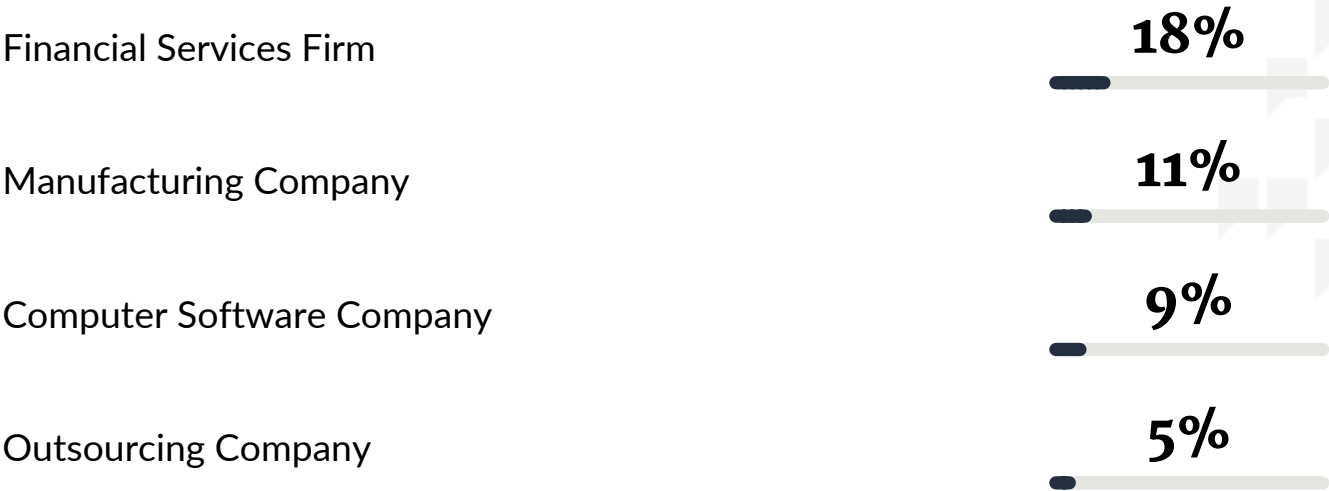
Vibin Thomas

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

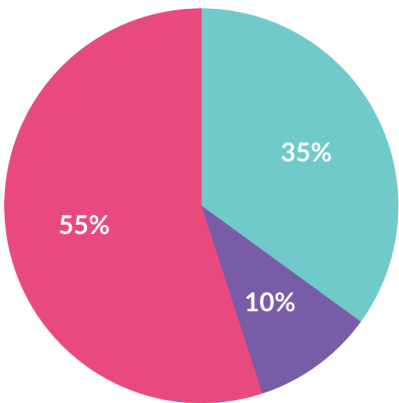
Top Industries

by visitors reading reviews

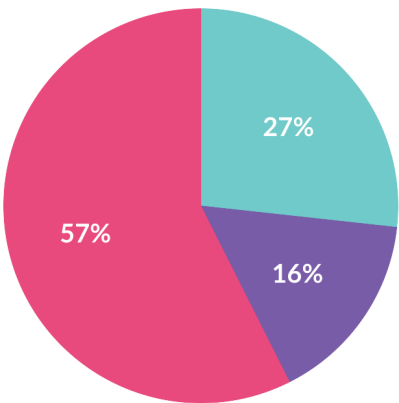


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944