

aws marketplace

**Illumio**

# Reviews, tips, and advice from real users



Powered by  PeerSpot



# Contents

Product Recap.....	3 - 5
Valuable Features.....	6 - 13
Other Solutions Considered.....	14 - 15
ROI.....	16 - 17
Use Case.....	18 - 22
Setup.....	23 - 25
Customer Service and Support.....	26 - 27
Other Advice.....	28 - 31
Trends.....	32 - 33
About PeerSpot.....	34 - 35

# Product Recap



Illumio

# Illumio Recap

Illumio Zero Trust Segmentation is a cloud and data center security solution that helps stop breaches from spreading across hybrid and multi cloud IT environments. The solution is designed to stop ransomware, contain cyber attacks, and reduce risk. With Illumio Zero Trust Segmentation, users can understand relationships and communications to map exposure risk of systems and data, identify the right security posture and secure applications through least-privilege policies, and ensure a Zero Trust security posture.

## Illumio Zero Trust Segmentation Features

Illumio Zero Trust Segmentation has many valuable key features. Some of the most useful ones include:

- **Scalability:** Illumio Zero Trust Segmentation scales up to 200,000 managed workloads or over 700,000 unmanaged workloads. These workloads can be in the cloud, on-premises, and in hybrid environments.
- **Single pane of visibility:** The solution's single pane of visibility improves your security posture and ability to prevent and respond rapidly to cyberattacks.
- **Simplicity:** With Illumio Zero Trust Segmentation, setting up groups and tags is simple. The solution is easy to integrate with next-generation firewalls and can also integrate with IT service management tools to import workload tags to provide more context to workloads.
- **Ransomware containment:** The solution provides enforcement boundaries to contain attackers from moving laterally across your organization, enabling security architects to immediately isolate any workload or endpoint compromised in an attack. Enforcement boundaries can be activated instantly through scripts or by manual control, isolating workloads and endpoints already infected from spreading across the organization.

## Illumio Zero Trust Segmentation Benefits

There are many benefits to implementing Illumio Zero Trust Segmentation. Some of the biggest advantages the solution offers include:

- **Visibility everywhere:** The Illumio Zero Trust Segmentation solution helps ensure that every interaction on your network is accounted for.
- **Least-privilege access:** By implementing Illumio Zero Trust Segmentation, your organization can prevent unexpected breaches from propagating.
- **Adaptability and consistency:** The solution guarantees consistent network behavior everywhere.

- **Proactive posture:** Using the solution enables your organization to always be on the lookout for an attack.
- **Improve breach containment:** With the solution, you can prevent unauthorized lateral movement and reduce your blast radius. Creating micro-perimeters around specific assets breaks up your attack surface and gives you the granular control needed to contain breaches.
- **Streamline policy management:** The solution enables organizations to decouple segmentation from the underlying network to define policies based on the language that IT uses. Illumio's human-readable labels make policy creation much simpler and faster than traditional network segmentation approaches like VLANs, IP addresses, and port numbers.

## Reviews from Real Users

Illumio Zero Trust Segmentation is a solution that stands out when compared to many of its competitors. Some of its major advantages are that it has a good auto policy writing feature, great mapping, and useful monitoring.

Shashi, Technical Consultant at a financial services firm, explains which features she really likes. “The [auto policy writing](#) is great. The feature will give you the option of inbound-outbound traffic. The Explorer allows you to know the traffic between source and destination. The illumination definitely stands out. Mapping is great. The application group mapping is useful.”

The solution has “helpful support, [useful monitoring](#), and high availability,” according to Edwin L., Security Architect at MGM.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Illumio serves as a single endpoint technology where I can implement various features, including a zero-trust network, north-to-south and east-to-west configurations, and micro-segmentation, all coming from one platform, which ultimately saves us time and money.”



**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

- ✓ “Illumio definitely demonstrates its value in money-saving capabilities, enhancing our lateral environment inside the organization and providing effectiveness overall once integrated.”



**Abhijit Kumar**

Security delivery specialist at a tech vendor with 10,001+ employees

- ✓ “The client is getting more security and is more confident in their network because they now have the micro-segmentation feature in their environment.”



**Utkarsh Shakya**

Cyber Security Architect at a tech vendor with 10,001+ employees



“I observe extensive return on investment with Illumio.”



**KlavsThaarup**

Senior Security Consultant at Orange Cyberdefense



“One big outcome we saw after implementing Illumio was a notable drop in lateral movement incidents.”



**Verified user**

DevOps at a marketing services firm with 51-200 employees



“Overall, Illumio is a powerful tool for micro-segmentation and zero trust security that provides strong visibility, flexible policy management, and effective threat containment, enhancing an organization's internal security posture.”



**Verified user**

Cybersecurity Engineer at a tech vendor with 10,001+ employees



“The strongest aspect of Illumio is the visual traffic interface, which allows us to see all traffic that communicates with our servers and allied companies.”



**Alark Singh**

IT Specialist at Allianz

## What users had to say about valuable features:

“The advantages of Illumio really stand out because they are not using the kernel module. The biggest thing is that the agents used, the software that goes onto the PCs or the servers, is not as comprehensive as that of Akamai. This might be better for some companies that want a light agent instead of a thick agent.

Illumio has some VPN features and encryption features that are not available in Guardicore.

Illumio's ability to contain threats through secure segmentation is positive. I would say it's a good part here.

They have some features that are not available in Akamai Guardicore..”

### **KlavsThaarup**

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“Illumio offers great features such as controlling east-west traffic within data centers and clouds, enforcing segmentation policies between workloads, and reducing the attack surface by limiting unauthorized lateral movement.

Illumio's segmentation rules without requiring anything are pretty unique. It also integrates well with other security tools, giving you a centralized view of policy enforcement across your environment. If you're looking for east-west traffic control and zero-trust architecture, it's a great fit.

From what I have seen, Illumio positively impacts organizations by giving them a much clearer picture of their internal traffic, allowing them to identify risky connections they didn't see before. It also speeds up compliance, as I have heard, since they can enforce least privilege rules across their environments much faster. By reducing lateral movement, it just makes their overall security posture a lot stronger. .”

**Verified user**

DevOps at a marketing services firm with 51-200 employees

[Read full review](#) 

“The best feature of Illumio is micro-segmentation. Within the same segment of a network or device, I can create micro-segmentation based on location, environment, and roles. I can customize what exactly each particular endpoint device is and accordingly write rules to manage communication through inbound and outbound rules, allowing or denying communication as required.

While working with micro-segmentation and setting rules based on roles or locations, managing and updating policies in Illumio does not take considerable time because I have intra-scope and extra-scope rules. If I make a rule and need to modify it, I simply adjust the scope accordingly. When a new workstation comes into the network, I only need to apply the labels to that workstation, and it merges into a policy automatically without needing to modify the policy unless absolutely necessary.

Deploying the VEN is straightforward, as I can deploy it on Windows, Linux, and macOS operating systems. In my organization, we have deployed it on approximately 300,000 devices, and it is easily manageable through Illumio. We have a cloud, SaaS-based environment of the PCE where I manage all those devices, making deployment very straightforward.

Illumio has positively impacted my organization by protecting devices not only from external threats but also from internal ones. If any single PC becomes compromised by an external or internal attack, I can isolate those PCs or devices. If any server becomes compromised, I can isolate it as well, which is a wonderful feature of Illumio..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

“The best feature that Illumio offers is that we can easily understand how to label the applications, how to install Illumio agent on the client machines, how to install the agent on the servers, and how to do the ring-fencing. The log analysis is very simple, and we can map the traffic very easily, such as the traffic view and map view. We have many views to do that, and then we have a topology environment where we can expand the topology and understand how we want to prepare our policy based on the requirement. These are some of the very good use cases that Illumio provides, which none of the other vendors can offer in such an easy and usable way.

“The most important feature is the traffic review analysis, where we use the draft view and the reported view that helps us understand how the application interacts with other applications in the environment, and based on that, we are able to define the policies.

“It has increased the business for the organization. We are creating business by supporting the client. The client is getting more security and is more confident in their network because they now have the micro-segmentation feature in their environment. This is new technology and that's how it helps the organization as a whole. The clients we support are benefited, and at the same time, we are making money out of it. This is definitely a good approach.

“After implementing Illumio, there has been significant progress. Most of the app owners now understand what applications are communicating, how these applications interact with others, and we are more aware of which application is talking to what other servers and applications, and their roles. For instance, whether an application is talking to the DB server or an app server. We have a more granular understanding of the traffic view. Additionally, after implementing Illumio, there is greater segmentation, and fewer incidents are occurring. There have been times when an attack was halted from expanding laterally..”

**Utkarsh Shakya**

Cyber Security Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“Illumio is a very good tool that is flexible, with policies written using labels such as environment, application, role, and location rather than IP addresses, making policy management scalable and easy to maintain in dynamic environments. However, the initial setup requires careful planning, and improperly configured policies can block communications between applications. Troubleshooting may require a deep understanding of traffic logs and flow data, alongside previously written policies. Additionally, agent dependency is a consideration since any agent-related issues can affect policy application, making proper monitoring of agent health crucial. Overall, Illumio is a powerful tool for micro-segmentation and zero trust security that provides strong visibility, flexible policy management, and effective threat containment, enhancing an organization's internal security posture. It is not just a security tool but a strategic solution for modern infrastructure security that can significantly reduce the risk of lateral movement and improve overall network security with proper implementation.

“The best features Illumio offers include real-time control of traffic between servers and allowing required communication based on specified ports while blocking unwanted ports. It provides breach containment, preventing communication on unapproved ports, and offers full visibility of traffic flows that helps in troubleshooting and audits, with traffic mapping generated by a central controller that analyzes and creates policies based on labels instead of IPs. Policy management is highly scalable, and the lightweight agent can be easily installed on each server, enabling policy simulation to check impact before enforcement using a draft view.

“These features are incredibly valuable, including predefined templates that save time and reduce manual errors, resulting in massive scalability that is suitable for larger enterprises, which represent the best features of Illumio for micro-segmentation and real-time visibility..”

**Verified user**

Cybersecurity Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“The best feature Illumio offers, in my opinion, is the visibility map, which provides a useful end-to-end traffic connection. It gives details at a granular level about what applications are communicating inside your network, making it easier to create policies. Once you know the communication paths and identify the legitimate users, you can effectively prepare those policies.

“The granular visibility provided by the visibility map changes the way we manage network security or policy creation by allowing us to directly refer to nano-segmentation. We can see which specific ports are being accessed, enabling us to segregate or segment the policy rules based on those security ports. This allows for more granular control over communication, tightening security. We have two modes of enforcement in Illumio; before applying enforcement rules, we utilize visibility to get details of the traffic, draft our policies, and ensure the targeted audience is met before enforcement. Initially, we allow traffic and then block everything else except the allowed policies on Illumio, which helps tighten the security of the east-west traffic within our network.

“I observed another important feature in Illumio—it is not just replacing the perimeter firewall. A perimeter firewall provides a different level of security, whereas Illumio controls the local firewall. Illumio coexists with other non-Illumio processes that control the local firewall, and in that scenario, it can detect and alert users about local firewall tampering, allowing for better control over workloads.

“Illumio positively impacts our organization through granular level segmentation of communication traffic. Initially, security controls depend on the network and applications, but with Illumio, we manage how one host communicates to another and the necessary paths that need to remain open, which reduces unauthorized communications. If any devices are compromised, Illumio instantly notifies us and isolates dangerous hosts, decreasing the spread of ransomware or other threats..”

**Abhijit Kumar**

Security delivery specialist at a tech vendor with 10,001+ employees

[Read full review](#) 

# Other Solutions Considered

“We were about to experience Guardicore, but Guardicore was costly. Illumio is top in the market, and from a cost perspective, it is cheaper than Guardicore, so we chose that..”

**Utkarsh Shakya**

Cyber Security Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“While choosing Illumio, we did not evaluate other options since we received an offer for a trial, and it turned out to be a wonderful experience without trying other vendors or technologies so far..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“Before using Illumio, we had not utilized a different endpoint security solution. We relied on Windows firewall and our own firewall, which was a legacy system that could not provide the micro-segmentation we required, prompting us to switch to Illumio for better security..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“We did not use anything previously. This is really the best product.

We have a Nebule product - a Nebule cloud, a Nebule solution that is LSDX, a VMware LSDX. That is also in place, along with Illumio. It is not yet live. We are focusing on Illumio for on-prem. Once it moves to the cloud, we have been considering both Illumio and LSDX..”

**Shashi**

Technical Consultant at a financial services firm with 10,001+ employees

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“Illumio definitely demonstrates its value in money-saving capabilities, enhancing our lateral environment inside the organization and providing effectiveness overall once integrated..”

**Abhijit Kumar**

Security delivery specialist at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“I cannot provide detailed information on ROI as it is handled by upper management. However, Illumio is known to be the cheapest solution among the security solutions we evaluated..”

**Alark Singh**

IT Specialist at Allianz

[Read full review](#) 

“In general, security products are defined as insurance or defense wall - relatively passive. Illumio does more than general security product, it provides East-West traffic flow visibility and auditorial log which benefits on daily operation and periodical auditing. The ROI is higher than expected..”

**Peter Cheng**

Owner at SiS International Limited

[Read full review](#) 

---

“I have seen a good return on investment with Illumio, and it definitely saves our time. Additionally, if we were to buy any other product besides Illumio, we would need to invest more. Illumio serves as a single endpoint technology where I can implement various features, including a zero-trust network, north-to-south and east-to-west configurations, and micro-segmentation, all coming from one platform, which ultimately saves us time and money..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

# Use Case

“We are using Illumio for network micro-segmentation to ensure that all applications comply with Dora compliance. This is an essential part of our infrastructure to ensure security and proper network segmentation..”

**Alark Singh**

IT Specialist at Allianz

[Read full review](#) 

---

“We use Illumio as our network security platform to protect our EC2 instances. We use Illumio on our EC2 instances to detect and respond to any instance that might occur on the network side. That is pretty much all we use it for. It is very easy to detect and respond using Illumio..”

**Verified user**

DevOps at a marketing services firm with 51-200 employees

[Read full review](#) 

“The main use case for Illumio involves working on any new applications enrolled into the architecture, where I focus on understanding the traffic and documenting rules. I often face issues with agent and PC console communication, so in those cases, I suspend the agent, check the services, and make sure to activate and deactivate. I perform all types of troubleshooting to ensure the agent communicates properly with the PC console and fetches the policies actively.

“For new applications onboarded into the infrastructure, I first work on understanding the application, the users, and whether it is in production, development, testing, or UAT, which involves grasping the basic structure. Then I work closely with application teams to identify what communication needs to be allowed and what is not required. After the agent is installed on those servers, we move them from idle to visibility to monitor traffic for a week. This involves exporting a report and closely collaborating with application teams to define which traffic requires rules and segregating the non-required traffic by source and destination. This documentation leads to a precise mapping of traffic, allowing me to create rules for the servers. The agents are eventually moved to visibility to selective enforcement for some and full enforcement for others, while also providing teams with guidance on future communications and necessary actions, all of which are clearly documented..”

**Verified user**

Cybersecurity Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“Illumio serves as our primary endpoint security solution, utilizing the VEN as an agent installed across each workstation, laptop, and server managed through the PCE, the Policy Compute Engine. We manage all endpoint devices, both managed and unmanaged, through the Illumio agent, which communicates with the PCE to monitor all behaviors involving high-level security between north-to-south and east-to-west traffic.

A specific example of how I use Illumio with endpoints to protect my laptop from outside threats involves internal threat protection as well. Suppose two computers are already in the same network domain. If one computer gets compromised by any means, the communication between the other computer would normally continue unprotected. However, when I use Illumio as a security device and install the secure agent on each workstation, if one workstation becomes compromised, I can protect the second one. This means I can protect communication between devices in the same network segment. I can restrict and manage the communication between these devices effectively.

In addition to our primary use case, we protect our devices and environment from ransomware attacks, and I have witnessed several scenarios where Illumio protects devices from such threats. Illumio PCE includes a map where I can see all communication similar to micro-segmentation, including details about the production environment, its location, and the web application. Everything can be micro-segmented, allowing me to segment the network and protect it comprehensively..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

“The main use case for Illumio is providing micro-segmentation where we don't want to segment the network based on IP addresses but rather segment them based on roles, applications, and environments. Everything that we do from the segmentation point of view is based on the label. Based on the label, we prepare the policies, and then we do the segmentation, which gives us a more granular approach and limits the attack surface from happening. Now the attack surface is limited, and this will happen if any attack occurs; we stop the lateral movement of the attack because we have segmented the environment.

“I am managing a project where the client needs Illumio, and we are helping with their environment on the segmentation approach. They have many applications in their environment, and we support them by understanding the environment and applications they have. When we have the full inventory of their applications, we ask them to do the labeling in Illumio based on information such as how many applications they have, what labels we have to give them, and under what categorization those labels should be. For example, which application should be part of this location, this role, this environment, and this application. Based on that, we have created an approach to help our client onboard the applications, wherein we have many activities happening. For example, we review their traffic, conduct ring-fencing, and understand what traffic goes through. After a few days, we understand the required traffic, based on that we draft the policy, have the policy review session, and then finally enforce the application. All of this occurs alongside the process from the client end; they follow all the processes, and we handle the technical part before finally enforcing the application.

“Illumio is deployed in the cloud environment in Azure..”

**Utkarsh Shakya**

Cyber Security Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“I was engaged in a deployment of Illumio, where in my previous project, I actually worked for 3,500 endpoints, so I needed to deploy the VENs on individual workplaces and then onboard them to PCE, then make them on segmentation, and finally, make their entire network in segmentation. I handled the entire deployments.

“Challenges in the sense of multiple applications present on a customer's premises require you to engage with the application owners first to understand their necessary communication paths. Once you deploy the VEN and obtain a visualized map over the PCE, you gain an understanding of how the communication is going, but you need to verify with the application owner whether the communication traffic between the applications and servers is legitimate or authorized or not, based on which you create the policies. I found that bit critical, engaging with the application owners and obtaining their confirmations. Apart from that, everything else goes smoother from my end. Every other scope and deliverables, whatever is possible by Illumio, turn out to be an almost smoother process.

“My main experience includes completing two projects. On both projects while installing the VENs, on one of the sites, we found that we needed to label manually as the CMDB was not integrated, necessitating us to understand the application's behavior, location, roles, and other metadata for all the workloads before preparing the labeling. In the other project, the CMDB was already present on the infrastructure, so it was easier to get authorized. Another use case involved using automation for Windows and Linux with Jenkins during the deployment of the VENs, spreading pairing profiles to all workloads, leading to smooth onboarding. It took some time to finalize the execution of the policies in draft mode before switching to enforcement mode, but it was more realistic and challenging to achieve the exact outcomes we expected..”

**Abhijit Kumar**

Security delivery specialist at a tech vendor with 10,001+ employees

[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.

“It's rather complex to install Illumio, but that would be the same for both vendors. There is no big problem when you're installing it. It's pretty much straightforward..”

**KlavsThaarup**

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

---

“I would rate Illumio Zero Trust Segmentation's setup a six out of ten. The tool's deployment took two weeks to complete. We relied on two people to help us with the deployment. .”

**Verified user**

Executive Director of Cloud Networking at a financial services firm with 10,001+ employees

[Read full review](#) 

“The initial setup is easygoing. There are complexities, but the product is very good. Once we get a good baseline and discover things we do not want, we can start blocking and micro-segmenting..”

**Verified user**

[Read full review](#) 

Senior Security Consultant at a tech services company with 11-50 employees

---

“Since implementing Illumio, my organization has seen a reduction in work effort, and it helps to secure the network efficiently. For example, we have several endpoint devices located in different locations. I can create extra-scope or intra-scope rules to simplify communication while managing their Windows firewall and other firewalls through Illumio..”

**Irfan Sharfi**

[Read full review](#) 

Security Professional at a tech vendor with 10,001+ employees

---

“The initial implementation is simple. It's not complex.

I was not there during the initial setup, however, the deployment might have taken about three months or so. That included the approvals and the entire setup process.

In terms of deployment and maintenance, it all depends on how many applications you're going to onboard. It's not a straight answer. It all depends on the amount of work you are doing in your organization. .”

**Shashi**

[Read full review](#) 

Technical Consultant at a financial services firm with 10,001+ employees

---

“The product's initial setup phase is not difficult. We are using a cloud version of the tool. Picking up the PC for the setup was difficult because Illumio's service provider took care of it. In our company, we only installed the tool on our devices, so it wasn't much of a difficult process. On a scale of one to ten, one is difficult, and ten is easy, I rate the setup phase as nine.

I didn't deploy Illumio. My company uses the cloud version of the tool. I created my account and paired my device, which was all that was required..”

**Vincent TOH**

[Read full review](#) 

Assistant Manager at KPMG S.A.

# Customer Service and Support

“Customer support from Illumio is exceptional. Whenever I raise a case with their support team, regardless of the priority level—P1, P2, P3, or P4—they generally reply within an hour and are available for a call whenever needed, providing a complete solution..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“Technical support could be better. When we get a reply from support engineers, it is not kind or empathetic. They also delay some responses - sometimes, not always. Maybe it depends from engineer to engineer. They could be a lot better, a lot more helpful..”

**Shashi**

Technical Consultant at a financial services firm with 10,001+ employees

[Read full review](#) 

“The support from Illumio Adaptive Security Platform was good. They always answered my questions and if I needed further help they would arrange a remote session with me.

I rate the support team from Illumio Adaptive Security Platform a four out of five..”

**Edwin Leong**

Security Architect at MGM

[Read full review](#) 

---

“We've contacted technical support and are currently working with a professional right now for a couple of days each month. So far, we haven't been too satisfied with the assistance they've provided. I'd rate them as okay. Sometimes we are required to wait for a resolution. It can take a while to get a response. We need a special environment, and it takes them time to help us which can be frustrating..”

**Verified user**

Owner at a financial services firm with 10,001+ employees

[Read full review](#) 

# Other Advice

“For others looking into using Illumio, I would advise purchasing and testing this product, as it will provide immense satisfaction regarding security and user-friendliness..”

**Irfan Sharfi**

Security Professional at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“Before, I mentioned that Illumio is not very comprehensive in comparison to Akamai. I said that they could have a lighter agent and also process level segmentation. There is something that's not perfect in Illumio that could be improved..”

**KlavsThaarup**

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“For others looking into using Illumio, my advice is to activate the agent on the local workloads and set it to visibility mode for at least two weeks to gather insights on all communication before finalizing security policies. The more time you spend in visibility mode, the better understanding you will have of internal traffic, making it easier to create effective policies.

“The technical training part on Illumio includes multiple certifications, and I recognize it as one of their finest initiatives. I gave this review a rating of 9 out of 10..”

**Abhijit Kumar**

Security delivery specialist at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“I give Illumio a rating of nine out of ten.

“I gave it a nine out of ten due to some small changes I previously mentioned regarding improvements needed for Illumio, such as the dependency on agent health and requests for a simplified dashboard along with AI-based auto policy recommendations. The policy creation process is mostly manual, so AI-based recommendations would be useful. It is an excellent tool for cybersecurity, especially for micro-segmentation, preventing attacks from spreading from one compromised server to others in the infrastructure. With some additional improvements, particularly for first-time users and their understanding, it could reach a perfect score of ten.

“Illumio is a great product for managing server-to-server communication properly. It is scalable and user-friendly, but first-time users may experience challenges understanding policy creation, so better guidance is necessary to enhance their learning process. My overall review rating for this product is nine out of ten..”

**Verified user**

Cybersecurity Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“One big outcome we saw after implementing Illumio was a notable drop in lateral movement incidents. Within the first few months, we had about a 40% reduction in potential attack paths. On the compliance side, we cut audit times in half. What used to take weeks to validate now takes just a few days. It has really helped us tighten up both security and operational efficiency.

Illumio delivers really solid results. Micro-segmentation is top-notch, and we saw real security improvements. Some of the finer automation and user experience aspects still require a bit of effort to get fully dialed in. Illumio is deployed in our organization in the public cloud, specifically [AWS](#). We use [AWS](#), which is Amazon Web Services, as our cloud provider. We did not purchase Illumio through the [AWS Marketplace](#).

Illumio is definitely a good solution if you have a lot of network traffic that you're dealing with. I rate Illumio a solid eight out of ten. .”

**Verified user**

DevOps at a marketing services firm with 51-200 employees

[Read full review](#) 

“I would advise others considering using Illumio to have a basic understanding of networking and some usage of protocols. They should be able to understand what TCP/IP is so they can look into the connections and understand what's happening. Some basic knowledge of networking is required before using Illumio, as well as the concept of micro-segmentation. We should have a proper purpose for using this tool.

“I believe the additional thoughts for Illumio are that it's the best in the market. It will remain the best in the market if they continue working on addressing bugs and if customer support is helpful, friendly, and available all the time; I think nobody is going to lose Illumio at all.

“We are the partner.

“On a scale of 1-10, I rate Illumio a 10. It's best in Gartner. It's the top product in the market for micro-segmentation. The GUI is very simple, and I think there could be nothing better than this..”

**Utkarsh Shakya**

Cyber Security Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

# Top Industries

by visitors reading reviews

Financial Services Firm

17%

Computer Software Company

11%

Manufacturing Company

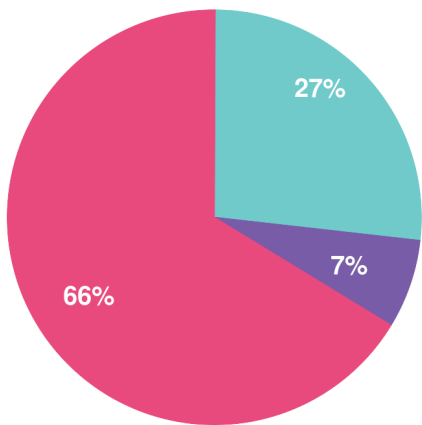
8%

Insurance Company

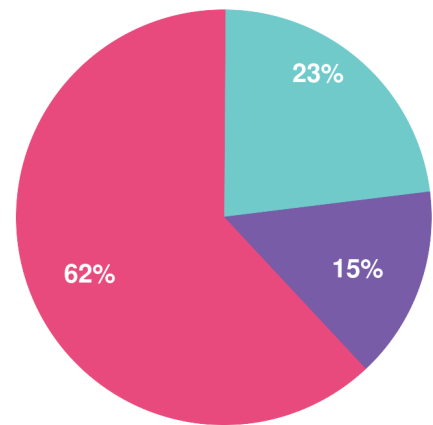
6%

# Company Size

by reviewers



by visitors reading reviews



Large Enterprise

Midsize 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 software running on AWS and other platforms. 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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944