aws marketplace

Corelight Open NDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Corelight Open NDR

Corelight Open NDR Recap

Corelight transforms network and cloud activity into evidence so that defenders can stay ahead of ever-changing attacks.

Delivered by our Open NDR Platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

Our on-prem and cloud sensors go anywhere to capture structured, industry-standard telemetry and insights that work with the tools and processes you already use. Corelight's global customers include Fortune 500 companies, major government agencies, and research universities.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Our company has seen massive improvements in cybersecurity position for our clients."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

- "Corelight Open NDR has had a positive impact on my company, providing visibility as the Suricata engine can scan huge volumes of traffic, including north-south and east-west, revealing signatures and exposures I was not expecting and enabling me to catch them with Suricata alerts."

Anthony Budrecki

Principle Security Architect at Eversource Energy

- "It's an easy way for us to get visibility in a client's environment."

Dan Jeske

Account Executive at Fishtech Group

"It's easy to create additional dashboards specific to supporting specific tasks."

HamadaElewa

Technical Sales Manager at Spire Solutions

"It is easy to deploy and easy to handle."

Muteb Alqahtani

Manage Consultant at SITE

"Corelight is easy to use."

José Luis Pozo

Pre Sales Technician at DotForce

"The most valuable feature is the embedded IDS from Suricata."

Verified user

Chief Executive Officer at NetMetrix

What users had to say about valuable features:

“The tool helps us track the traffic easily. Additionally, the soft analysis is very easy to learn due to the simplicity of the engine. It can integrate with multiple threat and intelligence feeds. This empowers the solution more than its powerful. It's also easy to create additional dashboards specific to supporting specific tasks. .”

HamadaElewa
Technical Sales Manager at Spire Solutions

Read full review

“Corelight provides a insight, visibility and a lot of data. No matter if you need detection for proactive defense or you need data for forensics, Corelight is the primary source of information for cyber security. The deployment is very quick and you are using it from the very beginning..”

José Luis Pozo
Pre Sales Technician at DotForce

Read full review

"Corelight Open NDR is a really powerful platform. Pairing up the sensors with Investigator, you are getting incredibly rich data, which we are also able to further enrich with additional feeds such as CrowdStrike or CISAIAS. We are getting really good intelligence on what is hitting networks, and it is a really good platform for diving extremely deep into that network traffic and doing analysis. We have been really impressed with the amount of features and continual development that Corelight has been putting into Investigator. On a regular basis, we are getting massive updates on both the machine learning detection modules that they have built in. This is obviously reducing our alert fatigue by having these machine learning processes identifying alerts or doing the triage for us. Additionally, we are getting access to more agentic processes within Investigator which further allows us to control, triage, and get access to the right information when we need it.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

"I appreciate the Fleet Manager feature of Corelight Open NDR, which allows me to manage the Suricata policy across my entire fleet of Corelight sensors. I also value the fact that Corelight has embraced the Suricata engine, giving me the benefits of an open-source platform and all that comes with that in terms of the open-source rule set that I can feed into the Suricata engine. I have a professional subscription, so I am getting some of the professional rules and all the open-source rules. The vast array of Suricata rules makes it an excellent model.

"Corelight Open NDR has had a positive impact on my company. The benefits include visibility, as the Suricata engine can scan huge volumes of traffic. I feed it both north-south and east-west traffic, gaining scans of traffic that I typically do not get a lot of visibility into at a detailed level and seeing signatures in my traffic that I was not expecting. Most of which turn out to be false positives, but the awareness of them being there is very beneficial because they are often associated with old code or bad group policies that have not been cleaned up, leaving holes and exposures that need to be addressed. I can catch these with the Suricata alerts.."

Anthony Budrecki
Principle Security Architect at Eversource Energy

Read full review

Other Solutions Considered

“I know our company selected Corelight to basically be its partner moving forward into this program we have with the Department of Defense and Department of War. They did look at a wide variety of other vendors, like the Darktraces of the world, and they really saw Corelight as a vendor they believed in. They believed in the product and believed in the vision that they had, and we have partnered with them very closely..”

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

“I don't have much visibility on other products. I did have a meeting with the Auvik people. We had sessions for their application. Auvik doesn't serve our purpose because it is mostly using machine language. It doesn't support rules to bring into the system. Auvik has machine learning that Corelight probably doesn’t have, but I would choose Corelight over Auvik or any other product. As a service provider, we pretty much rely on rules and IOCs..”

Muteb Alqahtani

Manage Consultant at SITE

Read full review

"I personally have not used anything other than Corelight. From my time before, I have been in the cyber industry for a little bit. I had a data security startup for several years. Just knowing what is going on in the industry, I have always heard positive things about Corelight. It was a known entity to me going as far back as five or so years ago. I knew about Corelight and I knew what they were doing. I knew that they had a good reputation. When I came here to work with Morphworks and ArrowPoint and saw that we were working with Corelight, I was very excited for that.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

"Before Corelight Open NDR, I did not use a different NDR solution; I had other security tools, but I did not have an NDR that I was feeding bulk packet ingestion into.

"I do not have experience with similar NDR solutions; however, what I can say is that before I implemented Corelight Open NDR, the one tool I did have was a NetScout nGeniusONE solution, which I got brought in to deploy and I manage that infrastructure. I use it a lot for service assurance and packet analysis once I know what I am looking for, but nGeniusONE cannot intelligently analyze the bulk of the packets that it digests and indicate which packets I need to look at.."

Anthony Budrecki

Principle Security Architect at Eversource Energy

Read full review

ROI

Real user quotes about their ROI:

"I believe I have seen a return on my investment with Corelight Open NDR. I have been part of many conversations about that and those are all positive conversations.."

Anthony Budrecki
Principle Security Architect at Eversource Energy

Read full review

"We immediately realized the solution's ROI. Its visibility into east-west traffic, being able to sample capture, gives a sense of traffic flow. Moreover, it's inexpensive.."

Dan Jeske
Account Executive at Fishtech Group

Read full review

"I think for what you are getting, you are getting a great deal. Corelight Investigator is sold as a software as a service license, and sensors are of course a one-time fee with their hardware maintenance. I think it is all at an appropriate market cost. On some opportunities we have looked at partnering with Corelight on, we see that we are able to provide very competitive pricing as partners going forward into certain opportunities. I think it is a very valuable price point where they have it right now.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

Use Case

"We use the solution for packet capture sampling. We offer it as part of our managed service. It's so we can identify east-west traffic on a customer's network.."

Dan Jeske
Account Executive at Fishtech Group

Read full review

"I have been using Corelight Open NDR solution for approximately three years. I leverage the Suricata engine heavily for alerting on indicators of compromise as my main use case for this solution.."

Anthony Budrecki
Principle Security Architect at Eversource Energy

Read full review

"Corelight is a network traffic analysis product. It is an enterprise solution of Zeek and Suricata. It is deployed mostly with physical sensors, although cloud, virtual and software sensors are available as well. We deploy it for our customers, and MSSP.."

José Luis Pozo
Pre Sales Technician at DotForce

Read full review

"I have been in my current role since August of last year, approaching nine to ten months. I am a growth and strategy lead at Morphworks and ArrowPoint. I also provide program management support on a Department of Defense contract where we heavily use Corelight products.

Our company has been using Corelight Open NDR for about three or four years as part of this program. I have been working alongside the Corelight team on this contract while exploring new opportunities for Corelight and us to grow together.

Specifically with what we are doing on this contract, there are adversaries to the United States that are attacking our critical industries, especially critical industries that tie to US federal government and Department of War. We help defense industrial base companies. They can be really small mom and pop shops making ball bearings that eventually end up in an aircraft carrier, or they could be a really large defense tech company doing something with artificial intelligence. Essentially, they are targets for our nation's adversaries. What we do is deploy Corelight sensors into their environments and we not only protect their networks by having those sensors in place, but also using Corelight Investigator platform to do managed detection and response. We gather intelligence on who is attacking these different critical companies for the government. The program that we are deploying these sensors under is structured so that the companies agree with the government that they will accept this protection and will provide the intelligence and data about what is happening on their network. We serve as the middle man in that process of deploying all these sensors, configuring all the environments, and providing some level of threat analysis and threat hunting. Additionally, we work alongside another team of analysts that are on Corelight Investigator platform as well, doing full threat hunting and identifying threats. When we identify significant alerts, there is an entire incident response and forensics package that is put together and sent back to those companies to let them know what has happened and what steps they need to take to make themselves whole again.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 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 was a consensus decision that I needed Corelight Open NDR to do large volume data ingestion and analysis because I cannot do it as a human, which was the specific tipping point that led to Corelight.."

Anthony Budrecki

Principle Security Architect at Eversource Energy

Read full review

"The initial setup was straightforward. When deploying Corelight, the customer just needs to put the solution on a VM. The only maintenance required is the maintenance of the license.."

Dan Jeske

Account Executive at Fishtech Group

Read full review

"It is very straightforward to choose one physical sensor because you have a sensor with all the installation pre-installed. It is a very straightforward solution because it has a sensory set already configured. You have to adapt it to integrate with your network, with packet brokers. This is the main step that we have to do to integrate with a network. It's not a complicated process.."

José Luis Pozo

Pre Sales Technician at DotForce

Read full review

"The initial setup is not straightforward. You need expertise for it. I rate the solution's documentation a six out of ten.

Deployment depends on the MVP, the amount and the capacity of the environment. If it's a huge customer, you will face big problem, and it will not be easy to implement. You will have multiple integrations, multiple positions to position the sensors. It will be easier to pick for the smaller customers or networks. Deployment can take be two weeks to three months to complete.

I rate the initial setup a five out of ten, where one is difficult, and ten is easy.."

HamadaElewa

Technical Sales Manager at Spire Solutions

Read full review

"Our deployments go very smoothly. Initially, our plan was to have on-site, in person install teams, but we found very quickly that the simplicity of the setup meant we could do everything remotely over the shoulder. All of our deployments involve shipping devices out to the end user, and then we just get on a virtual call and it involves plugging in a few things, and then we are able to connect it into Corelight Fleet Manager. We gather a few key pieces of data from the client ahead of time, we plug in that information including Internet Protocol addresses and some other straightforward configurations, and we are up and running. The deployments are very quick, and then in the first couple weeks, it is simply monitoring that traffic and seeing what is noisy, what is creating a lot of noise, and identifying those areas where we can tune rules to streamline the data that we are getting in to the information that we need to be seeing for proper threat detection.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

Customer Service and Support

"We had a couple of issues. We contacted their support, and they were helpful. They helped us a lot. They were very good. I would rate them a four out of five.."

Muteb Alqahtani
Manage Consultant at SITE

Read full review

"I have had great experiences with Corelight support, especially early on when getting to know the product and what happens under the cover. I use a lot of custom variables in my Corelight rules and my Suricata rules to filter out white noise, which brings in a lot of network objects that represent specific subnets on my network that I want to exclude from alerting. Corelight support was very helpful in showing me some tool sets they have under the covers that allow me to automate that process. I bring in hundreds of subnet variable definitions via an automated import process, enabling me to leverage all those variables in my Suricata alerts.

"Corelight support deserves an eight on a scale of one to ten, simply because I cannot imagine what a ten would be. I have never had issues with them, and they are top-notch support.."

Anthony Budrecki
Principle Security Architect at Eversource Energy

Read full review

"We definitely lean on Corelight support when we get to more unique or critical type issues. We find that we have very good support with them. We are able to get engaged, and we have access to a customer success manager that can help line us up. We also have a technical account manager and a whole team of people that are on call for us to reach out to. We also work closely and sit on their customer advisory board and take part in a number of product improvement meetings on a regular cadence. We are always sharing feedback, both technical support and product feedback, and we are hearing about new features well before or while they are in early development. We have a very close coordination with Corelight, and as a partner, we are looking at a number of different opportunities of how we can go to market together and further work together to provide different ways to get Corelight into the hands of people that need it. We have very close collaboration from a business to business standpoint, and I would say Corelight values us by making sure that we have these touch points at varying levels of the organization to help them improve their product and processes. I would probably say we are at an eight or nine as far as the quality of support, which I think is very reasonable. I think it has only been improving, and the customer success manager is a bit of a newer addition to the team, and I think we have been seeing positive impact from having them on that account team.."

Verified user

Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

Other Advice

“I don't have enough visibility in the competition in order to give you an accurate response to what could be improved. We are still new to this solution we don't know yet.

I would rate this solution an eight out of ten..”

Verified user
Chief Executive Officer at NetMetrix

Read full review

“It depends on the kind of customer, but I would recommend it for most companies that had a SOC. It is instrumental. I would rate this product a 10 out of 10. Corelight, including Zeek (former BRO) and Suricata, is well known by most cyber security analysts. For that reason, we have seen that people liked Corelight and Zeek. It adapts perfectly to the day to day work for people in security analytics..”

José Luis Pozo
Pre Sales Technician at DotForce

Read full review

“Explainable, structured network evidence like the data Corelight Open NDR provides is absolutely crucial compared to traditional black box logs that might lack the context an AI needs to reach an accurate verdict, as I look forward to incorporating large language models and AI into my SOC. Much of what I am doing this year is figuring out which rules I can use to detect which AI engines are

running under the covers that I might not be aware of.

“Corelight Open NDR has come in handy because I use Corelight and NetScout collaboratively now. I use the Corelight alerts to allow me to focus on the traffic that looks suspect, and then at that point, I dig into nGeniusONE, pull the packets from cache, and do the analysis. I did the Corelight deployment, and it was good; these are well-known appliances, brand name physical appliances configured as one would expect an enterprise appliance to be configured, running basically a Linux kernel with a web interface.

“In my environment, the deployment model for Corelight Open NDR is on-premises, but I can elaborate further if needed. I would rate this product an eight overall..”

Anthony Budrecki
Principle Security Architect at Eversource Energy

Read full review

“We are definitely staying aware of what Corelight's competitors are doing. I will say that we have made a strategic investment in partnering with Corelight, and we are really looking at expanding our opportunities to collaborate and deliver Corelight Open NDR and managed detection and response to other critical industries and other markets. It is definitely seeing either places where Corelight currently is or places where Corelight wants to be, and it very much aligns with a lot of what we believe, and we have this very close partnership with Corelight and a joint strategy we have to build towards some common goals.

Some things we are looking at is using our past performance on this contract that we are partnered on, protecting defense industrial base companies, and we are looking at other facets of critical industry, whether that be voting infrastructure at the state level, of which there has not only been a lot of press about, but also authentic attacks against and more and more legislation coming forward for protection of voting related systems. We are also looking at other facets of critical

infrastructure such as utilities and ports and how we can take a similar delivery model to them to protect them and provide them the additional value that the visibility that Corelight provides across someone's network. We are really moving past just providing a Corelight sensor and Corelight Investigator and Corelight Open NDR as a solution, and instead, we are packaging everything together and managing it on behalf of them should they not be able to take it on themselves internally.

I do not know exact figures, but across our program with these thirty or so companies that we have, we have detected somewhere between upwards of ten very serious activities over the past couple years that we have been able to get in front of and effectively prevent something from happening. These were nation state actor type threats. It is exactly what the program was set up for, as these companies are getting attacked by these advanced persistent threats, and we have been able to stop those. There is obviously plenty of activity happening day to day and alerts of varying criticality that we are managing, and we are reaching out to the customers on those, but as far as some really big ones, we have prevented some damage for sure. We have more than several success stories where something really serious was prevented. My overall review rating for Corelight Open NDR is nine out of ten.."

Verified user
Growth And Strategy Lead at a computer software company with 51-200 employees

Read full review

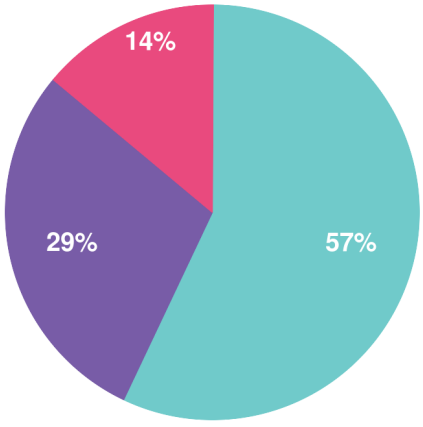
Top Industries

by visitors reading reviews

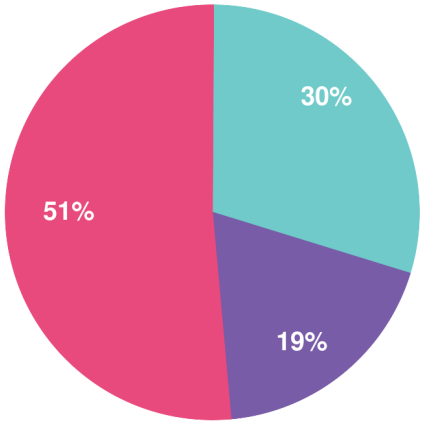
Financial Services Firm	12%
Government	12%
Computer Software Company	8%
Real Estate/Law Firm	8%

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 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