Network Detection and Response (NDR)

Buyer's Guide and Reviews

May 2020

IT Central Station
Unbiased reviews from the tech community

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

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a customized report personalized for you based on:

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

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

Get your personalized report here.

Contents

Vendor Directory

Awake Security	Awake Security Platform
Cisco	Cisco Stealthwatch
Darktrace	Darktrace
ExtraHop Networks	ExtraHop Reveal(x)
GoSecure	GoSecure Network Detection and Response
Lastline	Lastline Defender
LogRhythm	LogRhythm NetworkXDR
RSA	RSA NetWitness Network
Vectra AI	Vectra AI

Top Network Detection and Response (NDR) Solutions

Over 414,576 professionals have used IT Central Station research. Here are the top Network Detection and Response (NDR) vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

Views	Comparisons	Reviews	Words/Review	Average Rating
Number of views	Number of times compared to another product	Total number of reviews on IT Central Station	Average words per review on IT Central Station	Average rating based on reviews

Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows:

For each of **Reviews**, **Views**, and **Comparisons**, the product with the highest count in each area gets a maximum 18 points.
Every other product gets assigned points based on its total in proportion to the #1 product in that area.
For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's points for reviews would be 18 * 80% = 14.4.

Both **Average Rating** and **Words/Review** are awarded on a fixed linear scale.
For Average Rating, the maximum score is 28 points awarded linearly between 6-10 (e.g. 6 or below=0 points; 7.5=10.5 points; 9.0=21 points; 10=28 points).
For Words/Review, the maximum score is 18 points awarded linearly between 0-900 words (e.g. 600 words = 12 points; 750 words = 15 points; 900 or more words = 18 points).
If a product has fewer than ten reviews, the point contribution for Average Rating and Words/Review is reduced:
1/3 reduction in points for products with 5-9 reviews, two-thirds reduction for products with fewer than five reviews.

Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

All products with 50+ points are designated as a Leader in their category.

1 Cisco Stealthwatch

25,814 views **16,136** comparisons **36** reviews **497** words/review **7.9** average rating

2 Darktrace

28,531 views **20,594** comparisons **8** reviews **505** words/review **7.5** average rating

3 Vectra AI

6,128 views **4,645** comparisons **4** reviews **3,075** words/review **8.5** average rating

4 Awake Security Platform

2,200 views **951** comparisons **4** reviews **2,241** words/review **9.5** average rating

5 RSA NetWitness Network

81 views **56** comparisons **1** reviews **336** words/review **8.0** average rating

6 ExtraHop Reveal(x)

2,517 views **2,057** comparisons **0** reviews **0** words/review

7 Lastline Defender

1,049 views **619** comparisons **0** reviews **0** words/review

8 LogRhythm NetworkXDR

456 views **406** comparisons **0** reviews **0** words/review

9 GoSecure Network Detection and Response

2 views **0** comparisons **0** reviews **0** words/review

Top Solutions by Ranking Factor

Views

		VIEWS
1	Darktrace	28,531
2	Cisco Stealthwatch	25,814
3	Vectra AI	6,128
4	ExtraHop Reveal(x)	2,517
5	Awake Security Platform	2,200

Reviews

		REVIEWS
1	Cisco Stealthwatch	36
2	Darktrace	8
3	Vectra AI	4
4	Awake Security Platform	4
5	RSA NetWitness Network	1

Words / Review

		WORDS / REVIEW
1	Vectra AI	3,075
2	Awake Security Platform	2,241
3	Darktrace	505
4	Cisco Stealthwatch	497
5	RSA NetWitness Network	336

Cisco Stealthwatch

See 36 reviews >>

Overview

Cisco Stealthwatch uses NetFlow to provide visibility across the network, data center, branch offices, and cloud. Its advanced security analytics uncover stealthy attacks on the extended network. Stealthwatch helps you use your existing network as a security sensor and enforcer to dramatically improve your threat defense.

SAMPLE CUSTOMERS

Edge Web Hosting, Telenor Norway, Ivy Tech Community College of Indiana, Webster Financial Corporation, Westinghouse Electric, VMware, TIAA-CREF

TOP COMPARISONS

Darktrace vs. Cisco Stealthwatch ... Compared 27% of the time [See comparison]
FireEye Network Security vs. Cisco Stealthwatch ... Compared 5% of the time [See comparison]
Vectra AI vs. Cisco Stealthwatch ... Compared 4% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Comms Service Provider ... 30%
Software R&D Company ... 20%
Government ... 7%
Media Company ... 5%

COMPANY SIZE

1-200 Employees ... 13%
201-1000 Employees ... 10%
1001+ Employees ... 77%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Healthcare Company ... 24%
Financial Services Firm ... 16%
Manufacturing Company ... 8%
Transportation Company ... 5%

COMPANY SIZE

1-200 Employees ... 10%
201-1000 Employees ... 6%
1001+ Employees ... 84%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Cisco Stealthwatch

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Travis Bugh

The most valuable part is that Stealthwatch is part of a portfolio of security devices from Cisco, so while some of the competition may have other products that could be better or provide a better administrative experience, they don't have the breadth that Cisco does. Cisco literally can touch every single end point, every single ingress and egress point in the network. Nobody else has that. Stealthwatch has analytics and threat protection capabilities up there with the industry best. It's a super powerful database on the backend, basically giving y... [Full Review]

Technicab71a

The most valuable features are encrypted threat analysis and the ability to run jobs on entire flows. The reporting feature is helpful for creating documentation because you can export relevant information and paste it into the back of the report. I've found that the solution's analytics and threat detection capabilities are very useful. I would like it to be able to better integrate with Firepower, but it meets the needs that it was promising from the beginning. [Full Review]

NetworkAcb23

The most valuable feature of this solution is data hoarding because it catches threats on a frequent basis that we had no idea of. Like if certain hosts were talking to certain hosts. With this tool, we got that kind of information and it allows us to see when two hosts are talking when they shouldn't be talking at all. [Full Review]

NetworkE7689

The search options on Cisco Stealthwatch are the most valuable. You can get very granular with it, down to the kilobits or the seconds if you want. The product supports any time frame that you need, so that is nice. The solution affects network visibility in our company across all of our data, including our data center. All data transfers pass through our NetFlow collector. It's very easy to pinpoint any network anomalies or any type of suspicious behavior. NetFlow is very good at detecting those spikes and traffic. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Travis Bugh

The network visibility feature opens up a whole new pane of glass that didn't exist before, so when you talk about being able to look into your network and understand what's there for security events, impostering, and everything that Stealthwatch can bring to the table, there's nothing else that a typical customer's going to have installed today that will give them any of that information. Stealthwatch has definitely increased our threat detection rate. I would say on average probably close to 100%. Especially in the market that we play in, which is... [Full Review]

Technicab71a

We are a reseller, and we are able to show demos of this solution pretty quickly. It gets people really excited. The network visibility has vastly improved for the organizations that I assist with their services. Generally, they do not have lateral visibility into their network. We come in and deploy Cisco ISE, which helps them segment, but they still can't prove what is going on. Now, with this solution, they have the ability to not only show what a user has tried to do, but they can show where inside of the network it was stopped. From that point,... [Full Review]

NetworkAcb23

Cisco Stealthwatch has improved our organization's analytics and threat protection capabilities by catching threats early on. We are still at the baselining stage, but I can also say that our organization improved dramatically when we found out that a host was constantly talking to an FTP server. It turned out to be an employee that was going to be terminated and he was trying to pull data from the FTP server constantly. He pulled three or four GBs and we caught it with this tool. It saved us a net fortune. The solution has also increased our threat... [Full Review]

Cisco Stealthwatch

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Travis Bugh

I don't have a specific feature request, but my big push with Cisco has always been to make it easier for the administrators to use it. If you look at other products that they've been really successful within software space like Meraki, it's because a customer can jump right in and use it on day one and feel like they're accomplishing something with it. They don't have to have a Ph.D. Anything that we can do to make the customer experience better makes it easier for them to use it, which is what we want, and it also makes it easier for us to sell it... [Full Review]

Technicab71a

I would like this product to have better integration with Cisco Firepower. That is the easiest way to pair. Eliminating Java from the SMC would improve this solution. It would be better to let people know, upfront, that is doesn't give you nice, clear information, as seen in the demos, without Cisco ISE installed. Most of my customers are ISE-based so it doesn't matter, but I have to break the news to the ones who are not. [Full Review]

NetworkAcb23

One thing I would like to see improved is if it could automatically be tied through ISE, instead of you having to manually get notifications and disable it yourself. I am the only network admin at my facility, and when I'm on vacation for a week and there is an attack, I'm the only individual that gets alerts. Essentially there's a push button that you click to implement the policy through ISE to block that host or some other network essentially segregated from your internal network. I would like to see an automatic block function. I haven't noticed... [Full Review]

NetworkE7689

We don't use Cisco Stealthwatch for threat detection. We use it more for information gathering. We use better options for threat detection, i.e. Palo Alto firewalls for our security. I would like the search page available with Cisco Stealthwatch to be more intuitive. The previous release was better than the current one for the UI. We moved to the latest UI a couple of months ago, maybe like six months ago. I'm not a fan. I wish the search options were easier. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

NetworkAcb23

This solution is a little expensive. Open-source is obviously a key to victory in some people's eyes but with open-source, you can't pay anybody. So it could be a little cheaper, but it has great functionality. [Full Review]

NetworkEd59a

For our organization, it is cheap, but for other customers, it may be fairly expensive. As we are resellers of Cisco Stealthwatch, we hope to save time, money, and administrative costs once we start selling more of these solutions. [Full Review]

Darktrace

See 10 reviews >>

Overview

Darktrace is the world's leading machine learning company for cyber security.

Created by mathematicians from the University of Cambridge, Darktrace's Enterprise Immune System uses AI algorithms that mimic the human immune system to defend enterprise networks of all types and sizes.

Our self-learning approach is the first non-consumer application of machine learning to work at scale, across all network types, from physical, virtualized, and cloud, through to IoT and industrial control systems.

By applying its unique, unsupervised machine learning, Darktrace has identified 30,000 previously unknown threats in over 2,000 networks, including zero-days, insider threats and subtle, stealthy attacks.

SAMPLE CUSTOMERS

Irwin Mitchell, Open Energi, Wellcome Trust, FirstGroup plc, Virgin Trains, Drax, QUI! Group, DNK, CreaCard, Macrosynergy, Sisley, William Hill plc, Toyota Canada, Royal British Legion, Vitol

TOP COMPARISONS

Cisco Stealthwatch vs. Darktrace ... Compared 21% of the time [See comparison]
Vectra AI vs. Darktrace ... Compared 17% of the time [See comparison]
Palo Alto Networks Threat Prevention vs. Darktrace ... Compared 4% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 29%
Comms Service Provider ... 13%
Media Company ... 7%
Retailer ... 6%

COMPANY SIZE

1-200 Employees ... 21%
201-1000 Employees ... 25%
1001+ Employees ... 54%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 40%
201-1000 Employees ... 30%
1001+ Employees ... 30%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Darktrace

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

OseremeOsobase

The most valuable part of the product is the whole package. The features included in the Enterprise Immune System are complete and effective. Its detection engine is ridiculously good. [Full Review]

reviewer1260498

The Ability to drill right down into an event that has been identified as something of interest so that you can be assured if it is a valid event and therefore not suffer from loads of false positives. Once that initial assurance and confidence was there, you could easily rely on the dashboard and minimise the risk of constantly drilling into each and every event but pick the ones with most risk. [Full Review]

reviewer1248177

Once installed, it starts picking up and learning the network very well because it's got a powerful AI integrated into it. The user interface is very intuitive. The Dynamic Threat Dashboard is very nice, as it lists all of your threats and rates them, and then you can choose whether to investigate further. This solution has some good features for customization in terms of how you're tagging your network, which basically makes it easier to identify what is actually happening. You can see where the traffic is going, where it is coming from, and that s... [Full Review]

Tom Gamali

The most valuable feature is the alerts. The alerts are meaningful. The event rolls up into meaningful and actionable alerts rather than just being noise. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Philippe Panardie

Darktrace has improved our knowledge of abnormal phenomenen which could have potentially be hazardous for the organization.You have to be vigilant with GDPR compliance rules in Europe [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

OseremeOsobase

It is hard to really address what needs to be improved in the respect that it does everything I would expect of a superior solution. It is simple enough to use because the interface is quite simple, the setup is quick and painless — in only an hour the product is installed. Users can train on the system in less than three hours. When the configuration is complete they will already know what to do and they can just go on and use the product. I think that the price is quite good compared to other, similar products. They already have a plugin that you ... [Full Review]

Darktrace

Continued from previous page

reviewer1260498

The product is automated to a certain degree, but I think this could be improved. I'm looking for a way of being able to react to threats that are detected based on risk. Aside from that, there is nothing really that they could improve on, it's a product more suited to organizations with an SOC, security operations center, or a company with an IT team of network security members because it relies on constantly monitoring it to see information based on the risks of events. In our case, we have a small IT team, which means that a large amount of time ... [Full Review]

AsankaAbeyrathne

Darktrace needs to simplify most of the positive reports. We have to field all the positive reports, false positives, too. Sometimes we need to check false positives manually. We have to filter false positives. After that, we configure it again. Then, we want to analyze these false positives. That's the main thing. If we are assessing features, this should be easier to handle. Darktrace needs to automate the reports of false positives, botnets, and everything. So far, I think the solution is good. Not excellent, good. [Full Review]

Tom Gamali

The products is designed to monitor traffic sent and received via the corporate egress /network points. I would be interested to see further integration or development of a capability to obtain visibility of mobile devices such as Laptops and Mobiles, which operate outside of the network and may communicate specifically when off the corporate network. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

AsankaAbeyrathne

We are doing a monthly cost-basis. It's about 500,000 NKR because we are the first to implement it in Sri Lanka. We worked out direct pricing from Darktrace UK. After that, we selected a vendor in Sri Lanka. But the thing is, we are the first implementation here. I think they are actually undercharging and giving us the solution first because they want a reference from us since we are a bank in Sri Lanka. That's why they are doing it like that. There are no additional costs besides the license, except the 15% rate to the Sri Lanka government. [Full Review]

Vectra AI See 5 reviews >>

Overview

Vectra® is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to collect, store and enrich network metadata with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed.

SAMPLE CUSTOMERS

Tribune Media Group, Barry University, Aruba Networks, Good Technology, Riverbed, Santa Clara University, Securities Exchange, Tri-State Generation and Transmission Association

TOP COMPARISONS

Darktrace vs. Vectra AI ... Compared 61% of the time [See comparison]
Cisco Stealthwatch vs. Vectra AI ... Compared 11% of the time [See comparison]
ExtraHop Reveal(x) vs. Vectra AI ... Compared 2% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Comms Service Provider ... 26%
Software R&D Company ... 25%
Government ... 6%
Media Company ... 6%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Vectra AI

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

reviewer1259193

It gives us the point of where something is happening, which is the key thing for us. (I know that there is a back-end recall, which probably gives a lot more data, but we don't use that.) We then leverage our SIEM product to provide us logs from those specific sources that it's talking about, giving us that information. It is the accuracy of: It is happening here and on this particular host, then it's going to here to this particular host. It's that focus which is probably the most advantageous to us. The logic behind Vectra's ability to reduce ale... [Full Review]

reviewer1296420

One of the most valuable features of the platform is its ability to provide you with aggregated risk scores based on impact and certainty of threats being detected. This is both applied to individual and host detections. This is important because it enables us to use this platform to prioritize the most likely imminent threats. So, it reduces alert fatigue follow ups for security operation center analysts. It also provides us with an ability to prioritize limited resources. It aggregates information on a host and host basis so you can look at indivi... [Full Review]

reviewer1302852

The solution's ability to reduce alerts, by rolling up numerous alerts to create a single incident or campaign, helps in that it collapses all the events to a particular host, or a particular detection to a set of hosts. So it doesn't generate too many alerts. By and large, whatever alerts it generates are actionable, and actionable within the day. With the triaging, things are improving more and more because, once we identify and investigate and determine that something is normal, or that it is a misconfiguration and we correct it, in either of the... [Full Review]

reviewer1263180

We mainly use it for the detection types, checking dark IPS or command-and-control traffic. We bought Recall so we can have more information. Recall is an addition onto Vectra. We haven't enabled Recall yet, but we will. So, if there is an incident, we can investigate it a bit further with Vectra devices before going into other tools and servers. This gives us the metadata for network traffic. So, if we have a detection, we can check with Recall what other traffic we are seeing from that device, if there is anything else. It's mainly a quick and dir... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

reviewer1259193

The key improvement for us were: * The additional monitoring 24/7, and using the high fidelity alerting from Vectra rather than SIEM, This was our biggest change. We have managed to leverage that rather more than our SIEM, which just throws out loads of spam. * The FCA requirements to build on behavior monitoring. * The use case of the call center with its high turnaround of staff who are perhaps not as clued in or engaged in our user awareness program as they could be. * Lack of end user deployment is another big improvement. We wanted something th... [Full Review]

reviewer1296420

We have a limited use of Vectra Privileged Account Analytics for detecting issues with privileged accounts at the moment. That is primarily due to the fact that our identity management solution is going through a process of improving our privileged account management process, so we are getting a lot of false positives in that area. Once our privilege account management infrastructure is fully in place and live, then we will be taking on more privileged account detections and live SOC detections to investigate. However, at the moment, it has limited ... [Full Review]

reviewer1302852

What we have seen over the course of the three to four months it has been in place is that it has not found anything bad. That's good news because nothing specific has happened. But we have identified a lot of misconfigurations as well as some information on how applications are working, which was not known earlier. The misconfigurations that became known because of Vectra have been corrected. It has given us the opportunity to understand some of the applications better than we had understood them before because some of the detections required triag... [Full Review]

Vectra AI

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

reviewer1259193

Room for improvement depends on how their strategy and roadmap develops, as they have a lot of third-parties that they integrate with, e.g., more orchestration around what alerts and what to do with afterwards. They don't pretend to be working in that space. That is a third-party type activity. There are always the little things that they could do a bit better, like grouping or triage filters. Clearly, they've taken that onboard and developed those over the course of the last 18 months to two years to put these additional functions in. My guys are c... [Full Review]

reviewer1296420

You are always limited with visibility on the host due to the fact that it is a network based tool. It gives you visibility on certain elements of the attack path, but it doesn't necessarily give you visibility on everything. Specifically, the initial intrusion side of things that doesn't necessarily see the initial compromise. It doesn't see stuff that goes on the host, such as where scripts are run. Even though you are seeing traffic, it doesn't necessarily see the malicious payload. Therefore, it's very difficult for it to identify these type of ... [Full Review]

reviewer1302852

One thing which I have found where there could be improvement is with regard to the architecture, a little bit: how the brains and sensors function. It needs more flexibility with regard to the brain. If there were some flexibility in that regard, that would be helpful, because changing the mode of the brain is complex. In some cases, the change is permanent. You cannot revert it. I would like to see greater flexibility in doing HA without having to buy more boxes just to do it. Another area they could, perhaps, look at is with OT (operational techn... [Full Review]

reviewer1263180

We would like to see more information with the syslogs. The syslogs that they send to our SIEM are a bit short compared to what you can see. It would be helpful if they send us more data that we can incorporate into our SIEM, then can correlate with other events. We have mentioned this to Vectra. It does some things that I find strange, which might be the artificial intelligence. E.g., sometimes you have a username for a device, then it makes another. It detects the same device with another name, and that's strange behavior. This is one of the thing... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

reviewer1259193

We are running at about 90,000 pounds per year. The solution is a licensed cost. The hardware that they gave us was pretty much next to nothing. It is the license that we're paying for. I think if we outgrow our current hardware, then we will have a look at bigger hardware or some sort of distribution. I'm sure they have a number of different options for larger companies. I don't see that being a major issue for us in the next three to five years. We don't have complete visibility because we don't have all of that metadata surrounding it. Sometimes ... [Full Review]

reviewer1296420

At the time of purchase, we found the pricing acceptable. We had an urgency to get something in place because we had a minor breach that occurred at the tail end of 2016 to the beginning of 2017. This indicated we had a lack of ability to detect things on the network. Hence, why we moved quickly to get into the tool in place. We found things like Bitcoin mining and botnets which we closed quickly. In that regard, it was worth the money. Three years later, the license is now due for renewal so we will need to review it and see how competitive it is v... [Full Review]

reviewer1263180

The license is based on the concurrent IP addresses that it's investigating. We are around $300,000 a year for three years. We have 9,800 to 10,000 IP addresses. There are additional features that can be purchased in addition to the standard licensing fee, such as Cognito Recall and Stream. We have purchased these, but have not implemented them yet. They are part of the licensing agreement. [Full Review]

AWAKE Awake Security Platform

See 5 reviews >>

Overview

Awake Security is the only advanced network traffic analysis company that delivers a privacy-aware solution capable of detecting and visualizing behavioral, mal-intent and compliance incidents with full forensics context. Powered by Ava, Awake's security expert system, the Awake Security Platform combines federated machine learning, threat intelligence and human expertise. The platform analyzes billions of communications to autonomously discover, profile and classify every device, user and application on any network. Through automated hunting and investigation, Awake uncovers malicious intent from insiders and external attackers alike. The company is ranked #1 for time to value because of its frictionless approach that delivers answers rath... [Read More]

SAMPLE CUSTOMERS

Coming Soon...

TOP COMPARISONS

Darktrace vs. Awake Security Platform ... Compared 60% of the time [See comparison]
Vectra AI vs. Awake Security Platform ... Compared 19% of the time [See comparison]
Cisco Stealthwatch vs. Awake Security Platform ... Compared 11% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 22%
Comms Service Provider ... 21%
Healthcare Company ... 7%
Media Company ... 7%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

AWAKE Awake Security Platform

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Kristofer-Laxdal

What is impressive about the tool is the time to value. Plugging it onto our network, we have found things that other tools have just never seen. We found those issues quickly and were able to action against those issues, remediating them quickly. I don't know another product that delivers as much value so quickly. I have the tool set up to alert, be able to look at things, and put things together graphically. This helps to understand the fingerprints of the device, what the device has done, where it's been, and what it's doing on my network. It rea... [Full Review]

John Chesson

The most valuable feature is the ability to see suspicious activity for devices inside my network. It helps me to quickly identify that activity and do analysis to see if it's expected or I need to mitigate that activity quickly. One of the best use cases was when we knew that one of our vendors that came into our site had a ransomware event at their corporation. I was able to quickly find his device using the Awake system and determine that there was no threat in our system. Something like that usually would have taken four to five hours. It took m... [Full Review]

reviewer1217625

There are quite a few valuable features. The most valuable aspect of the tech is the fact that it's like a "force-multiplier." It will reduce the amount of time and effort it takes to triage a potential compromise. That's important because, in everyday slang, time is money. If you've ever done a business-impact analysis — business continuity — if an attacker can reduce the confidentiality, integrity, or availability of a given system, it will have a financial impact. The quicker you can eliminate or mitigate the compromise, or avoid it altogether, t... [Full Review]

reviewer1342227

The portion that I use the most is the Adversarial Modeling trend. This threat graphing is probably the most useful feature that we have right now. It displays the data that Awake collects, displaying it in a very easy to read and understandable manner. This is compared to other tools in this similar space, where I found the learning curve and the ability to understand what those tools were analyzing and reporting difficult because it took a bit more time to learn how they reported. The data science capabilities of this solution are good. It provide... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Kristofer-Laxdal

It is all about visibility. From an information security standpoint, the capability for the team to be able to single out devices to respond quickly and intelligently, to say for example, "It is this laptop (or endpoint) from this person in finance. I know exactly what it's doing, what's wrong, and I know how to fix it." So, they're empowered walking up to that department or individual. The face of information security used to be, "Oh, the security guys are on that floor." Now, there's a different take. "These guys know what they are doing and are h... [Full Review]

John Chesson

The way their algorithm works, they have a threat model that brings up the most concerning activities, pretty much like an analyst who is very knowledgeable. On a tier level, a Tier 4 analyst would recognize the suspicious activity. Their algorithm takes somebody who is a Tier 1 or Tier 2 and gives them that clarity at a glance. Their knowledge is pretty top-notch. I also have the added feature of having an analyst that I work with at Awake to help me interpret some of the risk, which is a top-level-analyst type of assistance. The biggest thing it h... [Full Review]

reviewer1217625

We had an event where an attacker tried to steal login credentials. We were able to find the targets on the network using Awake and we were able to turn on multifactor authentication, not only for those users but for the entire enterprise. We were discovering that that was a very common attack tactic. It was a driver for change. Now, all users at this company have multifactor authentication as a result of Awake's capabilities. For a long time I was the only person in our company doing security. We're a $30 billion dollar company. So you can imagine ... [Full Review]

AWAKE Awake Security Platform

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Kristofer-Laxdal

The only issue is that Awake affords you so much information behind its fingerprinting capability. When it does trigger, you need to have a hard look at what is going on because there is a reason for that trigger. They have worked very hard on the interface. I would like to see things laid out somewhat differently, and not due my familiarity with the tool. The tool has grown a lot since I started using it in October, and there is room for user interface improvements. I would like to see the capability to import what's known as STIX/TAXII in an IOC f... [Full Review]

John Chesson

There's room for improvement with some of the definitions, because I don't have time and I'm not a Tier 4 analyst. I believe that is something they're working towards. They're working with me to add new features to make it easier for me to tell what a threat is and determine whether it's important or not. They're making improvements and providing updates almost monthly now, so each time they make those improvements it gets clearer for me. [Full Review]

reviewer1217625

I would like to see a bit more in terms of encrypted traffic. With the advent of programs that live off the land, a smart attacker is going to leverage encryption to execute their operation. So I would like to see improvements there, where possible. Currently, we're not going to be decrypting encrypted traffic. What other approaches could be used? [Full Review]

reviewer1342227

Some of the searching capability is a bit hard to use without in-depth knowledge. In one of the earlier versions, there was a tool that helped you build some of your searches and help you correlate your data manually. This seems to have been removed in a later version. That is probably the biggest thing I've noticed. Be prepared to update your SOPs to have your analysts work in another tool separately. There are some limitations in the integrations right now. One of the things that I want from a security standpoint is integration with multiple tools... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Kristofer-Laxdal

I signed a three-year deal as it was most cost effective for my firm - with no doubt in my mind we will see ROI in year one. I am hoping to involve them in a managed network detection and response relationship as well, which is another one of their offerings. There are no additional costs. The product does what it says that it will do. [Full Review]

John Chesson

Compare the cost of hiring and retaining a sophisticated analyst to the Awake Security Platform. The solution pays for itself in a matter of months and goes on to save you money, longer-term. [Full Review]

RSA NetWitness Network

See 1 review >>

Overview

RSA NetWitness® Network exposes network data to enhance a security team's capabilities to detect and respond to today's advanced threats. RSA NetWitness Network provides immediate deep visibility for rapid detection, efficient investigation and forensics, in order to reduce dwell time. With unparalleled speed for real-time behavior analytics, RSA patented technology accelerates detection and investigation of threats as they traverse your network. RSA NetWitness Network provides real-time visibility into all your network traffic—on premises, in the cloud and across virtual environments. RSA NetWitness Network enables threat hunting with streamlined workflows and integrated, automated investigation tools that analysts use to hunt and monitor ... [Read More]

SAMPLE CUSTOMERS

Busan Bank, Banorte Bank, Eastern Bank

TOP COMPARISONS

Vectra AI vs. RSA NetWitness Network ... Compared 40% of the time [See comparison]
Darktrace vs. RSA NetWitness Network ... Compared 33% of the time [See comparison]
ExtraHop Reveal(x) vs. RSA NetWitness Network ... Compared 28% of the time [See comparison]

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

RSA NetWitness Network

Continued from previous page

Top Reviews by Topic

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

reviewer973458

When analyzing something, you have to click several times. It requires a lot of effort to find something. The sole purpose of NetWitness is to find text easily, so this is an area that needs to be improved. The scalability needs improvement, but I think that it is technically difficult. This is a complex tool to use. In the next release, if they could include a detection feature or improve the detection then I would like it better. [Full Review]

ExtraHop Reveal(x)

Overview

Reveal(x) provides the visibility, insights, and answers that security analysts need to respond quickly and confidently to the highest priority threats against their organization's critical assets. It starts by automatically discovering and classifying every device communicating across the network, and using machine-learning driven behavioral analysis to detect anomalous and malicious activity.

SAMPLE CUSTOMERS

Wood County Hospital

TOP COMPARISONS

Darktrace vs. ExtraHop Reveal(x) ... Compared 44% of the time [See comparison]
Cisco Stealthwatch vs. ExtraHop Reveal(x) ... Compared 20% of the time [See comparison]
Vectra AI vs. ExtraHop Reveal(x) ... Compared 10% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Software R&D Company ... 29%
Healthcare Company ... 20%
Comms Service Provider ... 10%
Insurance Company ... 8%

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

Lastline Defender

Overview

Lastline's unique approach to breach detection is the culmination of more than ten years of R&D specifically focused on advanced and evasive breach weaponry and tactics. The result is a software-based platform designed to integrate breach detection capabilities seamlessly into your existing security portfolio.

SAMPLE CUSTOMERS

CKE Restaurants Inc., WatchGuard, S&P 400 Financial Services Leader, Hewlett Packard, Gwinnett County Public Schools, Aerospace Innovator, Global Media Conglomerate, Cellopoint

TOP COMPARISONS

BitSight vs. Lastline Defender ... Compared 25% of the time [See comparison]
Darktrace vs. Lastline Defender ... Compared 21% of the time [See comparison]
Forcepoint Web Security vs. Lastline Defender ... Compared 14% of the time [See comparison]

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

LogRhythm NetworkXDR

Overview

LogRhythm NDR is a network security solution for detecting, qualifying, investigating, and responding to advanced network-borne threats. It provides the speed and full network visibility needed to combat attacks across your on-premise, remote, and cloud environments.

The solution surfaces these threats through centralized, machine-based analysis of network traffic, including TTP scenario-based modeling, IOC signature-based inspection, and behavioral analysis.

LogRhythm NDR leverages the power and capabilities of the LogRhythm NextGen SIEM platform, including patented and award-winning security analytics and embedded SOAR functionality.

LogRhythm NDR has enabled customers to successfully catch, investigate, and respond to an array of thre... [Read More]

SAMPLE CUSTOMERS

TOP COMPARISONS

Darktrace vs. LogRhythm NetworkXDR ... Compared 41% of the time [See comparison]
Vectra AI vs. LogRhythm NetworkXDR ... Compared 26% of the time [See comparison]
Palo Alto Networks Threat Prevention vs. LogRhythm NetworkXDR ... Compared 9% of the time [See comparison]

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

GoSecure Network Detection and Response

Overview

Endpoints Are the Start,

but Lateral Movement Could Be the True Goal

Breaches happen many ways. While endpoints are commonly thought of as the main target, in many cases they are simply the entry point to lateral movement. GoSecure Network Detection and Response identifies lateral movement to stop the breach from spreading.

Visibility Leads to Detection

Detection requires visibility. The better the visibility, the faster the detection. GoSecure Network Detection and Response quickly correlates endpoint and network activity, using our multi-observational analysis, to pinpoint suspicious/malicious intent and respond accordingly.

Multiple Sources for Better Visibility

Network Intrusion Detection System (NIDS)

GoSecure Managed Detection and R... [Read More]

SAMPLE CUSTOMERS

TOP COMPARISONS

* Data is based on the aggregate profiles of IT Central Station Users reviewing and researching this solution.

About this report

This report is comprised of a list of enterprise level Network Detection and Response (NDR) vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

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

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

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

IT Central Station helps tech professionals by providing:

- A list of enterprise level Network Detection and Response (NDR) vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station
244 5th Avenue, Suite R-230 • New York, NY 10001
www.ITCentralStation.com
reports@ITCentralStation.com
+1 646.328.1944