aws marketplace

ExtraHop Reveal(x)

# Reviews, tips, and advice from real users






Powered by PeerSpot

# Contents

# Product Recap

ExtraHop Reveal(x)

# ExtraHop Reveal(x) Recap

ExtraHop Reveal(x) offers advanced network visibility and threat detection through seamless integration with CrowdStrike. It enhances security with machine learning-driven behavioral analysis and customizable dashboards.

ExtraHop Reveal(x) excels in network detection and response by decrypting SSL traffic and providing real-time packet inspection. Users benefit from its dynamic triggers and historical data tracing. The platform is valued for its depth of information, powerful analytics, and cloud-based administration. It allows effective monitoring of attack chains and integrates with other solutions to boost security. However, there is room for improvement in pricing flexibility, licensing models, and integration capabilities, particularly with Microsoft Sentinel.

**What are ExtraHop Reveal(x)'s Key Features?**

- Seamless Integration: Collaborates with CrowdStrike for enhanced threat detection.
- Network Visibility: Offers comprehensive insights into network activities.
- Real-Time Packet Inspection: Monitors and analyzes traffic in real-time.
- SSL Traffic Decryption: Ensures visibility into encrypted communications.
- Machine Learning Analysis: Utilizes ML for behavioral pattern recognition.

**What Benefits Should Be Considered When Evaluating ExtraHop Reveal(x)?**

- Enhanced Security: Improves threat detection and response capabilities.
- Advanced Analytics: Provides in-depth analysis of network behavior.
- Cloud-Based Management: Simplifies administration and scalability.
- Ease of Use: Offers user-friendly, customizable dashboards.
- Comprehensive Visibility: Delivers detailed insights into attack chains and compliance monitoring.

ExtraHop Reveal(x) is employed across industries for network traffic monitoring, malware detection, and real-time analysis. Analysts use it for server-to-server networking insights and application troubleshooting. Companies leverage its capabilities for behavioral analytics and compliance monitoring without deploying sensors on individual devices.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

"The best features of ExtraHop Reveal(x) include the cloud-based Reveal(x) 360, which is an absolute plus; you've got one point of administration where you can attach multiple vendors or solutions or sensors, and that's good."

Henri Heuvel

Technical Consultant at Axians

"The best features of ExtraHop Reveal(x) for me are the depth it provides, especially the picturization where the connection is established; it's absolutely remarkable."

Verified user

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

"The solution offers a friendly GUI for security features."

Verified user

Network Consultant at a non-profit with 201-500 employees

"Reveal X integrates seamlessly with CrowdStrike. If you see something sketchy on the network, you can quarantine devices through ExtraHop and it'll push to the CrowdStrike server."

Jordan Swanson

Information Security Assurance Engineer at School District of Lee County

"With ExtraHop Reveal(x), it gives me more visibility into the packets. It doesn't provide the entire packet capture, but it offers more information on how connections are made at the network layer. This can be helpful for detecting network attacks. Additionally, I really like the customizable dashboards and reports. The incident dashboard and alerts provide a good summary initially, and diving deeper into them gives more detailed information. It's also great for analyzing specific attacks and victim logs. The feature that tracks the full attack chain makes it easier to monitor the progress of attacks. Plus, it's connected to the Netria.com app, which I find useful for certain tasks."

Verified user

Cyber security specialist officer at a financial services firm with 5,001-10,000 employees

"When there are performance issues with an HTTP app, ExtraHop enables us to identify the causes within a few minutes. We can see what transactions are being impacted by something that may be happening within the server environment."

Henry-Steinhauer

Systems Engineer at LifePoint Health

"ExtraHop Reveal(x) is one of the tools that works out of the box when it comes to threat hunting."

Verified user

Cyber Security Engineer II at a healthcare company with 10,001+ employees

## What users had to say about valuable features:

"I like their dashboards. It has machine learning, and it has great analytics for security, network, and microservice performance.

Out of the box, with very little configuration, it does more than all the other tools. The features that other vendors promise to be available within six months to a year of purchase are already available in this product.."

**John Boake**

Senior monitoring engineer at a financial services firm with 10,001+ employees

Read full review

"We had useful information within the hour of deployment. The ability to trace back for historical analysis, as well as the behavioral analysis done with the security information, puts the user in a position to make an informed decision to mitigate the performance or security incidents. Regarding the security incidents, Reveal (x) is able to create incident cards that guide your teams through the incidents and gives you the option to delve into the transaction detail to potentially view payloads as well. The ability to integrate with various other solutions enables improvement in existing processes.."

**Dawid Van Der Merwe**
Sales Engineer | Technical Sales | Pre-Sales at SUSE

Read full review

"Reveal X integrates seamlessly with CrowdStrike. If you see something sketchy on the network, you can quarantine devices through ExtraHop and it'll push to the CrowdStrike server.

It's a ton of data. CrowdStrike looks at anything that's on the machine and the network. Instead of having hard points on your network core switches with some antivirus on it or your firewall or rules at your internet service provider or things managing your cloud for access control, this lets you see actual traffic and it's a little bit more fluid in what you're allowed to see.."

**Jordan Swanson**
Information Security Assurance Engineer at School District of Lee County

Read full review

"The best features of ExtraHop Reveal(x) for me are the depth it provides, especially the picturization where the connection is established; it's absolutely remarkable. If I want to know a specific IP and which server it has been connected to, it's easy to gather those kinds of trees from the NDR.

"ExtraHop is very customizable, it's easy to access, and I can understand the flow where an IP address or email address has reached which level of security system; it's very easy to follow that flow.."

**Verified user**

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

"ExtraHop Reveal(x) is very easy to use and intuitive. ExtraHop Reveal(x) can pick up threats without any customization on the threat detection when none of my other tools can pick up. I've been told to make my other tools work how ExtraHop Reveal(x) works. I'm trying to get my SIEM to perform the way ExtraHop does out of the box.

For example, we're starting to ingest our DNS logs to be able to pick up on something that's called DNS tunneling. ExtraHop picks it up in the middle of it. My SIEM, however, didn't have the log. So, I have to work with the server team. It's been two-plus months trying to get those logs up and running, but I am still not there yet. The other tool I have didn't tell me for almost 24 hours.

ExtraHop was able to pick it up in the middle and detect there's DNS tunneling. ExtraHop Reveal(x) is one of the tools that works out of the box when it comes to threat hunting.."

**Verified user**

Cyber Security Engineer II at a healthcare company with 10,001+ employees

Read full review

“The best features of ExtraHop Reveal(x) include the cloud-based Reveal(x) 360, which is an absolute plus. You've got one point of administration where you can attach multiple vendors or solutions or sensors, and that's good.

“The plus is the capacity of the different sensors that the ExtraHop solution has; it's quite big compared to the price it costs, and the detailed dashboarding is a big plus to get proper insights on both traffic and asset visibility within the network.

“The machine learning-driven behavioral analysis feature is quite useful. I do quite a lot of POVs with customers for a period of four weeks, and I always tell them that in the first week, week and a half, the machine needs to learn the network. Customers appreciate it, so that's good.

“On the other side, it gives you clear insights into what the normal baseline would be and what the actual deviation is after machine learning has understood how the network functions. It's very useful..”

**Henri Heuvel**
Technical Consultant at Axians

Read full review

# Other Solutions Considered

"So, in my experience with ExtraHop Reveal(x), I've found it to be a reliable tool. I haven't come across anything that compares directly to what Reveal(x) offers. ."

**Verified user**

Cyber security specialist officer at a financial services firm with 5,001-10,000 employees

Read full review

"We considered using Riverbed's analysis tools for this type of process, but it never panned out. It was always a problem to get into the right spot to grab the data we needed, but that was always challenging with their devices.."

**Henry-Steinhauer**

Systems Engineer at LifePoint Health

Read full review

"We have used other solutions from other vendors like NetScout, Sinefa, etc. where the client budget, requirement and focus changed. Some clients prefer certain vendors since they might have a standing relationship with them.."

**Dawid Van Der Merwe**

Sales Engineer | Technical Sales | Pre-Sales at SUSE

Read full review

"At the moment, we are using different endpoint solutions, including EDR, and we have extra NDR solutions.

"XDR is from Microsoft, and MDR is not from Microsoft; it's ExtraHop.."

**Verified user**

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

"We've done our due diligence and research on other products such as Riverbed and NetScout. This product is by far the supreme leader. It does full decryption currently at a hundred gigabits per second on a single appliance. Their next generational appliances are going up to 400 gigabits per second. That's full decrypt, which means a consistent rate. So, it can decrypt packets and store over 4,000 metrics from these packets. It's an invaluable tool.."

**John Boake**

Senior monitoring engineer at a financial services firm with 10,001+ employees

Read full review

# ROI

Real user quotes about their ROI:

“It reduces our MTTR. The mean time to repair is reduced dramatically because you can quickly isolate where the problem is. I can quickly say the problem is not a network-related problem. It’s a server-related problem or an application-related problem. The return on investment on this one is probably seen in the first year of purchase.

We have some fairly hefty applications. We're a finance company. So, we're constantly processing banking information, credit card information, and online transactional information. It's constantly running through our mainframes or data centers. So, it's invaluable that we keep the lights on and these applications running as smoothly and as efficiently as possible..”

**John Boake**

Senior monitoring engineer at a financial services firm with 10,001+ employees

Read full review

“My clients do see an ROI from ExtraHop Reveal(x); they see the value of the solution within the network, and it gives them solid confidence that they actually do see everything that's going across it.

“Looking at the Dutch market, where I am based, and looking at the positioning and the customer base, for instance, educational customers with 20,000 clients find the price has a high impact on positioning it properly within educational environments.

“In contrast, if you look at healthcare, where there are quite a lot of devices in the network or people that come and go, the amount of devices can become quite high, impacting the licensing model of ExtraHop and therefore the cost. The cost and return on investment are relative; if you have an enterprise customer with a static environment, it's quite easy to accept the cost and therefore see the return on investment. However, with other verticals, it's a lot harder to position the solution successfully..”

**Henri Heuvel**
Technical Consultant at Axians

Read full review

# Use Case

"I'm on the cybersecurity team. I do a lot of the blue threat-hunting and incident response. The things I deal with have nothing to do with network performance, but I handle the detections and things that ExtraHop Reveal(x) can pick up.."

**Verified user**

Cyber Security Engineer II at a healthcare company with 10,001+ employees

Read full review

"It's used by application owners and network engineers for troubleshooting application performance issues or network performance issues.

It's a hybrid solution. We have on-prem sensors and trace appliances and a cloud control appliance.."

**John Boake**

Senior monitoring engineer at a financial services firm with 10,001+ employees

Read full review

"Being in a financial institution, we have certain regulations such as PCI DSS, so we want to ensure any connection from a non-PCA segment is not being connected to a core segment; vice versa connection should not happen. We have something called a server segment and a workstation segment, so apart from the whitelisted internet connection, no connection should be established from the server segment. These are the monitoring use cases we have implemented in ExtraHop Reveal(x) so far.."

**Verified user**

Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

"The typical use case for ExtraHop Reveal(x) that we use is from a security perspective, specifically Network Detect and Response. The ExtraHop solution has both the network analytics and the security side of it, and a typical use case is the security side of the entire solution.

"We position it in a network to do security-based analytics, detections, and threat and anomaly detection. That's what we position it for and use it for.."

**Henri Heuvel**

Technical Consultant at Axians

Read full review

“We are a healthcare organization with more than 80 facilities, but I'm the only one who uses ExtraHop. When there are performance issues with an HTTP app, ExtraHop enables us to identify the causes within a few minutes. We can see what transactions are being impacted by something that may be happening within the server environment.

We set up a number of traffic sources that are typically either ERSPANs or TAPs and place ExtraHop appliances at critical places within the network. That traffic is typically fed into a packet. We have four small devices designed to go into small data centers. We're continually rotating those around to different facilities to help identify issues. They have helped us to understand what's going on.

The ExtraHop appliance enables you to do what an expert using Wireshark can do. However, it's all in the firmware, so you can do real-time analysis without the need to boil terabytes worth of data to find out what's happening..”

**Henry-Steinhauer**
Systems Engineer at LifePoint Health

Read full review

“Initially, we deployed Reveal as a standalone solution for network detection and response. It provided us with data and analytics on server-to-server enterprise networking. We used it to gain visibility into the amount of traffic and where it's going. For example, it will say that 28 gigs of data went to Google and break that down based on all the sites that have been visited.

It also tells you about the authentication data and helps you visualize how data moves across your network. Based on that, you can adjust the routing tables to make things work a little more evenly. It will also help you identify specific types of malware and how it moves across devices, what protocols and ports it uses, etc.

Unlike Crowdstrike, Reveal(x) doesn't require you to deploy sensors. CrowdStrike puts a sensor on the computer, so I know exactly how many devices are going through it. It's roughly 50,000. Those aren't people using it. Those are just devices that exist in the world. ExtraHop just looks at traffic, so each device connected to the network goes through it, and that's around 230,000 devices, and it's monitoring all the traffic to and from the internet..”

**Jordan Swanson**
Information Security Assurance Engineer at School District of Lee County

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.

"The solution's initial setup process is easy. We have to scan the port and tune the configuration for deployment. It takes a week to complete the process.."

**Verified user**

Read full review

Presales Consultant at a tech services company with 201-500 employees

"The console is a cloud product. There's also an on-prem server that collects and aggregates the data and sends it to your cloud instance. There's an appliance and a cloud console. Deployment and maintenance require only one person. ."

**Jordan Swanson**

Read full review

Information Security Assurance Engineer at School District of Lee County

“The product's initial setup is not very complex, but I would not say it's a very simple process.

The solution is deployed on the cloud and on an on-premises model..”

**Amer_Alkhawaldeh** Read full review

Account Manager at a tech services company with 11-50 employees

“The initial setup was not complex. We found the implementation process to be quite simple and straightforward.

It took approximately three weeks to deploy the solution and to have everything up and running.

The great part about the solution is that maintenance is minimal. It's mainly just software upgrades when they're released. When upgrades are needed, our network team is able to handle everything in house..”

**Verified user** Read full review

Technical Account Manager at a security firm with 501-1,000 employees

"Setting up ExtraHop is complex because we needed a nuanced understanding of the data flows into our data center. We need to know where things are coming into the environment versus where we thought they were entering. It's a complicated process of setting up the network taps and sending the data into a packet broker that forwards it to our ExtraHop device.

The packet broker was required because we had so many different taps bringing data into the ExtraHop. ExtraHop only had four interfaces to receive data, yet we had 20 different taps that had been placed. Some of those taps required two interfaces each to absorb the data that was tapped.."

**Henry-Steinhauer**
Systems Engineer at LifePoint Health

Read full review

“It was pretty straightforward. After you've done it once or twice, it's pretty simple and straightforward.

It was really easy and straightforward for me. The problem is that there are so many bits and pieces that are required on the outside in order to get the inside working. It reads packet data. So, I have to somehow get the packets to the appliances. The complexities come in when you are trying to create the packet stuff on the outside.

It has taken us two years to do this implementation. The hardware is easy to put in, but I work with so many other groups that it's difficult to get the time and resources to get hardware racked, get IP addresses, and get cabling done. It's all done by different teams. Our company makes it difficult. If I was at my previous company, it would be a breeze because I would just order the hardware, and I would rack it myself. I would cable it myself, IP it myself, hook it up at the switch myself, and do all the configuration myself, but because I have to go through so many other teams and groups, it's much more difficult now..”

**John Boake**

Senior monitoring engineer at a financial services firm with 10,001+ employees

Read full review

# Customer Service and Support

"I would rate the technical support from ExtraHop a solid eight. It's not exceptional, but it's definitely not bad. There are a lot more worse examples in the market, so it's good and we are happy.."

**Henri Heuvel**
Technical Consultant at Axians

Read full review

"Problems with the response time from the technical support team crop up since support teams might be operating in a country with a different time zone. I rate the technical support an eight out of ten.."

**Amer_Alkhawaldeh**
Account Manager at a tech services company with 11-50 employees

Read full review

"We've never had to contact technical support. We haven't had any major issues. Therefore, I wouldn't be able to rate the level of their service. From a product perspective, it's been very good so far.."

**Verified user**
Technical Account Manager at a security firm with 501-1,000 employees

Read full review

“The solution's technical support is great. Unlike other vendors that take more than two months to fix simple problems, ExtraHop's technical support team does actual troubleshooting over the phone. A lot of times, they fix it on the back end without any intervention from me..”

**Verified user**

Cyber Security Engineer II at a healthcare company with 10,001+ employees

Read full review

# Other Advice

“If you want to implement the SOC, then you must use the ExtraHop for the SOC operating system.

I recommend the solution and rate it a seven out of ten. .”

**Seksan Srisakorn**
Business Development Manager at Westcon-Comstor

Read full review

“My advice to others considering ExtraHop Reveal(x) is don't doubt, just get it and make sure you have the money because the return on investment will prove itself, and you only need to have one problem for the solution to prove its value. On a scale of one to ten, I rate ExtraHop Reveal(x) an eight..”

**Henri Heuvel**
Technical Consultant at Axians

Read full review

"We have approximately two people who do the maintenance of the solution.

My advice to others is for them to make sure that ExtraHop Reveal(x) can see everything within their environment. Additionally, review the packet capture and look into the tuning features within it to tune your exceptions. They're pretty granular and don't tune them too broadly to where you exclude things that you want to see.

I rate ExtraHop Reveal(x) a seven out of ten.."

**Serena Bryson**
Information Security Program Manager at a non-profit with 11-50 employees

Read full review

"As for advice or recommendations for someone considering implementing ExtraHop Reveal(x), I'd say it's a good investment, especially considering its price point. It's a great product, particularly for enhancing security measures. Before installing this solution, it's important to consider its compatibility with your existing security infrastructure. While Managed Detection and Response (MDR) solutions are commonly used for comprehensive security, Reveal(x) stands out for its specific strengths in network security.

I would rate it 8 out of 10. ."

**Verified user**
Cyber security specialist officer at a financial services firm with 5,001-10,000 employees

Read full review

"I rate ExtraHop Reveal(x) 10 out of 10. This is more of a nice-to-have rather than

a must-have solution. Something like a CrowdStrike or a next-gen AV is an essential product, whereas NDR is more of a nice-to-have thing. If you only have a little bit of traffic, you're probably not going to get anything out of it.

It's better for a medium-to-large enterprise. It's more appropriate for companies wh a massfootprints or industrial applications using use nonstandard devices. It's helpful for things that use SCADA, the Internet of Things, somethingings that don't fit neatly into other management categories. Itty common for industrial, construction, or maintenance devices to be a little lackluster in their security.

Major breaches like the Colonial Pipeline hack and attempted hacks on nuclear power plants all went through Internet of Things vulnerabilities and other devices where security wasn't part of their plan. This helps you cover yourself by monitoring the traffic. With something like CrowdStrike, you need to put the CrowdStrike sensor on it, but Reveal(x) looks at everything on the network.."

**Jordan Swanson**
Information Security Assurance Engineer at School District of Lee County

Read full review

"ExtraHop Reveal(x) is a new solution for me, from an NDR SIM perspective, that's a monitoring solution we have just implemented. We are not sure how efficient an NDR is to detect network-level threats; it needs to be explored.

"At the moment, we don't use the machine learning driven behavioral analysis feature; we're not sure where the data will be hosted and where it will be sent, so we don't want to do any kind of AI-based and machine learning-based decision making.

"We don't want to decrypt any of the information; it's supposed to be captured based on the network flow of the packets without opening or reading them, considering the sensitive information stored under the packets.

“I have not put any statistics or metrics to evaluate the effectiveness of ExtraHop Reveal(x) at the moment; it's still on the roadmap. This is an experience from SIM, and many stakeholders also need to be given feedback on the effectiveness, especially to validate with the business if it's blocking any genuine operations which cause an impact or not.

“So far, I am using only EDR, the Microsoft EDR, for containment and related activities; there is no automation at the NDR level at the moment, but it is in the roadmap for future use.

“If you have proper network segmentation, then I would recommend going for this kind of NDR monitoring with ExtraHop Reveal(x) as it provides more insights about what is happening in the networks. If you don't have network segmentation and only small subnets of IPs, I suggest not to go for NDR solutions because they won't add any value, even if you have many solutions on your network.

“I would rate ExtraHop Reveal(x) eight to nine out of ten..”

**Verified user**
Assistant VP, Idm Compliance at a financial services firm with 1,001-5,000 employees

Read full review

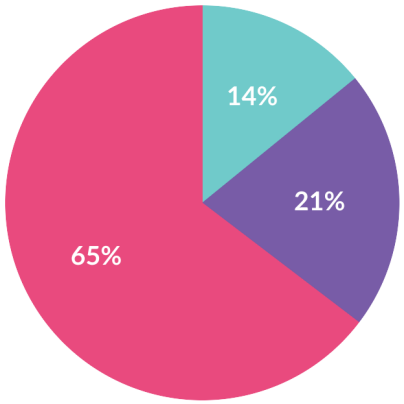
# Top Industries

by visitors reading reviews

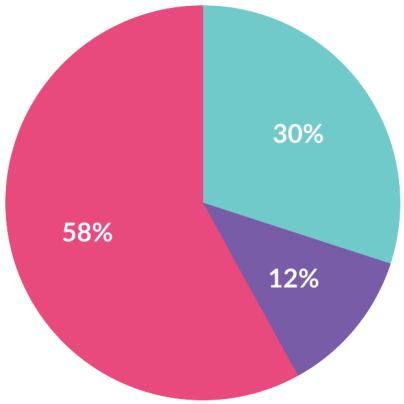
| | |
|---|---|
| Financial Services Firm | 15% |
| Manufacturing Company | 9% |
| Government | 8% |
| Healthcare Company | 8% |

# 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