aws marketplace

Red Canary

# Reviews, tips, and advice from real users






Powered by PeerSpot

# Contents

# Product Recap

Red Canary

# Red Canary Recap

Red Canary Managed Detection and Response (MDR) offers robust threat detection, rapid response capabilities, continuous security monitoring, and seamless integration with existing tools. Valued for its actionable reporting and proactive threat intelligence, it streamlines operations and enhances organizational efficiency and security.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

"Red Canary has impacted our organization positively by managing our security endpoints and being able to detect threats before they impact us negatively."

Anthony Tuhame

Information Technology Manager at Everseen

"Red Canary has positively impacted my organization because I don't have to spend and hire resources to look at logs, which has enabled us to do much more in terms of improving security across the organization."

John Hoffoss

Head of Information Security and Privacy at Ovative Group

"Red Canary has impacted my organization positively because we treat any ticket triggered by them as high priority due to the fact that 99 percent of the time it is a true positive."

Verified user

Security Analyst - Tier 2

"I recommended Red Canary to my friends who work in other organizations."

Shubham Biradar

SOC Analyst at Valorant

"The most valuable feature of the solution is its automation part."


Sagar Shekhar

Cyber Security Analyst at TIAA

"The near real-time review translates into near real-time action. So, in addition to alerting, Red Canary MDR has response playbooks built out."

Solomon Lesko

Account Manager at a computer software company with 51-200 employees

"The solution works well for what we use it for and the support and protection are good."

Verified user

Consultant at a financial services firm with 11-50 employees

## What users had to say about valuable features:

Red Canary detects threats and attack patterns, allowing us to assess any significant damage caused to the banking environment, particularly if protected data has been damaged or corrupted. It is valuable for security teams in banking industries that need to make informed decisions quickly. Red Canary solutions are useful for compliance with standards like FFIEC and PCI and are employed in medical operations for HIPAA compliance.

**Shubham Biradar**
SOC Analyst at Valorant

Read full review

"The most valuable feature of the solution is its automation part. If we have to perform MITRE ATT&CK, we have to do it step by step, wherein we have to run all the commands, while Red Canary MDR automates everything. We must run a single command, and Red Canary MDR will do everything on our behalf.."

**Sagar Shekhar**
Cyber Security Analyst at TIAA

Read full review

"The first valuable feature for me is the speed of response. It provides near real-time alert reviews. And then the near real-time review translates into near real-time action. So, in addition to alerting, Red Canary MDR has response playbooks built out.

So we're able to offload some of the immediate response actions. So if an endpoint is compromised, their response isolates that endpoint before it can do more harm.."

**Solomon Lesko**
Account Manager at a computer software company with 51-200 employees

Read full review

"The best features Red Canary offers are that they monitor our logs and have their own use cases, providing us with these tickets. If we miss anything, we treat Red Canary as a secondary triggering tool, so we use it as a secondary detection tool.

The most valuable feature in my day-to-day work is that those logs are monitored by actual experienced analysts from Red Canary. Although we have tools from our end with use cases, those can miss some events and incidents, but since Red Canary uses active, live agents to monitor and detect these anomalies, we rely on that feature for our security operation center.

Red Canary has impacted my organization positively because we treat any ticket triggered by them as high priority due to the fact that 99 percent of the time it is a true positive. They can isolate machines, which is a feature I really appreciate because if something happens on a weekend when we are not available, they can isolate it and contain the situation.."

**Verified user**
Security Analyst - Tier 2

Read full review

"One of the best features Red Canary offers is Threat Hunting because it searches for hidden threats in our environment. Instead of waiting for an alert to come, it can help us identify suspicious activity before it becomes a major security incident.

"I also appreciate the incident timeline feature because it shows the complete sequence of events during an attack. This makes it easier for us to understand how the incident started, what actions the attacker took, and how it progressed.

"Another valuable feature is analyst investigations, which provides dashboards where we can review detections and see the threats we have received and what we can do about them. I also appreciate the Detection Coverage feature, which shows which endpoints are protected and whether there are any gaps in monitoring. This is beneficial because it ensures all our critical systems are covered.."

**Anthony Tuhame**
Information Technology Manager at Everseen

Read full review

“In my experience, the best features Red Canary offers are their team, their monitoring team, their expertise at incident investigation, and a focus on suspicious or actual indicators of compromise to ensure that we're not spending time just reviewing logs, but that we're actually looking at things that may indicate we have broader issues.

The Red Canary team's expertise stands out compared to others I've worked with because their team is organized into smaller pods that support a given number of clients, so they're not just a bevy of operators going around the clock. The teams themselves have coordination and cohesion, and they get to know us. Their integrations into the different platforms and systems that we use all line up with our needs, whereas a number of other platforms offered a different variety of integrations that did not line up with our requirements.

Red Canary has positively impacted my organization because I don't have to spend and hire resources to look at logs, which has enabled us to do much more in terms of improving security across the organization. With the freed-up resources, we've been able to implement CSPM, SAST, software testing tooling, and engage much more closely with our developers and engineers to focus on secure architecture and design..”

**John Hoffoss**
Head of Information Security and Privacy at Ovative Group

Read full review

# Other Solutions Considered

"I previously used a different solution called Blue something, but I cannot recall the exact name. I decided to switch from that solution to Red Canary because they were a managed SOC provider and they were not good; they were very cheap, with very poor service.."

**John Hoffoss**
Head of Information Security and Privacy at Ovative Group

Read full review

"I have no idea if my organization evaluated other options before choosing Red Canary, as that was perhaps another person's or another team's decision. Our role is to utilize this application without involvement in purchasing or decision-making.."

**Verified user**
Security Analyst - Tier 2

Read full review

"Before choosing Red Canary, we did evaluate other options. One of the options we considered was Splunk, and we also considered Tines. We currently use both of these alongside Red Canary.

"We also evaluated CrowdStrike and Arctic Wolf. We compared them based on detection quality, pricing, false positive rates, and the ease of integration. We found that Red Canary and Tines were perfect for us. Red Canary gives us analyst-validated detections and has stronger threat hunting capabilities.."

**Anthony Tuhame**
Information Technology Manager at Everseen

Read full review

# ROI

Real user quotes about their ROI:

"I think that we have probably spent maybe 15% of the time that we were spending on incident investigation and system monitoring, demonstrating a return on investment.."

**John Hoffoss**
Head of Information Security and Privacy at Ovative Group

Read full review

"I believe we have seen a return on investment because we utilize Red Canary effectively. Any missed detection will definitely be triggered by Red Canary. I think it is a good investment since it provides accurate details.."

**Verified user**
Security Analyst - Tier 2

Read full review

"We have seen a return on investment, which comes from reducing the time and effort needed to detect and respond to threats. Red Canary filters out false positives and provides analysts that validate the detections. We spend less time investigating unnecessary alerts and have more time to handle real incidents. Red Canary has helped us validate these detections and respond to real incidents within 15 to 30 minutes.."

**Anthony Tuhame**
Information Technology Manager at Everseen

Read full review

# Use Case

We use Red Canary to monitor incoming and outgoing traffic. For example, when we receive an alert that data from our internal IP address to an external IP address has been transferred, we investigate using a Palo Alto firewall.

**Shubham Biradar**
SOC Analyst at Valorant

Read full review

"My main use case for Red Canary is to ensure I can sleep at night by getting 24/7 coverage by a capable team to investigate any alerts for the systems that we have in place to ensure we don't have any security or suspicious activity.

I can give you a specific example of a situation where Red Canary helped me out and made a difference: we've had more than a few instances where a user clicked on a phishing link, invoking connections to hostile sites. Through alerts in Defender, the Red Canary team identified, confirmed, and investigated the threat before they reset the user's credentials and contacted us to work with the user to resolve the situation.

I have at least one other instance where Red Canary investigated an alert and continued doing additional investigations of logging and activity from that user and their systems around that proximity to confirm that there was no further suspicious activity.."

**John Hoffoss**
Head of Information Security and Privacy at Ovative Group

Read full review

"My main use case for Red Canary is that a Red Canary analyst monitors our logs, and if they see any abnormality, they create a ticket that we use to analyze the situation. We assign that ticket and analyze it to ensure we have all the details needed. We use other tools to investigate, but we mainly rely on the evidence from Red Canary, and we can also use the isolate feature from Red Canary. There are threat reports and agents, and in our environment, we have endpoints and identity as well.

A recent situation where I used Red Canary to analyze a ticket involved an employee from the US who logged in from the UK, a country he had never visited before. Red Canary's analyst assumed that account was compromised, but after analyzing using our other tools, it seemed the login was legitimate. The user confirmed he had traveled to the UK and used one of our company phones to log into the account to check emails, so the alert triggered was a true positive but a legitimate anomaly.."

**Verified user**
Security Analyst - Tier 2

Read full review

"My main use case for Red Canary is as our managed detection and response solution to continuously monitor our environment for cyber threats. Whenever I log into the platform, I first check the dashboard to see if there are any new incidents or high-risk detections. Red Canary can analyze and validate those alerts before sending them to us, so I don't spend time reviewing thousands of raw alerts. This helps me and our team focus on incidents that are actually more likely to be threats.

"I want to discuss features such as the incident overview and the detection timeline. You can check which user and endpoint are affected, what process triggered the detection, how the attack progressed, and what techniques the attacker used.

"My use case also involves reviewing the investigation notes from Red Canary because they normally explain why the activity is suspicious, how confident they are in the detection, and what action they recommend. We also use the Threat Hunting feature, which is responsible for looking for suspicious patterns across our environment. Instead of waiting for an attack, the threat intelligence feature provided by Red Canary helps us understand emerging threats and whether they could affect our organization. Generally, we use Red Canary for threat detection and managed response.."

**Anthony Tuhame**
Information Technology Manager at Everseen

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 initial setup was quite straightforward. Their deployment team is extremely competent and worked with our security team to roll it out over a couple of weeks.."

**Solomon Lesko**

Account Manager at a computer software company with 51-200 employees

Read full review

"I cannot speak to the process to purchase Red Canary with certainty because I am an end user. Perhaps our managers or directors have a better answer regarding the purchasing process, but I do not know those details.."

**Verified user**

Security Analyst - Tier 2

Read full review

"My experience with pricing, setup cost, and licensing is that everything went very smooth. Pricing was straightforward, and we were done with setup during our POC, not having any additional work or rework that we had to do when we moved to production.."

**John Hoffoss**

Read full review

Head of Information Security and Privacy at Ovative Group

"The initial deployment of Red Canary MDR was simple and took a few days.

We have an agent on all the computers and Carbon Black feeds all the information to Red Canary MDR.."

**Verified user**

Read full review

Consultant at a financial services firm with 11-50 employees

"Regarding Red Canary's AI capabilities from a governance perspective, it has helped us maintain accountability by providing detailed incident reports. It also provides audit trails and investigation records. A feature I appreciate about Red Canary is that it supports role-based access. This means authorized users can view and manage security incidents. All of this helps us follow our security policies and meet compliance requirements.."

**Anthony Tuhame**

Information Technology Manager at Everseen

Read full review

"The initial setup of Red Canary MDR was very easy since we just had to run some simple commands.

The solution is deployed on-premises.

The deployment process takes five to ten minutes. ."

**Sagar Shekhar**

Cyber Security Analyst at TIAA

Read full review

# Customer Service and Support

We have a monthly catch-up call with the support team to discuss alerts. In emergencies, there is an on-call person available to resolve issues immediately.

**Shubham Biradar**
SOC Analyst at Valorant

Read full review

"We have our SOC and CERT incident response protocols to follow and when we have an issue or an outbreak, we can handle it on our own. I have not needed the help of technical support from the outside.."

**Verified user**
Cost Management Manager at a computer software company with 1,001-5,000 employees

Read full review

"The customer support has been really good from what I have seen. If I need more details about any incident, there is a contact us option to reach an agent, or another agent can substitute if the previous one is not available, allowing us to get additional details and opinions.."

**Verified user**
Security Analyst - Tier 2

Read full review

"Customer support is very good. We rarely talk with customer support because Red Canary has good documentation. Almost every issue we face is always included in the documentation, so we have not had to escalate many issues to customer support. When we do escalate them, we always get prompt responses. I found that the support team is very knowledgeable.."

**Anthony Tuhame**
Information Technology Manager at Everseen

Read full review

# Other Advice

I recommended Red Canary to my friends who work in other organizations. I guide them about this tool, share knowledge on its features, and explain the process of how we use it. I would rate the overall solution on a scale of one to ten as nine.

**Shubham Biradar**
SOC Analyst at Valorant

Read full review

"I am satisfied with this solution and it is very competitive with other similar EDR or MDR solutions because it provides very impressive information about the root cause of the threat, such as malware.

I rate Red Canary MDR a nine out of ten.."

**Verified user**
Cost Management Manager at a computer software company with 1,001-5,000 employees

Read full review

"I recommend Red Canary MDR to others because it is a good product.

If I had to do one of the projects in my company without Red Canary MDR, it would have taken me a lot of time to complete it.

I rate the overall solution a nine out of ten.."

**Sagar Shekhar**
Cyber Security Analyst at TIAA

Read full review

"My advice and recommendation to others looking into using Red Canary is to ensure that you have good endpoint coverage and integrate it with your existing security tools such as your EDR platforms because that is where you will get the most value. I also recommend training your security team to understand the investigation reports and remediation recommendations so that they can respond quickly. Finally, I advise always reviewing incidents regularly and using Threat Hunting, which is very effective, along with reporting features. If you do that, Red Canary will become a very effective extension of your security team. I would rate this review a 9 out of 10.."

**Anthony Tuhame**
Information Technology Manager at Everseen

Read full review

"We have been very happy with everything, from the sales process to the implementation and deployment playbook. I'm highly content.

The best advice I can give is that Red Canary works best with a very Microsoft-centric cloud strategy. So if a business aligns with that, it's a good fit. If it's not

Microsoft-centric, there might be other solutions that would fit better. That's my impression after the work we've done.

So far, we're pretty Microsoft-centric, so it's definitely the right fit for us.

Overall, I would rate it a nine out of ten because nothing is perfect. ."

**Solomon Lesko**
Account Manager at a computer software company with 51-200 employees

Read full review

"We use Red Canary as a secondary monitoring service so if our main tools miss any detection, Red Canary will detect it. We critically treat any alert from Red Canary as a high-priority ticket because it is most probably a true positive, but it can also be a legitimate anomaly, so we will treat it as a priority one case.

Red Canary serves as a secondary triggering tool, and we do not really use any kind of SLA or anything. They monitor and create threat tickets they believe are threats, and we use it as a secondary monitoring tool.

My advice to others looking into using Red Canary is to consider it as a good secondary detection tool, and they have good customer support. I would rate this product an 8 out of 10.."

**Verified user**
Security Analyst - Tier 2

Read full review

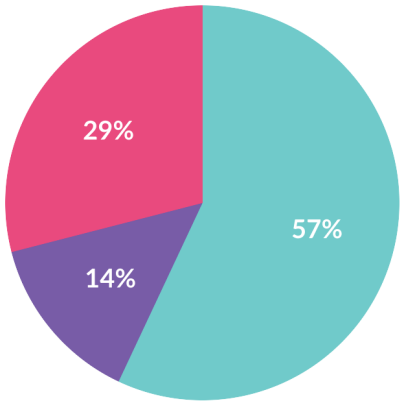
# Top Industries

by visitors reading reviews

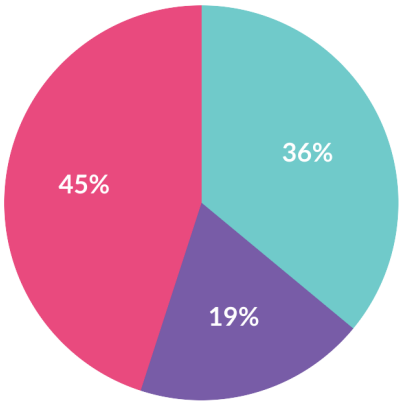
| | |
|---|---|
| Financial Services Firm | 9% |
| Construction Company | 8% |
| Manufacturing Company | 8% |
| Computer Software Company | 7% |

# 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