aws marketplace

CrowdStrike Falcon

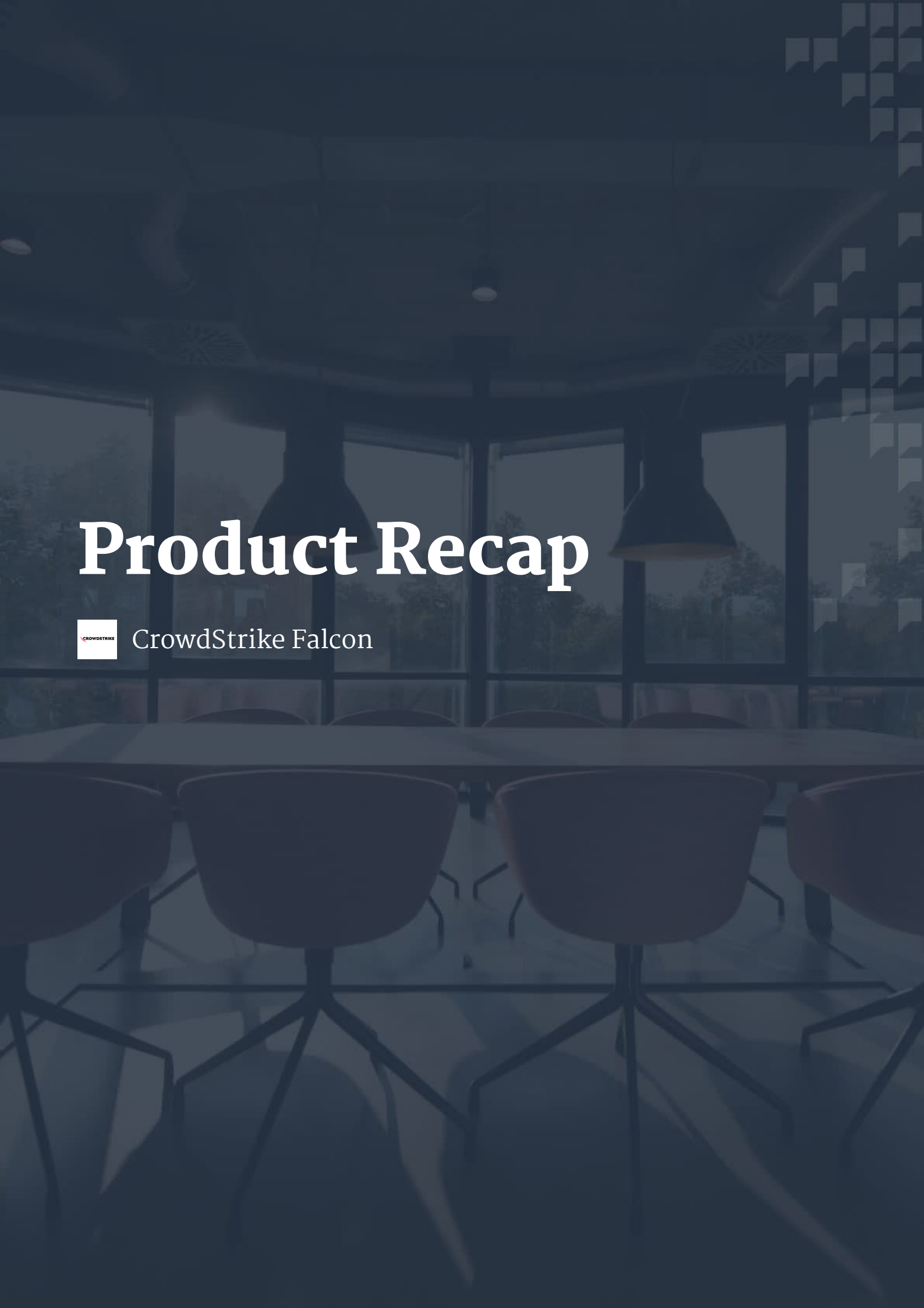
Reviews, tips, and advice from real users






Powered by PeerSpot

Contents



Product Recap

CrowdStrike Falcon

CrowdStrike Falcon Recap

CrowdStrike Falcon provides cutting-edge endpoint detection with automatic alerts, real-time monitoring, and seamless integration capabilities. Cloud-native architecture and AI-driven processes ensure scalable protection and efficient threat remediation.

CrowdStrike Falcon is recognized for its robust EDR and threat intelligence features that enhance security and streamline operations. Its lightweight agent minimizes system impact while offering real-time monitoring and detailed reporting. This platform uses cloud-native architecture for scalable, consistent protection, significantly reducing administrative demands. AI and machine learning empower precise threat hunting and behavioral analysis, which mitigates false positives and boosts cybersecurity efficiency. Users seek improvements in integration with other systems, reporting functions, and compatibility with specific operating systems. While the solution handles malware mitigation and threat response efficiently, suggestions for on-demand scanning, enhanced visibility, and better dashboard features are noted.

What are the key features of CrowdStrike Falcon?

- Automatic Alert System: Provides instant alerts to enhance threat detection.
- Robust EDR: Offers advanced endpoint detection capabilities.
- Threat Intelligence: Delivers detailed insights for proactive security measures.
- Real-time Monitoring: Enables continuous security assessments.
- Seamless Integration Options: Streamlines operations with existing infrastructure.
- Lightweight Agent: Minimizes system impact, maintaining performance efficiency.
- Cloud-native Architecture: Provides scalable, consistent protection against threats.
- AI and ML-driven Processes: Offers accurate threat hunting and behavioral analysis.

What benefits or ROI should users expect from CrowdStrike Falcon?

- Enhanced Security: Comprehensive protection for endpoints using cutting-edge technologies.
- Reduced Administrative Burden: Simplifies management of security incidents.
- Efficient Threat Remediation: Minimizes downtime with quick threat response actions.
- Improved Threat Visibility: Provides detailed reports and insights.
- Scalable Protection: Ensures adaptable security measures across multiple devices.

In technology sectors, CrowdStrike Falcon commonly supports endpoint protection and threat response initiatives, allowing companies to replace traditional antivirus systems with more advanced solutions. In finance, it secures sensitive data across multiple platforms, ensuring compliance. In healthcare, real-time security analysis protects patient data on critical devices like servers and laptops, utilizing AI to enhance cybersecurity defenses.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The most beneficial part is the active response capability of the product."

Waleed Omar

Information Security Specialist at Arab Open University

- "CrowdStrike Falcon has positively impacted endpoint security and reduced the response time for incidents and alerts."

Pavan Ingaleshwar

SOC Analyst at ISECURION

- "CrowdStrike Falcon helps with endpoint protection by having very low memory utilization and processor usage, so it doesn't impact the computer system performance, and the computer system works very fast compared to all other endpoint protection solutions."

Dipak M Gohil

IT Manager at Jord International Pty Ltd

"CrowdStrike Falcon serves as a next-gen AV, which basically does AI-based behavioral analysis to detect and act on malware or ransomware."

Jai Prakash Sharma

Executive Vice President Technology at InfoEdge India Ltd

"CrowdStrike Falcon features are robust and reliable."

Ashutosh Jha

Project Engineer at IT Solution

"I find nothing to miss in terms of stability; there are no glitches, and the solution is stable."

Bhupesh-Sharma

Large account Manager at Softcell Technologies Limited

"The most beneficial features of CrowdStrike Falcon are that it is easy to install, easy to manage, lightweight, and it can stop breaches."

BambangTrisilo

IT consultant at Asuransi Ramayana

What users had to say about valuable features:

"Among CrowdStrike Falcon's most valuable capabilities are its UEBA and SOAR functionalities, along with its seamless integration with any other SIEM solution.."

Rohith Kumar-Gurram
Cybersecurity Analyst at a computer software company with 51-200 employees

Read full review

"The ability to remote into other devices for investigation and the way it presents a graphical representation of the detection, like the parent-child process, are valuable features.."

Verified user
IT Specialist at a consultancy with 1-10 employees

Read full review

"The product's most valuable features include its global reach and extensive threat data. Its wide exposure helps gather diverse threat intelligence, crucial for effective security management.."

Mahmoud_Yassin
CTSO at Cyb3r

Read full review

"I like CrowdStrike's policies. The integration is easy to do. I can remember once when Falcon prevented a security breach occurred because someone clicked on a phishing link, and their credential was compromised. We used threat tracking to isolate the device from networks. ."

Verified user

Information Security Analyst at a manufacturing company with 1,001-5,000 employees

Read full review

"I like Falcon's threat detection and endpoint investigation features. It's a user-friendly solution. We determine the root cause of an alert and contact the end user via our Slack channel if necessary to gather additional information to determine whether they know about the activity. We can download and investigate the malicious file in the sandbox to see what's happening. We check to see if it has been executed. We can easily delete it in the CrowdStrike console if it hasn't. ."

Naveen Nelavigi

Senior Security Analyst at Ernst & Young

Read full review

“I like the feature called RTC, the remote time connector. It allows us to connect to a computer via the command line and execute commands for various functions and investigations. This eliminates the need for any additional programs. We can launch the connection and its subcommands from a single console.

The containment feature is another valuable tool. It allows us to isolate any machine exhibiting suspicious behavior or facing a detected threat. Once activated, containment immediately severs the machine's network connection and blocks user access..”

Verified user

Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

Other Solutions Considered

"I have used antiviruses like Symantec before. Compared to all of that, I found CrowdStrike quite striking. Even compared to Defender, I find CrowdStrike more appealing.."

Verified user
IT Specialist at a consultancy with 1-10 employees

Read full review

"We evaluated several other options before choosing CrowdStrike. Our decision was based on the product's effectiveness and ability to meet our security requirements.."

Mahmoud_Yassin
CTSO at Cyb3r

Read full review

"We previously used a different solution. We switched to CrowdStrike due to its comprehensive threat intelligence capabilities and global reach, which we found to be more effective for our needs.."

Mahmoud_Yassin
CTSO at Cyb3r

Read full review

"After evaluating SentinelOne, we found CrowdStrike to be a superior solution. CrowdStrike offers advantages in dashboard compatibility and a feature called Overwatch, which gives it a competitive edge.."

Khushru_Mistry
Chief Technology Officer at GM Modular

Read full review

"Microsoft Defender Threat Intelligence, IBM, and Cisco are some competitors. CrowdStrike entered the market with a USP to protect endpoint servers. It has a different approach. Malwarebytes has a similar setup. I prefer CrowdStrike, though.."

Dinesh Yadav
Sales Director at CLOUD MIND

Read full review

"We are an MSP and have used and provided IBM QRadar, Bit Defender, and CrowdStrike Falcon based on each client's requirements.

CrowdStrike Falcon is the most popular choice for our clients because of its price.."

Rohith Kumar-Gurram
Cybersecurity Analyst at a computer software company with 51-200 employees

Read full review

ROI

Real user quotes about their ROI:

"On the terms of investigating, I find it's quite easy to investigate an event and have a broader look at the event using CrowdStrike. I would rate the time saved around eight, nine, or even ten out of ten. Compared to Defender, it makes it faster to investigate.."

Verified user
IT Specialist at a consultancy with 1-10 employees

Read full review

"The product has a lot of use cases. There are companies that need to run their operations 24/7. It will be a big challenge if their server or infrastructure goes down. They cannot afford downtime. They need to choose the right solution for their needs.."

Dinesh Yadav
Sales Director at CLOUD MIND

Read full review

"The return on investment is evident in the enhanced security posture achieved through continuous monitoring and immediate isolation of compromised machines. This proactive approach not only mitigates risk but also provides significant peace of mind for our team, alleviating concerns and optimizing their performance.."

Verified user
Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

"CrowdStrike Falcon has demonstrably provided a positive return on investment. We've already encountered two specific instances where, without CrowdStrike, the company would have faced millions in damages. In one case, we would have likely lost our entire SAP system.."

Khushru_Mistry
Chief Technology Officer at GM Modular

Read full review

“The benefit I've seen is their backend, which powers the EDR, XDR, and NGAV. It's really good because it can detect anything due to the wide range of customers they have.

For example, one customer has a vulnerability because of a zero-day attack. All the other customers will benefit because it propagates to the cloud and analyzes if other customers are on the same version of the drivers or any other Windows patch. If they are, it will tell us that there's an issue and provide remediation steps. Many of our customers find this very helpful. It's called the CrowdStrike community..”

Abhishek A
Trainee Engineer at COMPASS IT Solutions & Services Pvt.Ltd.

Read full review

“The solution somehow doesn't allow intrusion and minimizes fraud or cyber-attacks. Within the time we're using it, CrowdStrike Falcon Surface detected a lot of intrusion from malicious individuals. It was able to prevent a lot of insider threats where people internally will want to run some malicious scripts within the environment.

It detects those malicious attacks quickly, and we can prevent them. It minimized a lot of cyber and fraud-related activities that could have cost the bank a lot of money..”

Ben Nnatuanya
Manager, Security Operations Centre at Phillips Consulting Limited

Read full review

Use Case

"We use Falcon to check the login attempts of the users. We can see who has logged in and when. We can see which workstation is assigned to each user. CrowdStrike helps us enforce policies, such as USB policies and users recycling passwords. ."

Verified user

Information Security Analyst at a manufacturing company with 1,001-5,000 employees

Read full review

"We use CrowdStrike Falcon as an XDR to replace our old antivirus solution.

We implemented CrowdStrike Falcon for better visibility into our environment and easy online access to the policies.."

Verified user

IT Workplace Coordinator at a consumer goods company with 1-10 employees

Read full review

"Our organization relies on CrowdStrike, a standalone endpoint security solution, to safeguard our bare-metal machines. CrowdStrike continuously monitors for threats on all endpoints. If it detects any suspicious activity, such as malware or malicious processes, it immediately alerts us for investigation. ."

Verified user

Vice President at a financial services firm with 10,001+ employees

Read full review

"I'm a security analyst. We get alerts on the cloud side that appear in the CrowdStrike console and also in our email. We can consolidate them on the console and check the process tree. You can see the hostname, user details, and all the information on the right side. On the file part, we can see whether the malicious file has been executed and decode it to see where the hash appears.."

Naveen Nelavigi

Senior Security Analyst at Ernst & Young

Read full review

"We rely on CrowdStrike Falcon for comprehensive threat detection, prevention, and valuable insights. This robust solution also offers identity protection features. Our dedicated team of six professionals effectively manages the platform, ensuring its effectiveness across multiple locations, including our data centers and core facility.."

David Leonard

Head Deputy Head of IT, Information Technology's Projects & Developments Center at a energy/utilities company with 201-500 employees

Read full review

"We use CrowdStrike Falcon for endpoint security and response, and Horizon to manage and protect our data.

Following a 2021 security incident, the general response team recommended implementing CrowdStrike. We adopted their suggestion and found its network threat detection and prevention capabilities invaluable.."

Verified user

Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The initial setup was straightforward, with the installation taking less than two hours. However, fine-tuning alerts and configuring rules required additional time and effort.."

Mahmoud_Yassin

CTSO at Cyb3r

Read full review

"Deploying CrowdStrike is straightforward. We initially had a technical representative guide us through the process, but now we can handle it ourselves for our clients.

One architect and two engineers are used for the deployments.."

Rohith Kumar-Gurram

Cybersecurity Analyst at a computer software company with 51-200 employees

Read full review

"It is deployed on the cloud. Its deployment is of moderate complexity. It is not easy, and it is also not difficult. Overall, it is easy to deploy and manage CrowdStrike Falcon across the organization.."

Ganesh-Jadhav

Senior Cyber Security Analyst at Securonix

Read full review

"The initial deployment presented some challenges due to the need to install the solution on all machines. This phase, requiring careful coordination among ten people over several weeks, involved connecting all the computers to the network. However, once this foundation was laid, the subsequent rollout proceeded smoothly.."

Verified user

Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

"The deployment of Falcon was relatively easy, with no major issues except occasional misconfigurations on the filter. The process for individual work sessions is fast, taking around a few minutes, but for servers, it requires more time due to the need for antivirus removal and sensor replacement, involving server restarts. Overall, the deployment time depends on the scope, ranging from minutes for work sessions to more extended periods for servers.."

Verified user

Read full review

IT Consultant at a comms service provider with 5,001-10,000 employees

"The initial setup of Crowdstrike Falcon was straightforward and efficient. The cloud-based deployment process was seamless for most components, with the exception of the sensors. Deploying the sensors to PCs was automated and hassle-free, requiring just a few minutes per device. However, to ensure the highest level of protection and customization, we opted to manually install the sensors on our servers. This hands-on approach allowed us to have greater control and assurance over the server deployment, ensuring the best possible protection for our critical infrastructure.."

David Leonard

Read full review

Head Deputy Head of IT, Information Technology's Projects & Developments Center at a energy/utilities company with 201-500

employees

Customer Service and Support

“I've found the technical support staff to be less knowledgeable than I'd expect. Ideally, they should have expertise in all CrowdStrike modules, as we utilize a wide range of them..”

ManojKumar42
Information Security Engineer at a university with 1,001-5,000 employees

Read full review

“While I've found screen sharing helpful with other support teams, CrowdStrike's technical support has never proactively suggested it. Instead, they've always initiated contact by calling me back after I submitted a ticket. We recently offered to screen share, but it seems it's not their preferred method. The support is good but it is not the best I have used..”

Verified user
Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

“The technical support is not very good. I would rate it as an eight out of ten. One improvement could be reducing the response time for cases, as waiting two or three days, even for less critical issues, can be a bit long. Additionally, a better feedback loop on submitted ideas would enhance the efficiency of communication with the product group, providing more clarity on whether proposed features or versions will be considered..”

Verified user

IT Consultant at a comms service provider with 5,001-10,000 employees

Read full review

“While the technical support meets all response time commitments outlined in our Service Level Agreement, some users believe they should strive for a higher standard – a Security Level Target. This means responding to security incidents immediately, not just within SLA windows. Security tools are crucial for our environment's protection, and their use shouldn't be limited by SLA constraints..”

Verified user

Head Cyberdefense at a tech vendor with 5,001-10,000 employees

Read full review

“Technical support depends on a system integrator.

CrowdStrike technical support regarding Identity Protection has a team, but if there's no issue with the agent, you can work it out yourself.

The support is good..”

Bhupesh-Sharma
Large account Manager at Softcell Technologies Limited

Read full review

“I would rate CrowdStrike's support team a three out of ten. Their support is unacceptable for us. We are doing some testing ourselves. When we found an issue where CrowdStrike should have blocked something but did not, we opened a ticket with CrowdStrike. They tried to communicate with us and looked at the files that we shared. We had updated signatures, and we shared with them the SHA values, but after that, they suddenly vanished. Just two days ago, I got an email from them that the engineer was on leave and he is back now. They asked us to perform the activity again, which is unacceptable.

When any issue happened with Symantec, we opened a ticket, and they would accept their mistake if something was not caught by Symantec. They would then update the definitions and send us the latest updates. This is the way to work on the latest technology trends..”

Jawaria Abbas
Security Engineer at a computer software company with 201-500 employees

Read full review

Other Advice

“I would rate CrowdStrike Falcon a then out of ten.

Before purchasing CrowdStrike Falcon I suggest checking the policies, particularly those regarding internet connections, and conducting a proof of concept..”

Verified user
IT Workplace Coordinator at a consumer goods company with 1-10 employees

Read full review

“Overall, it is a robust solution that meets our security needs. However, potential users should know the cost implications and ensure the product meets their requirements.

I rate it an eight. .”

Mahmoud_Yassin
CTSO at Cyb3r

Read full review

"I would definitely recommend CrowdStrike Falcon. It is better than other solutions, such as VMware Carbon Black. CrowdStrike is doing better in this space.

If you are using CrowdStrike Falcon for the first time, it will be easy for you. You can definitely use it.

Overall, I would rate CrowdStrike Falcon an eight out of ten. ."

Ganesh-Jadhav
Senior Cyber Security Analyst at Securonix

Read full review

"I would rate CrowdStrike Falcon a nine out of ten.

CrowdStrike Falcon is a great tool. Investing in proper training on the CrowdStrike Falcon platform is highly recommended for any organization seeking to maximize its potential and avoid navigation struggles within the console. However, it's important to note that effective utilization of Falcon without CrowdStrike's managed services necessitates the formation of a dedicated team responsible for managing the solution. ."

Verified user
Security Analyst at a insurance company with 1,001-5,000 employees

Read full review

"I would rate CrowdStrike Falcon a ten out of ten.

Our clients range from small up to enterprise level.

The maintenance is simple. We just need to stay on top of the updates.

CrowdStrike Falcon is user-friendly and the analysis provided is good making it an efficient solution.."

Rohith Kumar-Gurram
Cybersecurity Analyst at a computer software company with 51-200 employees

Read full review

"I would rate CrowdStrike Falcon a seven out of ten.

The maintenance is straightforward.

CrowdStrike Falcon is deployed independently in our environment and we have 30 users.

While CrowdStrike Falcon offers valuable security tools for larger organizations with extensive infrastructure, its complexity might not be ideal for smaller businesses with limited IT resources.."

Verified user
Vice President at a financial services firm with 10,001+ employees

Read full review

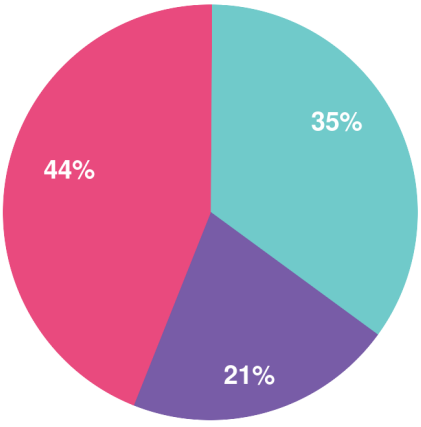
Top Industries

by visitors reading reviews

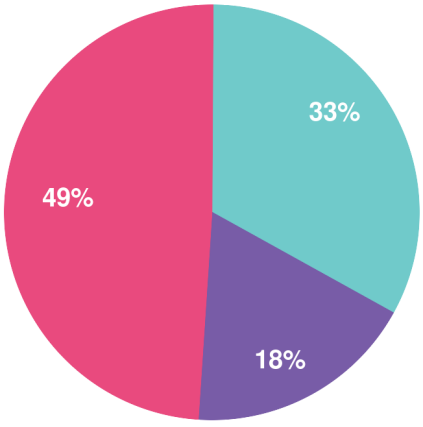
Financial Services Firm	11%
Computer Software Company	10%
Manufacturing Company	9%
Government	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

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

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

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

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944