aws marketplace

Upstream Security

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Upstream Security

Upstream Security Recap

Upstream Security provides a robust cybersecurity platform tailored for the automotive industry, addressing crucial security needs for connected vehicles.

Upstream Security focuses on enhancing vehicle cybersecurity by utilizing a cloud-based platform that offers comprehensive protection for connected vehicles. By integrating data from multiple sources and delivering advanced anomaly detection, it enables automotive companies to safeguard their vehicles against cyber threats effectively.

What are the key features of Upstream Security?

- Anomaly Detection: Identifies unusual behavior patterns to prevent unauthorized access.
- Threat Intelligence: Provides up-to-date information regarding potential threats and vulnerabilities.
- Data Integration: Aggregates data from various sources for a holistic security approach.
- Compliance Monitoring: Ensures adherence to industry-specific cybersecurity standards.

What benefits and ROI should users consider?

- Enhanced Security: Offers improved protection mechanisms that reduce cyber attack risks.
- Cost Efficiency: Minimizes the financial impact of potential cyber threats.
- Operational Integrity: Maintains uninterrupted vehicle operations by promptly addressing threats.
- Regulatory Compliance: Supports adherence to evolving cybersecurity regulations.

The platform is crucial in automotive sectors such as fleet management and OEMs, where securing connected vehicle ecosystems is of paramount importance. With industry-specific features, Upstream Security ensures that companies can implement effective security measures in their operations.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "This has really helped us as an OEM to secure connected fleet and meet regulatory requirements, which is eventually very important for us to be able to sell any data to the end customer."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

- "Upstream Security has positively impacted my organization as manual intervention has been reduced by 60% of the time, saving us considerable resources."

Puneet_Kumar

Security Professional at CSX

- "Upstream Security has positively impacted my organization by reducing the security risk for connected vehicles, avoiding recall and warranty costs, enabling faster incident detection and response, improving operational efficiency for fleet security, and managing regulatory compliance while reducing costs."

Samir Paul

Cloud Security Practitioner at a tech vendor with 10,001+ employees

What users had to say about valuable features:

Upstream Security's best features include having all the upgraded versions to protect us from the cyber attacks occurring in our environment, which provides a prominent defense against these threats.

Upstream Security has positively impacted my organization as manual intervention has been reduced by 60% of the time, saving us considerable resources. The guardrails provided by Upstream Security are essential and have protected us from external cyber attacks, resulting in an overall 30% reduction in cyber attacks that occurred in our network systems and connected devices from previous years to the current implementation. .”

Puneet_Kumar
Security Professional at CSX

Read full review

The best features Upstream Security offers revolve around the vehicle part, as it provides automotive-focused XDR, which is the best security feature. I value that agentless architecture is available, so no in-vehicle agent is needed, along with real-time monitoring, digital twin technology for vehicle behavior modeling, threat intelligence for the automotive ecosystem, and the Vehicle Security Operation Center, which is very important and new nowadays.

Out of the features I mentioned, such as the agentless architecture, digital twin technology, and Vehicle Security Operations Center, I do not have a specific favorite because when using tools Upstream Security, I must combine all those features, and each and every feature I mentioned is mandatory to be secure in the vehicle domain. ."

Samir Paul
Cloud Security Practitioner at a tech vendor with 10,001+ employees

Read full review

"Scalability was very important and Upstream Security was able to meet our requirement. They have a very good machine learning-based detection intelligence. The overheads are potentially operationally very minimal because they have an agentless working model. The cloud-based and agentless architecture works out extremely well for our organization, as we were looking for something on those lines. It has AI and machine learning powered detection and provides GenAI assisted investigations.

In addition to regulatory compliance support, the biggest strengths in summary are that it is cloud-native, agentless, an automotive extended detection and response platform, AI-driven anomaly detection, and digital twin-based visibility. It has the ability to secure our connected vehicle ecosystem at scale and supports our compliance requirements.

From the perspective of what we are referring to, the first thing that we had in our mind is that because of the connected car ecosystem, there are a lot of threats. The company has really benefited from the implementation of Upstream Security by reducing the business risk. From the perspective of regulatory readiness, we needed more than just documentation—we needed operational support and continuous monitoring that is aligned to UN regulation 155 and the ISO standard of 21434. Faster deployment occurred over time, as the start was slow but eventually there is less operational friction and the deployment is faster as time progresses. It has provided visibility through a 24 to 7 vehicle SOC, and we do not have siloed vehicle monitoring anymore. We are using Upstream Security for 24 to 7 fleet visibility. It provides fleet-wide visibility for connected vehicles, takes care of business risks, has helped us with compliance readiness, reduced time for investigating anomalies, and improved our detection capability of any kind of fraud or misuse. Customer impacting incidents have extremely come down.."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

Other Solutions Considered

Before choosing Upstream Security, we had a reference from one of our colleagues who worked in similar systems, which led us to choose it without evaluating other options available in the market.

Puneet_Kumar
Security Professional at CSX

Read full review

"We did not make a switch, and we did not have a solution before. We were looking at getting a solution and chose Upstream Security as our choice of solution. This was not a replacement. We evaluated Harman Shield and Argus Cyber security as the other two comparatives that we were comparing Upstream Security against, and we chose Upstream Security.."

TarunKumar11
Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

"We did not make a switch, and we did not have a solution before. We were looking at getting a solution and chose Upstream Security as our choice of solution. This was not a replacement, but we could look at choosing Upstream Security for all practical purposes. We also evaluated Harman Shield and Argus Cyber security. Argus and Harman Shield were the other two comparatives that we were comparing Upstream Security against, and we chose Upstream Security.."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

I have seen a return on investment with an overall reduction in resources, including a 60% time savings and a 30% reduction in cyber attacks compared to previous periods.

Puneet_Kumar
Security Professional at CSX

Read full review

After implementing Upstream Security, I have noticed specific outcomes such as a thirty to fifty percent reduction in cyber risk in connected fleets, a twenty to forty percent reduction in recall-related costs, and a forty to sixty percent faster incident detection.

Samir Paul
Cloud Security Practitioner at a tech vendor with 10,001+ employees

Read full review

"Mean time to detect came down significantly. Time to detect the anomalies in vehicles came down significantly, and mean time to respond as well to incidents and containing the incident that came down as well. Fleet visibility coverage went on to become significantly higher percentage connected vehicles being monitored. Cost avoidance also occurred because of proactive detection, defects were caught early, and warranty claim reduction came down. There are operational ROIs, warranty ROIs, compliance ROIs, deployment and operational ROIs, and business risk ROIs. We could measure cost avoidance, efficiency gains, revenue protection, and this actually sums up various things on which we could measure the ROI.."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

Use Case

My main use case for Upstream Security is securing the connected devices in our fleet of transportation trucks throughout the US.

We have devices placed in these trucks connected through Bluetooth, but we were concerned about potential attacks on the terminals. Upstream Security has enabled us to secure the channel through various protocols and utilize communication via HTTPS, allowing us to secure our operations using different layers of the Upstream Security application.

“This use case has proven to be successful and aligns well with the features we are satisfied with. .”

Puneet_Kumar
Security Professional at CSX

Read full review

My main use case for Upstream Security is the Synapse solution, which provides visibility of my cloud environment and primarily works for Kubernetes. It is a cloud-native automotive cybersecurity platform designed to protect connected vehicles, fleets, and the automotive ecosystem, APIs, and more. It is built as a vehicle-focused XDR platform using real-time data, vehicle APIs, and telemetry.

Regarding my main use case, I can say it is not a traditional IT security tool; it is purpose-built for vehicle fleets and mobility platforms. It includes features that improve specific workflows, such as vehicle and fleet cybersecurity, automotive-focused XDR, agentless architecture, real-time monitoring using telematics and API data, AI and ML-based anomaly detection, digital twin technologies, API and mobility service security, threat intelligence for the automotive ecosystem, and a Vehicle Security Operation Center (V-SOC).

“An example of how my team uses Upstream Security in our day-to-day work is as a specialized cybersecurity platform for connected vehicles with an e-mobility ecosystem providing real-time detection and response using vehicle and IoT data. .”

Samir Paul

Cloud Security Practitioner at a tech vendor with 10,001+ employees

Read full review

"The core problem that OEMs face, especially automotive companies who have to take care of cybersecurity for their connected car fleets and vehicles and mobility ecosystem, is securing connected vehicles and mobility ecosystems for cybersecurity threats and misuse. Upstream Security detects threats using existing vehicle telemetry, APIs, telematics, dealers, and mobility data. It helped us monitor fleets at scale, almost in a real-time basis and supported our cybersecurity compliance requirements. There is a UN regulation R155 and ISO 21434 that we needed to meet.

The number one feature of Upstream Security, based on their technical architecture, is how to inject and analyze data. Data comes in from all different sources, and we needed near real-time detection and anomaly detection within the platform, plus rule-based intelligence. The integration of telematics, over the air updates, APIs, diagnostics, and dealer data is the most important aspect that we used Upstream Security to ingest that data from various different fields and eventually analyze data for us.

Upstream Security is very important for organizations, especially OEMs. If there is a vehicle security operation center which has to be set up for 24 into 7 monitoring of the fleets, if we want to connect it to mobility, all of this involves integration of telematics, API, diagnostic, dealer data, and managing compliance at the end of the day is extremely important. This has really helped us as an OEM to secure connected fleet and meet regulatory requirements, which is eventually very important for us to be able to sell any data to the end customer.."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ 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.

Upstream Security is deployed in our organization using a private cloud hosted over AWS.

The cloud provider we use for our private cloud is Amazon AWS.

“We have the services hosted for the overall applications along with Upstream Security through the AWS Marketplace. .”

Puneet_Kumar

Security Professional at CSX

Read full review

"The setup was not straightforward. It takes time to be able to understand how the agentless model works and how the cloud-native deployment possibly works. There is a lot of handholding that is required before we start to implement and use Upstream Security for all practical purposes. There was a steep learning curve that was involved, but the help from Upstream came in extremely handy. There are limitations as well that needed to be understood before we could implement telemetry data into Upstream Security platform. Understanding how the platform works, how the agentless systems work, and how the cloud-based detection happens with the existing mobility data that we have did not make this entire experience at the start extremely smooth. It took a lot of sitting down with the experts and making a real good understanding of how the system works and how the integration works so that we became independent to a large extent, but we still have the support and maintenance from Upstream Security working for us.

In terms of pricing and licensing, we were able to get not a one-year deal but a five-year deal with Upstream Security. We have a long-term engagement and this gives us a better discounting mechanism as well for Upstream Security. As far as pricing is concerned, the pricing is quite comparative and is on the highest side. The basic model is that platform licensing is annual subscription over a period of five years. It manages all our fleets and vehicles and has data volumes. Setup and onboarding cost was one time for professional services for integration and telemetry normalization. We also have a managed SOC that is managed internally, so we are not taking the support of Upstream Security. We have in-house analysts who do the monitoring 24 to 7. Slowly and slowly, we also looked at getting more API security related modules and detection related modules from Upstream Security. Our licensing is therefore very aligned to fleet coverage, telemetry, integration, and use cases. It is not dependent on endpoint agents. Upstream Security was made known as to how many vehicles we would be talking of or the telemetric volume possibly is. As far as the setup cost is concerned, the setup cost includes data onboarding, ingestion mapping, money for and effort for detection tuning, baselining, integration with the various other platforms like SIEM, SOAR, ticketing, compliance workflows, training, and runbooks.."

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

Customer Service and Support

“Upstream Security's customer support does not require too much effort in order to make sure that we get the support when we require it. Because this is an enterprise software, the support that we have taken from Upstream Security includes a technical account manager who is named and associated with us. We have priority support where we have SLAs with respect to commitment on response times and resolution times. They have a defined escalation model and coverage across the globe in India, Europe, and the US. The SLAs are defined, the responsiveness is good, and the support quality has not been lacking. Our rating for this aspect is nine again..”

TarunKumar11

Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

Other Advice

For others looking into using Upstream Security, my advice is that when considering security for connected devices, whether Upstream Security or any other solution, they should discuss the latest cyber attacks and any malware incidents, ensuring these are included in the solutioning approach before deciding on a product to purchase. I rate Upstream Security a seven out of ten overall.

Puneet_Kumar
Security Professional at CSX

Read full review

My advice to others looking to use Upstream Security is to choose Upstream Security, as it is a perfectly good solution. While I have already provided relevant metrics for detection accuracy and capability, I would focus on these rather than the savings aspect, as I have not provided anything on the money-saving or resource-saving perspective. I believe I have covered all the features offered by Upstream Security. I would rate this product a nine out of ten.

Samir Paul
Cloud Security Practitioner at a tech vendor with 10,001+ employees

Read full review

“Upstream Security is both cloud-based and agentless in architecture, which works out extremely well for our organization, as we were looking for something on those lines. It has AI and machine learning powered detection and provides GenAI assisted investigations. In addition to regulatory compliance support, the biggest strengths are that it is cloud-native, agentless, an automotive extended

detection and response platform, AI-driven anomaly detection, and digital twin-based visibility. It has the ability to secure our connected vehicle ecosystem at scale and supports our compliance requirements.

Mean time to detect anomalies in vehicles came down significantly. It is not only mean time to detect but mean time to respond as well to incidents and containing the incident that came down as well. Fleet visibility coverage went on to become significantly higher percentage connected vehicles being monitored. Cost avoidance occurred because of proactive detection, defects were caught early, and warranty claim reduction came down. There are operational ROIs, warranty ROIs, compliance ROIs, deployment and operational ROIs, and business risk ROIs. We could measure cost avoidance, efficiency gains, and revenue protection, and this actually sums up various things on which we could measure the ROI. Our overall rating for Upstream Security is nine out of ten..”

TarunKumar11
Member Of Leadership Advisory Council at a tech company with 10,001+ employees

Read full review

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