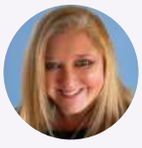
vorlon

CARGURUS CASE STUDY

CarGurus Chooses Vorlon to Drive Their SaaS App Ecosystem Security Program

"I love the ease of working with Vorlon and the hard work and tenacity they put into making sure the partnership was there with us in connecting our custom application to our SaaS applications, hearing our concerns, and use cases. There's an element of care there for our success."



Kelly Haydu

VP, Information Security, Technology and Enterprise Applications
CarGurus

CarGurus®

INDUSTRY

Online Automotive Marketplace

CHAMPION

Kelly Haydu

VP, Information Security, Technology And Enterprise Applications

Security challenges

- Identify and assess risk associated with the complex web of APIs connecting their proprietary platform to public SaaS applications
- Real-time threat detection and response across their application ecosystem
- Clear understanding of the potential impact of a third-party breach and how to recover
- Enforce good API security governance and ensure compliance with data privacy regulations like GDPR and CPRA

Results using Vorlon

- Comprehensive visibility into the complex web of applications, APIs, users, secrets, and data flows helps CarGurus identify and assess security risks more effectively
- Real-time threat detection and faster incident response by identifying anomalies in API traffic and integrating with their SIEM and ITSM
- Breach assessment and recovery protocols in case a SaaS vendor ever gets breached
- Proactive monitoring of API activity, enforcement of API security governance, and support for data privacy mandates like GDPR

CarGurus offers data-driven solutions for car shoppers and dealerships

CarGurus is a multinational online automotive platform that uses proprietary technology, search algorithms, and data analytics to provide more trust and transparency in the car buying and selling experience. The CarGurus platform gives consumers the confidence to purchase or sell a vehicle either online or in person, and it gives dealerships the power to effectively price, market, acquire, and sell vehicles, all with a nationwide reach.

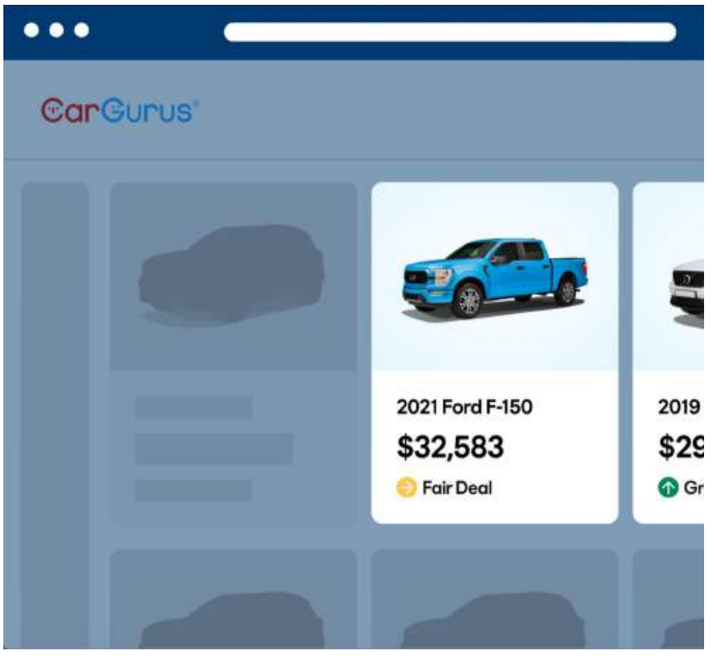
With more car listings than any other major online marketplace[1], CarGurus is the most visited automotive shopping website in the U.S.[2] The company also operates digital auto platforms in Canada and the United Kingdom.

CarGurus carries no inventory of its own. Instead, car dealers nationwide provide data to the marketplace platform about the new and used vehicles they have available for sale. The rapid exchange and presentation of data makes CarGurus highly invested in using APIs for both inbound and outbound data processing.

Taking inventory of inbound and outbound API traffic across CarGurus' complex SaaS ecosystem

During her four-year tenure at CarGurus, Kelly Haydu has acquired multiple areas of responsibility. She started with the security program and now covers IT and Enterprise Applications.

As she delved more deeply into the company's application security program, Haydu wanted an inventory of inbound and outbound API traffic, including connectivity between multiple SaaS applications and CarGurus' proprietary platform. "We saw an opportunity to establish a more sophisticated way of identifying those APIs, which led us to Vorlon," she says.



Gaining data flow visibility to understand risk

Next, Haydu set out to gain deeper visibility and assess risk across their complex web of applications, APIs, users, secrets, and data flows. Haydu explains, "We obviously have protections at the perimeter, with firewalls, gateways, and so on. Inbound and outbound traffic, including APIs, are monitored but we wanted to take it a step further and analyze who and how our open APIs are being used."

"Vorlon goes deeper than a simple discovery and inventory of our API ecosystem. It actually tells us what SaaS apps are doing and what data is moving between them. Data protection being critical to our security program, this level of visibility is important."

Kelly Haydu

VP, Information Security, Technology and Enterprise Applications

CarGurus

Creating a program to assess and recover from a potential SaaS vendor breach

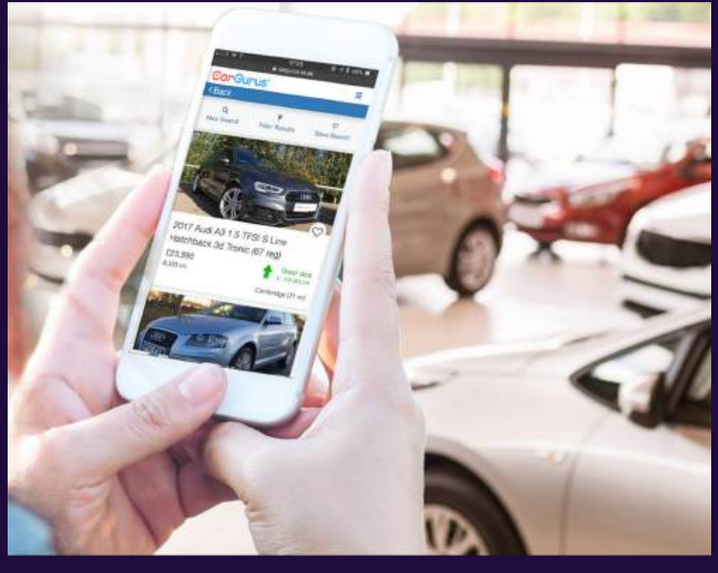
CarGurus relies on SaaS but recognizes the security risks they introduce. To mitigate these risks, they've developed a program to assess and recover from potential third-party application breaches. "We wanted to identify all the connection points within back-office systems, including both inbound connections and internal API usage," explains Haydu. "This allows us to proactively understand the security implications of a potential or suspected vendor application security breach, especially if that vendor is connected to other vendors within our system. Knowing these connections helps us understand the potential scope of compromise and determine the necessary steps, such as quarantining affected systems and/or notifying relevant parties meeting compliance requirements."

Integration with other tools facilitates threat detection and response and workflows

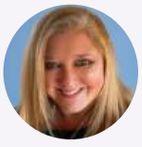
Haydu wanted to give real-time visibility to the Security Operations (SecOps) team so that anomalies in the inbound traffic or something they are unsure about can be sent to the company's SIEM where the SecOps team can quickly act on it. Vorlon identifies risks like unauthorized API activity, dormant secrets, and unusual data-sharing behaviors. "It's important to be able to aggregate all that information and put it into a real-time ticket to create an alert," says Haydu. "We can better understand our risk from the traffic and data that's potentially flowing in. It also helps with setting policies we want to put around that API, for example, whether or not to auto-block something."

Identifying and correcting API security policy drift

CarGurus crafts its unique security policies, meticulously outlining acceptable API usage, data access protocols, and third-party integration guidelines. With Vorlon, the company is able to take an even greater proactive stance in maintaining adherence to these policies. By continuously monitoring API activity and data flows, Vorlon can detect "policy drift"- instances where actual practices deviate from established policies. Vorlon flags these discrepancies, providing the security team with actionable insights to quickly rectify the situation and ensure ongoing compliance with API security governance standards.



"With Vorlon, we can take an even more proactive approach to monitoring our security policies, which helps us maintain a robust security posture."



Kelly Haydu
VP, Information Security, Technology and Enterprise Applications
CarGurus

Understanding data flows for compliance with GDPR and other regulations

Vorlon also helps CarGurus put context around where data is flowing, which is critical for compliance with data privacy regulations such as GDPR. "We have a presence in the UK and Dublin, Ireland, so we must ensure compliance with data privacy law in those countries," says Haydu. "Vorlon helps us identify the open APIs and who is connecting to our platform. We can see what the inbound requests are and more importantly, whether there is data feeding out of the organization to different geographic locations. Vorlon supports our privacy requirements and provides actionable insights to our security team and application owners."

Vorlon improves application ecosystem security with cross-functional collaboration

Vorlon can send step-by-step remediation guidance to internal application owners and enable break-the-glass remediations, like revoking risky access to the CarGurus platform, with just two clicks. This combination of enabling good hygiene and responding quickly to active threats helps ensure the business runs smoothly and securely.

"We already had strong platform engineering processes," says Haydu. "But Vorlon has improved cross-functional collaboration, from IT and SecOps to application development. Shared insights enable us to identify risks and detect third-party threats faster. Vorlon has delivered organization-wide benefits."

About Vorlon

SaaS moves fast—Vorlon's SaaS ecosystem security platform gives enterprises the context to move faster. By combining data flow visibility, posture and secrets management, and detection and response, Vorlon helps you see what's connected, what's at risk, and what to do next. With its agentless, patent-pending DataMatrix technology, Vorlon builds a live model of your SaaS environment to power fast, AI-driven remediation. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies to secure what others miss: the interactions between apps, identities, and data that power modern business. Learn more at vorlon.io.