Upstream case study

Solution integrated with the Microsoft Connected Vehicle Platform and other Microsoft services provides cybersecurity for connected cars

Connected car infrastructures can be exploited by hackers

Connectivity exposes vehicles to a wide array of new risks, such as cyber threats targeting their smart mobility services.

A cybersecurity solution that works with Microsoft services

Microsoft partner Upstream's C4 platform, which integrates with the Microsoft Connected Vehicle Platform (MCVP), protects connected vehicles from cyberattacks.

Using data and a digital twin to diagnose threats and ensure safety

With MCVP engines and data from connectivity providers, Upstream creates a digital twin of a connected vehicle service to identify security anomalies.

Microsoft

Upstream focuses on mobility service infrastructure and customer success

With offices and representatives in Israel, the United States, the United Kingdom, Germany, Japan, and Korea, Upstream helps corporations mitigate connectivity risks and ensure the safety and security of smart mobility solutions. The company's cybersecurity and data professionals maintain a clear focus on customer success, resulting in comprehensive protection of mobility service infrastructure, connected vehicles, and, most importantly, drivers and passengers.

Upstream is a graduate of the Microsoft ScaleUp program and has announced a partnership with Microsoft Azure Sentinel and the MCVP automotive team. Upstream's C4 (Centralized Connected Car Cybersecurity) platform, available in the Azure Marketplace and on AppSource, runs on customers' private clouds, utilizing multiple Azure connectors, storage, and processing capabilities, as well as prebuilt integrations with Azure Sentinel SIEM (security information and event manager).

How Upstream's C4 platform protects connected cars

The automotive market is undergoing massive disruption as connected car technology rolls out. As more vehicles become connected, the potential for hacking is going to increase substantially, so original equipment manufacturers (OEMs) and connected fleet security operators will need purpose-built protection.

Protecting connected cars is a complex problem involving multiple layers (drivers, mobile applications, vehicles, fleets), mountains of data flowing at high speed, and a specialized and discrete understanding of smart mobility business and usage type. Upstream's agentless and 100 percent cloud-based C4 platform ingests and normalizes all these data feeds, distilling cybersecurity insights that span the vehicle itself, telematics servers, and mobile applications. Upstream already ingests data from millions of vehicles across multiple automotive applications, significantly increasing the use cases for that data.

C4 offers in-depth integration with MCVP, Microsoft's automotive-grade development platform designed to accelerate the delivery of smart vehicle opportunities and mobility experiences. Playbooks reflect the collaboration of Upstream, Azure Sentinel, and MCVP, enabling the investigation, containment, and remediation of cybersecurity scenarios.

With prebuilt data ingestion capabilities using MCVP engines, Upstream leverages data feeds produced by OEMs or connectivity providers to create a digital twin of a connected vehicle service. It then uses this digital twin and a baseline of normal operation to identify security anomalies. C4 is prebuilt with an automatic library of policies designed to detect a large range of known attacks, from injection-based attacks and replay attacks all the way to advanced unknown attacks.

"As new automotive cybersecurity regulations and standards are demanded, OEMs must find additional ways to integrate cybersecurity into their operations. As such, our integration with the Microsoft Connected Vehicle Platform allows Microsoft automotive customers to build an automotive-fluent and seamlessly integrated cybersecurity solution into their enterprise."

- Yoav Levy, Co-Founder and CEO, Upstream