

Data Collection Disclosure

This page informs you of the data that is collected and transmitted by VicOne's security products, as part of providing you with the security functions of these products.

xNexus

Default (non-disableable) collection

It is necessary to collect this data to provide the security functions of this product. Therefore, you cannot disable these features. If you do not want VicOne to access this data, you should stop using the product.

Feature	Data Collected	Configuration	Purpose
Vehicle Anomaly Detection	<ul style="list-style-type: none">• Vehicle Telemetry Data• Vehicle ID• GPS Location	OEM vendor-controlled	<ul style="list-style-type: none">• Baseline comparison for abnormal behavior detection• Event correlation• Fleet route mapping
Vehicle Cybersecurity Detection	<ul style="list-style-type: none">• In-Vehicle IDPS (xCarbon) Detection Logs• Vehicle ID	OEM vendor-controlled	<ul style="list-style-type: none">• Includes IPS/WRS/CAN anomaly detection features

Configurable Features

Feature	Data Collected	Configuration	Purpose
N/A			

Note: The configuration column indicates which party controls whether this dataset is transferred to VicOne. 'OEM vendor-controlled' means the OEM customer decides which datasets are sent to VicOne as part of the product deployment.

When customers enable the xNexus analysis feature, vehicle telemetry data and detection logs generated by xCarbon will be uploaded to VicOne Cloud for processing by xNexus.

Data Controller & Privacy Contact

VicOne processes data as described above as data processor on behalf of its customers, on the basis of contract performance (Art. 6(1)(b)) and/or legitimate interests (Art. 6(1)(f)). For privacy inquiries or to exercise your data subject rights, contact gdpr@vicone.com. You also have the right to lodge a complaint with your local data protection authority.