EXTRAHOP

Automotive Industry: Protecting the Global Flow from Smart Factory to Connected Road

Keep Connected Vehicle Networks and Production Lines Free from Threats with ExtraHop RevealX™

Industry Challenges: From Smart Factories to Software-Defined Fragility

The automotive industry in 2026 has transitioned into a software-first ecosystem where the vehicle functions as a mobile data center. While the shift toward software-defined vehicles (SDVs) and autonomous mobility has unlocked new revenue streams, it has also introduced digital risks that threaten human safety and global production stability. Automotive leaders are currently navigating several critical friction points:

- **The Escalation of Nation-State Sabotage:** Geopolitically motivated adversaries have shifted their focus from intellectual property theft toward the functional sabotage of automotive infrastructure. By targeting the safety instrumented systems within smart factories or the over-the-air (OTA) update pipelines, nation-state actors can induce large-scale fleet recalls or paralyze entire regional production lines. Protecting the global flow of vehicles requires deep internal visibility to stop lateral movement before an adversary can execute destructive commands on a plant floor or within a vehicle-to-cloud gateway.
- **The Software-Defined Vehicle and the API Supply Chain Crisis:** Modern vehicles rely on millions of lines of code and thousands of third-party API integrations for telematics and navigation. Attackers exploit these trusted connections through a compromised tier-1 or tier-2 supplier to move from a partner network into the core production environment. Using hijacked service tokens, they can manipulate the software build process or inject malicious code into critical firmware updates, creating systemic safety risks that traditional perimeter defenses cannot detect.
- **The Visibility Gap in Smart Factories and Connected OT:** Automotive manufacturing relies on high-velocity, automated environments filled with unmanaged endpoints. These include robotic welders and programmable logic controllers (PLCs) that cannot support security agents. This agent blind spot allows attackers to establish a foothold and move laterally without detection. Organizations must have off-the-box visibility to identify protocol anomalies directly on the wire before they escalate into production standstills.
- **Regulatory Rigor and Vehicle Lifecycle Security:** 2026 mandates like UN R155 and UN R156 have shifted the burden of security to continuous monitoring. Manufacturers must provide an unalterable forensic record of security throughout the vehicle's entire lifecycle. Meeting these standards along with ISO/SAE 21434 and TISAX requires a definitive source of truth that proves the integrity of every network transaction between the vehicle, the cloud, and the manufacturing floor.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect high-velocity assembly and automated paint shop operations.

The Definitive Data Source for the AI-Enabled SOC

Provides high-fidelity wire data to power automotive SOC automation. This delivers unalterable ground truth to eliminate investigative friction and accelerate remediation.

AI-Powered Cyber Threat Detection

Identifies lateral movement and ransomware targeting OTA update pipelines and vehicle-to-cloud gateways using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility

Automatically discovers unmanaged IoT and OT assets like robotic welders and AGVs without installing software or risking production stability.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and PFS traffic to expose hidden threats without adding latency to time-critical automotive manufacturing schedules.

High-Fidelity Performance Metrics

Troubleshoots disruptions using 5,000+ wire data metrics for deep operational insight into network latency and automated production performance.

Continuous Forensic Capture

Maintains unalterable transaction records to satisfy UN R155, R156, and ISO/SAE 21434 audit requirements while accelerating root-cause analysis.

The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the unalterable ground truth required to secure the modern automotive ecosystem. By analyzing every packet at line rate, RevealX eliminates the visibility gaps that traditional security tools ignore. In an industry where a single minute of assembly line downtime can cost tens of thousands of dollars, RevealX delivers the real-time insights needed to maintain production uptime and brand integrity.

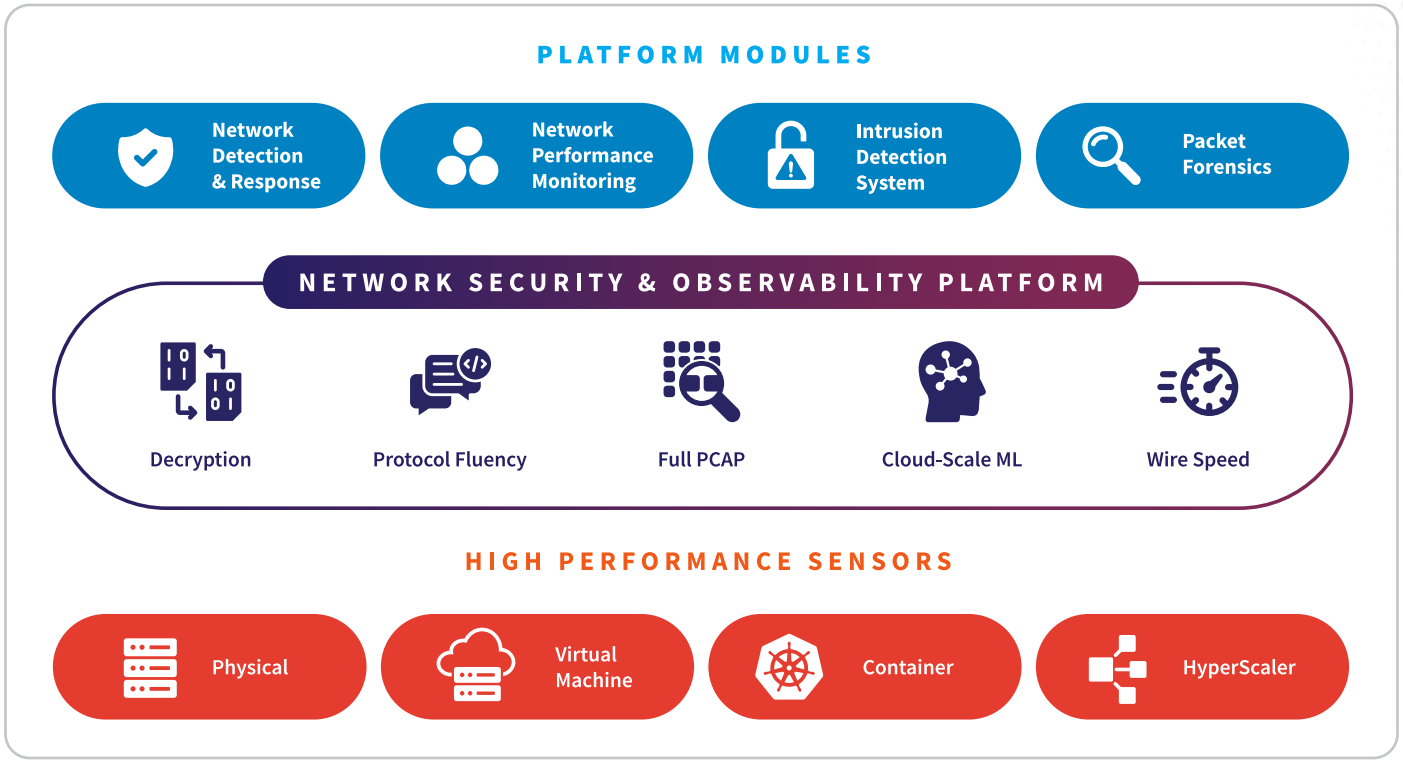
The platform solves the agent blind spot by providing agentless, passive decryption and monitoring of over 90+ protocols. This ensures that critical assets like robotic assembly arms, automated guided vehicles, and smart factory sensors are fully visible without risking system stability. By baselining normal behavior across these unmanaged devices, security teams can instantly detect anomalies that indicate an adversary has established a foothold on the factory floor or within a sensitive research and development lab.

To counter geopolitically motivated sabotage, RevealX identifies subtle shifts in network behavior that signify lateral movement from corporate IT into the operational heart of the production network.

By exposing hidden threats within encrypted traffic using strategic decryption, the platform stops attackers before they can manipulate software build servers or compromise the over-the-air update pipeline. This visibility extends to the sprawling supplier ecosystem, where RevealX monitors the integrity of tier 1 and tier 2 integrations to prevent partner-borne contagion from reaching core systems.

Beyond threat detection, RevealX accelerates incident response to meet the continuous monitoring requirements of UN R155 and R156. It provides a definitive forensic record of all network transactions, which eliminates the guesswork during investigations and allows for rapid root-cause analysis. This unified approach bridges the gap between the SOC and the NOC by combining security detection with performance metrics. By monitoring the health of critical transaction paths, RevealX ensures that security measures do not introduce latency, protecting the precision of software-defined vehicle operations.

ExtraHop NDR Platform



NDR Technology Use Cases for the Automotive Industry

Nation-State Attacks	Detects lateral movement and exfiltration in campaigns targeting proprietary EV battery tech, autonomous driving algorithms, and proprietary manufacturing blueprints.
Threat Detection & Response	Investigates hidden threats across converged IT/OT environments, filling visibility gaps in smart factories and assembly plants where agents cannot be deployed.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and protocol anomalies before they impact safety-critical production or fleet-wide OTA updates.
SOC Modernization	Unifies SOC and NOC workflows with AI prioritization to reduce alert fatigue, accelerating response times for critical manufacturing and V2X service delivery.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of UDS, Modbus, and MQTT commands for one-click root-cause analysis of production outages or vehicle gateway breaches.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate IT toward critical plant controllers and safety instrumented systems (SIS).
Cloud Workload Security	Provides agentless visibility for cloud-integrated vehicle-to-cloud (V2C) services, discovering shadow IT across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse targeting high-value engineering workstations and software build servers.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of trade secrets or total paralysis of the production line.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including robotic welders, AGVs, and telematics units that cannot host security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy assembly floor hardware and PLC stations.
AI Security	Monitors generative AI and autonomous agents used for design simulation, production optimization, or autonomous navigation in containerized workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that IEC 62443 zone/conduit policies and Purdue model segmentation are effective.

NPM Technology Use Cases for the Automotive Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for automated assembly and paint shop control sessions.
Operational Resilience	Resolves infrastructure degradation before it hits production continuity, ensuring availability for mission-critical ERP and supply chain services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between plant operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during PLM or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for V2X gateways and supplier traceability APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past assembly outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into transaction processing time versus network latency in high-volume manufacturing hubs.

Automotive Industry Compliance & Regulatory Use Cases

Vehicle Security	Global	UN R155	Continuous Monitoring: RevealX provides the unalterable forensic record required for CSMS certification and proves the security of the vehicle-to-cloud ecosystem.
Update Integrity	Global	UN R156	OTA Assurance: Monitors the integrity of the software update management system (SUMS). RevealX detects unauthorized changes to firmware update payloads.
Engineering Security	Global	ISO/SAE 21434	Lifecycle Monitoring: Supports cybersecurity throughout the vehicle development life cycle by providing deep visibility into V2X and telematics traffic.
Supply Chain Trust	Europe / Global	TISAX	Partner Auditing: Monitors data exchange with tier 1 and tier 2 suppliers. RevealX ensures that sensitive OEM blueprints and IP are not exfiltrated by third parties.
Operational Resilience	European Union	NIS2 Directive	Industrial Continuity: Identifies unauthorized pivots and “living-off-the-land” attacks. RevealX satisfies mandates for continuous monitoring of essential transport services.

Customer Benefits: Ensuring Production Resilience and Operational Continuity Across the Automotive Ecosystem

ExtraHop RevealX delivers tangible business outcomes for automotive leaders by transforming network data into actionable intelligence. Organizations achieve immediate ROI through the consolidation of security and performance monitoring tools, which reduces operational overhead while improving cross-team collaboration between the SOC and NOC.

A primary benefit is the significant reduction in mean time to detect and respond to systemic threats. By providing unalterable ground truth across the entire supply chain, RevealX ensures that security teams can identify lateral movement before it impacts assembly lines or vehicle safety systems. This proactive stance protects brand reputation and prevents the massive financial losses associated with production standstills or large-scale fleet recalls.

Furthermore, RevealX simplifies the complexity of 2026 regulatory compliance. The platform automates the data collection required for UN R155, UN R156, and TISAX reporting, allowing organizations to meet strict audit requirements with confidence. By maintaining continuous visibility into unmanaged IoT and OT assets, manufacturers can prove the integrity of their digital perimeters to partners and insurers. Ultimately, RevealX secures the global flow of automotive innovation by ensuring that the digital infrastructure supporting the physical world remains resilient, visible, and under control.

> "With ExtraHop, we're not spending time looking for a needle in a haystack. That means we can spend more time on projects that are strategically valuable to the business."

IT SECURITY MANAGER
American Transportation Manufacturer

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in the automotive industry:
Automotive Parts Supplier
Automotive Manufacturer

Or contact us to schedule your personalized demo and security assessment.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com