VicOne

Driving Automotive
Cybersecurity Forward

Safeguarding Software-Defined Vehicles

Enhanced Resilience via Integrated Detection and Prevention With NXP's GoldBox

The automotive industry is undergoing a significant transformation to meet the increasing demand for software-defined vehicles (SDVs). This shift opens up new opportunities for manufacturers (OEMs) and suppliers in the industry. Consumers now enjoy the seamless integration of fresh features through over-the-air (OTA) updates, eliminating the need for physical visits to service stations. This flexibility enables OEMs to continuously enhance their vehicles, introducing innovative business models such as on-demand features and subscription services.

However, despite the convenience brought by SDVs, the intricate and interconnected nature of modern vehicles raises challenges for OEMs and Tier 1 suppliers. As the automotive landscape becomes more connected and software-driven, it becomes a prime target for malicious actors, emphasizing the importance of robust security measures. One notable concern is evolving threats to in-vehicle networks. An illustrative example occurred in 2020 when researchers successfully injected malicious code causing a compromised in-vehicle infotainment (IVI) system to connect to a rogue Wi-Fi hotspot. This allowed them to inject malicious Controller Area Network (CAN) messages, enabling unauthorized car diagnostics.

To address these challenges, we integrated VicOne's xCarbon intrusion detection and prevention system (IDPS) with NXP's GoldBox vehicle networking development platform. The resulting automotive cybersecurity solution is designed to detect threats inside the vehicle and provide basic capabilities to combat ever-changing cyberthreats.

Unlocking Multilayered Security: How Does This Work?

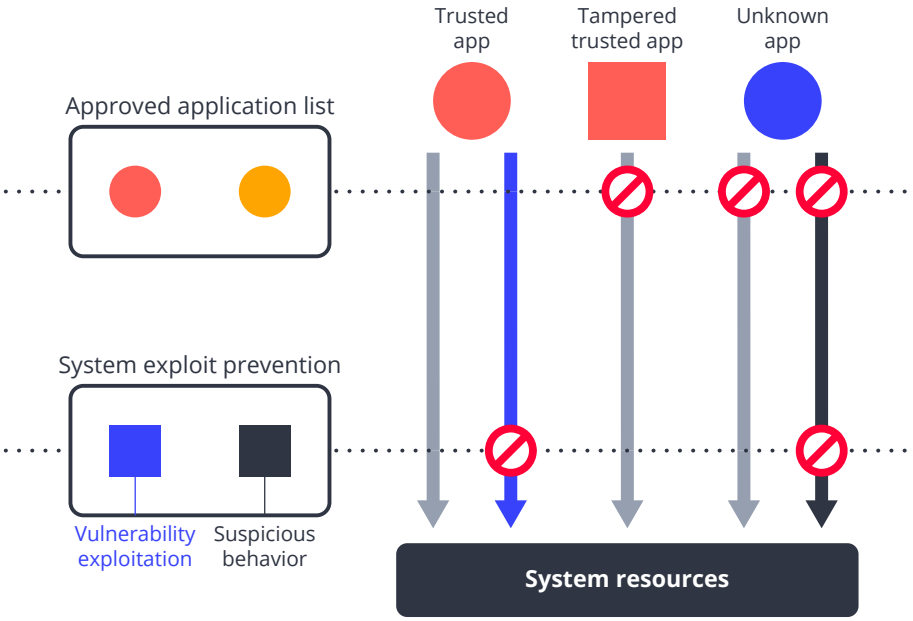
Our robust solution delivers a precise yet lightweight detection and response mechanism, effectively countering ever-evolving cyberthreats.

1. **Detect in Real Time**

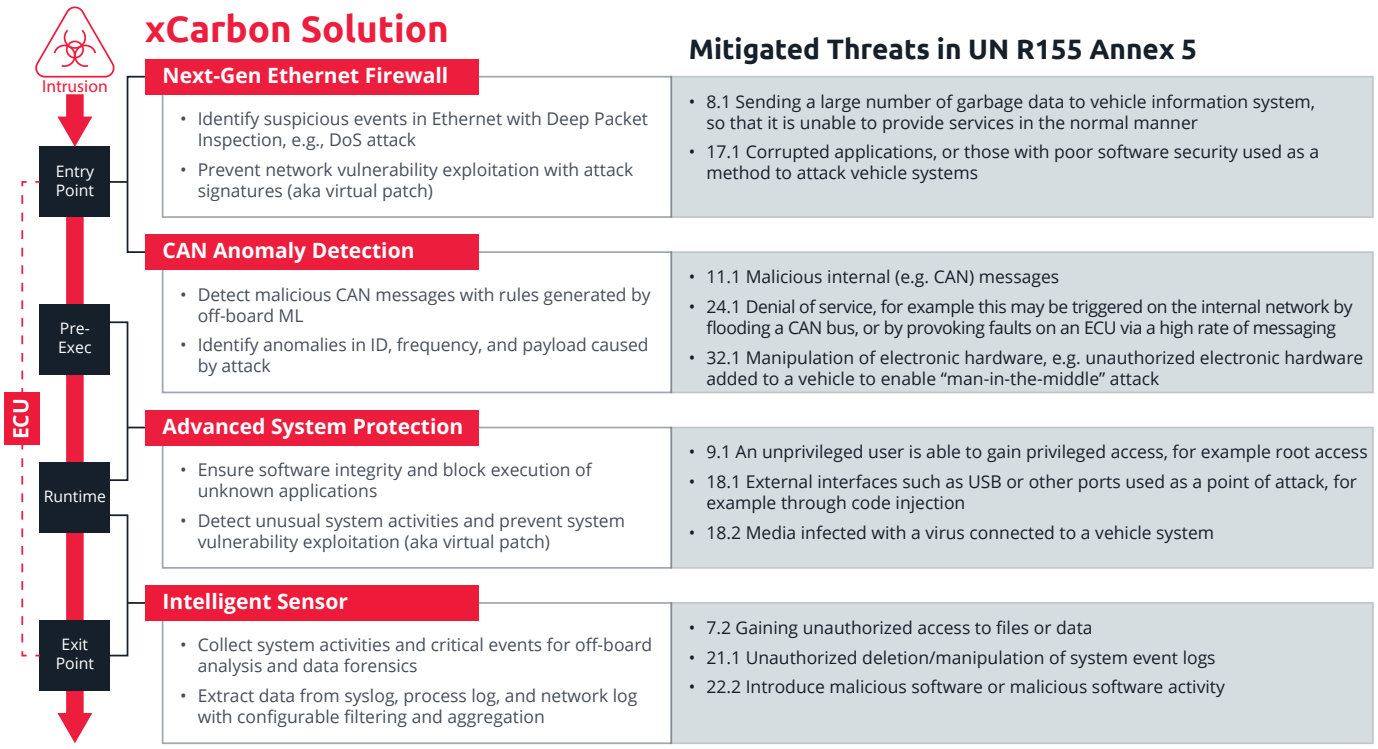
   To effectively thwart threats within in-vehicle networks, the use of deep packet inspection (DPI) is crucial in identifying suspicious events in Ethernet, such as denial-of-service (DoS) attacks, combined with the pre-integration of VicOne's xCarbon and NXP's GoldBox. This integration allows for real-time DPI analysis of Ethernet packets. In addition, with expert rules and virtual patching, xCarbon enforces attack signatures and security rules, so that OEMs can protect their systems without changes in their binary code and get an average of 102 days of protection before a vendor patch is available. These security policies and rules also help DPI prevent and block exploits faster and more accurately.

   Furthermore, xCarbon can distinguish between normal and abnormal operations on the CAN bus to detect malicious CAN messages, such as messages with abnormal IDs, frequencies, and data volume or traffic caused by attacks.

xCarbon can also detect malicious system activities or behavior to prevent system vulnerabilities from being exploited in advance. When vulnerabilities are discovered, virtual patching can prevent and block exploits by enforcing multiple layers of security policies and rules. xCarbon can also prevent unauthorized applications from running on the service-oriented architecture (SOA) by validating applications through the approved application list:



The following figure breaks down the cyberattack life cycle into its component stages to show how xCarbon can help on each stage:



2. **Analyze With Cloud-to-Car Visibility**
   Once malicious threats are detected, VicOne's xCarbon transmits the detection logs and system activities back to VicOne's xNexus vehicle security operations center (VSOC) platform for further threat investigation. To optimize bandwidth usage and save cost, xCarbon reports only high-confidence alerts to xNexus.

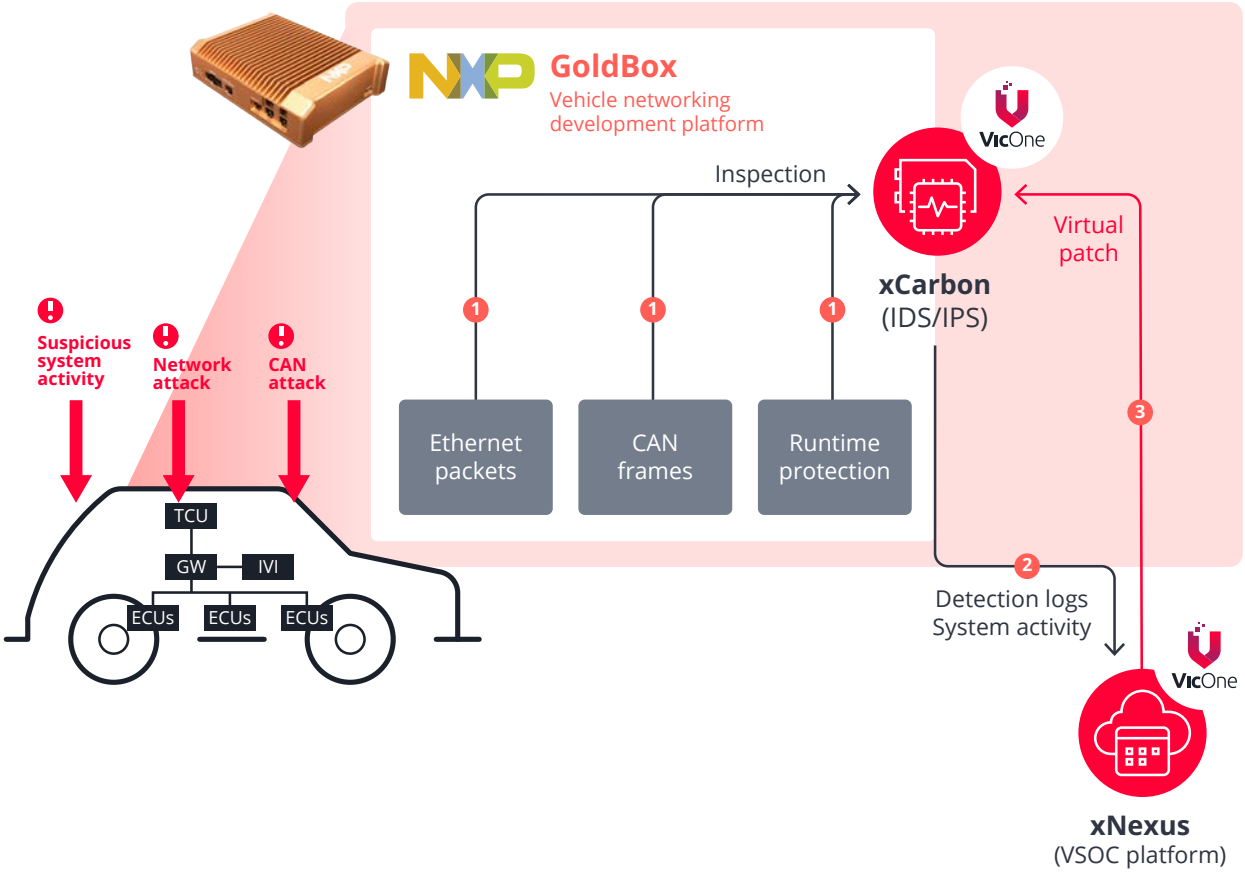
   Once vehicle telemetry data and detection logs are transmitted to the xNexus platform, it effectively correlates this information, providing an enhanced level of visibility and context to the VSOC. This enables the VSOC to identify threats and proactively search for potential risks. Unlike other solutions that inundate users with overwhelming and unexplainable anomaly events, xNexus can offer high-confidence security alerts with actionable intelligence, eliminating false positives and facilitating rapid investigation. xNexus is able to do this as it leverages over 30 years of threat intelligence from Trend Micro and round-the-clock vulnerability research by a global network of independent researchers through the Zero Day Initiative (ZDI). This extensive knowledge empowers xNexus' analytics engine to learn attack behaviors and stay ahead of constantly evolving cyberthreats, resulting in a higher rate of detection.

   In addition, through artificial intelligence–driven detection (machine learning), after detecting abnormal events, xNexus can correlate scattered events into "attack stories." These allow VSOC teams to conduct rapid investigation and proactive threat mitigation through rich actionable context, identifying potential threats before the attack chain is even completed.

3. **Respond via Unique Virtual Patch (Patent Pending)**
   As the automotive industry involves an increasing number of stakeholders and suppliers, the complexity of incident response becomes more challenging. To address this, the combination of the xNexus VSOC platform and the xCarbon intrusion prevention system (IPS) offers a solution that provides virtual patches for effective postproduction mitigations, enabling systems based on GoldBox to prevent network vulnerability exploitation with attack signatures and detection of unusual system activities.

   By leveraging virtual patching, xCarbon enforces attack signatures and security rules, allowing OEMs to protect their systems without making any changes. This approach provides an average of 102 days of protection while waiting for a vendor patch to become available. OEMs can deploy virtual patches without requiring code changes or firmware updates. This capability helps block zero-day exploits and gives OEMs more time to develop mitigation plans and solutions.

The following figure illustrates the multilayered protection platform for automotive connectivity domain controllers against network/CAN attacks:



Extra Benefit: Prevent Costly Vehicle Recalls With Patent-Pending Virtual Patching

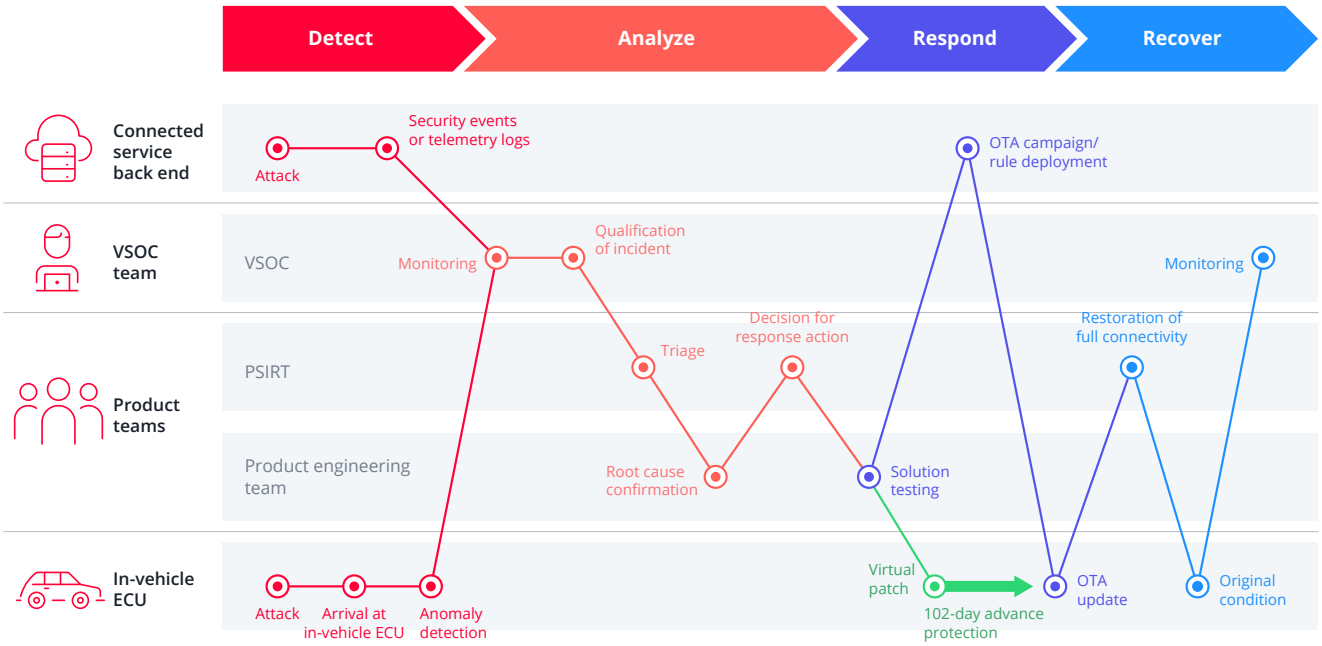
The beauty of OTA is that it can help OEMs to fix problems remotely. However, as noted by Forbes, "software updates have not historically been successful and may induce further costs if not well managed." In 2015, an automaker "realized a recall for a cybersecurity breach on vehicles without remote-reflash capability. The total bill was likely above $150M to fix given the costs of each jump drive that was snail-mailed to the 1.4M vehicle owners plus the resulting dealership costs for all of the owners who were unaware of their vehicle's USB drive." So, even if there is a vendor patch available after a while, many things can still go wrong and it can still be a painful process for OEMs.

In the current landscape of cybersecurity, dealing with cyberattacks involves a complex and lengthy process of detection and recovery. Patch management plays a crucial role in this scenario, requiring the regular application of patches, fixes, updates, and improvements to software to thwart potential vulnerabilities exploited by cyberthreats. In the automotive industry, this process unfolds when an attack targets an in-vehicle electronic control unit (ECU). The host intrusion detection system (IDS) identifies anomalies, triggering the product security incident response team (PSIRT) to isolate and address the detected issues.

However, the issuance of a fix is a time-consuming endeavor, stretching over months or even years. This is because of the necessity for the suppliers to develop the fix, contractual agreements in the purchasing process, and the OEM and suppliers undergoing their verification and validation (V&V) cycle to ensure the effectiveness of the mitigation. This fix is then provided with the subsequent service pack. The availability of penetration testers or the vehicles themselves can pose additional bottlenecks during this phase. Throughout this period, the vulnerability remains exploitable until a bug fix is delivered.

To date, the most practical response to a critical cybersecurity incident involves deactivating functionality to prevent exploitation, such as disabling wireless connections while awaiting a software patch from the vendor. However, this approach has its drawbacks, not only causing frustration for car owners and negatively impacting the brand, but also, as highlighted by Forbes, leading to costly vehicle recalls due to the absence of connectivity.

At this juncture, the implementation of xCarbon's virtual patching offers a solution by effectively blocking potential exploits before the release of the official vendor patch, leading to cost saving in insurance rates and incurring a lower cost than a physical software patch:



Conclusion

The integration of VicOne's xCarbon and NXP's GoldBox gives the following major advantages:

- Built-in security aligns strongly with compliance requirements such as the ISO/SAE 21434 cybersecurity standard and the UN R155 regulation, which advocates ensuring security in the entire vehicle life cycle.
- An integrated solution delivers comprehensive visibility from cloud to car, eliminating the blind spots of the entire vehicle ecosystem and accelerating investigation.
- The integration of VicOne's solutions with NXP's GoldBox improves overall compatibility and performance, and eliminates integration efforts.
- A modular design allows for streamlined customization, with a focus on minimizing any potential impact on ECU performance.
- Support for various operating systems, including Embedded Linux, Android Automotive OS, and QNX, ensures seamless integration.

To learn more about our proven success, read our solution brief "VicOne, NXP, AWS, and Inventec Collaborate on Pre-Integrated and Comprehensive Cybersecurity Solution for Software-Defined Vehicles."