VicOne

THE STATE OF AUTOMOTIVE CYBERSECURITY 2025

Highlights From the **VicOne 2025 Automotive Cybersecurity Report**

As vehicles transform into sophisticated, software-defined machines, the stakes for cybersecurity have never been higher. **The race to secure connected vehicles is on**, as unprecedented cybersecurity risks emerge with every new line of code and advanced feature.

In this overview, VicOne examines the key trends and insights arising from a landscape filled with risks as well as opportunities. From emerging AI security risks to predictions of future challenges, these highlights offer a snapshot of

an automotive cybersecurity landscape in a state of CONSTANT FLUX.

AI Revolutionizing Mobility,

REDEFINING RISKS

The integration of AI into vehicles unlocks transformative capabilities but introduces significant risks.

Core AI Risks in Automotive Security

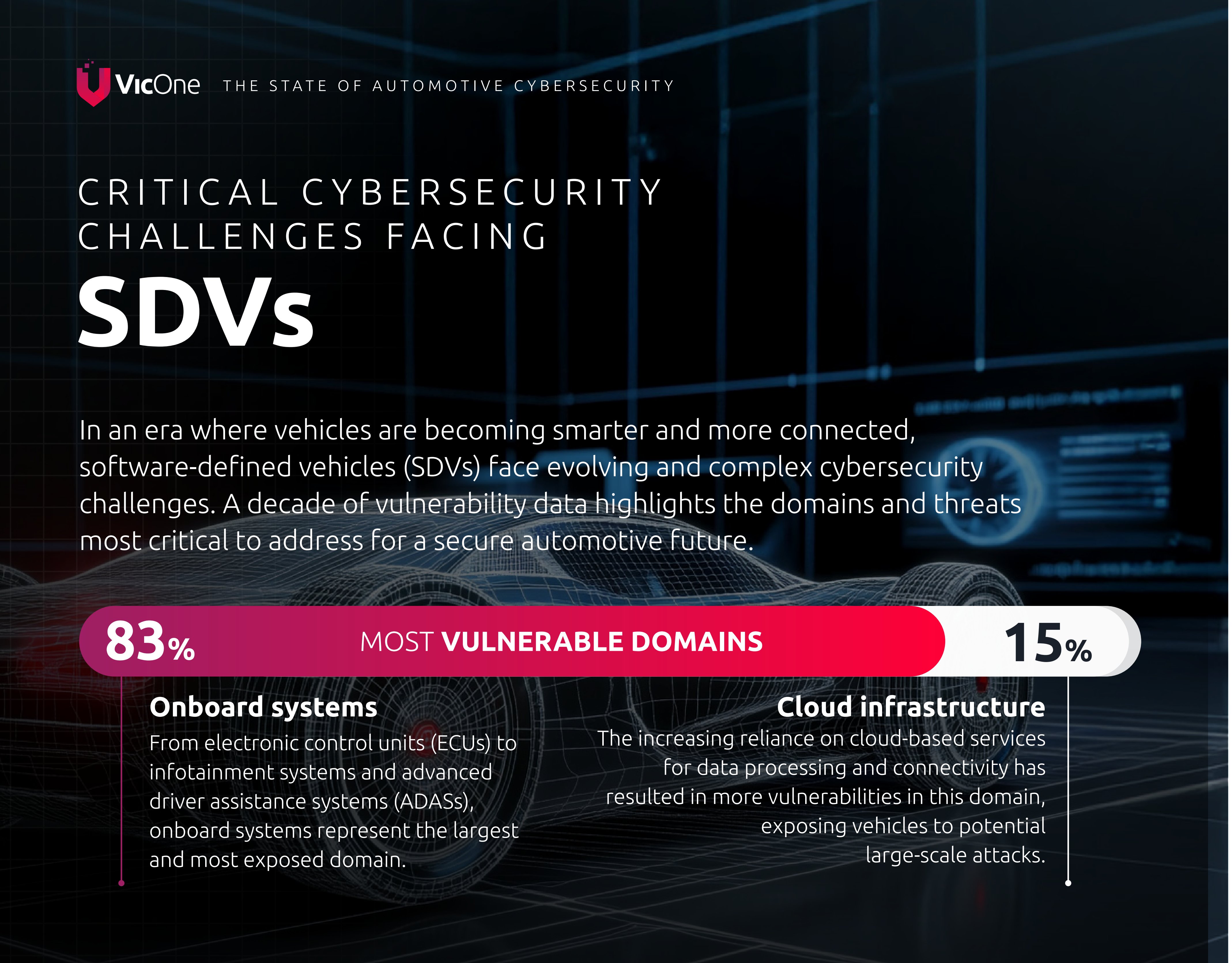
AI systems in vehicles introduce both **access and data vulnerabilities,** opening new attack vectors for cyberthreats.

Voice Assistance Systems: New Frontiers, New Risks

Voice assistants have revolutionized vehicle operation with hands-free functionality. But their dependence on voice recognition gives rise to **novel threats such as prompt injection attacks.**

Onboard AI Deployment and Expanded Attack Surfaces

Directly deploying AI models onto in-vehicle hardware ensures low latency and responsiveness for critical functions. However, chip-based AI accelerators can expose vehicles to **hardware-specific vulnerabilities.**



CRITICAL CYBERSECURITY CHALLENGES FACING SDVs

In an era where vehicles are becoming smarter and more connected, software-defined vehicles (SDVs) face evolving and complex cybersecurity challenges. A decade of vulnerability data highlights the domains and threats most critical to address for a secure automotive future.

83% MOST VULNERABLE DOMAINS 15%

Onboard systems

From electronic control units (ECUs) to infotainment systems and advanced driver assistance systems (ADASs), onboard systems represent the largest and most exposed domain.

Cloud infrastructure

The increasing reliance on cloud-based services for data processing and connectivity has resulted in more vulnerabilities in this domain, exposing vehicles to potential large-scale attacks.

TOP SECURITY CONCERNS

1,564 Supply chain vulnerabilities

With suppliers and third parties deeply integrated into the vehicle ecosystem, ensuring security across every link in this intricate network is a formidable challenge.

308 Third-party integration vulnerabilities

As vehicles depend more on external services, integrating third-party technologies has expanded the attack surface, introducing unforeseen risks.

295 Vehicle hijacking vulnerabilities

Exploits targeting SDV software can grant attackers remote control over critical vehicle systems, jeopardizing both safety and security.

*Out of a total of **2,271 SDV-related vulnerabilities** published from 2014 to 2024*

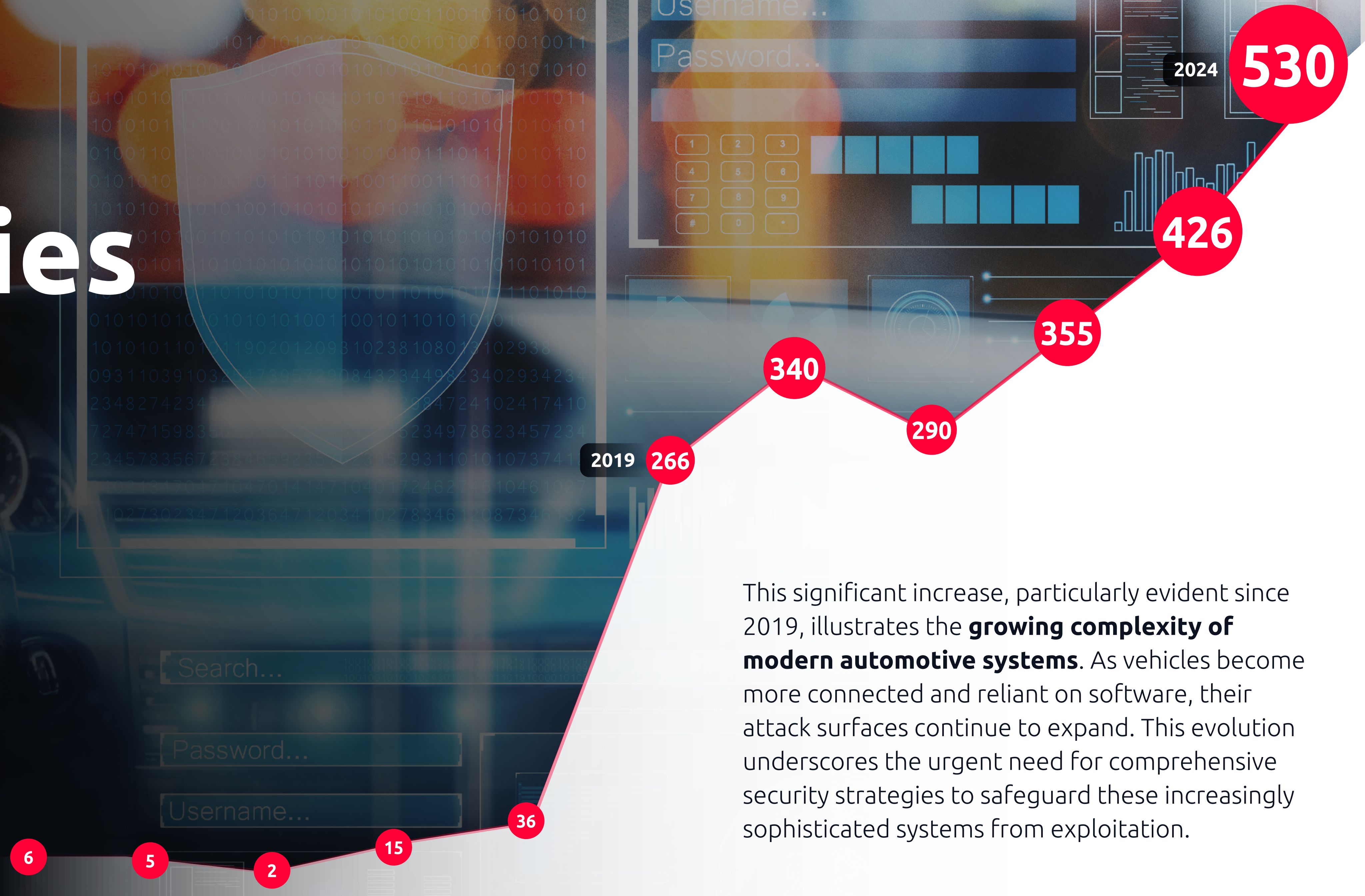
Automotive Vulnerabilities

ON THE RISE

In 2024 alone,

530 automotive vulnerabilities were identified,

capping a significant increase in vehicle-related security risks.



This significant increase, particularly evident since 2019, illustrates the **growing complexity of modern automotive systems**. As vehicles become more connected and reliant on software, their attack surfaces continue to expand. This evolution underscores the urgent need for comprehensive security strategies to safeguard these increasingly sophisticated systems from exploitation.

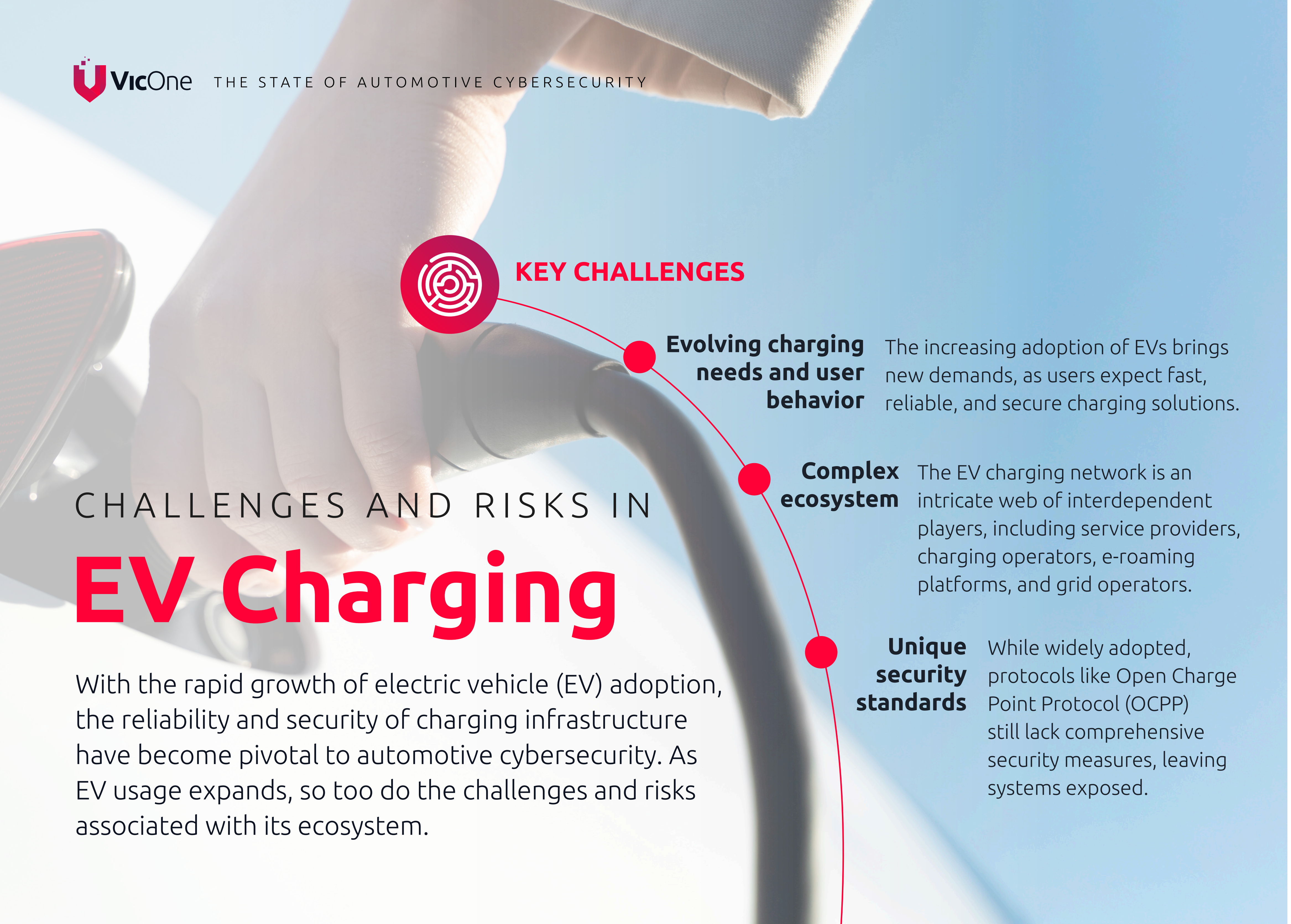
THE Soaring Cost OF CYBERATTACKS

The sharp increase in cyberattacks during the last quarter of 2024 significantly contributed to the surge in costs. Several prominent automotive companies were targeted, resulting in major data breaches that highlighted the critical importance of enhanced cybersecurity measures.

VicOne estimated the financial impact of reported cyberattacks on the automotive industry, focusing on three focus areas.

Cost	2022	2023	2024
Data leakage	$4.0M	$9.7B	$20.0B
System downtime	$802.7M	$2.5B	$1.9B
Ransomware damage	$242.8M	$523.6M	$538.2M
TOTAL	**$1.0B**	**$12.8B**	**$22.5B**

These factors point to the escalating financial impact of cyberattacks on the automotive industry.



CHALLENGES AND RISKS IN EV Charging

With the rapid growth of electric vehicle (EV) adoption, the reliability and security of charging infrastructure have become pivotal to automotive cybersecurity. As EV usage expands, so too do the challenges and risks associated with its ecosystem.

KEY CHALLENGES

Evolving charging needs and user behavior The increasing adoption of EVs brings new demands, as users expect fast, reliable, and secure charging solutions.

Complex ecosystem The EV charging network is an intricate web of interdependent players, including service providers, charging operators, e-roaming platforms, and grid operators.

Unique security standards While widely adopted, protocols like Open Charge Point Protocol (OCPP) still lack comprehensive security measures, leaving systems exposed.

EMERGING RISKS

Threats range from basic attacks such as **unauthorized port access** to sophisticated exploits that **disrupt communication** via radio frequencies.

Real-world risks include **power grid destabilization** and **data theft** through charging stations.

Researchers have uncovered flaws in protocols using tools like V2GEvil, demonstrating how hackers could **manipulate charging systems** and even broader grid infrastructures.

INSIGHTS FROM THE Underground

VicOne continuously monitors automotive-related discussions on underground forums across the dark web and deep web to gather intelligence and anticipate emerging threats. Our scanning of these forums reveals the **constantly evolving tactics** that attackers use to exploit vulnerabilities in modern vehicles. Indeed, car theft has advanced beyond traditional mechanical tools for breaking into locked vehicles.

Vehicle exploits and vulnerabilities

Exploits can enable theft, sabotage, or unauthorized control.

Hacking tools and tutorials

These lower entry barriers for attackers and increase risks of exploitation.

Connected vehicle and IoT device exploits

Weak security in IoT devices and apps can expose vehicles to remote attacks.

Corporate espionage and insider threats

Insider threats bypass traditional security measures.

Leaked corporate credentials and access data

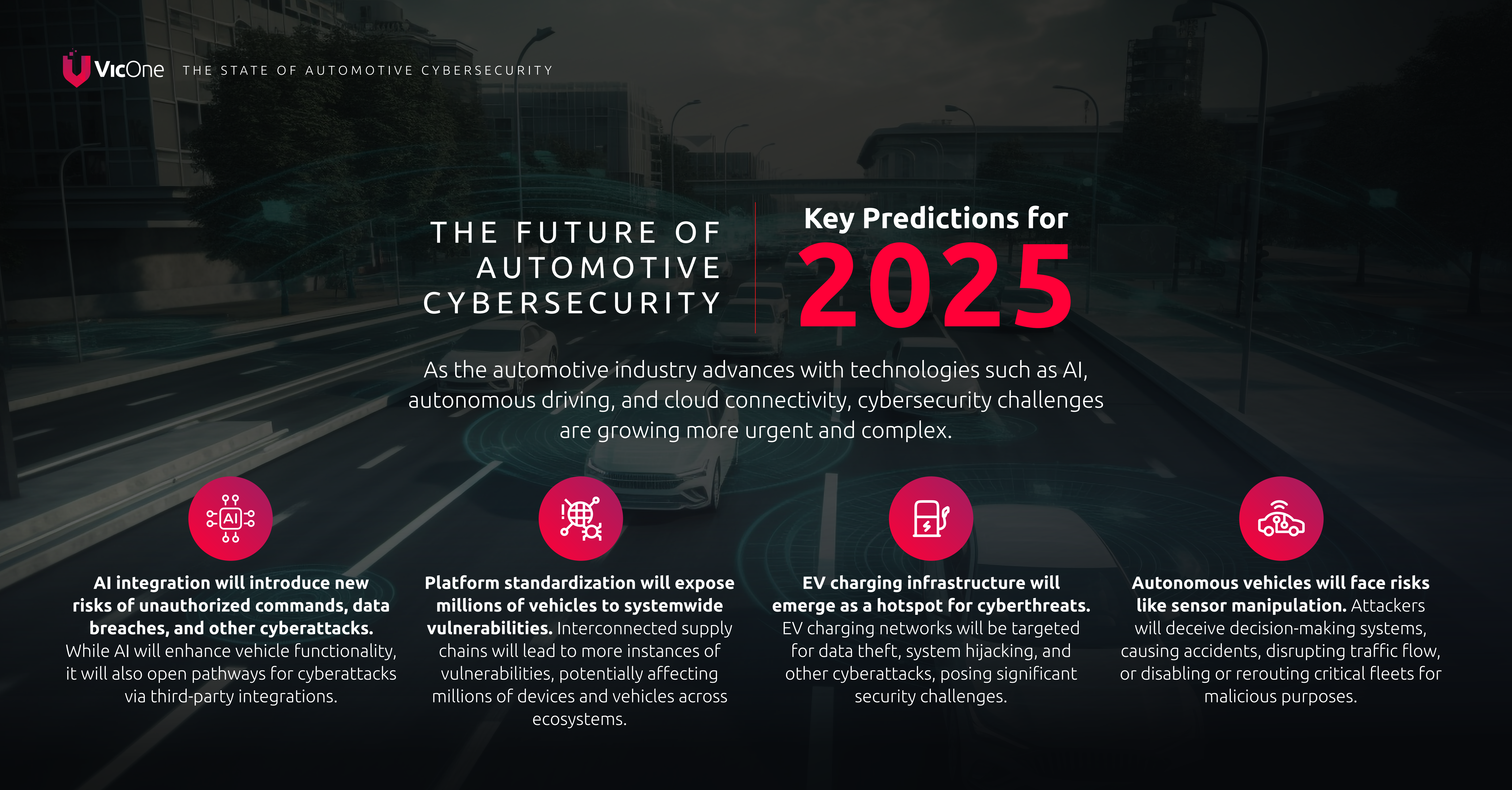
Unauthorized access can disrupt operations and steal sensitive data.

Stolen intellectual property and proprietary data

These could lead to higher risks of counterfeit parts, compromised software, and loss of competitive advantage.

Stolen data markets

Data breaches damage trust and might lead to regulatory penalties.



THE FUTURE OF AUTOMOTIVE CYBERSECURITY

Key Predictions for 2025

As the automotive industry advances with technologies such as AI, autonomous driving, and cloud connectivity, cybersecurity challenges are growing more urgent and complex.

AI integration will introduce new risks of unauthorized commands, data breaches, and other cyberattacks. While AI will enhance vehicle functionality, it will also open pathways for cyberattacks via third-party integrations.

Platform standardization will expose millions of vehicles to systemwide vulnerabilities. Interconnected supply chains will lead to more instances of vulnerabilities, potentially affecting millions of devices and vehicles across ecosystems.

EV charging infrastructure will emerge as a hotspot for cyberthreats. EV charging networks will be targeted for data theft, system hijacking, and other cyberattacks, posing significant security challenges.

Autonomous vehicles will face risks like sensor manipulation. Attackers will deceive decision-making systems, causing accidents, disrupting traffic flow, or disabling or rerouting critical fleets for malicious purposes.

VicOne

Shifting Gears

VicOne 2025 AUTOMOTIVE CYBERSECURITY REPORT

Unlock valuable insights into significant trends, in-depth analysis, and expert recommendations to help navigate the shifting landscape of automotive cybersecurity.

Download the full report