



EV Charging System Protection

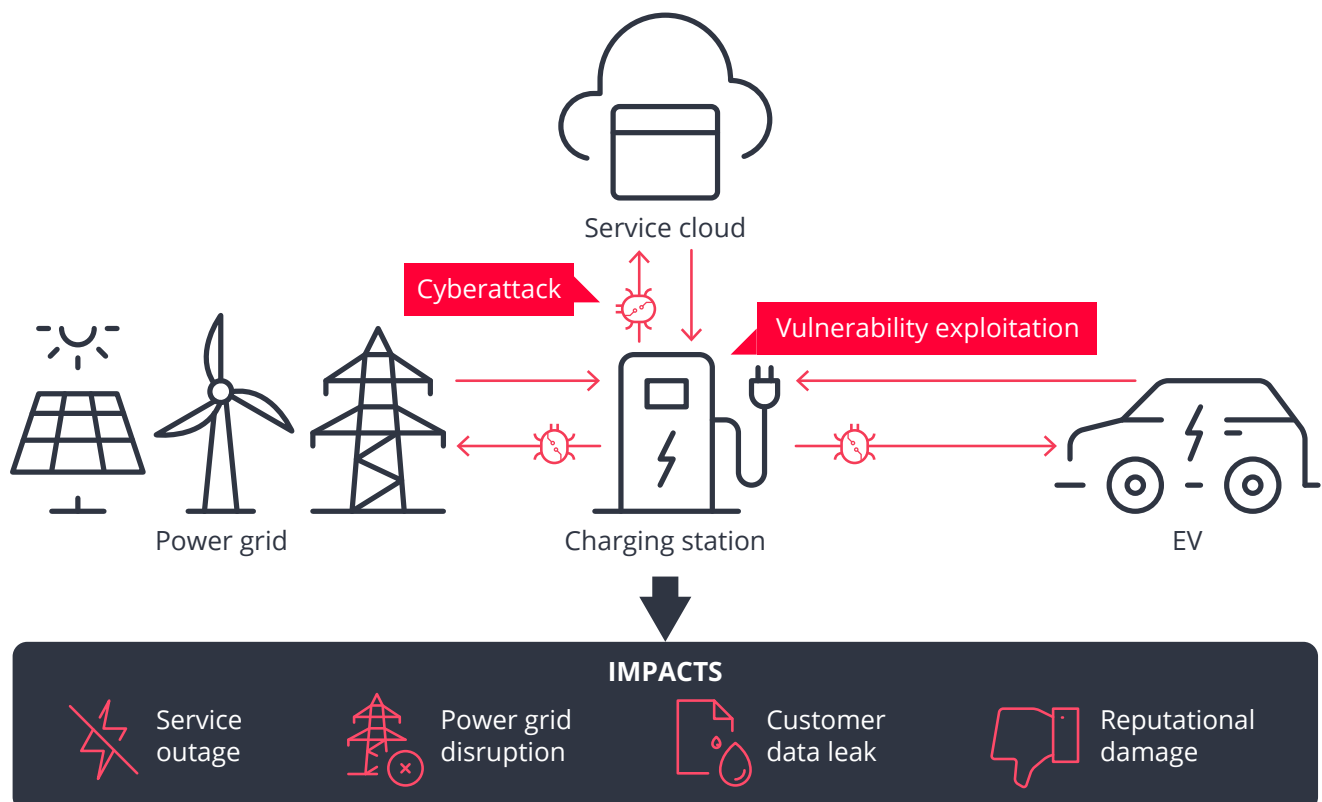
Securing Your EV Charging System by Monitoring for Software Vulnerabilities and Ensuring Attack Resilience

Relying Solely on Secure by Design Is Not Sufficient

Recent incidents of attacks on EV charging systems have shed light on two prevalent methods:

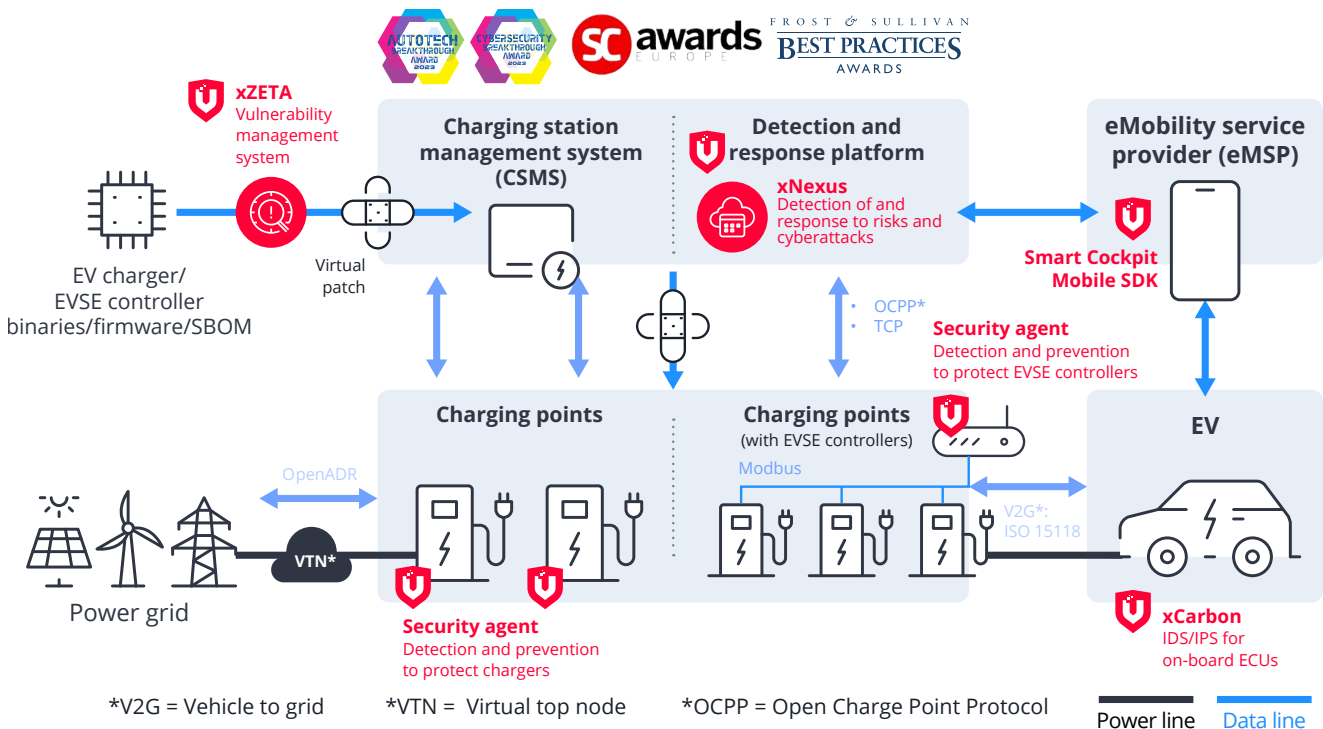
- Exploitation of open-source vulnerabilities in EV charging systems
- Cyberattacks on service clouds, EVs, and power grids directed toward charging stations

These attack vectors underscore the limitations of the Secure by Design principle. It has become evident that the current standard falls short in thwarting these types of threats and defending systems. Consequently, regulations are increasingly mandating comprehensive solutions to address these threats.



Award-Winning, Complete EV Charging System Protection

With our EV Charging System Protection solutions, we can strengthen your Secure by Design approach by extending protection to cover threats from exploits or unauthorized applications.



Key Features

- Detection of and Response to Security Risks**
 Our non-intrusive, cloud-based XDR platform enables timely detection of and response to security risks and cyberattacks based on CSMS data, without requiring hardware changes.
- Continuous Vulnerability Identification**
 Our solutions can automatically generate software bills of materials (SBOMs) so that you can continuously detect threats, including zero-day vulnerabilities and ransomware, in your EV charger's binaries and firmware.
- Resistance to Cyberattacks**
 Integrated security agents provide immediate detection and blocking of attacks, such as denial-of-service (DoS) attacks, on charging points.
- Unique Virtual Patch Technology**
 Our virtual patch technology offers 102 days of protection while waiting for vendor patches.
- Customer Success**
 Our solution has been adopted by Delta Electronics, a global leader in power and energy management solutions, to secure its EV charging infrastructure.

Benefits

- Get 102 days of protection, without requiring system changes.
- Easily meet the NIST IR 8473 cybersecurity framework profile, the ETSI EN 303 645 and ISA/IEC 62443 cybersecurity standards, and the UK's EV smart charging regulations.
- Reduce the vulnerability management process from 6 months to 2 weeks.
- Utilize unique zero-day vulnerability intelligence from the Zero Day Initiative (ZDI)* to get proactive protection.

*No. 1 in vulnerability discovery since 2007



EV Charging System Protection
 Copyright © 2024 VicOne Inc.
 All Rights Reserved.

Learn more about VicOne
 by visiting VicOne.com or
 scanning this QR code:

