The rapidly growing number of passenger and commercial Electric Vehicles (EVs) is driving the growth in EV charger infrastructure. This wave of EV is coming at us fast with the goal if achieving Net Zero emissions in the future. Governments are fueling this transformation with incentives and programs for Charge Point Operators (CPOs). The EV charging experience, however, is not as reliable as EV drivers expect it to be. Recent studies report Depending on a study, anywhere from 10%1 to 23% of EV chargers can be inoperable at any given time. This challenge with EV chargers has negatively impacted EV adoption and can lead to customer experience and perception problems for EV charger owners and operators. Just one negative experience at the EV station can cause long-lasting damage to their brand and reputation.

Automate the monitoring of all your EV Charger Ecosystem of assets for operations and cybersecurity

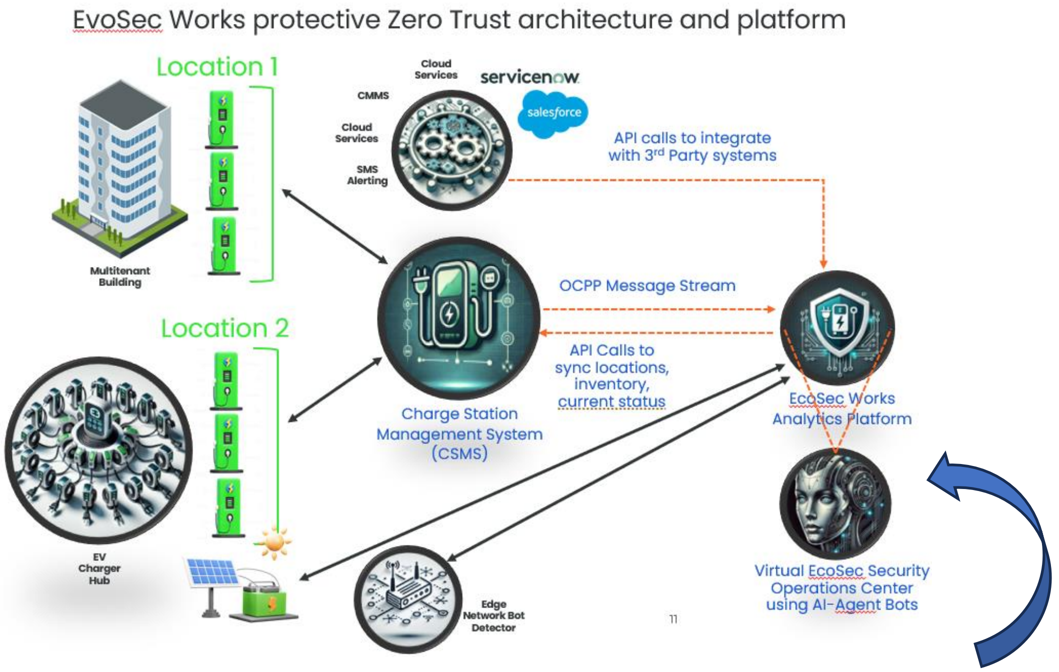
To provide a reliable EV charging service, the uptime and reliability of all assets involved must be measured and monitored. Cybersecurity is now becoming a more active problem beyond the vulnerabilities reported in networks; now, we are finding a number of attack vectors on EV chargers, their payment systems, and even infecting the cars/trucks that are using the chargers. Can you imagine how vulnerable a city bus fleet would be with no cybersecurity program in place? This is all part of O&M (operations) and cybersecurity can no longer be a siloed afterthought.

EcoSec's secret sauce is included in our first roll out of "EVSec Works", a single out of the box package that combines Infrastructure management, Cybersecurity, AI/ML, with Ease of use

ECOSEC WORKS IS SIMPLE TO USE WITH AUTOMATION VIA AI BOTS

No Cybersecurity expertise is required!

How it works


EvoSec Works protective Zero Trust architecture and platform
Location 1
Multitenant Building
Location 2
EV Charger Hub
Cloud Services
servicenow
CMMS
Cloud Services
SMS Alerting
salesforce
API calls to integrate with 3rd Party systems
OCPP Message Stream
API Calls to sync locations, inventory, current status
Charge Station Management System (CSMS)
EcoSec Works Analytics Platform
Virtual EcoSec Security Operations Center using AI-Agent Bots
Edge Network Bot Detector
11

Everyone else is doing just a sliver of what the entire system needs to work for EV charging (or other renewables, for that matter – and expensive system integration becomes the result), for example, focusing only on:

- Security and encryption of the car itself (but nothing else)
- Network security via firewalling of perimeters (this is not zero trust and won't alone get anyone near the future) (but nothing else)
- Cyber security and zero trust segmentation on the network level (eg Illumio) or other cyber giant alternatives (eg ZScaler or Fortinet) (hard to use and craves cyber expertise and dedicated sec ops teams)
- CSMSs with just basic monitoring capabilities (but no security and very inadequate automation for repairing and replacing equipment, tracking usage, predicting capacity needs, detecting errors, and no easy integration with other back-office system components).

None of the above are easy to use, integrated or share any key data between them, and none of them provide automation and productized AI/ML enough to help the EVCI management operator go through an effective workday. Too many tasks are manual, and the result is inadequate and failing low quality operations.

The Guardian ("GuarDiane") Observes and Deliver Insights, with Recommendations

Think of EVSec Works as your "Guardian AI Robot" making sure your EVCI works and your operations are safe and protected, without the user having to proactively do almost anything, but everything (state of system operations, health, configurations, software, traffic, usage, risks) is always verifiable.

The system leverages your CSMS APIs to access inventory data for sites and chargers. If available, it can analyze sessions, EV Charger Status, and OCPP message streams. EVSec can also analyze charger errors found in OCPP messages.

Manage every asset: All assets that affect the customer charging experience are maintained and managed. This includes not only the EV charger but the assets that make up the charging stations such as solar panels and batteries and enabling infrastructure. Through the connection with the CSMS, our system can automate keeping up with adds, move, and swap outs.

We keep your data in the country you want: Leveraging Microsoft Azure and AWS cloud infrastructure, we can put your data in the country and region they have data centers. Our cloud systems use the best practices to protect your EV Charger infrastructure data.

Simple to use and comes with clear advice: We design our systems, so you don't need to be an expert to understand what is being displayed. The AI Bots will make recommendations based on the discovered issue. We can notify you through email and/or send you monthly/weekly reports.

Cyber Vulnerabilities: EcoSec Works manages an active database of EV Charger and critical asset vulnerabilities, which are published as CVEs. In cybersecurity, a CVE, or Common Vulnerabilities and Exposures, is a publicly disclosed computer security flaw. The CVE system provides a standardized identifier for vulnerabilities and exposures, making it easier to share and communicate information across different tools and platforms. Each CVE entry contains a unique identifier, a description of the vulnerability, and references to additional information such as advisories or reports.

Clean and Normalized Data: You cannot gain analytical insights from bad data. Many systems have humans entering their data, which can lead to variations and mistakes. EVSec Works has filters that cleaning data entry mistakes and normalizing things like model names against a centralized and normalized asset library we maintain. This enables us to see consistent data for analysis across all our CPO customers to make the system smarter and benchmark normal device behaviors against odd anomalistic behaviors.

Trusted and Scalable Cloud Platform: our solution is built using cloud native best practices. For our customers, we make it "Click and Go" to gain instant value and de-risk your operation, and we advance your EV Charging network through maturity levels for cybersecurity. **Bad actors have weaponized AI to attack you and we have designed an AI system to fight back and defend!**

For more information or to request a demo contact info@ecosecworks.ai