

Contextualized Detection, Protection, and Posture Management Designed for EV Charging Sites and Energy Networks

Saiflow's Contextualized EV Charging Security Platform & Check Point's Industry-Leading NGFWs and Proactive IoT Protection

The global surge in Electric Vehicles (EVs) has accelerated the deployment of EV Charging Stations and fostered the expansion of Distributed Energy Resources (DERs), including solar panels, wind turbines, and various decentralized energy networks and microgrids.

Given their dispersed nature, EV charging sites and distributed energy networks heavily rely on internet connectivity and SaaS cloud platforms for remote management, maintenance, and enhanced overall energy network utilization. However, these networks and EV charging sites, characterized by unique architecture, protocols (such as OCPP, OCPI, and IEEE 2030.5), and energy flow controls, face significant cybersecurity risks. Issues include unprotected internet connectivity, insufficient authentication and encryption, absence of network segmentation, unmanaged energy assets, and more.

Check Point and Saiflow have joined forces to deliver a comprehensive EV Charging Hub and Energy Network cyber security solution, seamlessly integrating contextualized security, advanced detection capabilities, heightened observability, and proactive IoT protection. Saiflow's SaaS-based platform, tailored for the distributed nature of modern energy networks, not only natively supports standards and protocols but also combines energy telemetry with network data for comprehensive cyber event detection and risk assessment.

Paired with Check Point's industry-leading NGFWs and proactive IoT protection, featuring dedicated firewall policies, enforced authentication and encryption, enhanced visibility into the overall network posture, and dynamic network protection, our combined solution is uniquely crafted to meet the specific demands of EV charging and distributed energy networks.

KEY SOLUTION BENEFITS

Enhance the Cyber Resilience of Energy Networks:

- Mitigate the risk of targeted cyberattacks on energy and EV charging networks.

Ensure Uninterrupted Operations and Security:

- Proactively block cyberthreats while maintaining business continuity and availability.

Achieve Comprehensive Network Visibility:

- Attain full visibility into all connected assets and inventory throughout the energy network.

KEY SOLUTION FEATURES

- **Native built-in support for EV charging standards and protocols** -OCPP, OCPI, IEEE 2030.5, Modbus, OpenADR 2.0, IEC 61850, and more.
- **Consolidated and integrated smart grid telemetry**, network traffic, and other energy network activities to provide complete energy flow and charging operation observability.
- **Plug & Play integration** with OCPP-based EVSE, eliminating the need for agents or third-party system integrations.
- **End-to-end solution** covering energy networks and consumption processes.

Automated Firewall Policies Tailored To Your Network and Charging Site

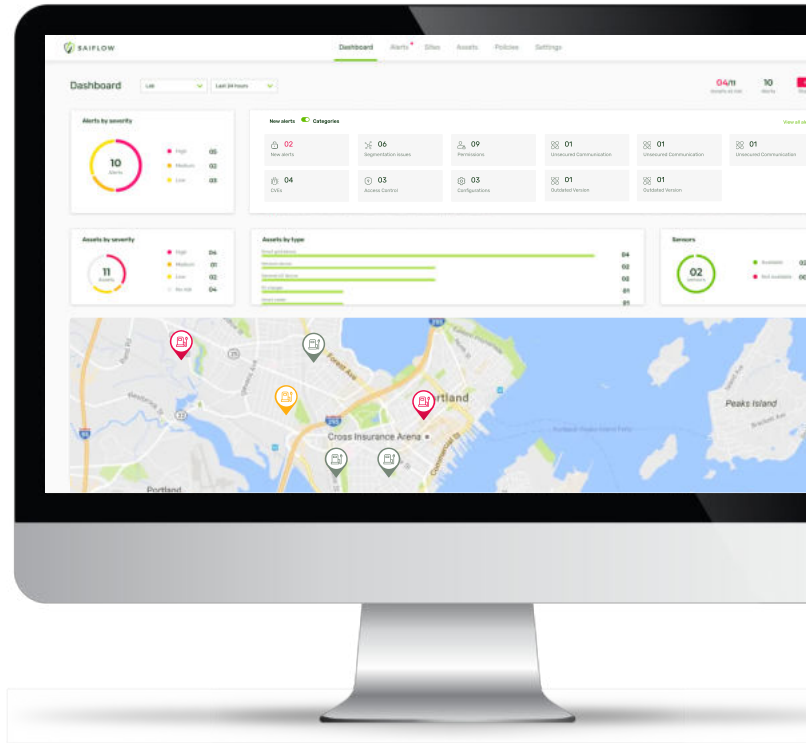
Utilizing SaiFlow's deep contextualized know-how in EV charging and distributed energy networks, SaiFlow's platform builds tailored "allow-list" firewall policies, based on known and required services for each asset in your energy network, including needed connections to the different SaaS and management platforms. The recommended policies can be automatically streamlined and enforced via Check Point's Security Gateways with **Quantum IoT Protect** on the different charging sites to strengthen the overall network resiliency.

Comprehensive Detection & Response to Threats Under a Unified System

SaiFlow's platform retrieves, in real-time, all network logs and FW dropped packets and sessions from Check Point's Security Gateways in the EV charging sites. The platform alerts in real time on possible cyber attacks and on any suspicious activities and unrecognized outbound traffic. All logs and alerts are visible in SaiFlow's platform to further investigate cyber incidents.

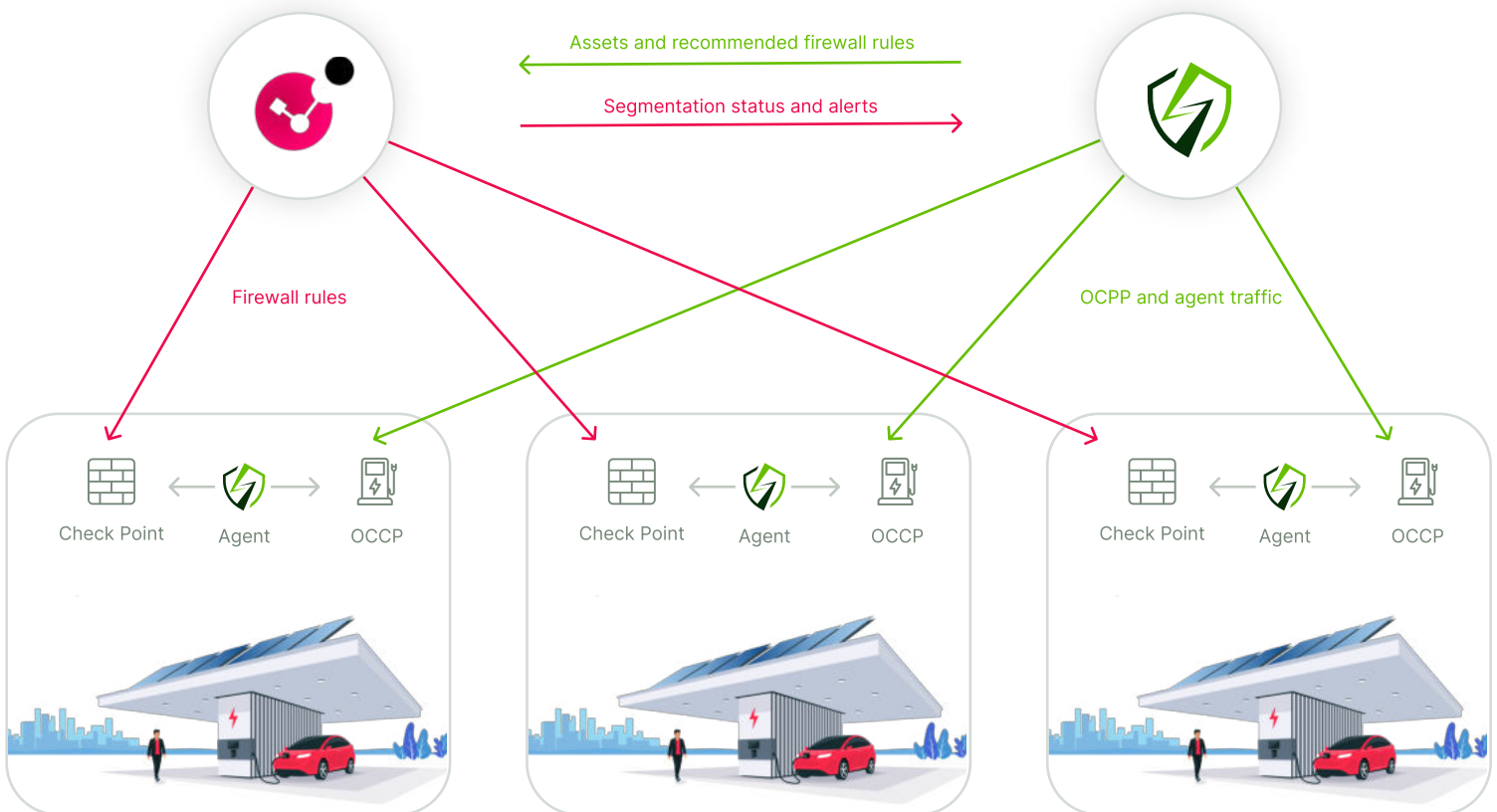
Full Visibility Into the EV Charging and Energy Network Structure

SaiFlow's platform maps and discovers all assets across the entire energy and charging network. The platform automatically pulls all Security Gateway information, parses the existing network policies, and builds a comprehensive network map of your entire energy infrastructure. You can easily view the network structure, quickly pinpoint all network segmentation issues, and mitigate the risk efficiently.



Check Point Security Management Platform

SaiFlow's Security Platform



About SaiFlow

SaiFlow is the leading cyber security company for distributed energy networks and electric vehicle charging sites and networks (www.saiflow.com).

SaiFlows provides contextual network cybersecurity solutions for EV charging sites and decentralized energy networks, including posture management, cyber monitoring, detection, and prevention abilities, all incorporating smart-grid and sensor data in establishing the baselines, correlations, and anomaly detection in the energy networks.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to corporate enterprises and governments globally. Check Point Infinity's portfolio of solutions protects enterprises and public organizations from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other threats. Infinity comprises three core pillars delivering uncompromised security and generation V threat prevention across enterprise environments: Check Point Harmony, for remote users; Check Point CloudGuard, to automatically secure clouds; and Check Point Quantum, to protect network perimeters and datacenters, all controlled by the industry's most comprehensive, intuitive unified security management; Check Point Horizon, a prevention-first security operations suite. Check Point protects over 100,000 organizations of all sizes.