BYOS

Securing EV Charging Networks against Cyber Attacks

The growth of electric vehicle (EV) charging networks has been significant in recent years, with many companies investing in building new charging stations and expanding existing ones. Governments and private organizations are recognizing the importance of investing in charging infrastructure to support the widespread adoption of EVs and promote a sustainable future, but are also recognizing that as electric vehicle (EV) charging networks have grown in popularity, so have the cyber threats facing them. EV charging networks are vulnerable to cyberattacks, which can cause significant disruption to the charging infrastructure and pose risks and serious consequences to the security and privacy of EV owners.

While these standards and practices evolve over the coming years, the growth of the Electrical Vehicle and charging station market continues. Today, there are more than 3 million Electric Vehicles (EVs) on the road, and more than 130,000 public charging stations across the United States. A September 2022 International Energy Agency report anticipates that the EV market will grow to more than 60% of all vehicles sold globally by 2030, requiring charging infrastructure to keep pace with this growth.

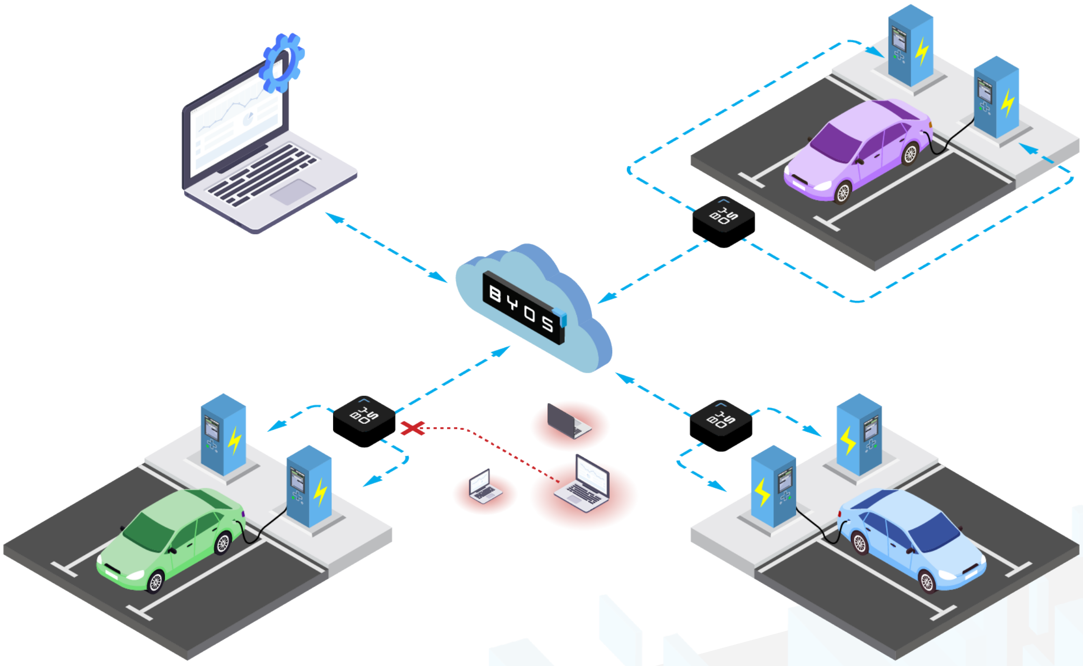
Given the pace of legislation in the United States, let alone globally, we must consider implementing cybersecurity solutions at the pace of market growth rather than the pace of legislation. As best practices and capabilities continue to evolve in the cyber domain, we cannot safely rely on legacy cybersecurity solutions to provide adequate protection for EV Charging stations into the future. Further complicating security for EV charging stations, each charging station (acting as a network endpoint) is vulnerable to being leveraged by a hacker as an attack vector to the power grid that's feeding the station.

The Challenges of Securing the Networks of EV Charging Stations

When drivers charge their vehicles, they are also establishing a data connection between their vehicle and the EV charging hub. EV charging infrastructure is like any network, vulnerable to the actions of cyber adversaries

- Unauthorized access to connected charging stations could result in loss of sensitive data, reputational damage and potential legal liabilities
- Firmware vulnerabilities may be exploited by bad actors to compromise the system's security and stability and potentially access the connected vehicles
- Malware and ransomware attacks which can compromise a charging station's software, enabling bad actors to steal sensitive data or take control of the station. Ransomware attacks can lock out station operators and demand payment for the restoration of the system's functionality

We propose a novel solution for EV charging station endpoints and networks via Bring Your Own Security's (BYOS) Microsegmentation platform. BYOS technologies decouple the protection from the IoT/OT asset, making them invisible to the network by providing "DFMP" (Decoupled First-Hop MicroSegmentation Protection). This unique approach protects network connected assets against multiple attack vectors across OSI layers 1-5. BYOS allows network owners secure remote access to their IoT/OT assets from any trusted or untrusted network or device while making it impossible for cybercriminals and adversaries to detect and target those assets. All attempts to scan, fingerprint, or enumerate are dropped at the BYOS Edge.



Visibility and Connectivity across a Nationwide Charging Infrastructure

Byos makes the entire network of chargers able to be administered and secured as a single system. Manufacturers and Network operators gain real-time visibility into the entire fleet of EV chargers from the Byos administrative console to monitor the security, usage & connection status, including external access by other third parties. Previously "air-gapped" chargers can now be connected securely without the typical risk, allowing for faster remote connectivity so that admins can perform firmware updates to address security vulnerabilities, improve performance, and add new features without worry.

Improve Uptime while Decreasing Cybersecurity Management Complexity

Uptime is crucial for electric vehicle (EV) charging stations as it directly impacts the availability and reliability of charging services for EV owners. By implementing robust cybersecurity measures, charging station operators can safeguard the systems from cyber threats and potential disruptions, and meet increasingly stringent regulations for uptime and longevity. Byos is enabling greater access to EV chargers by allowing for full control & visibility to EV chargers distributed across geographically diverse locations, and enables a more proactive approach with regular monitoring and software updates.

Lock Down Your Charging Network

Byos-protected devices are invisible to all other unauthorized devices on the network. This protection ensures that your devices are only communicating with other Byos-protected devices within the Byos Overlay. This core feature allows extremely limited access to be provided to third-parties so that they have access to ONLY the devices and users that need access, and only for specific periods of time and from specific geographies, and other specific parameters.

For EV Charger Manufacturers and Network Operators:

Byos is deployed as the gateway for both Wired and Wireless TCP/IP communications. It comes in a number of different form factors for different use cases.

Byos Secure Gateway Edge - a plug-and-play gateway applicable for deployment with Brownfield charging stations. It has three modes:

- Ethernet for wired connectivity
- Wi-Fi hotspot for wireless use cases
- Client Mode so the chargers can connect wirelessly to Wi-Fi networks in range.

Secure Embedded Edge - For custom and specific secure connectivity applications, the Byos System-on-Module can be embedded onto the EV charger's motherboard, sitting between the Network Interface and the CPU.

Secure Virtual Edge - For a full software deployment, the Secure Firmware Edge can be installed inside of the EV charger, sitting between the OS and the network interface.

Byos' Management Console and Secure Lobby help EV Charging Manufacturers, internal support teams, and IT/cybersecurity support to control and manage their fleet of Byos-protected EV Chargers. Byos enables:

- Real-time provisioning and policy-enforcement of thousands of EV Chargers
- Secure remote access to EV Chargers inside the Byos-cloaked network, without having to expose the network to the internet like other remote access technologies
- Connect your existing unconnected EV chargers to improve efficiency without exposing them to the network and adding risk

Byos is unique because it makes the EV Charging Network Invisible to Outsiders

Byos combines network/endpoint security with ease of use into one solution that is simple to deploy, manage, scale, without having to change the underlying network.

According to the Joint Office of Energy and Transportation, in FY22, States have spent more than $615M in planning for the implementation of EV Charging Infrastructure, with an estimated $885M to be spent in FY23 for more than 75,000 miles of identified charging corridors. Nationwide, the United States will spend billions of dollars planning and implementing EV charging infrastructure between now and 2030. Security of these stations must be a top priority in order to secure personal information, the charging stations, and the national power grid. The Byos solution offers a low-cost, high-security and highly scalable solution for these stations and associated networks. We can accommodate state-run security operation centers (SOCs) for these charging stations, private entity SOCs, or stand up our own SOC to provide 24-7 monitoring as your needs dictate.

If you're looking for more visibility across your EV charging network, or looking to securely add more connectivity, request a demo here: byos.io/request-demo