Solving Electric Vehicle Charging Risks with Zero Trust

Table of Contents

Executive Summary

The rapid global proliferation of Electric Vehicles (EVs) and their associated charging infrastructure presents an unprecedented opportunity — and a complex security challenge. EV charging relies on the instantaneous, interdependent convergence of internet communications, financial transactions, and electrical grid operations. This intricate dance, often occurring over distributed, cellular-connected hardware, exposes a vast new attack surface that traditional security measures are ill-equipped to handle.

This white paper outlines the critical security risks inherent in the modern EV charging ecosystem, from the inherent vulnerabilities of cellular connectivity to the operational challenges of managing widely dispersed devices. It then introduces Zscaler Cellular, a transformative solution that extends the principles of Zero Trust security directly into the cellular domain. By integrating with mobile networks, providing unparalleled inline visibility and control, and ensuring that every EV charger operates as an “island of one,” Zscaler Cellular offers a robust, scalable, and simplified approach to securing the EV charging infrastructure against evolving cyber threats, protecting revenue, and ensuring operational integrity.

Introduction: The Electrified Future and Its Hidden Risks

The shift to electric mobility is accelerating, driven by environmental mandates, technological advancements, and consumer demand. Central to this transformation is the EV charging infrastructure — a complex, distributed network of devices critical to the daily lives of millions. However, beneath the promise of sustainable transport lies a burgeoning security challenge that demands immediate attention.

Unlike traditional IT assets, EV chargers operate at the convergence of three highly sensitive domains: the internet for communications, financial networks for transactions, and the electrical grid for power delivery. This convergence, combined with the often-remote and cellular-dependent nature of their deployment, creates a unique and significant risk profile. This paper will delve into these intricate risks and present a modern, Zero Trust-based solution to secure the backbone of our electric future.

EV chargers exist in a unique situation, bringing complex technical services to broadly deployed locations, use cases and climates, all to ensure the simplest use by the consumers. If the EV charger is not functioning, the EV charger is not generating revenue, but is also impacting the reputation of the brand. Thus these technical assets must be available, functional and protected wherever they are in use.EV chargers are uniquely positioned, delivering intricate technical services across a wide array of locations, applications, and environmental conditions, all while aiming for the easiest possible consumer experience. The failure of an EV charger not only results in lost revenue but also damages brand reputation. Consequently, these essential technical assets must be consistently available, operational, and secure, regardless of their location.

The Challenge: Navigating the Complex Security Landscape of EV Charging

Securing an EV charging network is far more complex than protecting a typical enterprise data center. It involves managing distributed endpoints, real-time transactional processes, and critical infrastructure components, all while facing an increasingly sophisticated threat landscape. Often deemed part of Critical National Infrastructure (CNI), EV charging services also need to comply to regulations and standards, such as ISO27001 EV charging services are often considered part of Critical National Infrastructure (CNI) and, as such, must adhere to relevant regulations and standards, like ISO 27001.

2.1 The Critical Convergence of Networks

For an EV charging session to successfully occur, multiple disparate networks and protocols must flawlessly converge in real-time. This interconnectedness, while essential for functionality, creates numerous points of vulnerability. If focussed on the Internet communications:

Following standards like ISO 15118, the charger must communicate with internet-based services to:

- Register the Vehicle: This involves certificate validation of the vehicle's pre-installed certificates, establishing a secure information exchange, and confirming the vehicle's identity against a Public Key Infrastructure (PKI). This also validates the driver's contract and payment method, leveraging OCPI.

- Authenticate the Vehicle: A digital handshake initiated by the car is validated by an external, internet-based PKI, verifying the vehicle's legitimacy.

- Authorize Charging: Before power flows, the system verifies if the charging is allowed. This often involves checking the eMobility Account Identifier (EMAID), connecting to financial networks, and validating against the Charge Point Operator (CPO) backend via an internet connection. Only then is the EV charger signaled to deliver current.

- Financial and Billing Reconciliation: Post-charging, the CPO sends messages to roaming hubs via OCPI and transmits Charge Detail Records (CDRs) to billing operators. These transactions are critical for revenue assurance and fraud prevention

All these intricate steps happen in milliseconds, demonstrating a profound reliance on

uninterrupted, secure communication across internet, finance, and electrical networks. Crucially, much of this communication often occurs over networks that are not physically cabled, introducing additional complexities.

2.2. The Distributed Challenge of EV Infrastructure

The very nature of EV charging infrastructure presents a monumental security and operational challenge, in that EV chargers are installed everywhere — from public streets and shopping centers to private residences and corporate campuses. This geographic spread makes centralized, physical security impossible.

Rolling out dedicated wired network connections to each charger location is rarely feasible, functional, or cost-effective. Consequently, reliance on cellular connectivity is widespread.

2.3. The Inherent Risks of Cellular Connectivity

Cellular networks are the backbone of most EV charging deployments, but their traditional security models are insufficient for the demands of critical infrastructure. Historically, many cellular IoT devices initiate communications that go directly through a mobile network operator (MNO)/carrier network and then over the public internet to their destination. This path offers minimal inherent security beyond basic network functions, providing limited visibility and virtually no granular control over traffic content.

The alternative involves backhauling traffic from the MNO/carrier network using private networks (e.g., APNs or 5G Slices) into the customer's private network. While this allows for corporate security controls to be applied within the customer's network, it effectively extends the enterprise's attack surface out to the edge of the mobile network.

Both scenarios often provide only basic network-level functions, leaving significant gaps in granular visibility and control. Security teams typically lack the necessary tools to monitor and secure traffic originating from these devices, effectively placing these critical assets outside their operational control and security remit. This challenge is exponentially amplified for organizations operating EV infrastructure across multiple countries or geolocations. Each deployment necessitates negotiating and building bespoke network-level controls, vastly increasing complexity, operational costs, and the overall attack surface.

When EV chargers require remote support or maintenance, owners are often forced to extend their routable network via VPNs or private network extensions directly to the distributed charger locations. Additionally the third party supply chain and support requirements opens up access to EV chargers well beyond a firm's visibility and controls. The dependence on a third-party supply chain and external support personnel significantly expands the points of access to EV chargers, often placing them outside the firm's direct visibility and control. This dangerously broadens the enterprise network perimeter and exposes it to risks originating from these potentially compromised remote endpoints.

These inherent limitations in cellular security, coupled with the distributed nature and critical function of EV chargers, paint a clear picture of an industry facing significant, evolving cyber risks.

The Solution: Securing EV Charging with Zscaler Cellular and Zero Trust

Zscaler Cellular is a transformative solution designed to secure and simplify connectivity for cellular-connected IoT and mobile devices, including EV chargers, by integrating a Zero Trust architecture directly into the mobile network. By leveraging the Zscaler Zero Trust Exchange (ZTE), it extends industry-leading Zero Trust principles into the cellular domain, offering secure, scalable, and efficient connectivity for IoT ecosystems and mobile deployments.

This comprehensive solution directly addresses the challenges of securing billions of cellular-connected endpoints — especially in environments where traditional tools like VPNs, firewalls, and backhauling struggle to scale, provide adequate security, or simplify operations. Zscaler Cellular seamlessly integrates into existing telecom infrastructures to deliver an unmatched combination of security, visibility, and operational simplicity.

Zscaler Cellular is built upon three foundational pillars:

1. Resilient Global Integration directly into the global mobile network environment. This ensures that connectivity is inherently resilient, providing robust and seamless end-to-end service across any mobile network in over 180 countries. This global reach means that whether an EV charger is in New York or Nairobi, it operates under the same robust security umbrella.

2. Full Zero Trust Visibility, Protection, and Control – All traffic originating from or destined for SIM-initiated devices (like EV chargers) is routed directly through the Zscaler Zero Trust Exchange. This means there is no backhaul to a customer data center, and no unprotected communication. Instead, every connection is subject to inline inspection and policy enforcement. As the world's largest security cloud, Zscaler provides comprehensive threat prevention, data loss prevention (DLP), bandwidth control, and access policies, ensuring direct-to-application access is secure by design.

3. Delivering Each Cellular Device as an "Island of One", ensuring the principle of Zero Trust is microsegmentation and least-privilege access is implemented right down to the distributed EV charger. Zscaler Cellular enforces this by ensuring that nothing can communicate with, access, or even view anything else on the network unless explicitly permitted by policy. Each EV charger, and indeed each cellular-connected device, becomes an "island of one." All actions and communications are precisely controlled by the Zero Trust Exchange, drastically reducing lateral movement risk and preventing compromised devices from infecting others.

Unparalleled Value for EV Charging Operators

Zscaler Cellular directly addresses the security and operational challenges faced by EV charging infrastructure owners and operators, delivering critical benefits:

- **Resilient service delivery:**
  Leveraging the ubiquitous nature of multiple cellular networks, the Zscaler Cellular service will always be available to ensure delivery of the EV charger functions through the Zero Trust service from Zscaler.The Zscaler Cellular service, by utilizing the widespread availability of various cellular networks, guarantees the consistent delivery of EV charger functions via the Zscaler Zero Trust service.

- **Comprehensive Security for the Entire Charging Lifecycle:**
  All communications from the EV charger to the various internet, financial, and electrical networks and protocols — for registration, authentication, authorization, and reconciliation — pass securely through the Zscaler service. This ensures that every step of the charging process is protected against tampering, fraud, and cyber threats

- **Unparalleled Visibility into All Connections:**
  Operators gain unparalleled visibility into every legitimate and illegitimate connection attempt. This allows for real-time monitoring, anomaly detection, and forensic analysis, giving security teams the insight they need to understand and mitigate threats

- **Unparalleled Visibility into All Connections:**
  By enforcing least-privilege access and microsegmentation, Zscaler Cellular drastically shrinks the attack surface. Compromised devices are isolated, preventing them from being used as pivots for broader attacks against the network or adjacent systems. Eliminating the need for backhauling traffic, expensive VPNs to remote sites, or complex, region-specific security stacks streamlines operations and significantly reduces Total Cost of Ownership (TCO). Security management is centralized within the Zscaler Zero Trust Exchange, integrating seamlessly with existing enterprise security postures.

- As cellular technology evolves, Zscaler Cellular is built to scale with the demands of 5G, IoT, and future innovations, ensuring that EV charging infrastructure remains secure and adaptable.

Conclusion: Powering Secure, Trustworthy EV Charging

The future of mobility is electric, and the security of its underlying infrastructure is paramount. The intricate convergence of communication, financial, and electrical networks, coupled with the distributed, cellular-dependent nature of EV charging, presents unique and significant cyber risks. Traditional security models are simply inadequate for this new paradigm.

Zscaler Cellular offers the definitive solution. By embedding Zero Trust security directly into the cellular network, it provides EV charging operators with complete visibility, granular control, and robust protection for every charger, everywhere. It simplifies complex global deployments, reduces the attack surface, and ensures the integrity of every transaction and connection.

In an era where trust is paramount and threats are constantly evolving, Zscaler Cellular empowers the EV charging industry to confidently scale, innovate, and deliver on the promise of a secure, sustainable electric future.

Next Steps

To learn more about how Zscaler Cellular can secure your Electric Vehicle charging infrastructure and for a personalized demonstration, contact a Zscaler expert today. Visit the Zscaler Cellular website or request a demo to begin your journey to a more secure and resilient EV ecosystem.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**