



Guia do Comprador de Conectividade para o Carregamento de
Veículos Elétricos (2026)

7 Perguntas que as Equipes de Carregamento de Veículos Elétricos Devem Fazer ao Escolher seu Provedor de Conectividade

O guia completo do comprador de conectividade para os tomadores
de decisões sobre o carregamento de veículos elétricos, incluindo
SGP.32 (eSIM para IoT)

Abril de 2026

Para quem é este guia?

- Operadores de pontos de carregamento que gerenciam e escalam suas redes
- Fabricantes de pontos de carregamento
- Líderes de Produto, Operações, Engenharia e demais envolvidos na decisão de compra de conectividade

Por que a conectividade importa ao se escalar o carregamento de veículos

A forma como seus carregadores se conectam e se comunicam não deve ser tratada como um detalhe secundário. Em carregamento de veículos elétricos, a conectividade é um elemento central do desempenho, da escalabilidade e do controle da infraestrutura.

As redes de carregamento não operam em ambientes previsíveis. Carregadores residenciais frequentemente dependem de Wi-Fi que as operadoras não conseguem controlar, limitando a visibilidade e dificultando a gestão do desempenho. Já carregadores públicos podem ser implantados em locais onde a conectividade fixa é cara, lenta de instalar ou simplesmente inviável. Em ambos os casos, parte da experiência de carregamento depende de infraestrutura que está fora do controle da operadora.

A conectividade celular oferece às operadoras uma forma mais direta e controlável de conectar carregadores nesses ambientes. No entanto, colocar um carregador online é apenas o primeiro passo. O verdadeiro desafio é escolher um modelo de conectividade que permaneça confiável, gerenciável e flexível à medida que a rede cresce.

Por que a maioria das decisões de conectividade falha (e quanto custa isso)

Para equipes de carregamento de veículos elétricos, a conectividade costuma ser negligenciada até começar a causar problemas. Um carregador pode estar instalado, energizado e tecnicamente operacional e ainda assim falhar de formas que prejudicam a experiência do cliente, desaceleram as operações e aumentam os custos. Pode ocorrer que sessões não sejam iniciadas corretamente. Diagnósticos remotos podem ser limitados. Atualizações de software podem falhar. As equipes de Engenharia podem não saber se o problema está no carregador, na rede, no SIM ou no backend.

Em pequena escala, isso é gerenciável. Em grande escala, torna-se um custo operacional recorrente. Para os fabricantes de pontos de carregamento, a conectividade define como os carregadores são fabricados, enviados, instalados e mantidos ao longo do tempo. Para os operadores de pontos de carregamento (CPOs), ela vai muito além de simplesmente saber se um carregador está em funcionamento. Ela afeta a implantação, a integração de clientes, a

disponibilidade (uptime), a visibilidade, o diagnóstico remoto, a confiabilidade dos pagamentos, a conformidade regulatória e a facilidade com que a rede pode ser expandida.

À medida que as redes de carregamento de veículos elétricos crescem, espera-se que a conectividade faça muito mais do que apenas fornecer acesso. Os operadores precisam de visibilidade sobre o comportamento dos dispositivos, de uma comunicação segura entre os carregadores e os sistemas de back-end, de suporte para ações remotas e resolução de problemas, além de dados de conectividade que possam ser integrados diretamente com suas próprias ferramentas e fluxos de trabalho. Novos padrões, como o SGP.32, estão levando isso ainda mais longe, proporcionando aos fabricantes e CPOs maior flexibilidade em relação à conectividade, muito além da implantação.

As 7 perguntas sobre conectividade que determinam se sua rede escala ou colapsa

Se você é gerente de produto, engenheiro ou líder de operações em um fabricante de pontos de carregamento ou um CPO, estas são as perguntas que você deve fazer para avaliar a conectividade em termos práticos, tanto antes quanto depois da entrada em operação dos carregadores em campo.

O objetivo deste guia é simples: ajudar você a avaliar se um provedor de conectividade pode realmente atender às demandas da sua rede de carregamento e, com isso, do seu negócio. Essas perguntas não são teóricas. Juntas, elas determinam se a conectividade se tornará uma fonte de controle e escalabilidade ou uma fonte contínua de atrito, sobrecarga operacional e risco.

Com isto em mente, aqui estão sete perguntas sobre conectividade que você deve fazer desde o início:

-  Haverá cobertura onde nossos carregadores estiverem de fato implantados?
-  Quanto controle teremos após a implementação?
-  Quão fácil será resolver problemas quando algo der errado?
-  Com que tipo de suporte e SLAs podemos contar?
-  Como é feita a proteção da comunicação entre o carregador e o backend?
-  A conectividade será compatível com os sistemas que já utilizamos?
-  Como garantir a flexibilidade e adaptação da conectividade dos carregadores no longo prazo?

Vejamos estas perguntas em mais detalhes.





1. Cobertura

Haverá cobertura onde nossos carregadores estiverem de fato implantados?

A cobertura é um elemento fundamental em qualquer decisão sobre conectividade para o carregamento de veículos elétricos, mas também é uma das áreas mais propensas a simplificações excessivas. Você não deve apenas perguntar se um provedor de conectividade pode oferecer cobertura nos locais de implantação, mas também como ele faz isto.

A verdadeira questão não é se um provedor pode alegar cobertura em um país ou região. É se esse modelo de cobertura funciona de acordo com a forma como os carregadores são realmente construídos, implantados e operados ao longo do tempo.

Para os fabricantes de pontos de carregamento, o desafio surge logo no início. Um carregador pode ser projetado uma única vez, mas implantado em vários mercados com a presença de diferentes operadoras, qualidade de cobertura e condições comerciais. Se regiões distintas de implantação exigirem relações distintas com as operadoras ou estratégias de SIM, a complexidade aumenta rapidamente. Fabricação, logística, planejamento de estoque e suporte tornam-se mais difíceis de administrar. O que começa como uma decisão de conectividade pode rapidamente se tornar um problema de operações de produto e cadeia de suprimentos.

Para os CPOs, o desafio é diferente, mas não menos importante. Mesmo dentro de um único país, a qualidade da cobertura pode variar significativamente entre os ambientes onde os carregadores são implantados. Um posto de gasolina, ponto de varejo, terminal de transporte, hotel, local à beira da estrada, destino rural ou terminal público podem todos apresentar desempenho diferente, dependendo de qual rede é mais forte naquele local. A cobertura nacional significa muito pouco se o modelo ainda deixar as operadoras expostas a uma conectividade fraca em locais importantes.

É por isso que a cobertura deve ser avaliada como uma capacidade operacional, e não apenas como um mapa ou número de países. As equipes de carregamento de veículos elétricos precisam entender se o modelo do provedor lhes oferece flexibilidade depois que os carregadores estiverem instalados. A conectividade consegue se adaptar às realidades do ambiente de instalação? O carregador consegue se conectar de forma confiável no local onde está efetivamente instalado? O modelo de cobertura simplificará a implantação ao longo do tempo ou criará mais complexidade operacional à medida que a rede crescer?

O que uma boa cobertura deve lhe dar

Um modelo de cobertura mais robusto deve simplificar as operações, não multiplicá-las. Ele deve proporcionar um único relacionamento com o provedor, acesso a várias redes na maioria dos países e menos estratégias de SIM para gerenciar entre regiões.

Para os fabricantes de pontos de carregamento, isso significa menos unidades de manutenção de estoque (SKUs), logística mais simples e suporte mais fácil. Para os CPOs, significa que um carregador não fica preso a uma única operadora ou a um parceiro de roaming fraco quando há uma rede local melhor disponível. O resultado é um alcance mais amplo, maior resiliência e menos complexidade operacional à medida que a rede cresce.

Perguntas a fazer ao seu provedor

- Vocês oferecem acesso a várias redes nos países onde atuamos, ou ficamos limitados à cobertura de uma única operadora?
- Se a cobertura for fraca em um local de implantação, o carregador pode se conectar a uma rede disponível com melhor cobertura?
- Se implementarmos em vários mercados, precisaremos de diferentes SKUs de SIM ou de estratégias de conectividade distintas por região?
- Como vocês evitam o custo e a complexidade dos modelos tradicionais de roaming para implantações internacionais?
- O seu modelo de cobertura simplificará a implantação e o suporte ao longo do tempo, ou aumentará a sobrecarga operacional à medida que expandimos?

Para ver quais operadoras, e quantas, estão disponíveis pela emnify nas suas regiões de implantação, [clique aqui](#).



2. Controle

Quanto controle teremos após a implantação?

Para as equipes de carregamento de veículos elétricos, colocar um carregador em operação é apenas parte do trabalho. A questão mais importante é o que acontece depois. Uma vez que os carregadores são implantados em campo, quanto controle você realmente tem sobre a forma como eles se conectam, funcionam e consomem dados?

Redes de carregamento de veículos elétricos são difíceis de gerenciar manualmente. Os carregadores estão distribuídos por muitos locais e, muitas vezes, é difícil, caro ou indesejável acessá-los pessoalmente. Espera-se que eles permaneçam disponíveis sem intervenção manual constante. Se cada alteração de conectividade exigir um ticket de suporte, uma solicitação à operadora ou uma visita ao local, até mesmo ajustes simples se tornam lentos, caros e causam interrupções.

Um provedor de conectividade moderno não deve apenas fornecer um SIM e um sinal. Ele deve oferecer controle direto, imediato e remoto sobre o comportamento da conectividade em campo.

Na prática, isso significa poder bloquear ou permitir operadoras específicas para que o SIM possa se conectar à rede com melhor desempenho em uma determinada região. Significa controlar quais tecnologias de acesso de rádio (RATs) o SIM tem permissão para usar, definir limites e limites de dados para evitar excedentes e habilitar novas regiões ou zonas imediatamente à medida que as necessidades de implantação mudam. Também pode significar automatizar essas ações, para que seu modelo de conectividade responda mais rápido do que um processo de suporte manual responderia.

Para equipes de carregamento de veículos elétricos, esse nível de controle não é um luxo. É uma maneira prática de manter os carregadores funcionando bem sem enviar pessoas ao campo toda vez que algo precise ser alterado. Quanto mais for possível ajustar instantaneamente e remotamente, mais fácil se torna manter o tempo de atividade, proteger a experiência do cliente, controlar custos e adaptar a conectividade às condições operacionais reais.

O que um controle de conectividade melhor deve oferecer

Um modelo de controle de conectividade mais robusto deve permitir que suas equipes atuem em tempo real, por meio de uma plataforma ou interface de programação de aplicativos (API), sem esperar por uma operadora ou abrir tickets para alterações de rotina.

Isso inclui bloquear operadoras com baixo desempenho, ajustar políticas no SIM card, gerenciar limites de uso, habilitar novas regiões e automatizar respostas quando as condições mudam. Em vez de esperar que outra pessoa faça alterações de rotina, suas equipes devem ser capazes de agir imediatamente e manter a conectividade alinhada com o que a rede de carregamento e sua empresa realmente precisam.

Perguntas a fazer ao seu provedor

- Podemos bloquear ou permitir operadoras específicas remotamente?
- Podemos influenciar à qual rede um carregador se conecta em uma determinada região?
- Podemos alterar políticas de SIM card ou de dispositivos imediatamente, sem abrir um ticket de suporte?
- Podemos controlar nós mesmos o acesso RAT, os limites de dados e os limites de uso?
- É possível ativar novas regiões ou zonas de cobertura instantaneamente?
- Vocês oferecem suporte a automações que atuam em instâncias de conectividade ou condições estabelecidas por políticas?

Para ver como a emnify oferece controle instantâneo sobre a conectividade, explore nosso [tour pela plataforma](#).

3. Solução de problemas

Quão fácil será resolver problemas quando algo der errado?

O verdadeiro teste de um provedor de conectividade começa quando algo deixa de funcionar como esperado.

Um carregador pode ainda ter energia, mas não conseguir registrar as sessões corretamente. Ele pode deixar de enviar relatórios de forma confiável para o backend. Os diagnósticos remotos podem se tornar inconsistentes. Os fluxos de trabalho de pagamentos, autenticação ou suporte podem falhar. As equipes de engenharia e operações ficam então tentando descobrir se o problema está no carregador, no SIM card, no modem, na rede ou na plataforma de backend.

Quando falta essa visibilidade, a resolução de problemas se torna mais lenta, menos segura e muito mais cara.

É aí que a conectividade deixa de ser uma dependência de menor importância e se torna uma questão operacional que afeta diretamente o tempo de atividade, o custo de suporte, a reputação da marca e a experiência do cliente.

Para os provedores de carregamento de veículos elétricos, um suporte fraco para a resolução de problemas pode significar interrupções mais longas, mais incerteza e mais visitas desnecessárias ao local. Se as equipes não conseguirem determinar rapidamente se o problema está relacionado à conectividade ou ao dispositivo, a recuperação se torna mais lenta e mais cara.

O que importa aqui não é apenas se um provedor oferece suporte. É se ele dá às suas equipes a visibilidade e as ferramentas para diagnosticar e resolver problemas rapidamente por conta própria, de modo que o suporte se torne a exceção e não a regra.

- **Você consegue ver se o carregador ainda está conectado?**
- **Consegue saber quando ele esteve online pela última vez?**
- **Consegue identificar se o problema está no dispositivo ou na camada de conectividade antes de enviar um técnico ao campo?**

Quanto mais robusto for o modelo de diagnóstico, mais rápido as equipes poderão passar da incerteza à ação. Isso reduz visitas desnecessárias ao local, encurta os tempos de recuperação e ajuda a manter a confiança na rede de carregamento à medida que ela se expande.

O que um modelo de resolução de problemas robusto deve oferecer

Um modelo de resolução de problemas mais robusto deve oferecer às suas equipes visibilidade direta dos eventos de conectividade em tempo real e, tão importante quanto isso, tornar essa visibilidade utilizável.

Na prática, esse nível de insight é normalmente mais forte quando o provedor possui e opera sua própria rede central, em vez de depender inteiramente de camadas de conectividade de terceiros. Isso importa porque o provedor pode ver o que está acontecendo diretamente, identificar eventos mais rapidamente e ajudar as equipes a isolar a causa raiz com maior confiança.

Quando um provedor não possui sua própria infraestrutura central, ele essencialmente se torna um intermediário entre você e a operadora quando um problema precisa ser resolvido. Ele não consegue ver a causa raiz diretamente nem determinar como resolvê-la por conta própria, dependendo totalmente da operadora para fornecer insights. Isso não deve ser menosprezado. Quando seu cliente pergunta por que seu ponto de carregamento não está online e seu provedor não consegue dar respostas claras, a experiência do cliente fica imediatamente em risco.

Mas, a visibilidade por si só não é suficiente. O provedor também precisa exibir esses eventos de forma clara no portal e disponibilizá-los por meio de API, para que suas equipes possam solucionar problemas mais rapidamente, decidir mais cedo se a questão está relacionada ao dispositivo ou à conectividade e evitar visitas desnecessárias ao local.

Perguntas a fazer ao seu provedor

- Você possui e opera a rede central que lhe dá visibilidade sobre eventos de conectividade em tempo real?
- Quais eventos de conectividade você pode realmente exibir aos clientes no portal?
- Esses mesmos eventos também estão disponíveis por meio de API?
- Podemos saber quando um carregador foi conectado pela última vez e se o problema está relacionado ao dispositivo ou à conectividade?
- O seu modelo de resolução de problemas ajudará nossas equipes a resolver problemas mais rapidamente à medida que crescemos, ou nos deixará com mais ambiguidade?

Para saber mais sobre como a emnify oferece insights de conectividade em tempo real e resolução de problemas, leia nossa postagem no blog [“O que é uma rede central e como ela afeta os dispositivos celulares”](#).

4. Suporte

Com que tipo de suporte e SLAs podemos contar?

Mesmo com grande visibilidade e a resolução de problemas através de autoatendimento, ainda haverá situações em que as equipes internas precisarão escalar o problema para seu provedor de conectividade.

Quando isso acontece, a qualidade do suporte tem um efeito direto na experiência de carregamento. Se o suporte for lento, difícil de contatar ou incapaz de diagnosticar o problema adequadamente, o tempo de inatividade do carregador se prolonga, as visitas ao site aumentam e tanto as equipes internas quanto os usuários finais perdem a confiança na qualidade do serviço. Para empresas de carregamento de veículos elétricos, isso não é apenas frustrante. Isso afeta diretamente o desempenho da rede.

É por isso que o suporte deve ser avaliado como algo mais do que uma promessa genérica de assistência 24 horas por dia, 7 dias por semana. A verdadeira questão é com que rapidez o provedor consegue responder, até que ponto compreende o problema e quais compromissos de serviço está disposto a assumir.

Tanto para fabricantes de pontos de carregamento quanto para CPOs, a questão prática é simples: com que rapidez o provedor pode ajudar a colocar os carregadores de volta em operação?

Isso é ainda mais importante em mercados onde o tempo de atividade tem consequências comerciais diretas. Muitos operadores de carregamento de veículos elétricos, incluindo vários clientes da emnify, atuam no Reino Unido, onde a confiabilidade dos carregadores é fundamental para atender às expectativas regulatórias e manter o acesso a modelos de suporte apoiados pelo governo. Nesse contexto, é ainda mais importante que o provedor de conectividade garanta o tempo de atividade, em vez de se tornar mais um ponto de falha que dificulte alcançá-la.

Enxergue além da mera disponibilidade de suporte. Quais SLAs se aplicam aos tempos de resposta a incidentes? Quais compromissos de serviço se aplicam à própria plataforma de conectividade? O que acontece quando o problema está entre o carregador, a rede e o backend? Quais pacotes de suporte estão disponíveis e como eles diferem?

Também vale a pena entender como o suporte funciona na prática. Suas equipes estarão lidando com pessoas que entendem sobre a conectividade da Internet das Coisas (IoT) e as realidades operacionais do carregamento de veículos elétricos, ou com uma central de suporte genérica que trabalha seguindo um roteiro? Quando ocorre um incidente, o provedor consegue fornecer atualizações claras, explicar o que está acontecendo e ajudar sua equipe a decidir o que fazer a seguir?

Um suporte robusto não substitui boas ferramentas, visibilidade ou controle. Ele funciona como uma camada final confiável de escalonamento.

Como deve ser um suporte confiável

Um sinal revelador de que uma equipe de suporte é confiável é que, mesmo antes de você assinar o contrato, ela já está tentando entender seu projeto, e não apenas enviar cotações.

Um provedor mais sólido dedica tempo para entender seu modelo de implantação, os riscos operacionais e o que o sucesso realmente significa para sua rede de carregamento. Isso significa definir a solução certa desde o início, e não apenas oferecer a mais barata.

Uma vez que o serviço esteja em operação, o suporte também deve ser especializado. As equipes de carregamento de veículos elétricos devem ter acesso a pessoas que entendam de conectividade IoT e das realidades da operação de infraestrutura distribuída, e não a um helpdesk genérico de telecomunicações. Idealmente, isso significa um modelo dedicado de sucesso do cliente ou de suporte focado em IoT e capaz de compreender como as questões de conectividade afetam a operação de carregamento como um todo.

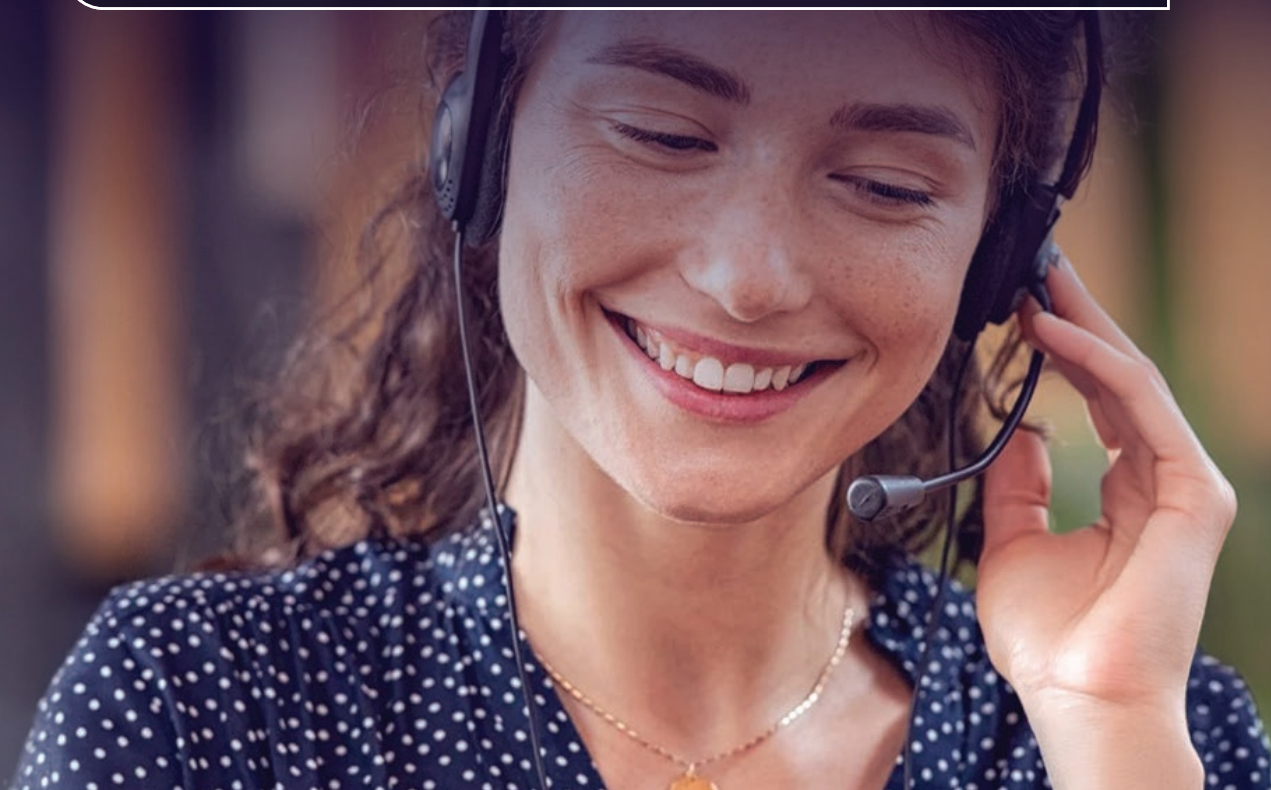
Tão importante quanto isso é a visibilidade. Um suporte robusto depende do acesso a eventos de conectividade em tempo real. Se o provedor não tiver controle suficiente sobre a camada de conectividade para ver diretamente o que está acontecendo, ele pode ser forçado a esperar por uma operadora de rede móvel (MNO) antes de poder responder com confiança. Nesse modelo, o suporte se torna mais lento, menos preciso e mais dependente do cronograma de terceiros. Mesmo quando as informações chegam, o provedor ainda pode ter controle limitado sobre a rapidez com que o problema pode ser resolvido.

Um modelo de suporte mais robusto oferece aos clientes tanto conhecimento especializado quanto insights diretos. Isso reduz o risco de o provedor atuar como uma camada intermediária entre o cliente e a rede e aumenta a chance de obter uma resolução mais rápida e bem informada quando algo der errado.

Perguntas a fazer ao seu provedor

- Vocês têm equipes dedicadas de suporte ou sucesso do cliente focadas em IoT?
- Como vocês adaptam a solução durante a pré-venda para atender ao nosso caso de uso, em vez de apenas cotar um pacote padrão?
- Vocês têm visibilidade direta dos eventos de conectividade em tempo real ou dependem da operadora de rede móvel (MNO) para fornecer essas informações posteriormente?
- Quanto controle vocês realmente têm quando ocorre um problema relacionado à rede?
- Que acordos de nível de serviço (SLAs) vocês oferecem para a resposta a incidentes, tempos de resolução e disponibilidade da plataforma?
- O seu modelo de suporte nos ajudará a resolver problemas mais rapidamente ou criará mais uma camada entre nós e a rede?

Para ver os pacotes de suporte disponíveis da emnify, incluindo tempos de resposta e SLAs de serviço, [clique aqui](#).





5. Segurança

Como é feita a proteção da comunicação entre o carregador e o backend?

Para equipes de carregamento de veículos elétricos, a segurança deve ser tratada como um requisito comercial, não apenas como um requisito de conformidade a ser cumprido.

Os carregadores não são dispositivos autônomos. São sistemas conectados que trocam dados constantemente com plataformas de backend para atualizações de status, diagnósticos remotos, alterações de configuração, gerenciamento de sessões e outras ações operacionais. Isso significa que a segurança da comunicação entre o carregador e o backend desempenha um papel direto no tempo de atividade, no controle, na confiança e na experiência do cliente.

Isso é especialmente importante em ambientes baseados no Open Charge Point Protocol 1.6 (OCPP 1.6), que ainda é amplamente utilizado no mercado de carregamento de veículos elétricos. O OCPP ajudou o setor a evitar o aprisionamento tecnológico e a melhorar a interoperabilidade, mas não elimina a necessidade de transporte seguro e implementação cuidadosa. Na prática, as operadoras ainda precisam refletir seriamente sobre como o tráfego do carregador é protegido, como as ações remotas são protegidas e qual a parcela dessa responsabilidade que recai sobre a camada de conectividade.

É aqui que o provedor de conectividade faz a diferença. A questão não é apenas se o carregador consegue se conectar ao backend; é como essa comunicação é protegida durante o trânsito, quão exposta ela fica à internet pública e quais controles existem para reduzir o risco.

Recursos como Cloud Connect, Internet Protocol Security (IPsec) e conectividade privada baseada em rede privada virtual (VPN) podem ajudar a criar caminhos de comunicação mais seguros entre carregadores e sistemas de backend. Isso reduz a dependência de rotas públicas abertas e dá às operadoras mais controle sobre as operações remotas.

E isso não se refere apenas a dados de status. A conectividade também pode apoiar comandos remotos, atualizações de firmware, diagnósticos e outras ações que afetam diretamente o comportamento do carregador em campo. Quanto mais críticas essas ações se tornam, mais importante é entender se o modelo de conectividade reforça a segurança ou deixa muito ao acaso.

Isso se torna ainda mais importante quando a infraestrutura de carregadores cresce além do simples carregamento. Algumas operadoras estão adicionando terminais de pagamento, recursos de ponto de venda (POS), circuito fechado de televisão (CCTV), alarmes ou outros dispositivos conectados no site. À medida que mais serviços são incorporados ao carregador ou ao seu entorno, os requisitos de segurança aumentam com eles. A conectividade não é mais apenas uma camada de transporte, ela se torna parte do modelo de confiança para o site.

O que uma conectividade segura para veículos elétricos deve oferecer

Uma conectividade segura para veículos elétricos deve fazer mais do que apenas criptografar o tráfego. Ela deve reduzir a exposição, dar às operadoras mais controle sobre como os carregadores se comunicam e tornar as ações remotas mais seguras para serem realizadas em escala.

Na prática, isso significa criar um caminho mais controlado entre o carregador e o backend, em vez de enviar tudo pela internet pública aberta. É aqui que recursos como IPsec e Cloud Connect se tornam importantes. O IPsec ajuda a criar um túnel privado e criptografado para os dados que circulam entre os carregadores e os sistemas de backend. O Cloud Connect cria uma conexão confiável entre o provedor de conectividade e o ambiente de nuvem do cliente. Juntos, eles ajudam as operadoras a proteger a comunicação entre o carregador e o backend e a reduzir a exposição desnecessária.

Isso é ainda mais importante em ambientes OCPP 1.6, onde a camada de conectividade pode precisar fornecer uma camada adicional de proteção em torno do tráfego do carregador, diagnósticos remotos, atualizações de firmware e comandos do carregador.

Um provedor de confiança também deve ser capaz de demonstrar padrões de segurança reconhecidos, como a ISO 27001, além de proteções práticas na própria camada de conectividade.

Perguntas a fazer ao seu provedor

- Como você reduz a exposição à internet pública para a comunicação entre o carregador e o backend?
- Vocês oferecem suporte a caminhos de comunicação controlados e privados, como IPsec ou Cloud Connect?
- Como vocês ajudam a proteger diagnósticos remotos, atualizações de firmware e comandos do carregador?
- Que proteção adicional seu modelo de conectividade oferece em ambientes OCPP 1.6?
- Quais padrões de segurança ou certificações reconhecidas você pode comprovar?

Para saber como a emnify ajuda a proteger sua rede de pontos de carregamento com um modelo de conectividade seguro por padrão, explore nossa [oferta de segurança de conectividade](#).

6. Integrações

A conectividade será compatível com os sistemas que já utilizamos?

As equipes de carregamento de veículos elétricos não querem que a conectividade fique isolada em um silo operacional.

À medida que as redes de carregamento crescem, os dados e o gerenciamento da conectividade precisam ser incorporados aos sistemas que as equipes utilizam diariamente. Isso pode incluir plataformas de gerenciamento interno, ferramentas de observação, fluxos de trabalho de suporte, sistemas de relatórios, ferramentas de implantação ou mecanismos de automação. Se a conectividade puder ser gerenciada apenas por meio de um portal separado com opções de integração limitadas, ela rapidamente se tornará mais uma fonte de atrito.

Esse desafio se torna ainda mais evidente quando as operadoras trabalham com vários provedores de conectividade. Cada provedor pode expor os dados de maneira diferente, oferecer um nível distinto de granularidade, suportar um modelo de API diferente ou apresentar tipos de eventos distintos. O resultado é uma visibilidade fragmentada e trabalho de integração duplicado. As equipes de produto e de engenharia precisam, então, normalizar dados inconsistentes, dar suporte a múltiplas interfaces e criar processos internos em torno de níveis desiguais de controle.

Para os fabricantes de pontos de carregamento, isso afeta a facilidade com que os dispositivos podem ser implantados, ativados e suportados em escala. Para os CPOs, isso afeta o quão bem a conectividade pode ser incorporada às operações do dia a dia. Se o estado do carregador, o estado da conectividade e os dados sobre incidentes residirem em sistemas separados, as equipes perdem tempo alternando entre ferramentas e contornando pontos cegos.

É por isso que a integração deve ser avaliada como parte essencial do modelo de conectividade. Um provedor mais robusto deve permitir que as equipes acessem dados e controles de conectividade através dos mesmos sistemas que já utilizam para monitorar, solucionar problemas e operar sua rede.

O que as integrações robustas devem oferecer

Integrações robustas devem oferecer às suas equipes uma única camada operacional para trabalhar e não múltiplas visões desconectadas de diferentes operadoras.

Na prática, isso significa eventos de conectividade em tempo real em todas as redes suportadas, apresentados em uma única plataforma e disponibilizados por meio de API. Significa também que as ações de gerenciamento de conectividade não ficam restritas a um portal, mas podem ser integradas diretamente aos sistemas que suas equipes já utilizam diariamente.

Isso é importante porque, assim que os dados de conectividade ficam fragmentados, os fluxos de trabalho também se fragmentam. As equipes de produto, engenharia e operações acabam alternando entre ferramentas, normalizando dados inconsistentes e contornando pontos cegos. Um modelo mais robusto oferece a elas uma única fonte de verdade para a visibilidade e uma única interface para a ação, facilitando a automação de fluxos de trabalho e a operação em escala.

Perguntas a fazer ao seu provedor

- Vocês fornecem eventos de conectividade em tempo real para todas as redes suportadas em uma única plataforma?
- Esses mesmos eventos estão disponíveis por meio de API, e não apenas no portal?
- As ações de gerenciamento de conectividade podem ser integradas aos nossos próprios sistemas e fluxos de trabalho?
- Se trabalharmos com várias operadoras, como vocês evitariam a visibilidade fragmentada e o esforço duplicado de integração?
- O seu modelo de conectividade nos oferece uma camada operacional para nos desenvolvermos, ou são várias?

Para saber mais sobre a conectividade em tempo real e o mecanismo de eventos de rede da emnify, e como ele pode ser integrado aos seus sistemas, consulte nossa [documentação do produto](#).

7. Preparação para o futuro

Como garantir a flexibilidade e adaptação da conectividade dos carregadores no longo prazo?

Para as equipes de carregamento de veículos elétricos, garantir a conectividade no longo prazo significa manter a flexibilidade muito tempo depois que um carregador foi implantado. À medida que as redes crescem, as condições de mercado mudam e os requisitos regionais evoluem, as equipes precisam de um modelo que possa se adaptar sem forçar mudanças de hardware em campo.

É aqui que o SGP.32 se torna relevante. O SGP.32 é o padrão da Associação Global de Sistemas de Comunicações Móveis (GSMA) para o gerenciamento remoto de perfis eSIM na IoT. Em termos simples, ele permite que um dispositivo mantenha o mesmo hardware físico do SIM card enquanto altera ou adiciona perfis de operadoras remotamente ao longo do tempo.

Isso é importante porque muda o momento em que as decisões de conectividade precisam ser tomadas. Em vez de definir todas as opções de operadora na fábrica ou na instalação, os fabricantes de pontos de carregamento e os CPOs podem manter mais flexibilidade após a implantação do carregador.

Para as equipes de carregamento de veículos elétricos, isso cria um modelo mais preparado para o futuro para lidar com novas regiões, mudanças na estratégia de conectividade, requisitos de operadoras locais e longos ciclos de vida dos carregadores.

A oportunidade do SGP.32 para fabricantes de pontos de carregamento Um único SKU para implantações em escala

Para os fabricantes de pontos de carregamento, a oportunidade é clara. Os carregadores podem sair da fábrica com um perfil bootstrap já configurado, proporcionando-lhes um ponto de partida ativo para a conectividade desde o primeiro dia. A partir daí, a conectividade pode evoluir ao longo do tempo com a adição de novos perfis de operadoras à medida que os requisitos mudam, criando um modelo de fabricação muito mais flexível.

Em vez de incorporar diferentes estratégias de SIM em variantes de hardware distintas, os fabricantes de pontos de carregamento podem trabalhar com uma única SKU e tornar a conectividade mais uma decisão de software. Isso reduz a logística de SIM, evita a troca física de SIMs e facilita o suporte a múltiplas regiões de implantação e requisitos dos clientes ao longo da vida útil do carregador.

A oportunidade do SGP.32 para CPOs

Mais opções quando a estratégia de rede muda em campo

Para os CPOs, a oportunidade é igualmente relevante. À medida que os carregadores são implantados em diferentes mercados e ambientes de instalação, o SGP.32 facilita a alteração ou adição de perfis de operadoras sem a substituição de hardware.

Um CPO pode implantar um carregador em um novo local e descobrir que o perfil do provedor atual oferece desempenho pouco confiável ali. Sem trocar de hardware ou de SIM card, é possível adicionar um perfil de operadora local mais adequado. A mesma lógica se aplica ao entrar em uma nova região, ao atender a requisitos regulatórios ou ao ajustar a estratégia de operadora ao longo do tempo.

A vantagem é a mesma: a conectividade passa a ser mais uma decisão de software e menos dependente de uma troca física de SIM em campo.



O que um modelo SGP.32 robusto deve lhe oferecer

Um modelo SGP.32 robusto deve lhe oferecer a capacidade de transformar a logística do SIM em uma decisão de software.

Isso significa que você não está mais preso a um pedaço de plástico toda vez que a conectividade precisa mudar. Em vez de trocar SIM cards, substituir hardware ou gerenciar múltiplas variantes físicas, as equipes podem adaptar a conectividade remotamente à medida que os requisitos evoluem. Isso cria um modelo operacional mais flexível e preparado para o futuro, tanto para os fabricantes de pontos de carregamento quanto para os CPOs.

Também deve ficar claro como essa flexibilidade é oferecida na prática. Quem controla o gerenciador remoto (eIM) de eSIM IoT? Como os perfis adicionais são gerenciados? Quais opções de fallback estão disponíveis? Quanta complexidade operacional é realmente eliminada e quanta é simplesmente transferida para outro lugar?

Para as equipes de carregamento de veículos elétricos, esses detalhes são importantes, porque o valor do SGP.32 não é o padrão em si. É a flexibilidade operacional que a implementação correta pode proporcionar ao longo da vida útil do carregador.

Perguntas a fazer ao seu provedor

- Como seu modelo de conectividade pode nos ajudar a manter a flexibilidade à medida que nossas necessidades de implantação mudam ao longo do tempo?
- O que o seu modelo SGP.32 realmente nos permite fazer após a implantação?
- Os carregadores podem sair da fábrica com um perfil bootstrap já configurado?
- É possível adicionar perfis posteriormente sem substituir o hardware?
- Com que facilidade a conectividade pode ser localizada com base no local onde o carregador está implantado?
- Quem controla o eIM, e o que isso significa operacionalmente para nós?

Para saber como é fácil gerenciar vários perfis do SGP.32 através do portal da emnify, [confira nossa demonstração aqui.](#)

Conclusão

No carregamento de veículos elétricos, a conectividade tem um efeito direto nas métricas que mais importam: tempo de atividade do carregador, sessões de carregamento bem-sucedidas, velocidade de implantação, eficiência do suporte, confiabilidade do pagamento e a experiência do cliente. É por isso que ela não deve ser avaliada como uma compra de commodity ou um detalhe final da implantação.

Fazer essas sete perguntas desde o início ajuda a proteger sua empresa e a apoiar o crescimento futuro. Elas ajudam você a testar se um provedor pode fazer mais do que apenas alegar cobertura. Elas mostram se o modelo de conectividade por trás da sua rede ajudará você a manter o controle à medida que os carregadores se expandem para mais locais, mais regiões e condições operacionais mais exigentes. Mais importante ainda, elas ajudam você a avaliar se esse modelo irá apoiar a experiência do cliente pela qual sua empresa é avaliada.

Os melhores provedores devem ser capazes de responder sim a um conjunto claro de resultados:

- Cobertura que funciona nos ambientes onde seus carregadores realmente operam
- Um sistema de controle que permite que suas equipes atuem imediatamente, sem depender de tickets
- Solução de problemas que reduz ambiguidades e evita visitas desnecessárias ao site
- Suporte que responde rapidamente e compreende as realidades das operações de IoT
- Segurança que protege a comunicação entre o carregador e o backend
- Integrações que se adaptam aos sistemas que suas equipes já utilizam diariamente
- Um caminho preparado para o futuro que mantém a conectividade flexível ao longo da vida útil do carregador

Tanto para fabricantes de pontos de carregamento quanto para CPOs, o objetivo não é escolher a oferta mais simples no papel. É escolher um modelo de conectividade que apoie o negócio em todas as fases de crescimento.

Se você deseja discutir suas necessidades ou gostaria de uma segunda opinião sobre os pontos fortes do seu modelo atual, onde ele está apresentando riscos e onde é possível obter mais flexibilidade, [entre em contato](#) e vamos explorar como a emnify pode apoiar suas operações de carregamento de veículos elétricos.

Comece hoje mesmo

