The EV Charging Connectivity Buyer's Guide (2026)

7 Questions EV Charging Teams Must Ask when Choosing Their Connectivity Provider

The complete connectivity buyer's guide for EV charging decision-makers, including SGP.32 (IoT eSIM)

April 2026

Who this guide is for?

- Charge point operators managing and scaling their network
- Charge point manufacturers
- Product, Operations, Engineering leaders and anybody else in your connectivity buying group

Why connectivity matters at EV charging scale

The way how your chargers connect and communicate should not be treated as an afterthought. In EV charging, connectivity is a core part of how infrastructure performs, scales, and stays under your control.

Charging networks do not operate in neat, predictable environments. Home chargers often rely on Wi-Fi that operators cannot control, limiting visibility and making performance harder to manage. Public chargers may be deployed where fixed connectivity is too costly, too slow to install, or simply not practical. In both cases, part of the charging experience depends on infrastructure outside the operator's control.

Cellular connectivity gives operators a more direct and controllable way to connect chargers across these environments. But getting a charger online is only the first step. The real challenge is choosing a connectivity model that stays reliable, manageable, and flexible as the network expands.

Why most EV connectivity decisions fail (and what it costs)

For EV charging teams, connectivity is easy to overlook until it starts causing problems. A charger can be installed, powered, and technically operational, yet still fail in ways that damage the customer experience, slow down operations, and drive up costs. Sessions may not start properly. Remote diagnostics may be limited. Software updates may fail. Engineering teams can be left guessing whether the problem sits with the charger, the network, the SIM, or the backend.

At small scale, that is manageable. At scale, it turns into a recurring operational cost. For charge point manufacturers, connectivity shapes how chargers are built, shipped, deployed, and supported over time. For charge point operators (CPOs), it shapes far more than whether a charger is online. It affects rollout, customer onboarding, uptime, visibility, remote troubleshooting, payment reliability, compliance, and how seamlessly the network can scale.

As EV charging networks grow, connectivity is expected to do far more than provide access. Operators need visibility into device behaviour, secure communication between chargers and backend systems, support for remote actions and troubleshooting, and connectivity data that can feed directly into their own tools and workflows. New standards such as SGP.32 are pushing that even further, giving charge point manufacturers and CPOs more flexibility over connectivity long after deployment.

The 7 connectivity questions that determine if your network scales or breaks
If you are a product manager, engineer, or operations leader at a charge point manufacturer or CPO, these are the questions you should be asking to evaluate connectivity in practical terms, both before and after chargers go live in the field.

The goal of this guide is simple: to help you judge whether a connectivity provider can truly support the demands of your charging network and, with that, your business. These questions are not theoretical. Together, they determine whether connectivity becomes a source of control and scale, or an ongoing source of friction, support burden, and operational risk.

With that in mind, here are seven connectivity questions you should be asking from the start:

- Will coverage work where our chargers are actually deployed?
- How much control will we have after deployment?
- How easily can we troubleshoot issues when something goes wrong?
- What support and SLAs can we rely on?
- How is charger-to-backend communication secured?
- Will connectivity integrate with the systems we already use?
- How do we keep charger connectivity flexible and future-proof over time?

Let’s look at each of these questions in more detail.

1. Coverage

Will coverage work where our chargers are actually deployed?

Coverage is a basic part of any EV charging connectivity decision, but it is also one of the easiest areas to oversimplify. You should not only be asking whether a connectivity provider can provide coverage at your deployment sites, but how they do it.

The real issue is not whether a provider can claim coverage in a country or region. It is whether that coverage model works for the way chargers are actually built, deployed, and operated over time.

For charge point manufacturers, the challenge appears early. A charger may be designed once, but deployed across multiple markets with different operator footprints, coverage quality, and commercial conditions. If different deployment regions require different operator relationships or SIM strategies, complexity builds fast. Manufacturing, logistics, inventory planning, and support all become harder to manage. What starts as a connectivity decision can quickly become a product operations and supply chain problem.

For CPOs, the challenge is different but no less important. Even within one country, coverage quality can vary significantly across the environments where chargers are deployed. A forecourt, retail site, transport hub, hotel, roadside location, rural destination, or public hub may all perform differently depending on which network is strongest there. National coverage means very little if the model still leaves operators exposed to weak connectivity at important sites.

This is why coverage should be evaluated as an operational capability, not just a map or a country count. EV charging teams need to understand whether the provider's model gives them flexibility once chargers are in the field. Can connectivity adapt to the realities of the installation environment? Can the charger connect reliably where it is actually deployed? Will the coverage model simplify deployment over time, or create more operational complexity as the estate grows?

What good coverage should give you

A stronger coverage model should simplify operations, not multiply them. It should give you one provider relationship, access to multiple networks in most countries, and fewer SIM strategies to manage across regions.

For charge point manufacturers, that means fewer stock keeping units (SKUs), simpler logistics, and easier support. For CPOs, it means a charger is not stuck with one operator or a weak roaming partner when a better local network is available. The result is broader reach, stronger resilience, and less operational complexity as the network grows.

Questions to ask your provider

- Do you provide access to multiple networks in the countries where we operate, or are we tied to a single operator footprint?
- If coverage is weak at a deployment site, can the charger connect to a better available network?
- If we deploy across multiple markets, will we need different SIM SKUs or separate connectivity strategies by region?
- How do you avoid the cost and complexity of traditional roaming models for international deployments?
- Will your coverage model simplify deployment and support over time, or add more operational overhead as we scale?

To see which operators, and how many, are available from emnify in your deployment regions, click here.

2. Control

How much control will we have after deployment?

For EV charging teams, getting a charger online is only part of the job. The bigger question is what happens next. Once chargers are deployed in the field, how much control do you actually have over the way they connect, behave, and consume data?

EV charging networks are hard to manage manually. Chargers are distributed across many locations and are often difficult, costly, or undesirable to access in person. They are expected to stay available without constant manual intervention. If every connectivity change requires a support ticket, an operator request, or a site visit, even simple adjustments become slow, expensive, and disruptive.

A modern connectivity provider should not just give you a SIM and a signal. They should give you direct, immediate, and remote control over how connectivity behaves in the field.

In practice, that means being able to block or allow specific operators so the SIM can attach to the network that performs best in a given region. It means controlling which radio access technologies (RATs) the SIM is allowed to use, setting data limits and thresholds to avoid overages, and enabling new regions or zones immediately as deployment needs change. It can also mean automating those actions, so your connectivity model responds faster than a manual support process ever could.

For EV charging teams, this level of control is not a nice-to-have. It is a practical way to keep chargers performing well without sending people into the field every time something needs to change. The more that can be adjusted instantly and remotely, the easier it becomes to maintain uptime, protect the customer experience, control cost, and adapt connectivity to real operating conditions.

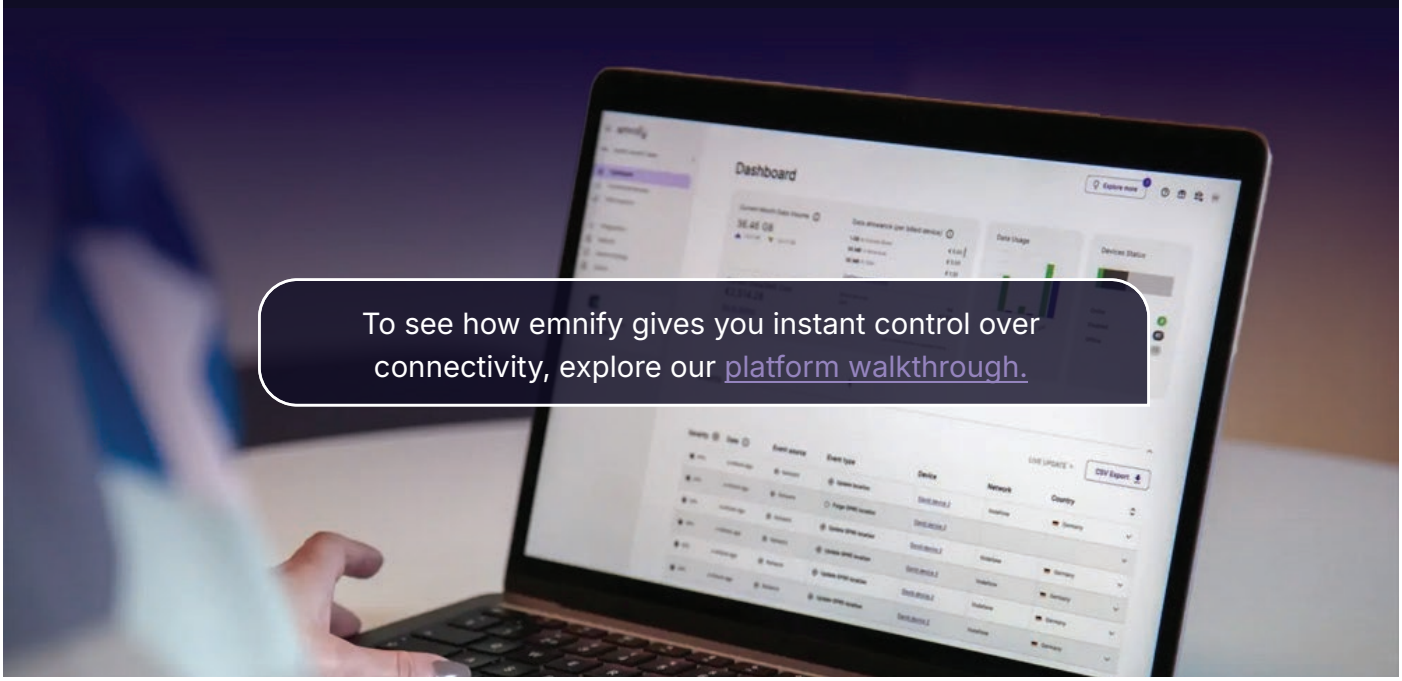
What better connectivity control should give you

A stronger connectivity control model should let your teams act in real time, through a platform or application programming interface (API), without waiting on a carrier or raising tickets for routine changes.

That includes blocking underperforming operators, adjusting policies on the SIM, managing usage limits, enabling new regions, and automating responses when conditions change. Instead of waiting for someone else to make routine changes, your teams should be able to act immediately and keep connectivity aligned with what the charging network, and your business, actually needs.

Questions to ask your provider

- Can we block or allow specific operators remotely?
- Can we influence which network a charger connects to in a given region?
- Can we change SIM or device policies immediately, without opening a support ticket?
- Can we control RAT access, data limits, and usage thresholds ourselves?
- Can new regions or coverage zones be enabled instantly?
- Do you support automations that act on connectivity events or policy conditions?



To see how emnify gives you instant control over connectivity, explore our platform walkthrough.

3. Troubleshooting

How easily can we troubleshoot issues when something goes wrong?

The real test of a connectivity provider begins when something stops working as expected.

A charger may still have power yet fail to log sessions properly. It may stop reporting reliably to the backend. Remote diagnostics may become inconsistent. Payment, authentication, or support workflows may break. Engineering and operations teams are then left trying to work out whether the issue sits with the charger, the SIM, the modem, the network, or the backend platform.

When that visibility is missing, troubleshooting becomes slower, less certain, and far more expensive.

This is where connectivity stops being a background dependency and becomes an operational issue that directly affects uptime, support cost, brand reputation, and customer experience.

For EV charging providers, weak troubleshooting support can mean longer outages, more uncertainty, and more unnecessary site visits. If teams cannot quickly determine whether the problem is connectivity-related or device-related, recovery becomes slower and more expensive.

What matters here is not just whether a provider offers support. It is whether they give your teams the visibility and tools to troubleshoot and resolve issues quickly themselves, so support becomes the exception rather than the default.

- **Can you see whether the charger is still connected?**
- **Can you tell when it was last online?**
- **Can you identify whether the problem sits with the device or the connectivity layer before dispatching a field technician?**

The stronger the troubleshooting model, the faster teams can move from uncertainty to action. That reduces unnecessary site visits, shortens recovery times, and helps maintain confidence in the charging network as it scales.

What a strong troubleshooting model should give you

A stronger troubleshooting model should give your teams direct visibility into real-time connectivity events, and just as importantly, make that visibility usable.

In practice, that level of insight is typically strongest when the provider owns and operates its own core network rather than relying entirely on third-party connectivity layers. That matters because the provider can see what is happening directly, surface events faster, and help teams isolate root cause with greater confidence.

When a provider does not own its own core infrastructure, it essentially becomes a middleman between you and the operator when an issue needs troubleshooting. It cannot see the root cause directly or determine how to resolve it itself, and is instead fully dependent on the operator to provide insight. This should not be taken lightly. When your customer is asking why their charge point is not online and your provider cannot give clear answers, the customer experience is immediately at risk.

But visibility alone is not enough. The provider also needs to surface those events clearly in the portal and make them available through API, so your teams can troubleshoot faster, decide sooner whether the issue is device-related or connectivity-related, and avoid unnecessary site visits.

Questions to ask your provider

- Do you own and operate the core network that gives you visibility into real-time connectivity events?
- Which connectivity events can you actually surface to customers in the portal?
- Are those same events available through API as well?
- Can we tell when a charger was last connected and whether the issue is device-related or connectivity-related?
- Will your troubleshooting model help our teams resolve issues faster as we scale, or leave us with more ambiguity?

To learn more about how emnify offers real-time connectivity insights and troubleshooting, read our 'What is a Core Network and how does it affect cellular devices?' blog post.

4. Support

What support and SLAs can we rely on?

Even with strong observability and self-service troubleshooting, there will still be situations where internal teams need to escalate to their connectivity provider.

When that happens, the quality of support has a direct effect on the charging experience. If support is slow, hard to reach, or unable to diagnose the issue properly, charger downtime lasts longer, site visits increase, and both internal teams and end users lose confidence in service quality. For EV charging businesses, that is not just frustrating. It directly affects the performance of the network.

This is why support should be evaluated as more than a generic promise of 24/7 help. The real question is how quickly the provider can respond, how deeply they understand the issue, and what service commitments they are willing to stand behind.
For charge point manufacturers and CPOs alike, the practical question is simple: how quickly can the provider help get chargers back online?

That matters even more in markets where uptime has direct commercial consequences. Many EV charging operators, including several emnify customers, operate in the United Kingdom (UK), where charger reliability is critical to meeting regulatory expectations and maintaining access to government-backed support models. In that context, it is even more important that the connectivity provider enables uptime rather than becoming another point of failure that makes it harder to achieve.

Look beyond support availability alone. What SLAs apply to incident response times? What service commitments apply to the connectivity platform itself? What happens when the issue sits between the charger, the network, and the backend? What support packages are available, and how do they differ?

It is also worth understanding how support works in practice. Will your teams be dealing with people who understand Internet of Things (IoT) connectivity and EV charging operational realities, or with a generic support desk working from a script? When an incident happens, can the provider give clear updates, explain what is happening, and help your team decide what to do next?

Strong support does not replace good tooling, visibility, or control. It sits behind them as a reliable final layer of escalation.

What reliable support should look like

A tell-tale sign of a reliable support team is that, even before you sign with them, they are trying to understand your project, not just send quotes.

A stronger provider takes the time to understand your deployment model, operational risks, and what success actually looks like for your charging network. That means shaping the right solution up front, not just offering the cheapest one.

Once the service is live, support should also be specialized. EV charging teams should expect access to people who understand IoT connectivity and the realities of operating distributed infrastructure, not a generic telecommunications helpdesk. Ideally, that means a dedicated customer success or support model focused on IoT and able to understand how connectivity issues affect the wider charging operation.

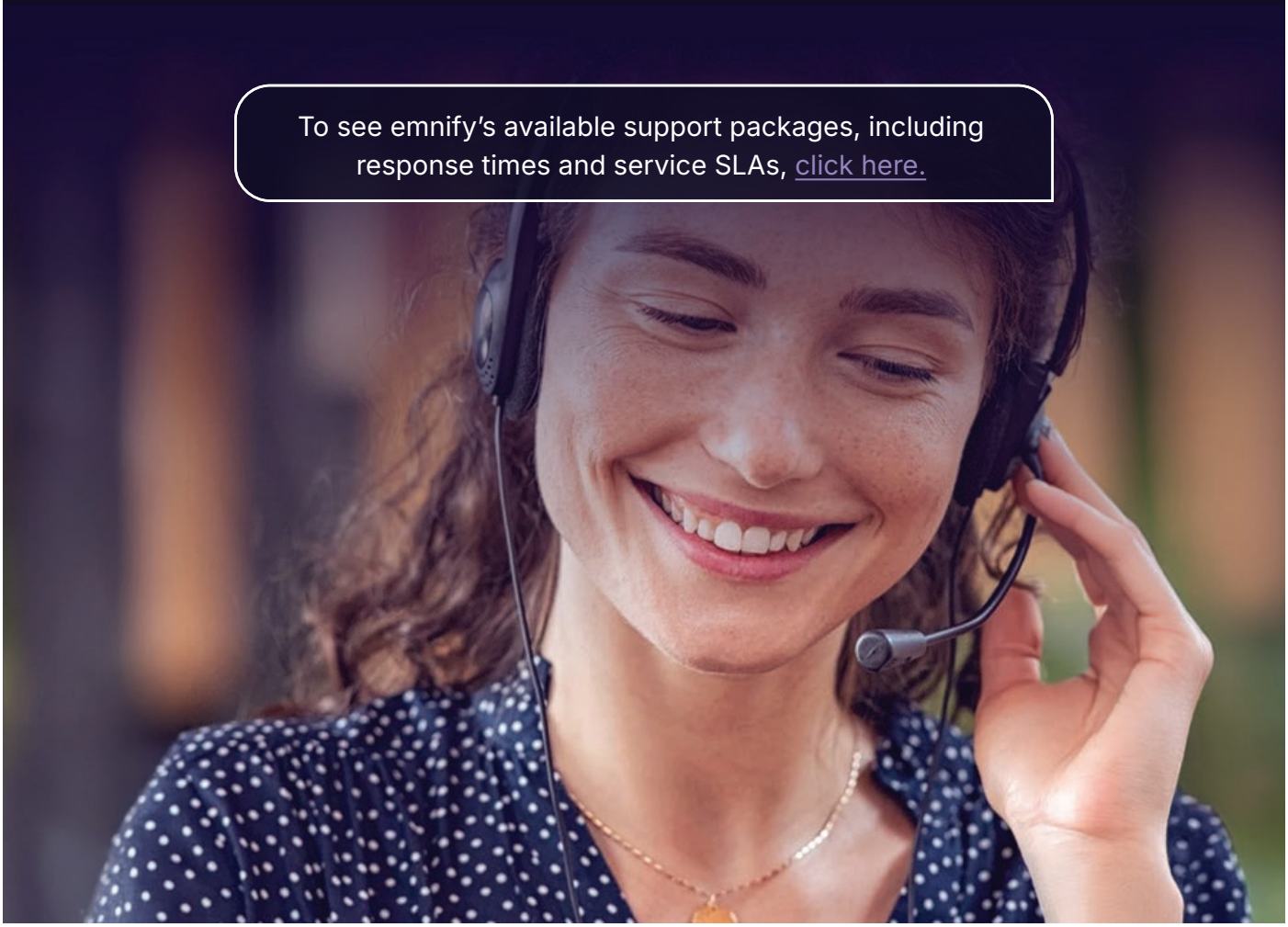
Just as important is visibility. Strong support depends on access to real-time connectivity events. If the provider does not own enough of the connectivity layer to see what is happening directly, they may be forced to wait on a mobile network operator (MNO) before they can respond with confidence. In that model, support becomes slower, less precise, and more dependent on another party's timeline. Even when information does arrive, the provider may still have limited control over how quickly the issue can be addressed.

A stronger support model gives customers both expertise and direct insight. It reduces the risk of the provider acting as a middle layer between the customer and the network, and increases the chance of faster, more informed resolution when something does go wrong.

Questions to ask your provider

- Do you have dedicated IoT-focused customer success or support teams?
- How do you tailor the solution during pre-sales to fit our use case, rather than just quoting a standard package?
- Do you have direct visibility into real-time connectivity events, or do you rely on the MNO to provide that information later?
- How much control do you actually have when a network-related issue occurs?
- What service level agreements (SLAs) do you offer for incident response, resolution times, and platform availability?
- Will your support model help us resolve issues faster, or add another layer between us and the network?

To see emnify's available support packages, including response times and service SLAs, click here.



5. Security

How is charger-to-backend communication secured?

For EV charging teams, security should be treated as a business requirement, not just a compliance box to tick.

Chargers are not standalone devices. They are connected systems that constantly exchange data with backend platforms for status updates, remote diagnostics, configuration changes, session management, and other operational actions. That means the security of charger-to-backend communication plays a direct role in uptime, control, trust, and the customer experience.

This is especially important in environments built on Open Charge Point Protocol 1.6 (OCPP 1.6), which is still widely used across the EV charging market. OCPP has helped the industry avoid lock-in and improve interoperability, but it does not remove the need for secure transport and careful implementation. In practice, operators still need to think seriously about how charger traffic is protected, how remote actions are secured, and how much of that responsibility sits with the connectivity layer.

This is where the connectivity provider matters. The question is not just whether the charger can reach the backend. It is how that communication is secured in transit, how exposed it is to the public internet, and what controls exist to reduce risk.

Capabilities such as Cloud Connect, Internet Protocol Security (IPsec), and virtual private network (VPN)-based private connectivity can help create more secure communication paths between chargers and backend systems. That reduces reliance on open public routes and gives operators more control over remote operations.

And this is not just about status data. Connectivity may also support remote commands, firmware updates, diagnostics, and other actions that directly affect charger behaviour in the field. The more critical those actions become, the more important it is to understand whether the connectivity model strengthens security or leaves too much to chance.

This becomes even more important when the charger estate expands beyond charging alone. Some operators are adding payment terminals, point of sale (POS) capabilities, closed-circuit television (CCTV), alarms, or other connected devices at the site. As more services sit on or around the charger, the security requirement rises with them. Connectivity is no longer just a transport layer. It becomes part of the trust model for the site.

What secure EV connectivity should give you

Secure EV connectivity should do more than encrypt traffic. It should reduce exposure, give operators more control over how chargers communicate, and make remote actions safer to perform at scale.

In practice, that means creating a more controlled path between the charger and the backend, rather than sending everything across the open public internet. This is where capabilities such as IPsec and Cloud Connect become important. IPsec helps create a private, encrypted tunnel for data moving between chargers and backend systems. Cloud Connect creates a trusted connection between the connectivity provider and the customer's cloud environment. Together, they help operators protect charger-to-backend communication and reduce unnecessary exposure.

That matters even more in OCPP 1.6 environments, where the connectivity layer may need to provide an additional layer of protection around charger traffic, remote diagnostics, firmware updates, and charger commands.

A strong provider should also be able to demonstrate recognised security standards, such as ISO 27001, alongside practical protections in the connectivity layer itself.

Questions to ask your provider

- How do you reduce exposure to the public internet for charger-to-backend communication?
- Do you support controlled, private communication paths such as IPsec or Cloud Connect?
- How do you help secure remote diagnostics, firmware updates, and charger commands?
- What additional protection does your connectivity model provide in OCPP 1.6 environments?
- Which recognised security standards or certifications can you demonstrate?

To learn how emnify helps secure your charge point network with a secure-by-default connectivity model, explore our connectivity security offering.

6. Integrations

Will connectivity integrate with the systems we already use?

EV charging teams do not want connectivity to sit in an operational silo.

As charging estates grow, connectivity data and management need to feed into the systems teams use every day. That may include internal management platforms, observability tools, support workflows, reporting systems, deployment tools, or automation engines. If connectivity can only be managed through a separate portal with limited integration options, it quickly becomes another source of friction.

This challenge becomes even more visible when operators work across multiple connectivity providers. Each provider may expose data differently, offer a different level of granularity, support a different API model, or surface different event types. The result is fragmented visibility and duplicated integration work. Product and engineering teams then have to normalize inconsistent data, support multiple interfaces, and build internal processes around uneven levels of control.

For charge point manufacturers, this affects how easily devices can be deployed, activated, and supported at scale. For CPOs, it affects how well connectivity can be embedded into day-to-day operations. If charger state, connectivity state, and incident data live in separate systems, teams lose time switching between tools and working around blind spots.

This is why integration should be evaluated as a core part of the connectivity model. A stronger provider should allow teams to access connectivity data and controls through the same systems they already use to monitor, troubleshoot, and operate their network.

What strong integrations should give you

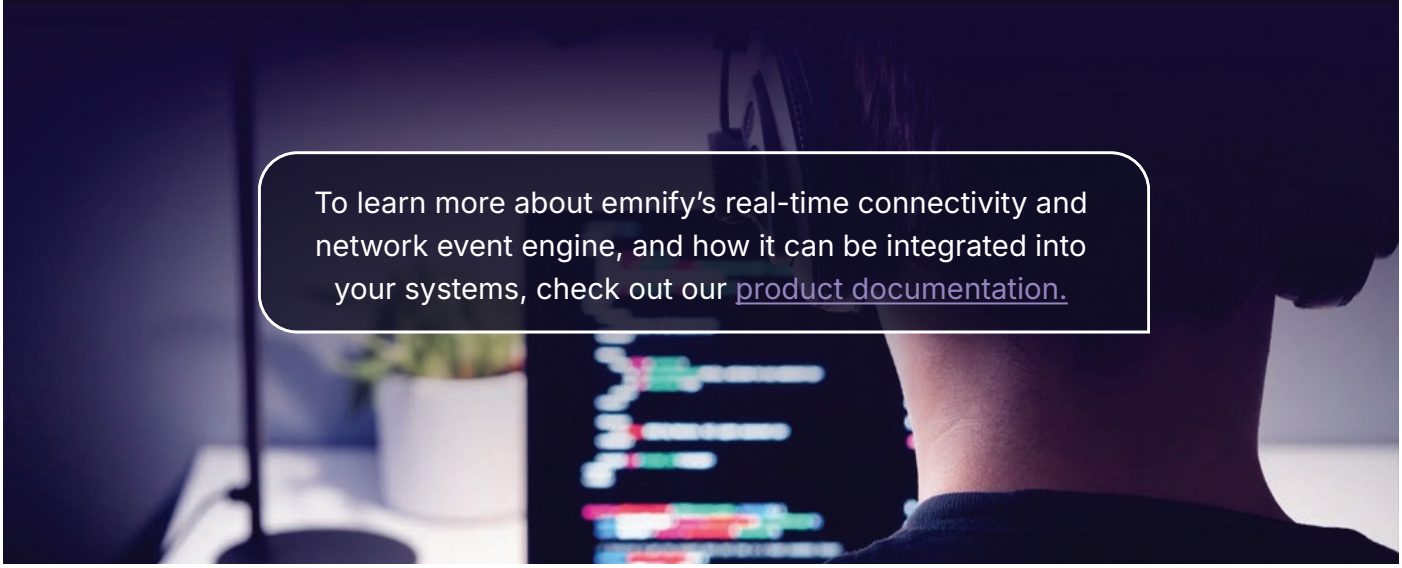
Strong integrations should give your teams one operational layer to work from, not multiple disconnected views from different operators.

In practice, that means real-time connectivity events across all supported networks, surfaced in one platform and made available through API. It also means connectivity management actions are not locked inside a portal, but can be integrated directly into the systems your teams already use every day.

That matters because as soon as connectivity data is fragmented, workflows become fragmented too. Product, engineering, and operations teams end up switching between tools, normalizing inconsistent data, and building around blind spots. A stronger model gives them one source of truth for visibility and one interface for action, making it easier to automate workflows and operate at scale.

Questions to ask your provider

- → Do you provide real-time connectivity events across all supported networks in one platform?
- → Are those same events available through API, not just in the portal?
- → Can connectivity management actions be integrated into our own systems and workflows?
- → If we work across multiple operators, how do you prevent fragmented visibility and duplicated integration effort?
- → Does your connectivity model give us one operational layer to build around, or several?



To learn more about emnify's real-time connectivity and network event engine, and how it can be integrated into your systems, check out our product documentation.

7. Future-proofing

How do we keep charger connectivity flexible and future-proof over time?

For EV charging teams, future-proofing connectivity means keeping flexibility long after a charger has been deployed. As networks expand, market conditions change, and regional requirements evolve, teams need a model that can adapt without forcing hardware changes in the field.

This is where SGP.32 becomes relevant. SGP.32 is the Global System for Mobile Communications Association (GSMA) standard for IoT eSIM remote profile management. In simple terms, it allows a device to keep the same physical SIM hardware while changing or adding operator profiles remotely over time.

That matters because it changes when connectivity decisions have to be made. Instead of locking every operator choice in at the factory or at installation, charge point manufacturers and CPOs can keep more flexibility after the charger has already been deployed.

For EV charging teams, that creates a more future-proof model for handling new regions, changing connectivity strategy, local operator requirements, and long charger lifecycles.

The SGP.32 opportunity for charge point manufacturers

One SKU for scaling deployments

For charge point manufacturers, the opportunity is clear. Chargers can leave the factory with a bootstrap profile already in place, giving them a live starting point for connectivity from day one. From there, connectivity can evolve over time by adding new operator profiles as requirements change, creating a far more flexible manufacturing model.

Instead of building different SIM strategies into different hardware variants, charge point manufacturers can work toward a single SKU and make connectivity more of a software decision. That reduces SIM logistics, avoids physical SIM swapping, and makes it easier to support multiple deployment regions and customer requirements over the life of the charger.

The SGP.32 opportunity for CPOs

More options when the network strategy changes in the field

For CPOs, the opportunity is just as relevant. As chargers are deployed into different markets and site environments, SGP.32 makes it easier to change or add operator profiles without replacing hardware.

A CPO may deploy a charger at a new site and discover that the current provider profile delivers unreliable performance there. Without changing hardware or swapping SIMs, a more suitable local operator profile can be added instead. The same logic applies when entering a new region, responding to regulatory requirements, or adjusting operator strategy over time.

The advantage is the same: connectivity becomes more of a software decision and less dependent on a physical SIM change in the field.

What a strong SGP.32 model should give you

A strong SGP.32 model should give you the ability to turn SIM logistics into a software decision.

That means you are no longer tied to a piece of plastic every time connectivity needs to change. Instead of swapping SIMs, replacing hardware, or managing multiple physical variants, teams can adapt connectivity remotely as requirements evolve. That creates a more flexible, future-proof operating model for both charge point manufacturers and CPOs.

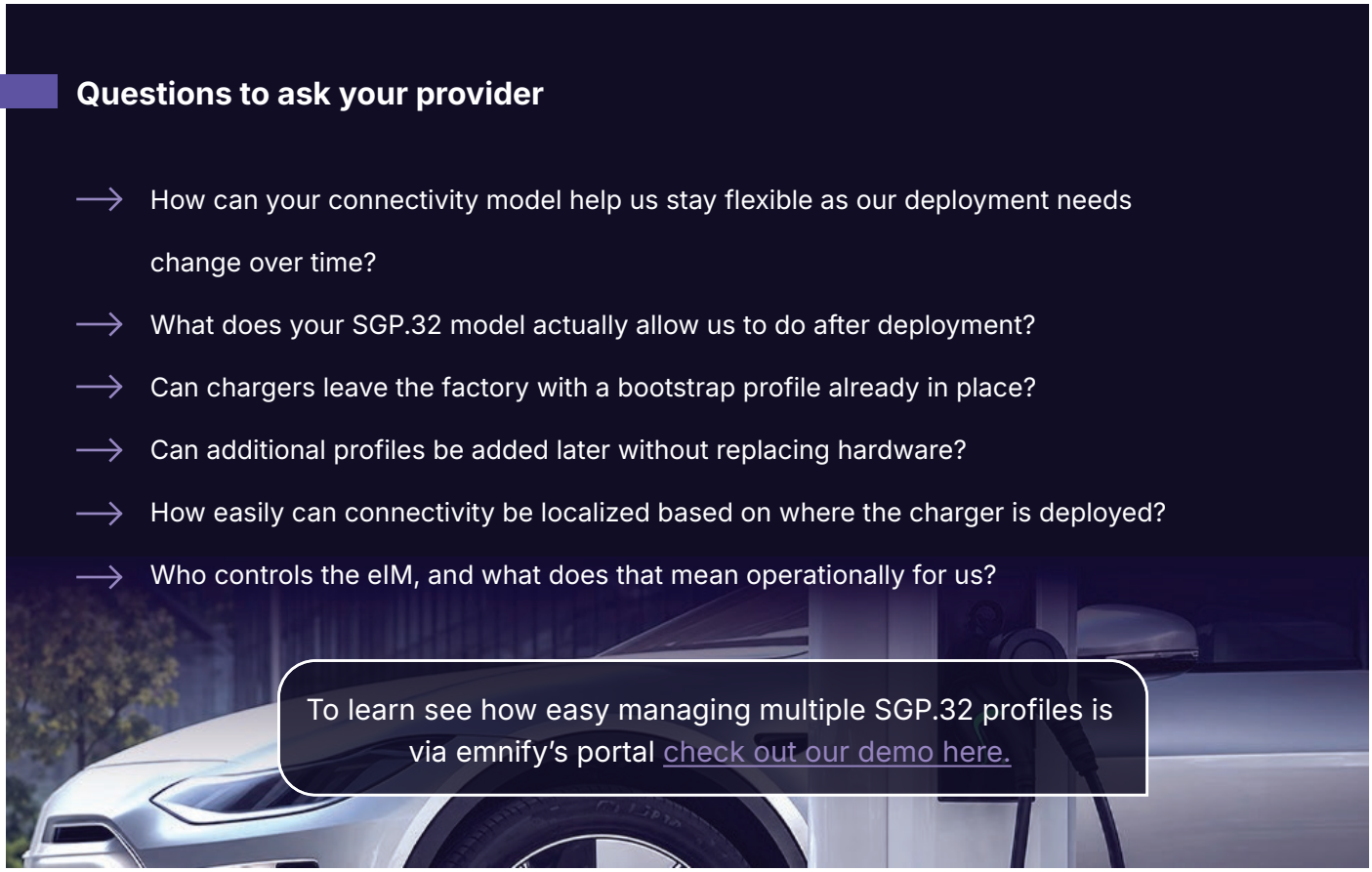
It should also be clear how that flexibility is delivered in practice. Who controls the eSIM IoT remote manager (eIM)? How are additional profiles managed? What fallback options are available? How much operational complexity is actually removed, and how much is simply moved elsewhere?

For EV charging teams, those details matter. Because the value of SGP.32 is not the standard itself. It is the operational flexibility the right implementation can unlock over the life of the charger.

stronger provider should allow teams to access connectivity data and controls through the same systems they already use to monitor, troubleshoot, and operate their network.

Questions to ask your provider

- How can your connectivity model help us stay flexible as our deployment needs change over time?
- What does your SGP.32 model actually allow us to do after deployment?
- Can chargers leave the factory with a bootstrap profile already in place?
- Can additional profiles be added later without replacing hardware?
- How easily can connectivity be localized based on where the charger is deployed?
- Who controls the eIM, and what does that mean operationally for us?



To learn see how easy managing multiple SGP.32 profiles is via emnify's portal check out our demo here.

Conclusion

In EV charging, connectivity has a direct effect on the metrics that matter most: charger uptime, successful charging sessions, rollout speed, support efficiency, payment reliability, and the customer experience. That is why it should not be evaluated as a commodity purchase or a final deployment detail.

Asking these seven questions up front helps protect your business and support future growth. They help you test whether a provider can do more than claim coverage. They show whether the connectivity model behind your network will help you stay in control as chargers scale across more sites, more regions, and more demanding operating conditions. Most importantly, they help you assess whether that model will support the customer experience your business is measured on.

The strongest providers should be able to answer yes to a clear set of outcomes:

- Coverage that works in the environments where your chargers actually operate
- Control that lets your teams act immediately, not wait on tickets
- Troubleshooting that reduces ambiguity and avoids unnecessary site visits
- Support that responds fast and understands the realities of IoT operations
- Security that protects charger-to-backend communication
- Integrations that fit into the systems your teams already use every day
- A future-proof path that keeps connectivity flexible over the life of the charger

For charge point manufacturers and CPOs alike, the goal is not to choose the simplest offer on paper. It is to choose a connectivity model that will support the business at every stage of growth.

If you want to discuss your needs, or would like a second view on where your current model is strong, where it is creating risk, and where more flexibility is possible, get in touch and let's explore where emnify can support your EV charging operations.

Get Started Today

Osprey Charging Network

[EV customer case study for credibility]

[G2 reviews for credibility]