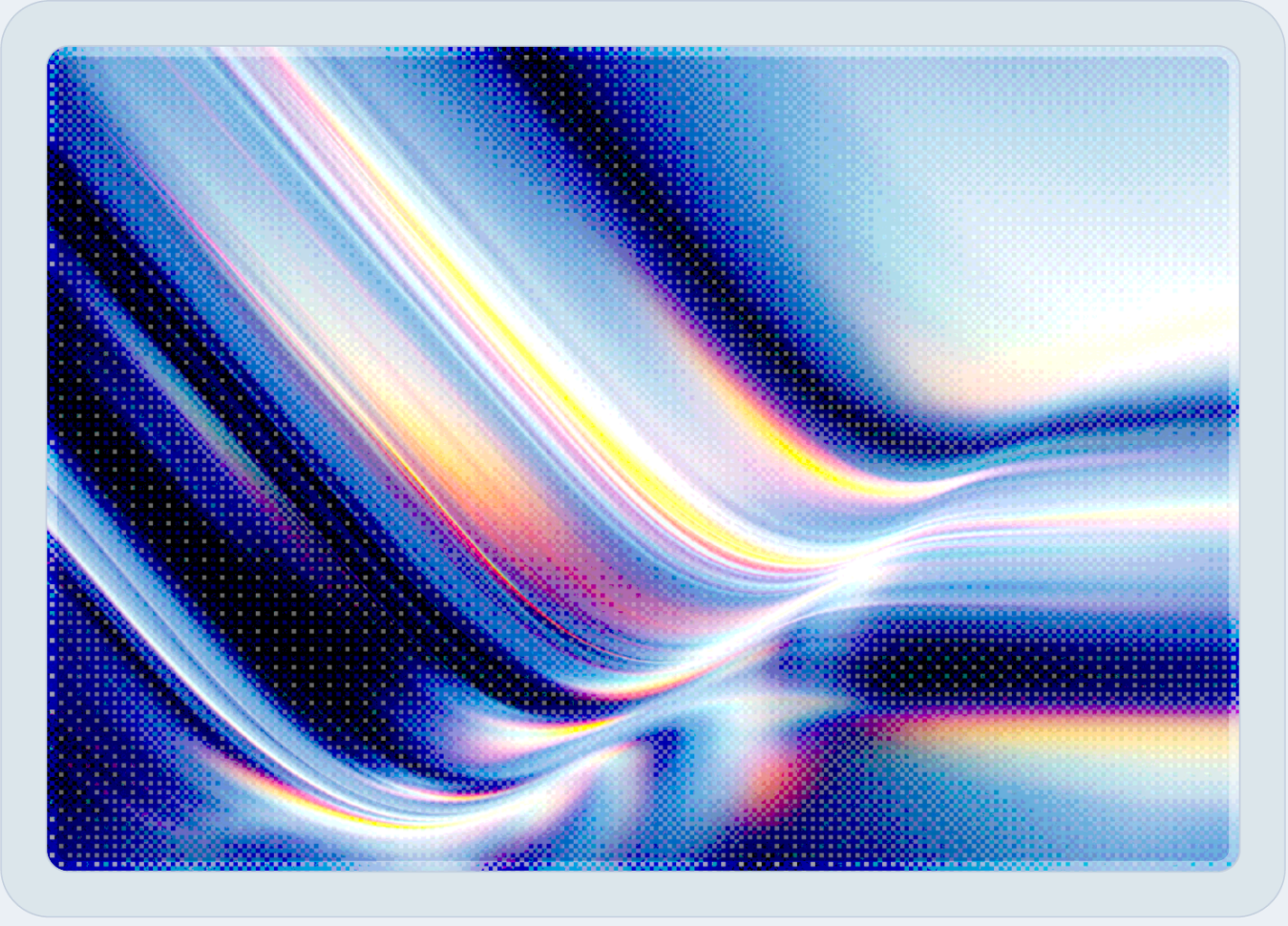
CSAI Foundation | Cloud Security Alliance

The Remote Off Switch: Vendor-Cloud Account Takeover as Fleet-Scale Physical Risk

Security Implications and Guidance for Cloud-Managed Energy, Vehicle, and Infrastructure Devices

2026-11-07

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

A large and growing population of physical assets, including rooftop and utility-scale solar inverters, home batteries, EV chargers, and passenger vehicles, accepts operational commands from a manufacturer-operated cloud. Unless devices enforce local limits, whoever controls that cloud tier can command the fleet. The vendor's identity and management plane, including the way devices authenticate to it, is therefore a primary attack surface alongside the device itself. Public research from 2024 through 2026 has repeatedly shown that the path to fleet control can run through ordinary web flaws. Examples include password-reset weaknesses in a solar monitoring portal [4], self-registration into a vehicle dealer portal [6], takeover of an employee account on a connected-car admin panel [5], and device impersonation on a cloud message broker using predictable credentials [7].

The 2022 KA-SAT incident shows the end state in practice, although it involved a satellite network operator rather than a device vendor. An attacker who reached the network's management segment issued legitimate management commands to a large number of modems at once [1], and 5,800 Enercon wind turbines in Germany lost remote monitoring and control as collateral damage [2]. Commands sent through a compromised vendor cloud are syntactically legitimate, so they are hard to distinguish from normal operations. Their physical consequence also scales with fleet size, which is why researchers have warned that coordinated manipulation of distributed generation could destabilize power grids [3].

Organizations should inventory every asset with a vendor-cloud control path, require local-autonomy and safe-state behavior when the cloud is lost, and contract for blast-radius limits on bulk commands to contain a cloud that turns hostile. Policy is beginning to move in the same direction. Lithuania has restricted vendor remote access to energy assets, and the European Commission has proposed a framework for designating high-risk suppliers to critical infrastructure [11][12].

Background

Traditionally, a command to stop a generator, open a breaker, or disable a vehicle came from local operators or from within a segmented control network. That model no longer describes a large and growing class of devices. Residential and commercial solar inverters, battery storage systems, EV chargers, heat pumps, and connected vehicles are typically sold with a manufacturer-hosted cloud service that provides monitoring, firmware updates, remote configuration, and in many cases direct

operational control. The device keeps an outbound connection to that cloud, so traffic passes customer firewalls without any inbound exposure. The vendor's backend becomes a single point of command for every unit in the field.

This architecture creates a hierarchy of authority that is often not documented for the asset owner. At the bottom sits the owner's consumer account, which can usually start, stop, or reconfigure that owner's devices. Above it sit installer and dealer accounts, which often manage hundreds or thousands of customer sites. Above those sit vendor support and administrative consoles, the firmware distribution pipeline, and the device-identity infrastructure (often an MQTT broker) that decides which messages a device will trust. Each tier carries more authority than the one beneath it, and compromising a tier effectively compromises everything that tier can command.

This note does not ask whether individual connected devices have vulnerabilities, which is well established. It asks what happens when the vendor cloud itself becomes the attacker's tool. The distinction matters because controls that protect against single-device compromise, such as network segmentation at the customer site, do little against a command that arrives over an allowed outbound channel from a trusted vendor. The same architecture also exposes owners to disablement without any attacker, when a vendor changes policy, enforces a commercial restriction, or exits a market. Both cases have the same root cause: physical operation depends on a remote party whose control the owner cannot verify or limit.

Security Analysis

Paths to the Switch

Public incidents and research cluster into three paths to fleet control through a device vendor's cloud, each exploiting a different tier of the authority hierarchy. The first path is account takeover at the customer or partner tier. In its March 2025 SUN:DOWN research, Forescout Vedere Labs disclosed 46 vulnerabilities across Sungrow, Growatt, and SMA, three of the top ten solar inverter vendors [3]. For Growatt, the researchers described a cloud-based takeover in which unauthenticated endpoints allowed an attacker to enumerate usernames, reset account passwords to a default value, and retrieve other users' plant and device information [4]. The automotive sector has shown the same pattern. In 2024, Sam Curry and colleagues found that registering an account on Kia's dealer portal gave access to backend dealer APIs that could map a license plate to a vehicle and then issue commands such as unlock and start [6].

The second path targets the vendor's own administrative tier. In research published in January 2025, Curry and Shubham Shah reported an arbitrary account takeover flaw affecting a Subaru employee account on the STARLINK admin panel. The flaw allowed them to remotely start, stop, lock, and unlock target vehicles and to retrieve location history [5]. A single employee identity carried fleet-wide authority. Neither the Kia nor the Subaru flaw was reported as exploited maliciously, and both were fixed. Each nevertheless showed that a web-tier identity weakness translated directly into physical control of vehicles at scale.

The third path skips accounts entirely and attacks the trust between devices and the vendor's messaging and update infrastructure. On March 4, 2026, the German security firm Jakkaru published research on APsystems EZ1-M microinverters showing that the devices authenticated to a cloud MQTT system using static keys derived from sequential, predictable serial numbers [7]. By impersonating a legitimate device, the researchers used retained messages to push malicious firmware and showed they could take full control of an inverter, including selectively and simultaneously shutting down systems. pv magazine reported that roughly 100,000 vulnerable devices were reachable online and that the vendor has since deployed unique per-device credentials and signature verification [7]. Jakkaru also reported using AI models to help reverse-engineer the firmware [7], an early indication that the cost of discovering such flaws may be falling. A related pattern appeared in July 2026, when the Chaos Computer Club reported a vulnerability in older Hoymiles HM-series microinverters and criticized devices that accept over-the-air firmware updates without authentication. Hoymiles said it would release a firmware update and stated that its current product portfolio is not affected [13].

A fourth case widens the frame. The KA-SAT incident involved a network operator's management plane rather than a device vendor's cloud. It is still the closest public example of commands that were legitimate in form being issued maliciously to a device fleet at scale, and it is discussed further below. The table below summarizes the three vendor-cloud paths alongside this analogous case.

Path	Tier compromised	Public example	Demonstrated capability
Customer/partner account takeover	Owner, installer, or dealer accounts	Growatt cloud (2025) [4]; Kia dealer portal (2024) [6]	Hijack accounts and control associated devices; start and unlock vehicles
Vendor administrative takeover	Employee and support consoles	Subaru STARLINK admin panel (2025) [5]	Start, stop, lock, unlock, and track vehicles

Path	Tier compromised	Public example	Demonstrated capability
Device impersonation and unauthenticated device channels	Cloud broker, device identity, and firmware update path	APsystems MQTT (2026) [7]; Hoymiles HM series (2026) [13]	Push firmware; selectively and simultaneously shut down inverters
Analogous case: management-plane compromise	Network operator's management segment	KA-SAT (2022) [1][2]	Issue legitimate commands to many devices simultaneously, damaging them

From Single Device to Fleet: Why the Physical Risk Scales

The KA-SAT incident is the clearest public example of a management-plane compromise carried out in practice. According to Viasat's overview, an attacker exploited a misconfigured VPN appliance to reach the trusted management segment of the KA-SAT network. Beginning on 24 February 2022, the attacker used that access to execute legitimate, targeted management commands on a large number of residential modems simultaneously, overwriting flash memory and knocking tens of thousands of previously active modems offline [1]. SentinelLabs analyzed the AcidRain wiper used against the modems and reported that 5,800 Enercon wind turbines in Germany could no longer communicate for remote monitoring or control [2]. In May 2022, the EU and its member states attributed the KA-SAT cyberattack to the Russian Federation [19]. Two lessons transfer directly to vendor clouds. First, the commands were legitimate in form, which defeats detection approaches that look for malformed traffic. Second, the damage persisted on the endpoints: some modems were restored with over-the-air updates, but Viasat shipped tens of thousands of replacement units where those updates were insufficient [1].

The physical consequence of a vendor-cloud compromise grows with the size and type of fleet. A single hijacked inverter primarily affects its owner, but distributed generation is aggregated across hundreds of thousands of sites. Forescout's analysis warned that coordinated load-changing attacks against such fleets could trigger emergency grid measures, disconnections, or blackouts [3]. Forescout also noted that 53% of solar inverter manufacturers and 58% of storage system providers are based in China [3]. During political debate, a European Parliament member put the share of EU-imported PV inverters that are Chinese at 80% [12]. These figures describe manufacturer origin rather than cloud concentration. Combined with market-share concentration among the largest vendors, however, they suggest that a limited number of vendor clouds may hold command authority over a substantial share of a region's distributed energy resources.

The same reasoning applies beyond energy. In vehicle fleets, the immediate risks are theft, stalking, and immobilization rather than grid effects. In commercial EV charging networks, a fleet-wide stop affects mobility services as well as individual owners, as the roughly 25,000 commercial JuiceBox chargers that Canary Media described as effectively bricked after their vendor's exit illustrate [9].

Non-Adversarial Disablement Uses the Same Switch

The remote off switch does not require an attacker. In November 2024, Deye-branded inverters in the United States, including Puerto Rico, displayed a message stating the unit was not allowed for use in that country and stopped operating. Heise reported that Sol-Ark said the affected units were Deye-branded devices sold outside authorized channels, while Deye denied remotely controlling the devices [8]. The cause remains disputed, and this note does not attribute it. The episode nevertheless showed owners discovering, after purchase, that a remote party could plausibly render their generation equipment inoperable. Similarly, when Enel X Way exited the North American market in October 2024, home JuiceBox chargers continued charging but lost connectivity-dependent features. Commercial stations, by contrast, were expected to stop working entirely once software support ended. Canary Media estimated that roughly 125,000 chargers were affected, about 25,000 of them commercial units [9].

The contrast within the JuiceBox case is instructive for design. Units built to fall back to local operation degraded gracefully, while units whose basic function depended on the cloud failed outright. The Enercon turbines in the KA-SAT case likewise lost remote monitoring and control, but the company said they continued operating in automatic mode [2][20]. Local autonomy in a safe state is therefore a security property, not merely a reliability feature, because it bounds the damage from losing the cloud, whether through an attack, a business decision, or a bankruptcy. It does not, however, contain a cloud that remains connected but hostile. The APsystems firmware push [7] and the KA-SAT flash overwrite [1] would not have been prevented by local fallback, and containing that threat requires the additional controls described in the Recommendations, such as signed commands and limits on bulk actions.

Undocumented Control Channels and the Policy Response

A further complication is that owners may not know every path by which a device can be commanded. In May 2025, Reuters reported, based on two unnamed sources, that undocumented communication devices had been found in some Chinese-made solar inverters. One source said that over the past nine months, undocumented communication devices including cellular radios had also been found in some batteries from multiple Chinese suppliers [10][21]. Reuters was unable to determine how many units had been examined, and a Chinese embassy spokesperson rejected the characterization [10]. If confirmed at scale, such channels would undermine the common mitigation of controlling a device's network egress,

because a cellular path bypasses the site firewall entirely. This remains a report rather than an established, generalized fact. It does, however, strengthen the case for verifying communications hardware during procurement.

Policy has begun to treat vendor remote access to energy assets as a distinct risk. In November 2024, Lithuania's parliament adopted legislation restricting remote access to solar, wind, and storage installations above 100 kW by entities from countries deemed national security threats, including China, without banning the equipment itself [11]. In January 2026, the European Commission proposed a revision of the EU Cybersecurity Act that would establish a framework for designating high-risk ICT suppliers to critical infrastructure. In presenting it, Executive Vice-President Henna Virkkunen cited dependency on a limited number of solar inverter suppliers as a significant security risk [12]. These measures focus on supplier nationality. The incidents above, which involve Korean, Japanese, German, and Chinese vendors, suggest that the underlying exposure exists regardless of where the vendor is headquartered: a vendor cloud with unbounded fleet authority.

Recommendations

Immediate Actions

The first priority is visibility into which physical assets can be commanded from outside the organization. Many organizations have deployed inverters, chargers, building systems, or fleet vehicles without recording that each one is controllable through a vendor portal. The steps in this section are designed to be achievable in the near term.

Organizations should begin by inventorying every asset with a vendor-cloud control path and recording which accounts (owner, installer, integrator, vendor support) hold command authority over it. With that inventory in hand, they should enforce phishing-resistant multi-factor authentication on every vendor portal account that supports it, and document the portals that do not support MFA as accepted risks. Dormant installer and integrator accounts deserve particular attention, because they may retain authority long after commissioning and should be removed or disabled.

Two further actions establish how each asset behaves when the vendor relationship fails or is abused. Organizations should test whether each asset class continues operating in a safe state when cloud connectivity is severed, and record the results. Testing should take place in a controlled test environment or a scheduled maintenance window, coordinated with the vendor and, for grid-connected assets, with

the interconnecting utility where required. In parallel, organizations should ask each vendor in writing whether its support staff can issue commands to customer devices, how that access is authenticated, and whether customers are notified when it is used.

Short-Term Mitigations

Over the next one to two quarters, organizations should turn these findings into procurement and architecture requirements. Device identity should rest on unique per-device credentials, never on serial numbers or other enumerable values. Firmware and operational commands should be cryptographically signed so that a compromised broker cannot forge them, and the APsystems remediation illustrates this change [7]. Contracts should require vendors to enforce rate limits and blast-radius caps on bulk commands, apply multi-party approval to fleet-wide actions, and expose a command audit log the customer can retrieve. Where the asset's function allows it, owners should prefer equipment that offers a documented local-control mode and an owner-controlled setting that disables remote operational commands while preserving telemetry.

Network controls complement these contractual measures. Outbound connections from devices should be restricted to documented vendor endpoints, and anomalous egress should be monitored. For high-consequence assets, procurement should include a hardware review for undocumented radios, given the reporting described above [10][21]. Security operations teams should also bring vendor-portal sign-in events and configuration changes into their monitoring scope where vendors expose them, because a takeover of an installer account will otherwise be invisible to the asset owner.

Strategic Considerations

At the strategic level, organizations should treat each device vendor's cloud as a critical third party whose compromise has physical consequences, and assess it as rigorously as they assess cloud infrastructure providers. Tabletop exercises should include a "hostile vendor cloud" scenario in which every device from one manufacturer receives a shutdown or unsafe configuration at the same time, and should test how long manual recovery would take. The KA-SAT experience indicates that recovery from endpoint-level damage can require physical work or hardware replacement at many sites [1][2]. The exercise should therefore measure truck rolls and spare inventory, not just backend restoration.

Utilities, grid operators, and regulators should consider aggregate exposure across vendors rather than only supplier nationality. A useful metric is the share of regional distributed capacity that any single vendor cloud can command. That metric can be paired with per-device ramp-rate limits and backend-enforced caps on how much aggregate capacity any single command or operator can move within a given interval. End-of-life risk also deserves contractual attention. Purchasers of long-lived assets should

seek commitments covering local-operation fallback, transfer of control on vendor exit, and documentation sufficient for a third party to operate the fleet, a need the JuiceBox case illustrates [9]. Finally, if AI-assisted reverse engineering continues to lower the effort required to find device-identity flaws, as the APsystems research suggests [7], organizations should anticipate more frequent disclosures and plan accordingly.

CSA Resource Alignment

CSA's Zero Trust Guidance for IoT [14] directly addresses the problem described here. Its five-step methodology begins with defining the protect surface and mapping transaction flows, and it can be applied to vendor-cloud control. In that setting, the protect surface is the device's operational function, and the transaction flow that most needs mapping is the command path from vendor backend to device. The guidance's emphasis on continuous authentication, least privilege, and device criticality tiers supports this note's recommendations to remove standing installer authority and to require per-device credentials for high-criticality assets.

The Zero Trust Guidance for Critical Infrastructure [15] addresses secure remote access to OT and ICS environments. Its remote-access principles can be extended to distributed energy resources once their aggregate capacity becomes grid-relevant, which makes it a relevant reference for utilities evaluating whether vendor clouds should hold operational authority over generation assets at all. CSA's 2026 Zero Trust Guidance for Achieving Operational Resilience [16] covers enterprise, cloud, OT, and supply chain environments. It provides the testing methods and resilience metrics needed for the "hostile vendor cloud" tabletop exercise and for measuring recovery time after fleet-wide disablement.

For control selection, the IoT Controls Matrix v3 [17] provides 198 controls for enterprise IoT systems, including identity and access management controls and a new incident management domain, which map to the procurement requirements in this note. For the vehicle cases, CSA's Observations and Recommendations on Connected Vehicle Security [22] remains the organization's dedicated connected-vehicle publication. It dates from 2017 and predates the dealer-portal and admin-panel research discussed above, but it offers a baseline for assessing vehicle connectivity. Where vendor platforms embed AI-driven energy management or agentic automation that holds cloud credentials, the AI Controls Matrix (AICM) v1.1 [18] provides identity, supply chain, and third-party assurance controls that apply to those components. Organizations can also use STAR-style questionnaires (CAIQ) to request structured assurance evidence about vendors' cloud management planes.

References

[1] Viasat. "KA-SAT Network cyber attack overview." Viasat, March 2022.

[2] SentinelLabs. "AcidRain: A Modem Wiper Rains Down on Europe." SentinelOne, March 2022.

[3] Forescout. "Forescout Vedere Labs Uncovers Severe Systemic Security Risks in Global Solar Power Infrastructure." Forescout, March 27, 2025.

[4] The Hacker News. "Researchers Uncover 46 Critical Flaws in Solar Inverters." The Hacker News, March 2025.

[5] Sam Curry. "Hacking Subaru: Tracking and Controlling Cars via the STARLINK Admin Panel." samcurry.net, January 2025.

[6] Sam Curry. "Hacking Kia: Remotely Controlling Cars With Just a License Plate." samcurry.net, September 2024.

[7] Marian Willuhn. "AI-enabled hacks expose remote shutdown risk in microinverters." pv magazine, April 7, 2026.

[8] heise online. "Photovoltaics: Deactivated Deye and Sol-Ark inverters in the USA." heise, November 2024.

[9] Canary Media. "Enel X Way abandoned its US EV charging customers. What happens next?." Canary Media, October 23, 2024.

[10] pv magazine. "Hidden devices found in Chinese-made inverters in the US, reports Reuters." pv magazine, May 14, 2025.

[11] pv magazine. "Lithuania bans remote Chinese access to solar, wind, storage devices." pv magazine, November 18, 2024.

[12] pv magazine. "EU to ban Chinese inverters? Commission proposal in cybersecurity mulls high-risk vendors list." pv magazine, January 20, 2026.

[13] pv magazine. "Hoymiles issues response after security vulnerability identified in older microinverters." pv magazine, July 13, 2026.

[14] Cloud Security Alliance. "Zero Trust Guidance for IoT." CSA Zero Trust Working Group, 2025.

[15] Cloud Security Alliance. "Zero Trust Guidance for Critical Infrastructure." CSA Zero Trust Working Group, 2024.

[16] Cloud Security Alliance. "Zero Trust Guidance for Achieving Operational Resilience." CSA Zero Trust Working Group, 2026.

[17] Cloud Security Alliance. "IoT Controls Matrix v3." CSA IoT Working Group, April 2022.

[18] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2025.

[19] Council of the European Union. "Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union." Council of the EU, May 10, 2022.

[20] Saur Energy. "Loss of control over Enercon Wind turbines due to satellite outage highlights cyber risks." Saur Energy International, March 2, 2022.

[21] Reuters (via Insurance Journal). "Rogue Communication Devices Found in Chinese Solar Power Inverters." Insurance Journal, May 16, 2025.

[22] Cloud Security Alliance. "Observations and Recommendations on Connected Vehicle Security." CSA IoT Working Group, May 2017.