Cybersecurity Technical Overview

March 2025
V1.2

1.63MW Venco Campus Netherlands
Installed by Alius Energy

The Growing Threats to the Global Energy Sector

In today's interconnected world, the energy sector stands out as a prime target for cyber threats stemming from multiple sources. Such threats range from financially-driven schemes executed by cyber criminals to politically motivated attacks orchestrated by nation-states.
In 2024 alone, cyber-hacking victims worldwide (from all sectors) paid out $814 million following ransomware attacks - and that's just what was reported.*

2019

A Utah-based renewable energy provider was hit by a cyber attack that caused site downtime due to a vulnerability in Cisco firewalls.

Source

2023

Denmark's critical infrastructure experienced the largest cyber attack in its history, with 22 solar energy companies breached in just a few days, due to a vulnerabilty in Zyxel firewalls.

Source

2024

Pro-Russian hackers launched an attack on Lithuanian solar energy sites via its PV monitoring software. The hackers targeted hospitals and military academies, deleting sensitive data and demanding ransoms to cease the attack.

Source

Unsecured PV systems pose critical business risks

Solar power is a fast-growing component of the global energy mix, constituting a significant part of the total energy production for numerous countries such as the Netherlands, Germany, and the US. It's already a critical power source that helps lower electricity costs and ensure business continuity for many companies. While offering sustainable energy solutions, PV systems also introduce new avenues for cyber threats. At the heart of each system is the inverter, an Internet of Things (IoT) device that is usually connected to the Internet to enable system monitoring and control. This makes it much more susceptible to cyberattacks compared to a well-shielded gas or coal power station.

Solar is used to power an increasing number of on-site energy loads such as batteries, EV chargers, and HVAC systems, and this will be increasingly the case as we transition to the age of energy management systems. An unsecured PV system not only threatens business continuity but can also serve as an unwitting gateway for hackers to access energy loads as well as an organization's wider digital platforms, causing further material, financial, and reputational damage.

Common cyber risks include:

Data leak and penalties

Hackers can take advantage of vulnerable PV systems to steal private data residing on an organization's internal networks resulting in a data breach that forces the victim to pay hefty fines.

Remote control and Denial-of-Service (DoS)

When a business falls victim to DoS attacks or remote-control breaches, it faces significant disruptions. Ransomware can hold critical data hostage, while remote control and DoS attacks and breaches may bring essential services to a complete standstill.

Compliance exposure

As new cyber regulations are introduced, PV site owners must take proactive measures to ensure their systems remain compliant and avoid the risk of product recalls or financial penalties if their networks are compromised.

* https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025

SolarEdge Cybersecurity Overview

Your security is at the core of our business

SolarEdge is a one-stop shop for solar power, selling inverters, Power Optimizers, and cloud-connected system monitoring solutions to residential and commercial customers worldwide, serving millions of end users. From SolarEdge's very first product right up until our current offering, cybersecurity has been a central component of SolarEdge product development and future roadmaps, evolving with the latest technology and ever-evolving cyber threats. We strive to keep our customers constantly protected by implementing advanced cybersecurity measures at every step of our product and system architecture design, through to coding and testing.

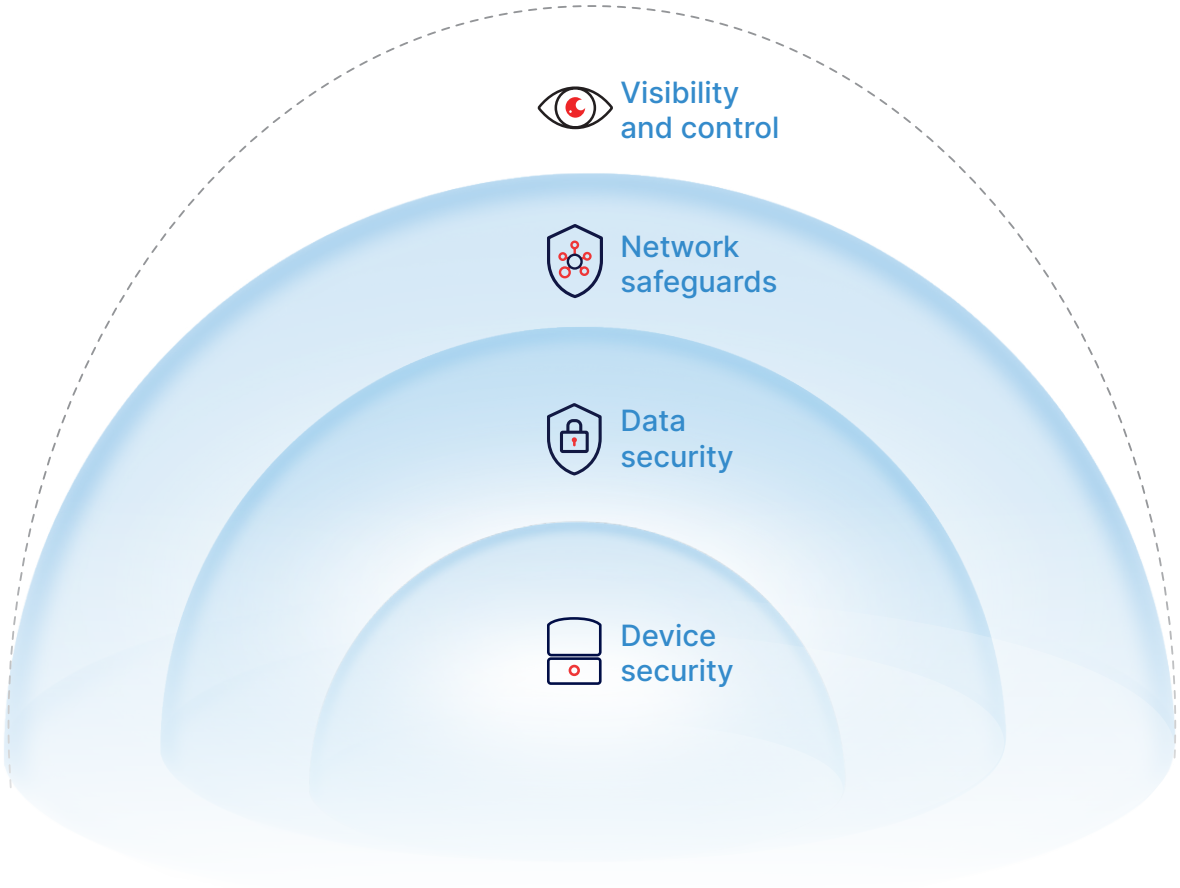
Just like PV safety, PV cybersecurity is non-negotiable

Similar to team sports, cybersecurity requires a collaborative and cross-disciplinary effort to succeed. Each product's security is only as good as the security of the company that manufactures it and administers its operations. Led by a dedicated team of cyber experts, SolarEdge works hard to maintain our position at the forefront of PV cybersecurity.

Internet-connected products must also remain ahead of regulatory requirements to ensure that its cybersecurity solutions are standardized and harmonized with the latest requirements of the relevant regulatory bodies. By actively participating in various cyber-related technical committees, SolarEdge can be sure that our product design is aligned with upcoming regulations, and that our devices comply with the latest cyber reference guides and DER cybersecurity standards.

SolarEdge's product security approach

We have developed a holistic four-pillar approach that considers all aspects of product security and is detailed in the following sections of this document:



As regulations in this important field evolve, SolarEdge maintains active engagement with relevant standards and regulations worldwide, as outlined in Chapter 3: Standards Certifications and Regulatory Compliance.

Contents

1. Document Scope

The purpose of this document is to provide SolarEdge customers and system owners with a comprehensive overview of SolarEdge's cybersecurity design and implementation.
SolarEdge cybersecurity measures follow the principles presented in:

- The European Union's Radio Equipment Directive (RED) Article 3.3
- The European Union's NIS2 regulation
- The European Union's Cyber Resilience Act
- ETSI-303-645: Cyber Security for Consumer Internet of Things
- ENISA cybersecurity guidelines and reporting requirements
- UL-2941: Standard for Cybersecurity of Distributed Energy and Inverter-Based Resources
- NIST IR 8498: Cybersecurity guidelines for Smart Inverters
- IEEE 1547.3: Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
- FCC's "U.S. Cybersecurity Labeling Program for Smart Devices"
- NARUC/NASEO Cybersecurity Baselines for Electric Distribution Systems and DER
- ISO-27001 (2022): Information security, cybersecurity and privacy protection — Information security management systems – Requirements
- OWASP (for application security)
- Secure software development best practices, such as IEC 62443-4-1

A full list of certifications, compliance and associated declarations is provided in Chapter 3: Standards Certifications and Regulatory Compliance.

1.1. Products in scope

The following SolarEdge products are included in the scope of this document:

- Residential inverters
- Commercial inverters
- SolarEdge TerraMax™ Inverter
- SolarEdge web and mobile applications
- SolarEdge API and grid services
- SolarEdge ONE Controller for C&I
- SolarEdge ONE Controller for Residential

Throughout this document, the security features and capabilities described are assigned to the "Gateway Device":

- In installations where a single inverter is installed, the Gateway Device is embedded within the electronics of the inverter itself, and its communication board
- In sites where several inverters are skidded or connected in a leader-follower set-up; the leader inverter typically acts as the sole Gateway Device. As such, it manages the cybersecurity aspects of all external communications from the system to the backend, over the internet. In specific cases, other installation topologies are supported to accommodate bespoke needs
- In C&I installations managed by the SolarEdge ONE for C&I platform, the SolarEdge ONE Controller may act as a gateway device

SolarEdge Power Optimizers, batteries and smart devices such as switches, meters and water heaters are excluded from the scope of this document as they are not directly accessible from the internet and rely on the Gateway Device for cybersecurity. According to customer needs, EV chargers can be separately connected to the internet. We recommend doing so under a dedicated VLAN.

Legacy systems: Products manufactured prior to 2020 might include lesser capabilities than the ones described in this document.

2. SolarEdge Product Security

The following is an illustration of a typical SolarEdge C&I system, highlighting the four pillars that combine to protect our products from cyber threats (device security, data security, network safeguards, visibility and control). The subsequent sections of this chapter drill down into the various features that constitute this holistic approach to SolarEdge cybersecurity. In addition to this example below, local connection is also possible for commissioning and configuration.

Additional illustrations of a typical SolarEdge system with the TerraMax inverter and a typical SolarEdge residential site, can be found in this document's Appendix.

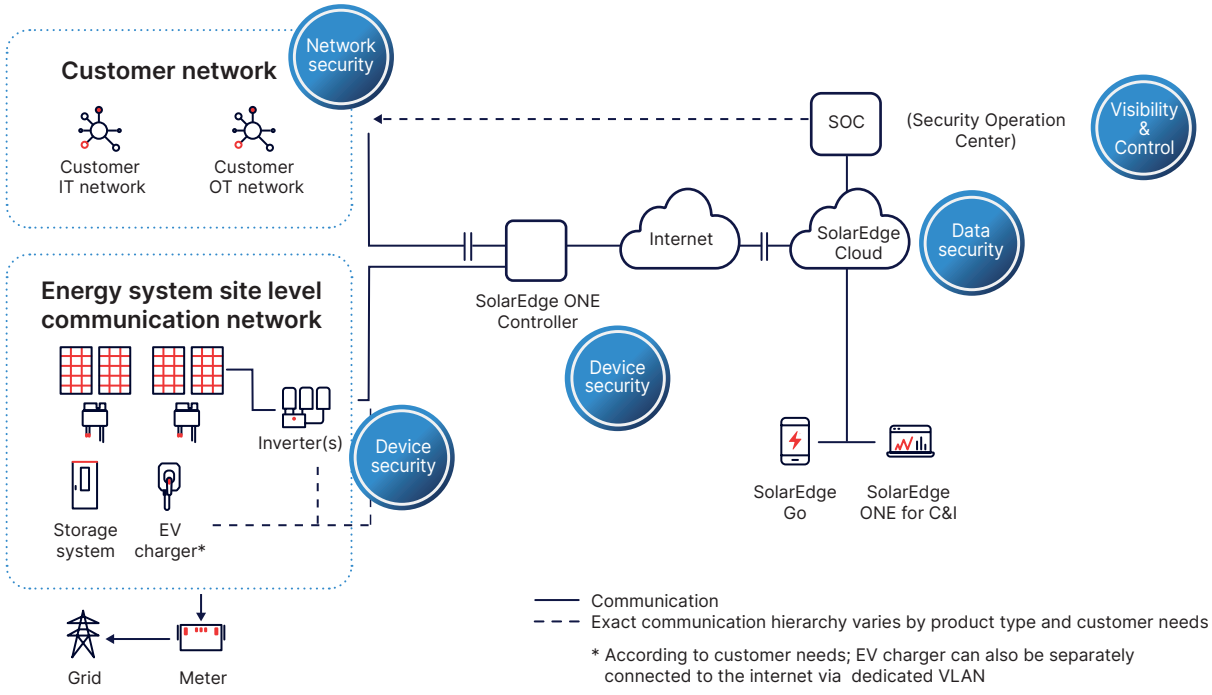


Figure 1: Diagram of typical C&I system outlay in steady state operations

2.1. Device security

SolarEdge device security is based on periodic threat analysis exercises and risk assessments, ongoing internal manual and automated code scanning and design reviews as well as on annual penetration testing cycle, performed both internally and by third-party auditors.

2.1.1. Access controls

Inverter Product activation

- Each SolarEdge inverter comes with its own unique Wi-Fi access password which is generated using strong randomization algorithms and is handled as protected information from the assembly line stage. This provides security by design for sites, and eliminates the risks involved with default password use, while maintaining a quick and foolproof installation process
- Customers can view a product's unique Wi-Fi access password on the physical label printed on each device
- The strong unique machine-generated password is supplemented by a physical access requirement during the initial product commissioning
- Activation of a SolarEdge product during commissioning can only take place by owners of a SolarEdge installer account that have completed SolarEdge's installer onboarding
- Users must be logged in to their account via the mobile app, to activate a SolarEdge product during commissioning
- Only when the user meets the following three verification factors, can they activate the product:
  - Logged in as an installer
  - Unique password is known
  - Has physical access to the device
- When a user or installer connects to the inverter's secure Wi-Fi access point, their role and permissions are verified by validating a time-limited token provided by the connecting entity.
- For inverters in sites without internet access, installers must log in before leaving areas with connectivity. They will remain logged in for a time-limited period. Once connectivity is restored, the installer will associate themselves with the device's serial number and site to finalize the process.
- During a successful activation, an initial key exchange is performed between a deployed system and the central SolarEdge monitoring system. This exchange provides a strong initial level of authentication, without the need for user-generated or memorized passwords.
- For the ONE Controller, a dedicated Wi-Fi access point is used for setup and commissioning and there is a separate secure commissioning and activation process.

Remote access controls

- Users and installers must use SolarEdge's dedicated, limited interfaces to access and manage the device. A strict set of roles and permissions (RBAC) is enforced allowing different permissions for system owners, installers, support personnel, etc.
- In cases where third parties such as local utilities require access to data generated by the device, a "View Only" mode can be enabled, providing limited "Read only" access to the inverter's status and configurations. To obtain this access, users must have physical access to the device, and knowledge of its unique Wi-Fi password
- Any remote access is only via SolarEdge and approved technology partner applications, i.e. through the SolarEdge cloud and after proper authentication by the relevant SolarEdge platform and is based on unique credentials
- To log in, installers are required, at a minimum, to use their unique credentials. Additional identification methods utilize the installer's device and include biometric options (such as facial recognition or fingerprint scanning), as well as PIN codes and pattern-based authentication
- Users' passwords follow best practices for password complexity which are periodically updated. The password complexity requirements consider NIST 800-63-B guidelines.
- Application access or user browsing communication is over TLS 1.2+ (HTTPS) connection (transitioning to TLS 1.3+)
- SolarEdge proactively monitors for leaked installer passwords, system owner monitoring portal credentials and other potential indicators of a compromised system
- Any access attempt to the device is logged and monitored

Coming soon in 2025:

- MFA for installer accounts
- SSO and federated SSO for installer and large accounts
- SAML2 compatible authentication

Local network access control

SolarEdge inverters are designed to support fast, functional and secure local installation for SolarEdge installers, including the configuration of network parameters for Wi-Fi connection. During installation, before the Gateway Device is configured, the installers use a dedicated secured Wi-Fi channel between the SolarEdge installation app and the SolarEdge installed system (as the access point). This secured Wi-Fi channel is based on the following principles:

- The device acts as a local Wi-Fi access point to the SolarEdge installer application
- The Wi-Fi host channel is closed by default
- Wi-Fi connectivity is activated only when needed to facilitate designated tasks, and is turned off right after to minimize signal detection by individuals in proximity
- To turn on the Wi-Fi signal again, users and installers are required to press a physical button located on the device (see Figure 2)

To establish Wi-Fi connection, move the inverter red ON/OFF/P switch to "P" position, and release within 2 sec.

Move and release

Figure 2: Schematic of the Wi-Fi signal button

- At all other times, the devices' Wi-Fi access point is not operational and casual Wi-Fi scanning will not reveal the Gateway's access point
- Secured access:
  - Each Gateway has a unique Wi-Fi password of 8 bytes
  - The Wi-Fi encryption protocol is WPA2
  - Wi-Fi LAN communication is implemented with security-related best practices for strong authentication (802.1x) and encryption algorithms (WPA2-PSK with 128-bit AES keys)
- SolarEdge ONE Controller uses a separate secure mechanism for local access

Physical access control for inverters

SolarEdge's security approach assumes that the system owner handles the inverter the same way a breaker box would be, in providing basic physical protection from an unauthorized person who may attempt to physically access the hardware or penetrate the LAN. While local access is considered a low likelihood attack vector, the device still implements some protections such as closing all debug ports, secure boot, secure storage mechanisms and other device level protections. In addition, the product local connectivity architecture assumes integration of various energy devices (SolarEdge and other third-party devices) and supports secured connectivity.

The architecture is based on the following security principles:

- Wired connectivity preferred over wireless communication, where available
- Physical access security:
  - All unused interfaces (services/ports) of the Gateway Device and inverters are disabled. Only specified, protected ports are open to communication, allowing access to pre-determined, secure services
  - Debug Ports are closed
  - Physical anti-tamper mechanisms, including aluminum casings with specialized hex screws
- When connectivity over a physical distance is required:
  - Wi-Fi can be used instead of Ethernet
  - A short-range radio communication is used
  - The short-range radio communication is based on Thread© protocol following strict security requirements. This enforces proximity to the Gateway to initiate access and establish a secure connection
  - SolarEdge uses this secure link to transmit periodic telemetry data from the Gateway and other onsite SolarEdge equipment. This link is also used for provisioning and software update purposes

  - The short-range wireless communication is encrypted and designed to ensure that the interruption of communication between devices within a single site will not interrupt equipment outside of that installation
  - Unauthorized devices cannot access the established networked and share communication with the connected devices
- Devices do not support the automatic discovery and connect capabilities such as those provided by UPnP, thus preventing the establishment of unauthorized and unknown connections. They must be manually paired
- Input validation – data sent from any connected devices to any other device is scanned and verified including by the Gateway Device
- Limited access to local devices – monitoring, configuration and version updates are performed through the Gateway Device (if configured to do so). No direct access/login to the local devices is enabled

2.1.2. System integrity

A major risk in embedded devices is the cyber attacker's ability to manipulate the firmware and change device behavior. Various security mechanisms are embedded in the SolarEdge Gateway and other devices to verify the device software integrity.

Secured software update

Remote software update mechanism is an important support mechanism and a critical requirement in every cybersecurity architecture. A new software update (version) may include new functionalities, software bugs fixes and/or address software stability issues fixes, and/or address new cyber threats or security vulnerabilities.

The versions are controlled, regularly monitored and undergo best practice risk assessments. New versions are delivered to the devices using SolarEdge's secured remote software update mechanism:

- Remote software update can only be performed after the device initiates a communication channel with the SolarEdge backend
- Integrity of all firmware applied on the device is cryptographically authenticated
- Firmware versions cannot be downgraded
- The firmware and software executables are validated upon receipt, and rejected in case of malicious code
- The firmware and version update process apply protections against receipt or installation of corrupt upgrades
- The minimal security and software update support period for all SolarEdge devices is aligned with regulatory requirements
- SolarEdge supports a safe and gradual fleet roll-out of updates

Whitelisting mechanisms

To prevent code manipulation before accessing or executing files, the device verifies the signature of executable files in run-time. In the event of validation failure, the device reports to the cyber monitoring center and takes necessary actions to return to a safe status.

Secure boot (coming soon)

SolarEdge is working to incorporate a secure boot mechanism in Nexis products, a hardware-based security feature that ensures only trusted and verified software components are loaded during the boot process.

This security measure is planned to be included in SolarEdge Nexis inverters being released in 2025 and onwards by validating the integrity of the firmware, operating system, and critical drivers. Secure boot protects against unauthorized modifications, malware, and rootkits, providing an additional layer of defense against low-level security threats.

To prevent fileless malware from operating in the system's memory (RAM), the Gateway resets itself periodically when the inverter isn't generating power, deleting memory and temporary files, then returning to secured signed firmware and executables.

2.1.3. Runtime security

Dedicated agent

SolarEdge integrates advanced IoT anti-malware agents on its inverters, providing the following security enhancements:

- IoT protection against zero-day attacks (that target unknown security flaws in a code) and real-time prevention capabilities
- Dedicated Kernel-based file protection (Read/Write/Execute) in addition to existing OS (operation system) mechanisms
- The agent solution continuously monitors security events and blocks or alerts the SolarEdge security team (alert notifications are transmitted in near real-time to our security operation center)

Control flow integrity

SolarEdge's advanced IoT security agent includes a security layer called Control Flow Integrity (CFI). The Gateway real-time execution is protected against hostile malicious manipulation attempts in the production line and in the field. Additionally, the agent and device protect code integrity by:

- A verification layer to check and permit legitimate code updates
- A dynamic mechanism that verifies and permit only legitimate code pages are loaded into memory

Memory protections

The agent continually monitors for and protects against Memory Corruptions thus preventing memory management vulnerability exploitation. It also monitors every page loaded into memory to detect and prevent different exploitation stages.

Security events monitoring

Events sent from the device monitoring agent are fed into a monitoring dashboard and SIEM/SOC environment, and the fleet is monitored for anomalies and unexpected behaviors. These data feeds can be made available to customers and government enforcement agencies upon request.

Device vulnerability management

All SolarEdge device software and firmware is included in a vulnerability management program that consists of automated and manual tracking for open source and third-party vulnerabilities, internally found vulnerability management, bug bounty and responsible disclosure programs and software and firmware regular updates.

2.1.4. Data integrity and secrecy

A major risk in embedded devices is the cyber attacker's ability to steal or manipulate sensitive or operationally critical data and configurations. Various security mechanisms are embedded in SolarEdge inverters to verify the device data integrity.

Secure storage with ARM TrustZone for SolarEdge Nexis Inverters (coming soon)

Sensitive security data, cryptographic keys, and critical configurations in Nexis inverters will be stored securely using our secure storage solution. Leveraging ARM TrustZone technology and SoC-specific hardware features, our secure storage is isolated from the main operating system and applications, providing an extra layer of protection against unauthorized access and tampering.

This hardware-based security approach is designed to ensure that the most valuable assets remain confidential and secure, even in the face of sophisticated attacks and direct remote device breaches. Backup of the Gateways' configurations data is stored in SolarEdge servers, and can be reloaded to the Gateway, returning it to a safe and working mode.

Offline mode

The entire SolarEdge onsite systems continue to perform their duties even without internet connectivity. If internet connection is lost, only online functions will be impaired, such as the ability to remotely monitor PV system performance as well as carry out remote support. However, core functions will continue to operate. These include, among others, storage operation, PV production, grid and regulatory compliance and more.

Authenticated and encrypted communication

All relevant communication is encrypted and authenticated using up-to-date and recommended Cryptographic mechanisms. This includes any significant IP communication, any Radio Communications including Wi-Fi, and any communication to or from the backend services.

Approved cryptographic tools

SolarEdge inverters use only approved and recommended methods of communications, including strict selection of cipher suites and TLS versions to approve secrecy for years to come, and the guarantee of forward-secrecy for all substantial communications.

2.1.5. Logging and monitoring

SolarEdge constantly monitors the inverter fleet activity in the face of the ever-evolving landscape and cyber threats. The following section describes the logging processes of the inverters.

Device level logs

The following actions are performed:

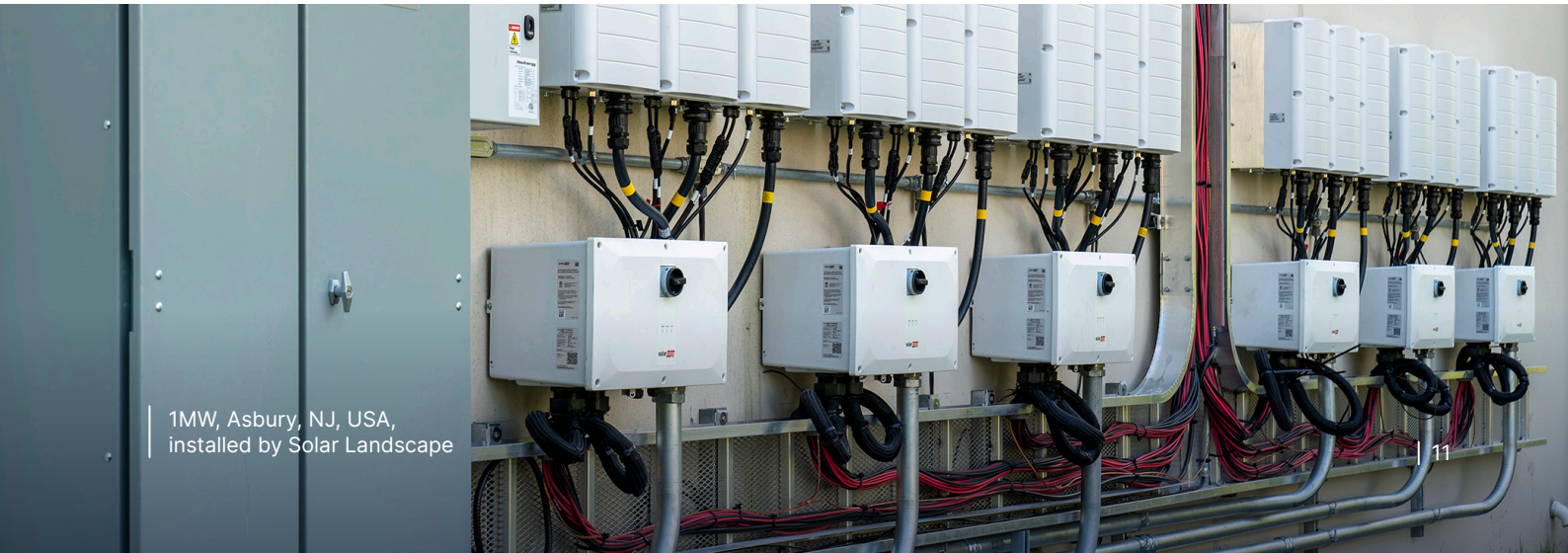
- Logging is enabled by default on start-up
- For each event, the Logs record, where applicable, the user, role, event identifier and event timestamp
- The security Logs capture the following cybersecurity events:
  - Detected code tampering
  - Detected malicious code
  - Detected failure of event logging
  - Successful login events
  - Unsuccessful login events
- Additional logs are collected to identify potential indicators of compromise of cyber-physical nature. Such indicators include overheating, internal fan performance, as well as other electric power export parameters
- Security logs are accessible for privileged users only
- Logs are kept for 6-24 months, depending on log type
- In case of connectivity loss, devices will retain logs in internal memory for a period sufficient for retroactive analysis.

For information regarding the SolarEdge ONE Controller gateway device logging regime, please contact a SolarEdge representative.

System level logs

SolarEdge incorporates a best-of-breed, time-based database system that indexes all Monitoring Platform infrastructure and networking logs into time-based indices, integrating a time-based dashboard that allows SolarEdge to search past and present logs, as well as to investigate past and present incidents. Server logging is a vital part of SolarEdge's security architecture. As a result:

- The server's log files are part of the security monitoring infrastructure, enabling SolarEdge to investigate security incidents, perform root cause analysis, etc.
- Access privileges to the server's log files are limited to authorized users only, protecting them from unauthorized modification or deletion.



1MW, Asbury, NJ, USA,
installed by Solar Landscape

2.2. Data security

SolarEdge does not collect and store highly sensitive data such as payment information or PII. However, it still vigilantly treats all data with the utmost care and complies with the latest cyber requirements and privacy regulations.

2.2.1. Application security (AppSec)

Backend platform

The SolarEdge Monitoring Platform and backend services are developed using modern secure development processes including source code scanning, secure development, penetration testing, configuration monitoring, secure code review, secure design and more.

Client mobile and web applications

SolarEdge client mobile and web applications including SolarEdge Go, SolarEdge Designer, SetApp, Mapper and mySolarEdge, monitoring web client, Grid Services, SolarEdge ONE and APIs, are reviewed for security vulnerabilities, and use the minimal privileges required on the mobile device. Login to the applications is performed vs. the backend services and is planned to include SSO, Federated SSO & MFA starting in Q3 2025. Data is stored securely at rest and is encrypted in Transit. Mobile application frameworks are used for development making reverse engineering more difficult and the application building blocks more secure.

Regular security testing

SolarEdge application clients and backends undergo regular internal and external penetration testing. Application security at SolarEdge is performed according to OWASP frameworks with adaptations to the unique PV environment.

2.2.2. Data privacy and integrity

Device data

- No personal data is stored on SolarEdge devices, such as inverters or gateways. Therefore, no data encryption mechanism is being used for storing personal user data on the device
- The variables which are measured in real-time and collected are network health, device consumption and complete power flow visibility of the system: consumption, production and import/export data
- Stored passwords are salted and hashed
- No Plain text usernames and passwords are stored on the device
- The confidentiality of data transiting between a device and the cloud is protected, using best practice cryptography (as described in the Secured Communication section)
- Resetting a device back to its factory state removes any collected data from the device
- Secured storage - sensitive security data, cryptographic keys, and critical configurations are stored securely using our product's secure storage solution. Leveraging ARM TrustZone (for inverters) technology and SoC-specific hardware features, our secure storage is isolated from the main operating system and applications, providing an extra layer of protection against unauthorized access and tampering. This hardware-based security approach ensures that the most valuable assets remain confidential and secure, even in the face of sophisticated attacks and direct remote device breaches
- SolarEdge hardware does not include sensing capabilities (except for temperature) and is not capable of audio and video recording by design

SolarEdge Cloud and web applications data

Stored data

- SolarEdge leverages its own private cloud located in Europe
- SolarEdge adheres to a transparent data collection and processing policy, as outlined in its Privacy Policy
- SolarEdge data privacy policy fully complies with GDPR regulations
- SolarEdge uses various security controls to protect user and account data in its private cloud environment
- The stored data in the SolarEdge cloud includes:
  - Identifying details about the site, as reported by the installer in consent with the site owner
  - System performance energy production and consumption data
- Users can request to delete their personal data (by email to privacy@solaredge.com)

Financial Theft and Fraud Protection

- The installation process of a SolarEdge system does not involve credit card details or any other form of payment data
- SolarEdge products are designed to safeguard data integrity and secure device operations, also regarding the impact on the financial aspects of the system performance. Such aspects include the integrity of revenue grade metering functions, protections against export limitations imposed by local distribution utilities, and jurisdiction-specific functions such as REC (renewable energy credit) generation and reporting

Web and mobile applications

Applications access to data is secured by design, as follows:

- Every user requires a username and password for applications authentication
- From Q3 2025, installers may use Multi-factor Authentication (MFA)
- Application access is limited according to defined SolarEdge policy
- Role-based Access Control (RBAC) is used in the SolarEdge platform, with a “least privilege” design concept employed
- The applications undergo penetration testing to detect common vulnerabilities such as the OWASP Top 10 and others, at least once a year
- Bug Bounty Program - SolarEdge offers compensation to cyber experts who report cybersecurity vulnerabilities. The compensation offered is at the company's discretion, and is based upon risk, impact, ease of exploitation, quality of the report, and additional considerations (read our Cybersecurity Policy)

GDPR (General Data Protection Regulation)

SolarEdge provides global services and maintains a significant presence in Europe, fully complying fully with GDPR requirements, including:

- Lawful, fair, and transparent processing
- Limitation of purpose, data, and storage data subject rights
- Consent
- Personal data breaches
- Privacy by design - technical controls
- Data Protection Impact Assessment
- Data Protection Officer
- Awareness and training

2.2.3. Advanced hosting facilities

Data location

SolarEdge stores data generated by its products in three dedicated hosting facilities in Germany.
The sites comply with the following standards:

- ISO 9001:2015 Quality Management Systems Standard - the world’s leading quality management standard that provides a clearly structured and systematic approach to maintaining and improving customer experience.
- ISO/IEC 27001:2005,27001:2013 and 27001:2022 Information Security Management System Standard - the most widely accepted certification available for supporting Information security, cybersecurity and privacy protection. ISO 27001 ensures that:
  - Risks and threats to the business are assessed and managed
  - Physical security processes such as restricted/named access are enforced consistently
  - Audits are conducted regularly at each site, including tests of security and CCTV planning and monitoring

All applicable internal SolarEdge systems similarly comply with ISO 9001:2015.
As SolarEdge expands its product portfolio, this section may be updated to include additional cloud computing locations in the future.

Physical security

Physical security measures of the dedicated hosting facilities include:

- Presence of security guards, alarm systems and CCTV
- The system's continuity is protected via a UPS device and backup generators
- A method of electronic Access Control based on swipe cards is implemented throughout the premises
- A water detection system is operational in the data center, alongside a water-based fire suppression system

2.2.4. Vulnerability monitoring

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.
SolarEdge has implemented and continuously adjusts its server monitoring strategy, using a variety of technological solutions and best practices:

- Establishment of organization-defined metrics to be monitored
- Based on the above, implementation of continuous performance monitoring using technological tools
- Ongoing security control assessments in accordance with the organization's monitoring strategy

USA, Installed by Isolara Solar Power

2.3. Network safeguards

SolarEdge systems are connected to the internet to enable detailed monitoring data, continuous remote support, remote device updates and cybersecurity monitoring. SolarEdge systems internet connectivity is designed and implemented, supporting restrictive cybersecurity requirements, and is continuously tested and updated according to the Distributed Energy Resources Threat Models.

2.3.1. Secured networking

Secured and encrypted communication

All internet and wireless communication are encrypted and authenticated with best of class encryption and modern standards and cryptographic suites, using SOG-IS “Agreed Cryptographic Mechanisms” and other guidelines as a basis for cryptographic mechanism and cipher suite usage.

Out of bound communication option (cellular)

Inverters support internet connectivity over an optional cellular modem, thus generating an airgap from the client’s network and providing the highest possible level of protection for the client IT network while maintaining connectivity. In this setting, multiple SolarEdge devices may communicate between themselves over a separate radio network, dedicated non-IP wired network or over a separate client-managed IP network, according to the installation and client needs.

Asymmetrical communication

The security of the Gateway’s internet connection is based on all internet connections being initiated by the SolarEdge Gateway and devices. Had the field-deployed devices had open receiving channels such as a user log-in page, those could be exploited by cyber threat actors that query the device to look for open ports and search for service vulnerabilities. To mitigate this risk, SolarEdge devices are designed with a secure communication mechanism, in which Gateways receive messages from the servers only when the Gateway initiates contact with the servers, polling for new commands and transmitting new data.

The devices are not exposed to the internet and cannot be accessed or detected by internet scanners. The designed solution masks the Gateways from potential hackers and effectively renders them invisible to scanning attacks.

2.3.2. Low attack surface

No open ports

The design and implementation of all SolarEdge devices include attack surface minimization at all levels. This ensures only needed IP ports are open at the software level. In addition, on the device level, unused interfaces and debug ports are closed and protected if they are not needed.

Wi-Fi scanning

To perform initial commissioning, the inverters must generate a Wi-Fi network to act as an access point (AP). This is limited only to situations in which the device has not already been commissioned or does not have an active internet connection which allows internet-based operation. Turning on the AP also requires a reboot or physical press of a button where applicable. These measures prevent the device from being visible to neighbors, passerby’s or anyone actively scanning for available Wi-Fi networks.

2.3.3. Input validation

Cloud connection

SolarEdge private cloud communication

The communication between the Gateway Device and SolarEdge cloud is designed with the following multi-layer protections:

- Firewall
- Web Application Firewall (WAF) and Global Load Balancer (GLB)
- Internal IPS to APP Server
- ACL (Access Control List) Network Segmentation
- ACL (Access Control List) Internal Platform
- Internal network segmentation and zero-trust network architecture

Local site connection

All communication between devices in a local site include strict input validation for SolarEdge and third-party devices to ensure malformed input will not be accepted on device-device and user-device communication.

2.4. Visibility and control

The purpose of this section is to outline product security features developed to facilitate ongoing monitoring and response. The primary goal of the features described here are to provide customer IT administrations and cybersecurity managers with tools to prepare and respond to cyber threats, focusing on data flow visibility, communication channels and real-time system performance to enable security monitoring and anomaly detection.

2.4.1. Internet connectivity control

The purpose of this section is to describe product security features that provide granular control over internet connectivity modes. This allows customers with high security requirements to connect the devices in configurations which minimize network risk to a very high level.

Offline operation modes

As described in the Offline mode section, the Gateway and the entire SolarEdge onsite system continue to perform their duties even without internet connectivity. If there's a cyber threat, customers can configure their Firewall to temporarily block internet connectivity. Data will temporarily be stored cyclically for up to two weeks on the devices and will be sent once connectivity resumes.

Multiple connectivity options

Based on our customer cyber and IT policy, SolarEdge inverters can securely connect to the internet either via local Ethernet, Wi-Fi or cellular modem. The network safeguards described in section 2.3 are in place, regardless of the physical layer.

Gateway devices (SolarEdge ONE Controller) can be connected to both Wi-Fi and Ethernet simultaneously, with Ethernet service as the primary connection. If the Ethernet connection fails, communications will automatically switch to Wi-Fi. The gateway device does not use cellular connectivity.

"Safe mode" – one-way communication

SolarEdge provides an extra security mechanism called One-Way Communication, or "Remote Support" for the inverters. When this feature is enabled, all incoming commands to the device (from the SolarEdge cloud) are dropped and not processed. In such a scenario, all external access is limited unless a person is physically present by the system and opens a temporary access window for remote support or software updates.

2.4.2. Cybersecurity data sharing

Vulnerability disclosure

SolarEdge supports and encourages coordinated vulnerability disclosure (CVD) regarding its products. As part of SolarEdge's cyber policy, SolarEdge maintains a disclosure procedure and bug bounty program. Every reported vulnerability in SolarEdge products or applications which receives a CVE, is documented and shared publicly. The latest, up-to-date information can be found on our Coordinated Vulnerability Disclosure Policy webpage.

Integration with SIEM/SOC solution

SolarEdge has implemented a robust system where alerts and events from our extensive network of millions of installed inverters are continuously streamed into a Security Operations Center (SOC). This allows for real-time monitoring to swiftly detect any unusual activity across the entire fleet. This data can be made available to customer SIEM/SOC solutions or service providers, both in single-site context as well as per customer account.

2.4.3. Secure installation guidance

Firewall configuration guide – FQDN

Managers must configure firewall policies using whitelists that will enable communication between on-site inverters and SolarEdge function-specific FQDNs (Fully Qualified Domain Names).
The whitelists also enable device-to-device support operations.

Mandatory Whitelist FQDNs

The following FQDNs must be whitelisted to enable data transmissions from the inverter:

Function	FQDN	Protocol	Port
IOT Communication	prodfqdn.solaredge.com	TCP	443
Secure Onboarding	svcfqdn.solaredge.com	TCP	443
Security Monitoring	svcfqdn.solaredge.com	TCP	443
Time Synchronization	time.google.com * IP addresses may change based on geographic location. Make sure to use the FQDN and not the IP address.	TCP	123
Time Synch Backup	www.google.com * IP addresses may change based on geographic location. Make sure to use the FQDN and not the IP address.	TCP	80
DNS Lookup	www.google.com	TCP	53
Remote Installer access	portia-tu.solaredge.com	TCP	5555
Support Remote access	serminv.solaredge.com	TCP	2222
Software Updates	Whitelist CloudFront Edge Servers docs.aws.amazon.com	TCP	443
Connectivity and Latency (ping)	8.8.8.8	ICMP	

Optional White List FQDNs

The following FQDNs can be whitelisted to support optional functions:

Function	FQDN	Protocol	Port
Cloud communication	prodfqdn.solaredge.com	TCP	22222 / 22221
Software updates	https://embedded-repo-dev.s3.eu-central-1.amazonaws.com	TCP	443
RSSH	linux-prod.solaredge.com	TCP	2222

For the SolarEdge ONE Controller FQDN list, please request the list from your local SolarEdge representative.

In some cases, karamba-proxi.solaredge.com will appear as the Security Monitoring FQDN, until the migration is finalized.

3. Standards Certifications and Regulatory Compliance

SolarEdge's Certification reports can be accessed from here.

3.1. Cybersecurity certifications

3.1.1. ISO27001

- SolarEdge is ISO 27001 certified. ISO/IEC 27001 is an international standard on how to manage information security. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure. Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit. By adhering to the standard, SolarEdge is attesting to its adoption of security information practices across its network and systems.

  SolarEdge is compliant with the latest version of the ISO 27001: standard, published in 2022 (ISO 27001:2022)
- Adhering to this standard includes activities such as, and not limited to:
  - Written internal policies, guidelines, and documented practices for the safe handling and protection of data
  - Phishing e-mail testing of SolarEdge employees
  - Internal audits of the security and privacy program
  - Third-party audits of the security and privacy program
  - A risk assessment and risk management process to regularly review the threats the company is exposed to
  - A program to ensure security in SolarEdge human resources processes
  - Processes and procedures to ensure that security incidents are discovered in a timely manner and dealt with effectively
  - Timely patching applied against known vulnerabilities
  - Protecting systems from malicious code
  - Locking down software and hardware to restrict unnecessary services

3.1.2. ETSI-303-645

SolarEdge inverters are ETSI-303-645 certified. This standard outlines baseline security requirements for consumer Internet of Things (IoT) devices, providing a comprehensive framework to ensure IoT devices and systems are secure by design. It addresses critical areas such as data protection, vulnerability management, software updates, and user access control, aiming to mitigate the most common and impactful threats in the IoT landscape.

By aligning with ETSI EN 303 645, SolarEdge demonstrates its commitment to embedding robust security measures within its IoT products and infrastructure. The standard requires the implementation of security practices such as:

- Strong password policies and the elimination of universal default passwords
- Regular security updates to the inverter to address known vulnerabilities
- Proactive measures to prevent unauthorized access and tampering
- Clear and accessible user information to enable safe and informed use of devices

3.1.3. SSDLC

- Our software is engineered with security at its core, leveraging a Secure Software Development Life Cycle (SSDLC) framework to embed robust security measures throughout the development process, ensuring protection against code vulnerabilities and minimizing security risks
- SolarEdge uses an array of methodologies for its hardware and software development processes. We practice secure software development procedures, including periodic automated and manual vulnerability testing
- The vast majority of code in SolarEdge products originates from internal development teams. These teams undergo secure coding practices training
- SolarEdge does not subcontract code development in its products.
- In cases where external libraries are used, or of software related partnerships, compensating security controls such as audits are in place to ensure the quality of code in the context of secure development.
- Open-source software is scanned for known vulnerabilities as part of software development and deployment processes
- Production source codes are stored in local source control systems protected by physical and password/private key authentication
- Our SSDLC level is aligned with the requirements presented in IEC 62443-4-1

3.2. Regulatory compliance

3.2.1. UK Product Security and Telecommunications Infrastructure (UK-PSTI)

SolarEdge products comply with UK-PSTI requirements. Refer to the certification here.

3.2.2. Radio Equipment Directive (RED), article 3.3

SolarEdge inverters comply with all relevant cyber requirements of the Radio Equipment Directive (Article 3.3).

3.2.3. NIS2 – “Essential Entity” level compliance

- SolarEdge complies with all relevant cyber requirements of the NIS 2 directive in all applicable European Union member state markets.
- SolarEdge complies with the NIS 2.0 regulation under the heightened security requirements of an “Essential Entity”

3.3. Upcoming regulations

- Cyber Resilience Act

  SolarEdge products are developed in line with the upcoming requirements of the Cyber Resilience Act, expected to be made mandatory in the 2026-2027 timeframe
  Learn more.
- NIST Smart Inverter Guidelines

  SolarEdge products fully meet the guidelines described under the 2024 National Institute for Standards and Technology (NIST) IR 8498 “Cybersecurity for Smart Inverters” guidelines for Residential and Light Commercial Solar Energy Systems
  Learn more.
- NARUC/ NASEO

  SolarEdge products meet the cybersecurity baselines described by the United States National Association of Regulatory Utility Commissioners (NARUC) for Distribution systems and DERs
  Learn more.

4. Appendix - Solution Diagrams

- **Typical site with SolarEdge TerraMax™ Inverter:**
  The following is an illustration of a typical SolarEdge commercial system with the TerraMax inverter, highlighting the different pillars that combine to protect our products from cyber threats (device security, data security, and visibility and control).

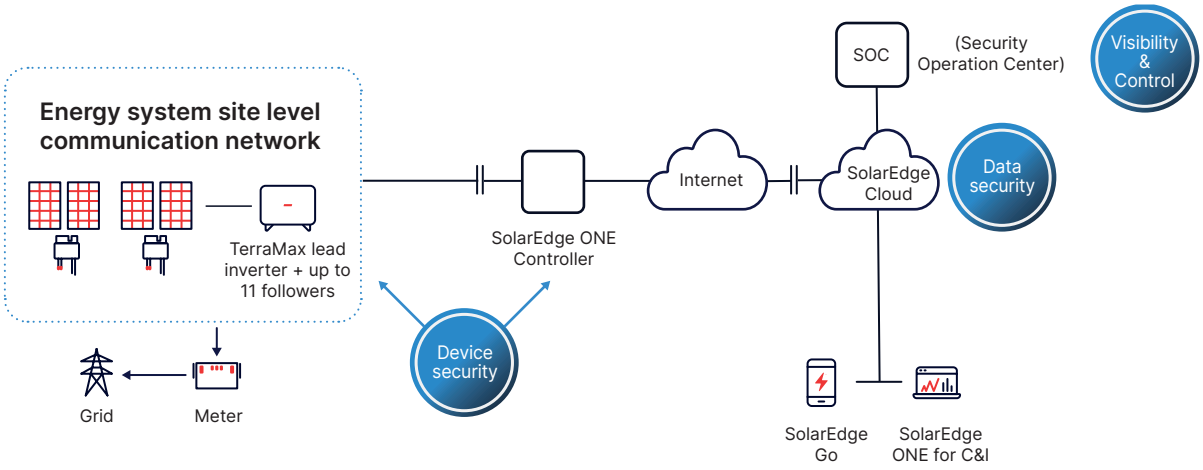


Figure 3: Typical SolarEdge TerraMax Inverter installation

- **Typical site with SolarEdge Residential system:**
  The following is an illustration of a typical SolarEdge residential system, highlighting the different pillars that combine to protect our products from cyber threats (device security and data security).

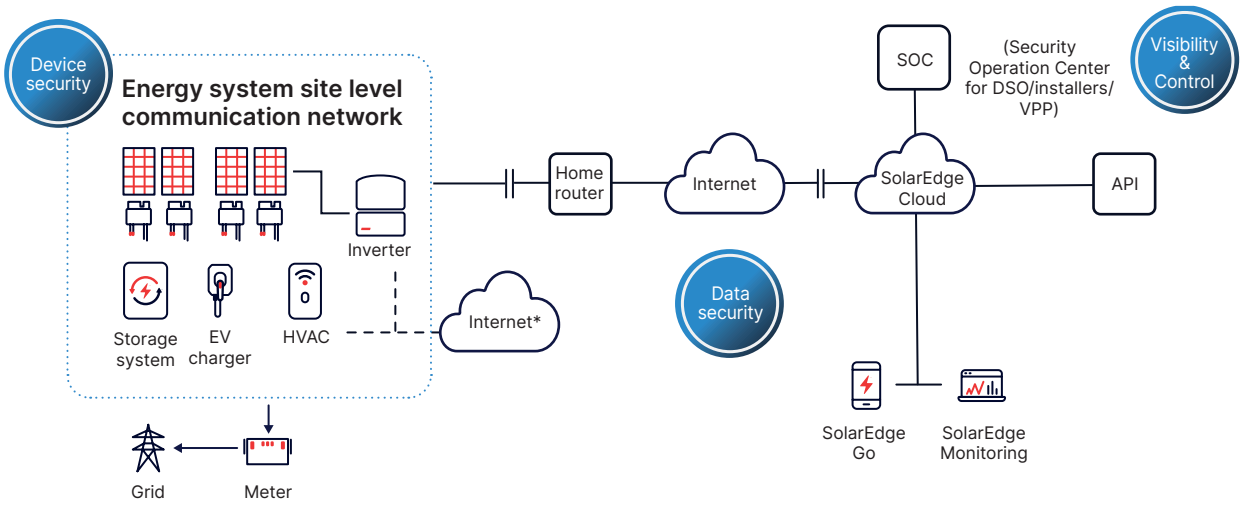


Figure 4: Typical SolarEdge Residential installation