Cybersecurity

for Connected Energy Ecosystems

Begin ▶

Introduction

Cyber attackers are constantly evolving and as utilities becomes increasingly connected and digitized it is becoming critically important to secure the connected energy ecosystem. For example a coordinated cyber attack on EV charging stations could have devastating impacts to a country. The Netherlands, for instance, has the highest number of EV charging points per square kilometer in Europe[1]. By 2030, there are expected to be 1.7 million EV charging points[2], supporting 1.9 million EVs. Imagine if a cyber attacker set them all to maximum charge capacity simultaneously—there would be an instant demand for 6.3GW of energy (assuming a minimum charging draw of 3.75kw per charging point), resulting in brownouts, blackouts and damage to the connected energy infrastructure and EVs. The impact of such an attack grows if EV chargers of 22 kW AC, 50 kW DC, or ultra fast DC chargers of 100kW+ are factored in, making EV charging stations a very attractive target for cyber attackers wishing to cause regional or national impacts.

Electrification of the transport sector is one of many examples of the transition to clean energy to be deployed globally for the US, Europe and China to meet their commitment to carbon neutrality by mid-century. But the rapid growth and increasing complexity of this ecosystem has outpaced the generation of national and international standards, leading to concerns about cybersecurity. The extremely interconnected nature of the connected energy ecosystem means that a cyber attacker could exploit weak cybersecurity at one point in the ecosystem, and once inside, infiltrate other parts of it to cause damage, steal information or disrupt services elsewhere.

The threat is real, and the capabilities of cyber attackers are constantly evolving. It is becoming critically important to secure the connected energy ecosystem, but how?

Connected Energy Ecosystem Trends

Government regulations and financial incentives to establish clean, renewable connected energy ecosystems are a powerful driver for change. These are creating new power consumption and generation models, leading to a rapidly evolving connected energy ecosystem with clean, renewable electrical power generation and storage technology integrated into buildings. By combining these with other smart building technologies, even more energy efficiency and cost reductions can be achieved. This results in an energy efficient building ecosystem that automatically self-optimizes to maximize user comfort while reducing carbon emissions, building operations and maintenance costs.

Examples of intelligent energy optimization are:

- Automatically switching off a heat pump when a window is opened.
- Using intelligent lighting systems that maximize natural lighting through intelligent window blind management.
- Automatically switching lights off in unused rooms.
- Storing surplus solar energy in battery storage systems for later use, or to offset bills by sending into the local distribution grid.

Solutions like these that adjust with building occupancy have led to the creation of smart building management systems. Further integrations include automated security systems such as motion sensors, video cameras and access control systems — these can not only reduce energy bills but can also contribute positively to the more efficient management of buildings.

Electrification of transport is another significant part of the connected energy ecosystem. Although EVs make up a small proportion of vehicles on the road, sales are rising as battery technology improves. Current global projections indicate that one in ten vehicles purchased in 2025 will be battery-powered and by 2040, the world will need some 12 million public charging points and $400 billion spent on infrastructure[3].

A recent development in smart buildings is the integration of EV charging points into building infrastructures. This provides the EV user with the ability not only to charge the EV, but also to use surplus energy stored in EV batteries, providing an additional renewable energy source for the building that can be used elsewhere in the connected energy ecosystem if required.

> By 2040
>
> the world will need some 12 million public charging points and $400 billion spent on infrastructure

Security Risks and Challenges in the Connected Energy Ecosystem

Like many new technological areas, the connected energy ecosystem has been driven by individual or competing entities with a focus on consumer uptake and profitability. Cybersecurity and ease of integration with other systems has often been an afterthought. This has led to an extremely heterogenous and rapidly expanding ecosystem which has outstripped the ability to create national and international regulations or frameworks to ensure that components can interoperate securely. However, the diverse range of technologies and lack of standardization is not the only challenge to security. There are also challenges in securing the processes and people that operate and use it.

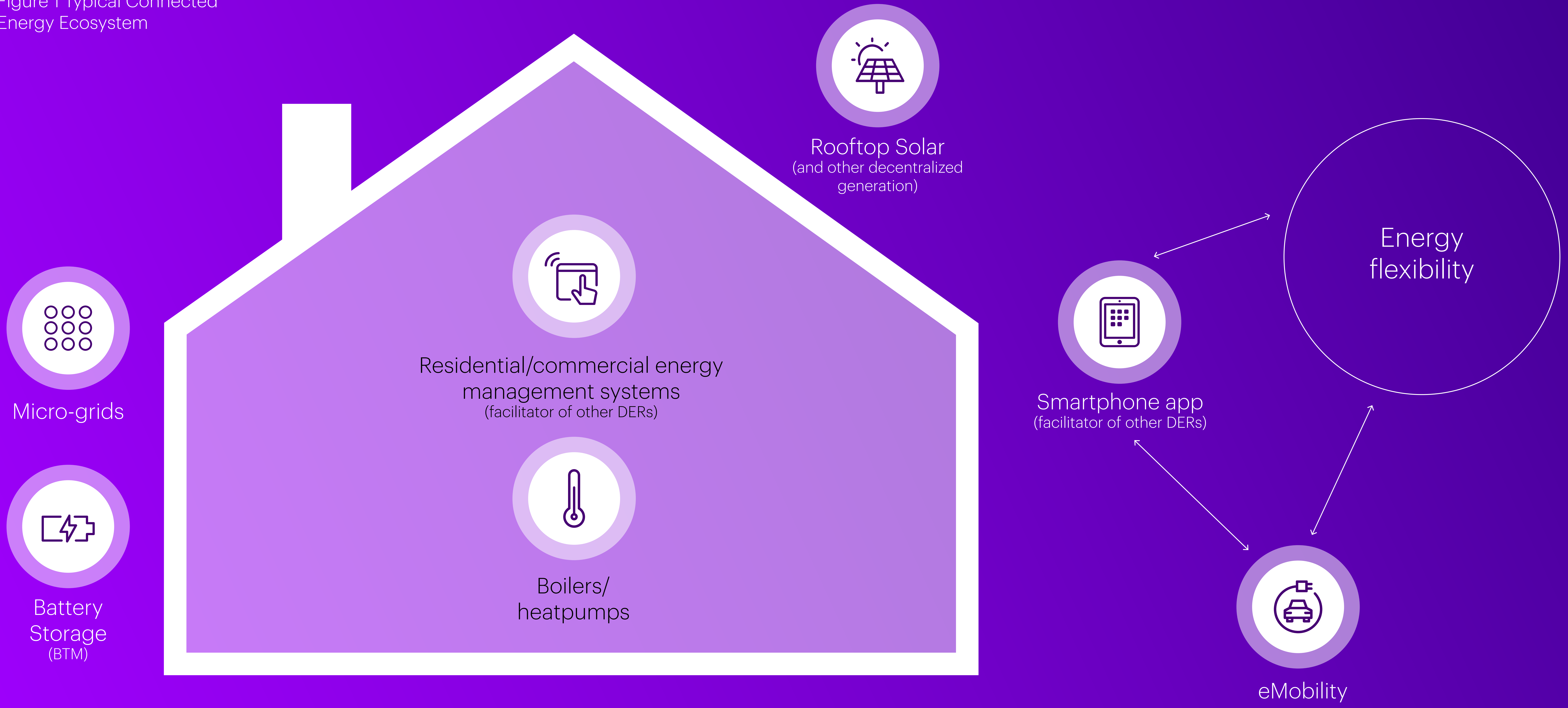
The motivations of cyber attackers for targeting the connected energy ecosystem are clear. By penetrating it at a weak spot, hackers could use trusted channels to infiltrate other ecosystem components to:

- Disrupt connected energy distribution and storage networks.
- Cause physical damage to off-grid charging assets and energy storage infrastructure.
- Steal personal information such as payment details for use in identity theft and other fraudulent activities.
- Steal, modify, destroy or leak sensitive commercial information such as company IPs or customer records, causing reputational damage, impacting competitive advantage causing loss of new business and revenue, and potentially leading to regulatory fines.
- Disrupt connected energy ecosystem services through the installation of ransomware.
- Cause health, safety and environmental (HSE) risks by overcharging or discharging batteries and damaging EVs or storage infrastructures.

Because of the rapid development of smart connected technology and associated communication protocols, connected energy ecosystems security is immature. Service providers and device manufacturers often have little or no experience of IT security, let alone internet of things (IoT) security.

Distributed Energy Resources (DER)

Figure 1 Typical Connected Energy Ecosystem



Rooftop Solar
(and other decentralized generation)

Micro-grids

Residential/commercial energy management systems
(facilitator of other DERs)

Boilers/ heatpumps

Battery Storage
(BTM)

Smartphone app
(facilitator of other DERs)

Energy flexibility

eMobility

Figure 1 shows a typical connected energy ecosystem, with many different types of services, devices, operators, service providers and users for:

- Rooftop solar (and other decentralized means of electricity generation).

- Boilers and heat pumps integrated into the building energy management systems.

- Intelligent/smart lighting systems that maximize the use of natural light through automatically adjustable blinds.

- Automated HVAC control that adjusts the heating or cooling effieincy based on room occupancy.

Home Energy Monitoring displays (also called In House Displays – IHD). These are wirelessly connected to the smart meter, and allow home energy consumption to be shown in real time, and can be used to show daily, peak and average consumption, helping users optimize their energy consumption. Integrated sensors and actuators throughout the home for providing information to home automation and energy management systems to optimize heating, cooling, lighting and shade as part of home energy management systems.

- Integrated battery storage systems to store surplus energy. These may be solely for use by the building users/occupants or integrated with commercially-operated energy micro grids.

- E-mobility – including EV charging points (private or commercially operated).

- Commercially operated schemes for providing discounted charging facilities nationally and internationally through easy-to-use payment options, providing consistent vehicle charging facilities away from home.

- Smart phone apps providing integrated internet access for remote control of building management systems to control lighting, heating, window blinds, or to access building security systems such as connected doorbells alarms and video cameras remotely.

Inadequate security in any of these systems could enable cyber attackers to penetrate the internal networks within the building. Once inside, they could take control of systems, extract personal information such as payment details, or penetrate further into the connected energy ecosystem through trusted channels.

Regardless of how innocuous a connected device is, weak security will be exploited to penetrate defenses. For example, cyber attackers penetrated the network security of a Las Vegas casino to steal customer credit card details by infiltrating through an inadequately secured connected thermostat in a fish tank in the casino lobby[4].

Unfortunately, security cannot be ensured by technology alone. Securing the connected energy ecosystem requires secure technology combined with security-aware people and security-enforcing processes. Common people, process, and technology problems are shown below.

[4] Internet of Business: Hackers steal casino's customer data via connected fish tank

Security requires a seamless combination of people, process and technology

Typical people and process challenges in connected energy

- **Lack of international standards** has led to a heterogenous ecosystem with no consistent approach to interoperability or security, leaving many potential security gaps to be exploited by cyber criminals.
- Many connected energy **solutions are used by non-security-aware individuals** (e.g., members of the public). Processes must promote good security practices in users without compromising the user experience or impacting cost.
- New privacy-protecting **regulations such as GDPR** ensure that personal information is protected from misuse and unauthorized disclosure. This requires service providers to create processes to ensure individuals' **explicit consent to the use of their personal data**, and to ensure that their data is used legally and is always adequately protected.
- Organizations in the ecosystem must ensure that their **employees are regularly trained** in good security practices, that processes are in place to support them, and that they are aware of what actions to take if they detect or suspect a **cyber breach**.
- Security governance must be regularly reviewed and updated to ensure that the people and processes used for cyber defense remain effective against new and emerging threats.
- Security processes must ensure that people are aware of **good security hygiene** and aid them by enforcing a strong security culture.
- Governance processes must ensure that **security testing** is performed regularly, and all **failures tracked** through to remediation.

The general lack of security awareness in the population means that security defenses must be quick and intuitive to use while maintaining their effectiveness.

Typical technical challenges in connected energy

- Many devices used in the connected energy ecosystem (e.g., EV charging points) are in **public locations.** They need physical security so they cannot be broken into to gain access to stored secrets or other information that could be used to bypass cyber security.
- Pressures to be price competitive mean that most IoT devices are designed to minimize unnecessary cost. This frequently means that **security features**, such as hardware encryption or hardware root of trust and even additional memory to enable software updates or patching, are **not included in the design**, making security updates challenging.
- Many device manufacturers are relatively new to the concept of smart connected devices and have **little or no experience with secure software** development processes or the need for security testing of systems and devices (e.g., penetration tests).
- Unlike consumer high-tech which is refreshed every couple of years, **IoT devices have long design lives.** This means they become **comparatively obsolete** after a few years, and so maintaining the currency of security systems can be challenging.
- **Regular Device Patching** must be secured so that only known, trusted software updates and patches are applied.
- IoT devices have high availability expectations, and so **patch application can be problematic** if devices stop providing services while patch is being applied—which may impact customer satisfaction and safety.
- **Secure device identity** mechanisms must be applied so that only known, trusted and authorized devices can connect to networks. MAC and IP addresses are not suitable because they can be spoofed, copied or transferred to other devices.
- All IoT devices that process **customer information** must do so in **a secure and privacy-preserving** manner, and incorporate suitable hardware defences (e.g., secure encrypted storage and encrypted communication channels).

Regulations in the Connected Energy Ecosystem

The decentralized and international nature of the connected energy ecosystem means that it is impossible for any individual participant to enforce a consistent and holistic approach to security across the ecosystem. The adoption of international standards is therefore becoming a priority. Front running countries such as the Netherlands, France, Germany and the UK are beginning to introduce regulations to protect their connected energy infrastructures, but international standards are required to ensure interoperability of devices operated in different countries and guarantee safe and secure integration.

Unfortunately, regulatory bodies tend to be slow moving in comparison to the cyber threat. New regulations require extensive reviews and modifications to satisfy all participants, so that by the time they have been released, the cyber threat will have developed further. And legally enforced regulations and standards would not in themselves be enough to ensure effective protection of security and privacy. Regulatory compliance is only the starting point and not the target state for effective cyber resilience. Compliance must be regarded as the minimum baseline for cyber defense. To protect cybersecurity and privacy, regulations must be augmented by strong security governance strategies, blending people, process and technologies together to form an agile, resilient and multi-layered set of cyber defenses that adapt and evolve to combat the ever-changing cyber threat.

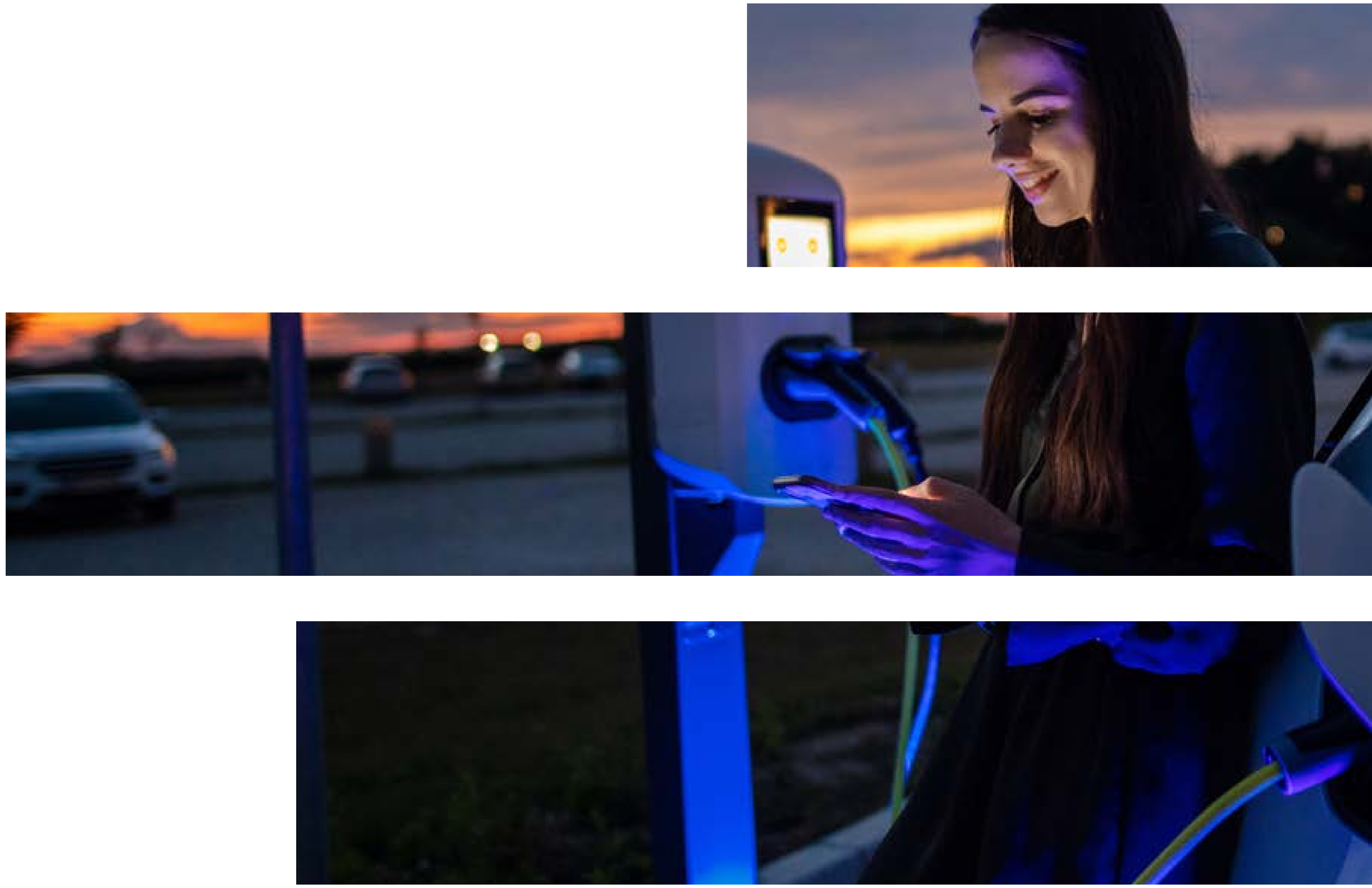
An important aspect of strong security governance is recognizing the possibility that defenses will be breached at some stage, so it must include strategies and tools for early cyber breach detection, threat containment and damage limitation. Areas for consideration are business continuity, loss prevention and regulatory compliance, with relevance to privacy protecting regulations such as the General Data Protection Regulation (GDPR).

> International standards are required to ensure interoperability of devices operated in different countries and guarantee safe and secure integration

A Paradigm Shift: Moving from assuming trust to proving trust

Typically, security defenses have focused on perimeter defenses to restrict access to trusted, authenticated identities, but trust-based models fail spectacularly when trusted identities are stolen or misused. The COVID-19 pandemic accelerated the move to remote internet connectivity for work and e-commerce, and many organizations were unprepared for this sudden transition. With greater reliance on on-line channels, cyber criminals ruthlessly exploited this lack of preparedness for safe remote access.

The modern cyber attacker is equipped with sophisticated weapons for guessing or stealing weak passwords, knowing that the human factor is generally the weakest link. By using malware-infected emails, sophisticated social engineering and web redirection techniques, people can be fooled into revealing their identity credentials. This, combined with a lack of effective remote identity verification techniques such as multi factor authentication, has led to an increase in cybercrime through cyber criminals assuming the identity of trusted entities.



Moving to Zero Trust

Because of its extremely diverse range of technologies, service providers and users, the connected energy ecosystem is particularly vulnerable to breaches of trust. Although it can be reasonably expected that an e-mobility service provider or microgrid operator will have security defenses integrated into their solutions and security-aware teams to monitor and maintain them, the same cannot be said for households running connected energy solutions. Many (most) domestic users of connected energy solutions have little or no knowledge of good security practices. They may have obsolete and insecure devices connected to their home networks, making them a prime target for hackers wishing to penetrate the ecosystem.

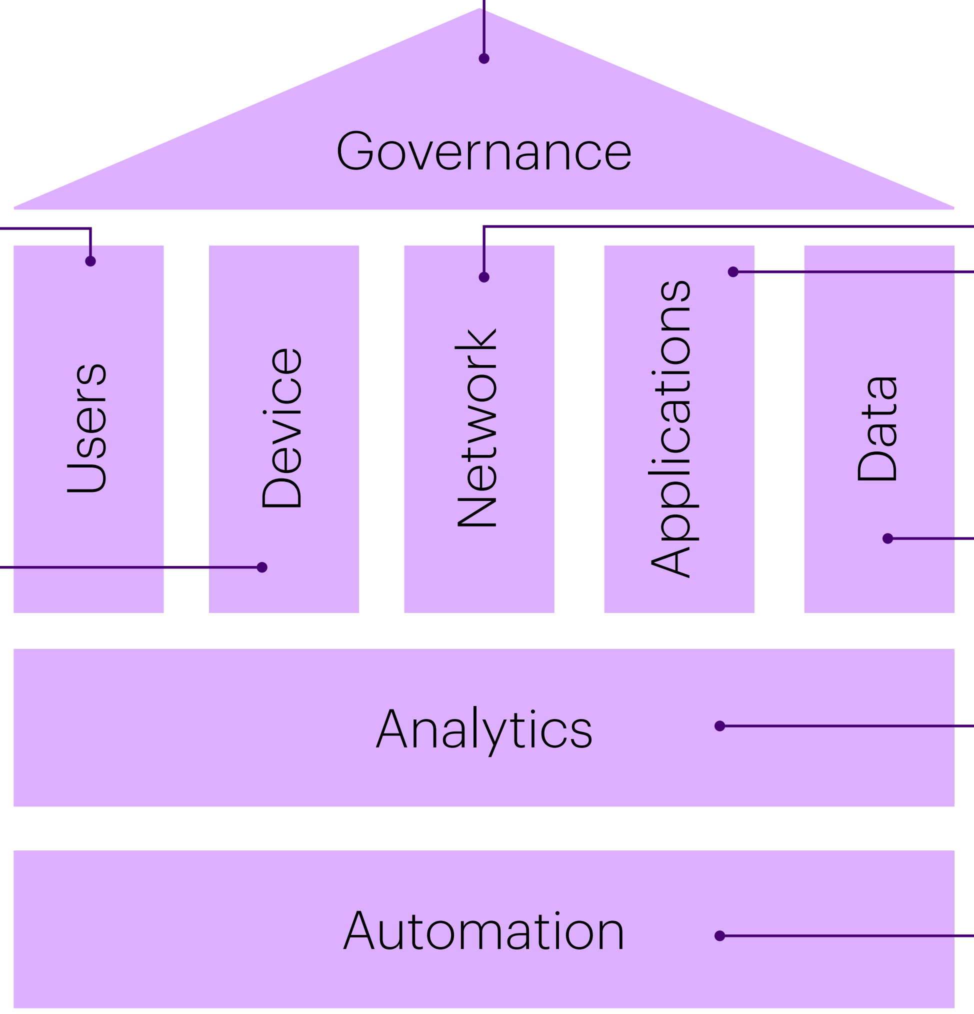
Consequently, security models used within the connected energy ecosystem must assume that there has been compromise somewhere in the system and adopt a defensive posture against it.

Service providers and operators within the connected energy ecosystem need therefore to move away from trust-based models. They should instead adopt a zero-trust security model in which no identity is trusted, and all actions are validated against a set of predefined rules. This is the only means by which an ecosystem member can interact with others safely and securely.

> Many domestic users of connected energy solutions have little or no knowledge of good security practices.

How to Implement Zero Trust Models

All security models require strong governance. Zero trust security is no different, but it is based on five fundamental pillars, supported by a strong foundation of automation and analytics to enable it to scale, as shown in Figure 2.



Security governance
Coordinate, enforce and evolve the organization's security activities with security governance that identifies and protects business-critical systems through a combination of people, process and technology.

Users
Strengthen access controls with Multi-Factor Authentication for remote access and access to sensitive information (using location, time, device identity, etc. as additional factors). Ensure access permissions are centrally managed and set to the minimum required for the user to perform their role.

Device
Implement strong device identity management, and police endpoints so that only authorised devices with up-to-date patch lists can connect to internal networks. Use automated scanning to validate network endpoints and devices.

Network
Partition internal networks into access-controlled subnetworks to add additional layers of protection to sensitive company resources and systems.

Applications
Control access to information and systems by only allowing approved applications to be used.

Data
Data is the most essential asset in the connected energy ecosystem. Identify and tag all sensitive data so that its use can be policed.

Analytics
Use analytics to detect anomalous behaviours and trigger alerts when unusual activities are spotted.

Automation
Use automation to enforce policies and rules so that security is effective without slowing day to day operations.

Security Governance

This is an organization's approach to security in terms of controlling, directing, assessing and evolving its security defenses. Unfortunately, it is unreasonable to assume that all connected energy ecosystem users will be aware of the need for strong security governance, particularly domestic users. This means that service providers, system integrators and device manufacturers have a duty of care to ensure that their offerings are secure and private by default, but they must not assume implicit trust. They must ensure that users are guided towards best practice without adversely impacting the user experience—a difficult balancing act that requires careful consideration.

Key components for strong zero trust security governance are:

Understand your business operational priorities and protect these with appropriate security controls. This ensures that the most robust security defenses and controls are used to protect business-critical assets and operations.

Understand the users, devices, information flows and data within your organization and establish a set of automated rules to control access to and use of them.

Review the secure software development lifecycle process (SSDLP) regularly to ensure that it evolves to adapt to new technologies and threats.

Create an organizational structure with clearly defined security roles/responsibilities (ownership, responsibility, terminology and reporting, including interaction with regulatory authorities and tracking of security roadmaps).

Raise security awareness through regular employee security training so that bad practice is eliminated, and good security practices are engrained in your organization.

Automate security processes and rule checking whenever possible to ensure simplification and a standardized approach to enforcement in a non-intrusive manner.

Understand how your offerings will be used outside your organization (e.g., devices, services or solutions), and incorporate security mechanisms that eliminate the possibility of intentional or unintentional misuse.

Data

Data is your most critical asset. Strong data governance is required to ensure that all sensitive data is adequately protected. Unauthorized disclosure (leakage), misuse or manipulation of data can have extremely severe repercussions including:

- Regulatory fines for data breaches of personal information such as credit card details.
- Loss of shareholder value or loss of competitive advantage if the company IP is stolen or leaked.
- Potential safety issues if data is manipulated to cause smart connected devices and interconnected systems to malfunction or be operated in a malicious manner to cause service outages or disruption.
- Tarnished public image and loss of digital trust through negative publicity, resulting in loss of customers and associated loss of profitability.

Governance around protecting data must ensure that:

- All sensitive data is identified, and automated rules are in place to restrict its access and use.
- Access is restricted to authorized individuals. Sensitive data should be protected by additional authentication mechanisms.
- Appropriate encryption methods are used to protect data in motion and at rest.
- Anonymization and pseudonymization technologies are used to protect PII and other sensitive personal information.
- Automated access monitoring and logging is used to detect, report and prevent anomalous data access/use.
- Automated data loss prevention mechanisms are in place to prevent malicious or unintentional data leakage.
- Regular testing of backup and restore mechanisms takes place to ensure their effectiveness.
- Automated restrictions are in place to prevent data being accessed from or sent to unauthorized geographies.
- Controls are in place to enable individuals to securely access their personal information in accordance with local privacy regulations.

Users

Know who has access to your systems! This is particularly important for connected energy ecosystem service providers who interact with other service providers, consumers and customers. Automated processes to prevent unauthorised or unknown users from gaining access must be in place , such as:

Strong password policies to eliminate weak, easily guessable passwords and to educate users about good security hygiene (such as not divulging their passwords to others, no matter how trusted or senior they are). In the case of password policies for use by customers or other third parties in the connected energy ecosystem, a balance must be struck between ease of use and security, so a light touch multifactor authentication should be used.

Multi factor authentication (MFA) to authenticate identities for all employee remote access. For connected energy ecosystem service providers, additional identity confirmation should be used when customers or other third parties make or collect payment information. Low friction mechanisms such as fingerprint, pin codes or one-time passwords are acceptable methods of providing additional identity confirmation without impacting the user experience.

Policy of least privilege, where each authorized identity is allocated the bare minimum access rights required to perform their role.

Centralized role-based access control (RBAC) to control access rights and privileges. Each individual identity must be associated with a user group relevant to their role. Each identity in a user group derives their access rights from that group. If their role changes and they require different access rights, they must be moved to a user group with the appropriate access rights.

Integration of identity management systems with your company joiner/leaver mechanisms so that when somebody leaves the company, their identity authentication and access rights are automatically revoked.

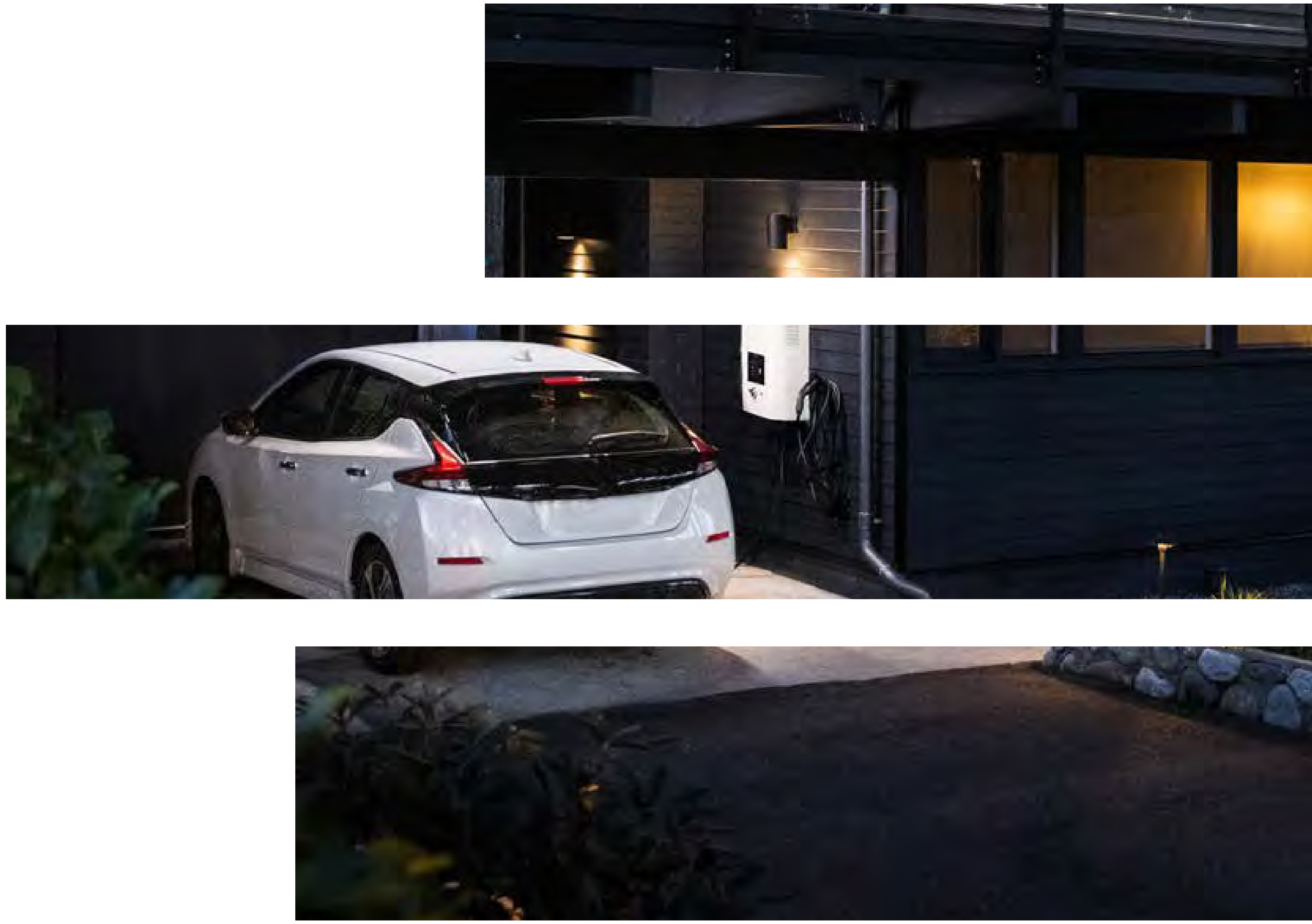
Regular reviews of user accounts. Unused accounts should locked/removed as appropriate to prevent misuse.

Preventing hackers gaining access by brute force by automatically detecting multiple consecutive logs in failures, locking accounts for a period and generating alerts.

Network

Controlling who and what can connect your internal networks is of paramount importance; your rules for zero trust network access must enforce strong control over this. Additional network defenses can be realized through internal network segmentation, which means that rather than having a flat network topology, your network is segregated into access-controlled subnetworks with predefined and automated access rules.

This enables fine grained, rule-based access and control of information flows between networks and subnetworks. It also significantly reduces the addressable attack surface by restricting visibility of and access to information flows and other connected entities. Networks should be automatically scanned to ensure that no unexpected users or devices have connected. All unexpected connection requests should be silently ignored and discarded, and failed connection requests from valid identities (e.g., incorrect password) should result in the associated account being locked. Regular penetration testing and associated remediation activities should be performed to ensure that network defences are strong and evolve to combat new and emerging threats.



Device

Devices used within the connected energy ecosystem, particularly those associated with EV charging, will be in publicly accessible locations, making them vulnerable to physical tampering. Within the consumer space (e.g., smart buildings) many devices may run with insecure default settings and obsolete or out of date (unpatched) firmware and software images, jeopardizing the security of the network to which they are attached, and perhaps the entire ecosystem.

To strengthen ecosystem security, set up automatically enforceable rules to ensure that:

- Only devices with valid and authenticated identities can connect to your systems. Use high entropy identification mechanisms so that if the identity of one device becomes known, the identities of other devices cannot be easily guessed.
- Use devices with hardware security mechanisms to ensure that devices are running trusted software and firmware versions.
- Only allow devices with the latest approved hardware, software and firmware versions to connect. Automatically quarantine devices until they are appropriately patched or upgraded so that unpatched or obsolete devices with known vulnerabilities cannot be exploited.
- All device firmware, software and application upgrades must come from approved sources (e.g., using CA issued certificates or signatures).
- Adapt mobile device security policies to accommodate BYO devices so that employees can use their own mobile devices to connect to company networks and use them for work activities. Integration of BYO devices must consider the appropriate level of security control, but at the very least must ensure that only company-approved applications can access corporate resources, and that these have come from company-approved sources.

If you are manufacturing devices for use by third parties, or that are in publicly accessible places (e.g., smart building energy management systems, or EV Charging points) consider how the devices will be used, who will use them, and for what. Limit configuration options to a small number so that the device cannot be set up in an insecure manner. Consider completely automated set up of devices via QR codes, for example which can be scanned to identify the device and automatically integrate it into the building management system with no need for additional configuration.

Also consider the need for secure 'end of life' for devices and ensure that you have mechanisms for preserving the security and privacy of an individual if they decommission a device or transfer ownership to another.

Devices deployed in remote locations that provide safety-related services, or which process personal information such as payment details (e.g., EV Charging stations) must incorporate adequate physical security to prevent tampering. There have been many examples of payment card details being stolen by physical tampering of commonly used devices in the public domain, such as ATM machines.

Physical security measures to be considered are:

- Fitting deterrent anti-tamper mechanisms such as hardened casings, tamper proof screws and panel open alarms, which are activated by microswitches to report when access panels have been removed
- Disabling debug/maintenance and removable media ports to prevent access to sensitive information or unauthorized reprogramming of devices
- Fitting GPS location tracking/vibration sensors to detect stolen devices
- Installing remote lock/remote wiping to prevent stolen devices being re-used elsewhere.

Applications

Ensure that information can only be accessed through approved applications, and that they are up to date.

Access to your networks and information systems must be controlled by automatically preventing access if the application:

- Is not approved or authorized by your IT department.
- Does not have a valid, approved signature.
- Is not the most current, approved version.
- Is running on an unrecognized/ unauthorized device.

If developing applications as part of an integrated solution for controlling such things as Connected Home Energy management systems, or for remotely programming EV charging, consider that the users will very likely have no appreciation of security. The applications should require minimal user set up to enable them to perform their role, and must:

- Be developed using a secure software development lifecycle that incorporates OWASP recommendations[5].
- Be penetration tested to ensure that all interfaces are secure.
- Adopt the principles of data minimization by not collecting or storing non-essential information.
- Ensure compliance with privacy regulations, and if processing payment details, comply with industry standards (e.g., PCI[6] for electronic payments).
- Incorporate multifactor authentication mechanisms to validate user identity if sensitive information is being exchanged, accessed or modified.

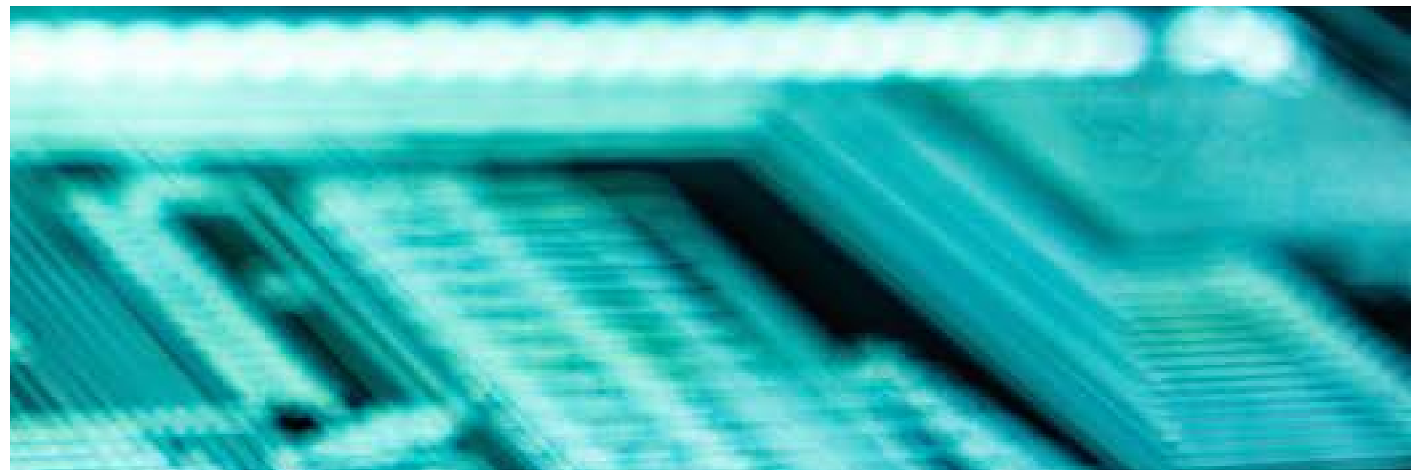
[5] OWASP The Open Web Application Security Project is a nonprofit foundation that works to improve thsssse security of software

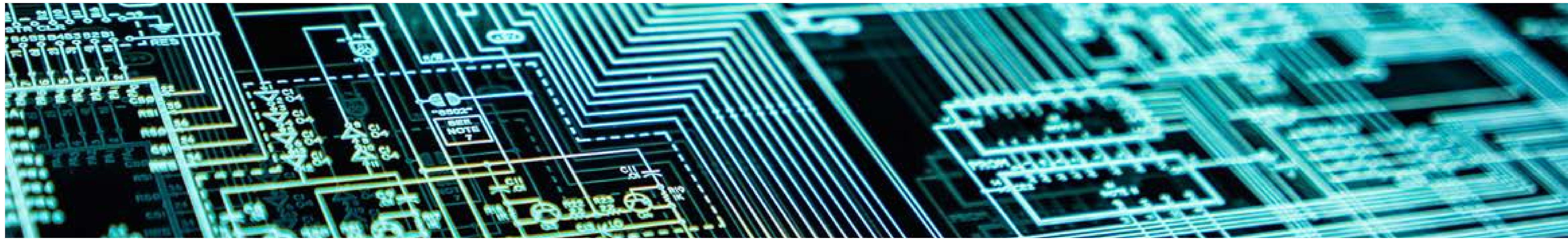
[6] The Payment Card Industry Data Security Standard

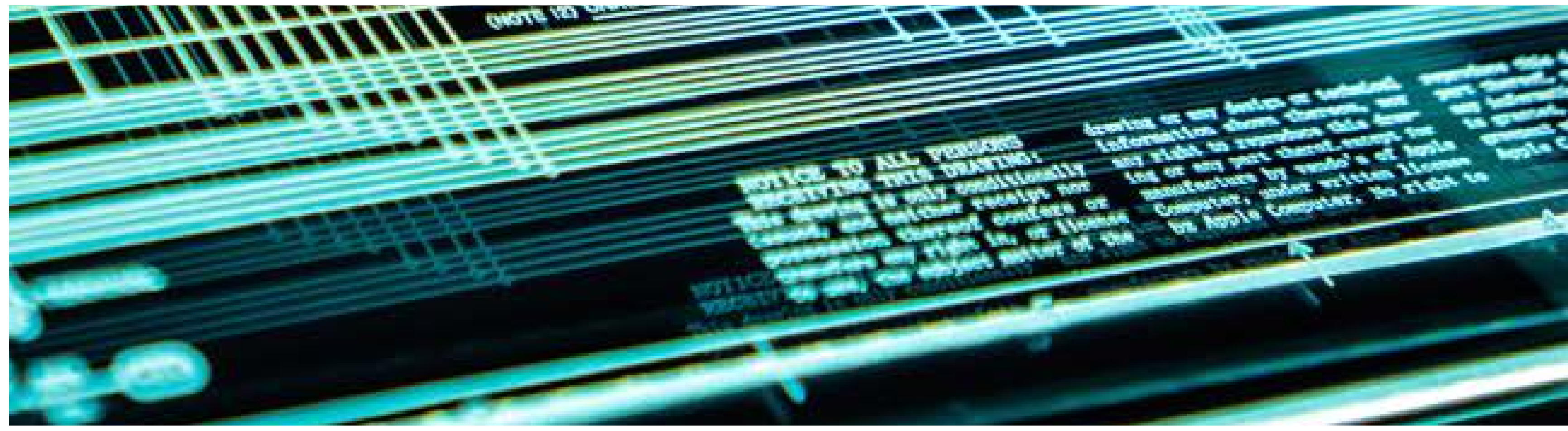
Analytics

Typically, a set of access and usage rules should be applied in the workplace. Logs associated with usage, performance, access and errors should be automatically collected and scanned to build up a picture of normal operation and detect anomalous actions. Additional safeguards can be put in place by collecting logs relating to behavioral attributes such as user, device and network flows. These will allow the detection of deviations from permitted actions, and dynamic risk scoring to be used to request additional identity authentication if risk scores reach a threshold based on anomalous or other unexpected behaviors.

For example, additional proof of identity can be requested if an individual attempts to access sensitive information from a personal device, or at an unusual time or location. Advanced analytics mechanisms can integrate information from firewalls and network monitoring mechanisms with reports from threat databases, so that patterns associated with malware, ransomware, social engineering and other malicious activities can be scanned for and automatically prevented.







Automation

Automation underpins effective security implementation. Ecosystem service providers can enable automated mechanisms to scan security logs and access patterns to detect anomalous behaviors (which could include unauthorized access to systems through hidden "backdoors" installed by malicious actors in third party devices or applications).
Not all anomalous behavior will indicate cyber intrusion. Some could be indicative of employee error, device failure or fault. Regular model tuning will be required to avoid false positives caused by genuine access attempts that trigger alerts.

It is unrealistic to expect domestic connected energy ecosystem users to have incorporated security scanning within their home network. However, automating the set up and configuration of IoT devices and applications that you provide for use within smart buildings will ensure that they conform to your recommended security practices. This not only ensures that your applications and devices are installed and set up securely, but also helps to create a positive user experience, enhancing brand image.

How Accenture can help

Accenture brings deep expertise in Connected Energy and EV, IT and OT security, a broad market understanding, and industry knowledge to develop and provide secure solutions.

Value proposition

Highly Experienced OT and IoT Security Team

We have a large global team of with over 7500 OT and Industry X security professionals across multiple disciplines. The team has extensive OT security skills in diverse industries, leveraging a unique OT cybersecurity approach, methodology and assets.

From an IoT perspective, Accenture provides a wide range of security services to enable the benefits of using IoT technologies while maintaining the required security and privacy measures, ensuring availability, integrity, confidentiality and safety through orchestrated security measures on IoT devices, systems and integrated components. Accenture's approach to IoT Security helps the client to establish an effective end-to-end security strategy across the IoT ecosystem, using the most advanced technologies on the market and security frameworks such as NIST and MITRE.

Truly Global Partner

One cohesive team will scale across the globe as the client requires and ensure consistency in the definition and execution of activities and deliverables across regions.

End-To-End Cybersecurity Player

We have 20+ years in serving global organizations to assess, define, deploy and manage (end-to-end) their cybersecurity programs. We have global scalability to support security strategy, cyber defense, digital identity, application security and OT managed security services (MSS).

OT Security Technology Ecosystem

Accenture maintains strong alliances, partnerships and joint initiatives with a large pool of security, cloud, and technology vendors as well as system integrators and OEMs, while always respecting a vendor-neutral position.

Innovative Approach to Cybersecurity

We have made significant and sustained investments in experts and innovation centers, generating insights and assets to build forward-looking OT security capabilities aligned with business strategy. We are also actively participating in the entities framing and building the cybersecurity regulation space.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Song, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries.

We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com

699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries

Disclaimer
This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

References

[1] Small but mighty: The Netherlands' leading role in electric vehicle adoption, ICCT, February 2021

[2] Dutch government to invest €30m in public charging stations, Fleet Europe, July 2020

[3] Global EV charging points hit 1 million threshold, Bloomberg, 2020

[4] Hackers steal casino's customer data via connected fish tank, Internet of Business

[5] OWASP The Open Web Application Security Project is a nonprofit foundation that works to improve thsssse security of software

[6] The Payment Card Industry Data Security Standard

Contacts

Allan Haughton
Principal Director,
Technology OT Security

Karen Vickery
Senior Principal,
Europe Industry X

Samuel Linares
Managing Director,
Global Industry X and
OT Security Lead

Maikel Van Verseveld
IX Global Delivery Lead

Sanda Tuzlic
Managing Director, Global
Connected Energy Lead