IoT Security:
Empowering the Evolution of IoT

WHITE PAPER 10.2025

IoT Security: Why It Matters for Your Business

For years, we've all talked about the future of business regarding digital transformation. However, business has already transformed: You now work and innovate digitally. Your customers also make purchasing decisions and transactions online. The future of business technology is not transformation but evolution.

The emergence and rapid expansion of the Internet of Things (IoT) is a clear example. Our day-to-day lives are marked by myriad interactions with connected devices that generate terabytes of real-time data.

It's estimated that by 2030, the number of IoT devices will reach over 40 billion. Moreover, the IoT market could generate $2.65 trillion in value.

IoT Market in 2030

40 BILLION
IoT Devices Worldwide

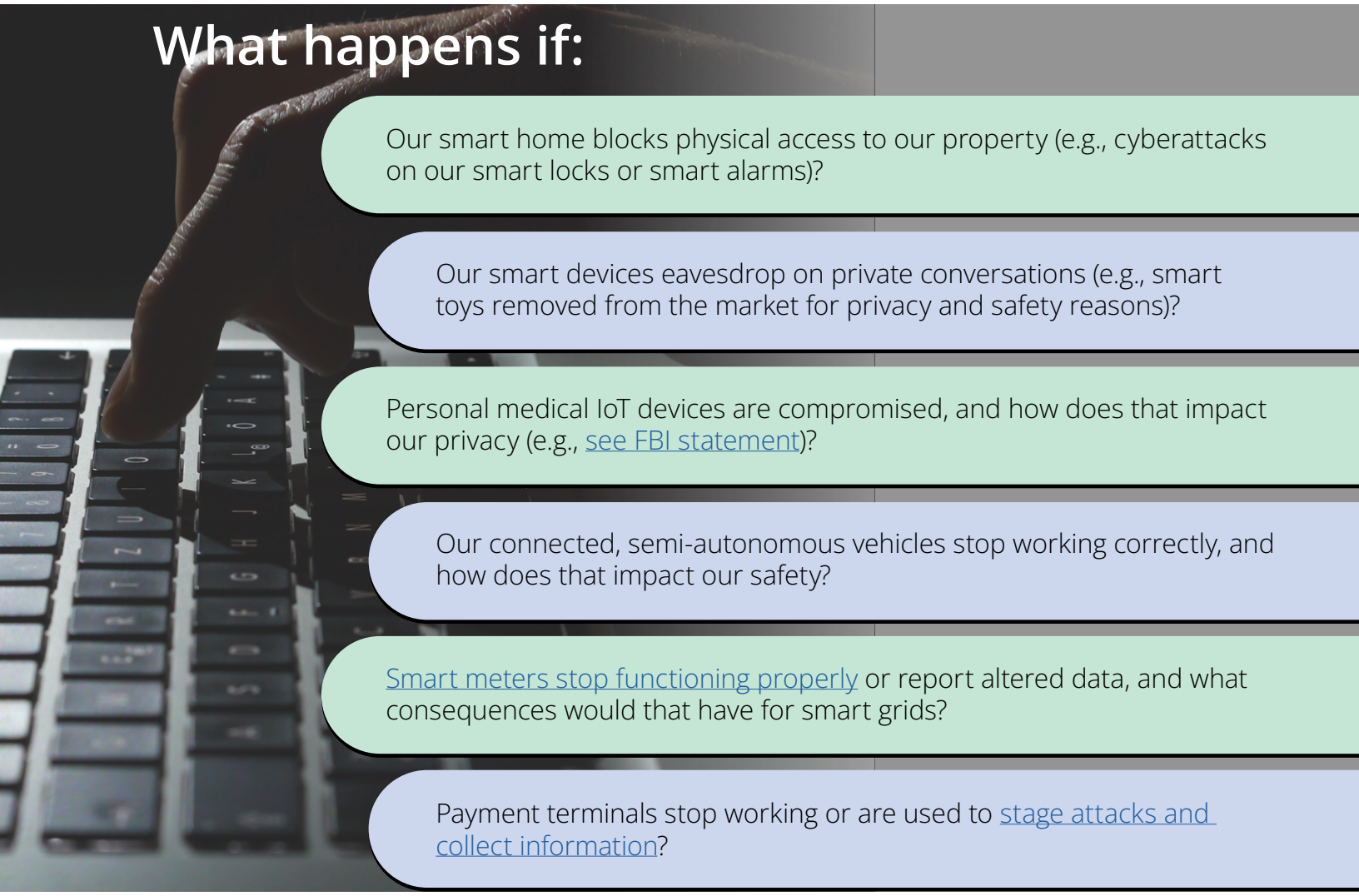
$2.65 TRILLION
Market Value

Still, enormous opportunity comes with risks. As IoT has matured and evolved, data is created and transmitted at every node of the value chain. It stretches from manufacture and distribution to point-of-sale and the consumer. Each connection point allows cybercriminals to access critical systems and sensitive customer data.

Using multiple IoT solutions is becoming more pervasive in our daily lives and will continue to be in the future. What will the impact of cyberattacks be?

Contents

Telit Cinterion



What happens if:

- Our smart home blocks physical access to our property (e.g., cyberattacks on our smart locks or smart alarms)?
- Our smart devices eavesdrop on private conversations (e.g., smart toys removed from the market for privacy and safety reasons)?
- Personal medical IoT devices are compromised, and how does that impact our privacy (e.g., see FBI statement)?
- Our connected, semi-autonomous vehicles stop working correctly, and how does that impact our safety?
- Smart meters stop functioning properly or report altered data, and what consequences would that have for smart grids?
- Payment terminals stop working or are used to stage attacks and collect information?

To protect against such threats, organizations must take a comprehensive, systemwide approach to evaluate risk and defend complex IoT ecosystems.

For over 30 years, we have embedded innovative security technology into every layer of our customers' IoT strategy to evolve faster than malicious attackers. Leveraging the experience of two leaders in the IoT industry, Telit Cinterion has the knowledge and expertise to help you protect your IoT deployment.

In this white paper, our IoT security experts provide an overview of the current and future cyberthreat landscape. In addition, we offer proven solutions to help you create value through multilayer, end-to-end IoT security.

The IoT Threat Landscape: Understanding the Growing Risks

Cyberattacks on IoT infrastructure have grown exponentially in the last few years. In the first half of 2021 alone, there were **1.5 billion IoT cyber incidents**. That six-month total was 639 million more attacks than occurred in all of 2020. With the global IoT market projected to grow at a compound annual growth rate (CAGR) of 11.4%, attacks seem likely to increase.

1.5 Billion Cyberattacks
First Six Months of 2021

639 Million More Cyberattacks
Than All of 2020

To better protect your IoT strategy, you must understand why such attacks are on the rise and why IoT makes such a tempting target for cybercriminals.

The Current State of IoT Security: By the Numbers

IoT's proliferation has been matched by the increased attacks on its expanding surface. In the past few years alone:

- **Fifty-seven percent of IoT devices** were found to be vulnerable to medium- to high-level attacks
- New attacks can arise as quickly as **15 minutes** following the publication of common vulnerabilities and exposures (CVE) lists
- New attacks have occurred in as little as **five minutes** after a device is connected to the internet

These indicators provide an essential window into the nature of the threat facing your IoT strategy. Understanding that every additionally connected node in the chain creates an amplified vulnerability is crucial. These susceptibilities make IoT systems attractive to criminals probing them for new devices and weaknesses. Their distributed nature means detection and prevention are necessary across the IoT value chain.

What Do IoT Cybercriminals Want?

IoT cybercriminals target your connected infrastructure hoping they can:

Steal your confidential and personal data. Data thieves can extract sensitive information about your company or intellectual property. They can also access your customers' personally identifiable information (PII) to sell in the underground economy or reuse in further advanced attacks.

IoT ransomware and extortion. A threat agent steals or encrypts data in IoT devices. Then they demand a ransom to recover the data or regain full control of the devices. This attack type could be more pervasive in the coming years due to multiple factors. A similar approach is used to extort a company with threats of releasing sensitive customer information.

Shut down or disrupt services. Attacks may target the functionality of your IoT systems, requiring replacement hardware or full system re-installation. Malware can also corrupt storage repositories and wipe critical files.

Create IoT botnets. A botnet is a group of hacked computers or coordinating systems within your environment. Criminals often leverage them to execute a distributed denial of service (DDoS) attack across your organization.

Data alteration. Attacks could modify IoT data (e.g., data from sensors) to commit fraud or create inconsistencies in the data. Altering data could have different consequences depending on the IoT vertical.

Traffic rerouting. Alter legitimate IoT solution communication flows to create service disruptions or forward all traffic to illegitimate third-party entities. This attack directly impacts data confidentiality and integrity.

Attacks targeting IT infrastructure are often designed to give hackers direct control of key systems. This strategy allows them to remain dormant and collect valuable information from inside your environment on demand.

Attacks in the IoT space have been increasing. As a result, multiple international entities (e.g., the FBI) have given several public warnings regarding the rising risks to companies and end users.

Due to the multiple risks and related impact scenarios, companies could face several direct and indirect consequences, including:

- **Financial impacts (e.g., loss of revenue)**
- **Brand reputation**
- **Legal or regulatory issues (e.g., losses due to potential legal claims)**

Moreover, as many IoT solutions are interconnected, these risks could spread through other systems and infrastructures. The potential consequences would increase dramatically.

Why Is IoT Infrastructure Such a Tempting Target for Cyberattacks?

You increase the attack surface when connected devices stretch across your entire ecosystem. According to TechTarget, the greatest security risk to an IoT environment is its scale.

Adopting IoT solutions in an infrastructure without security policies and procedures could increase the risk of "shadow IoT." These IoT ecosystems could be interconnected with IT and OT environments and an easy entry point for attackers.

Such devices' lack of visibility and management could introduce multiple critical risks for organizations. There have been multiple data breaches in which IoT devices have been the first entry point, including:

- Hotel smart locks were hijacked with IoT ransomware to lock guests out of their rooms
- Multiple cases of security breaches in IoT-enabled vehicles
- A casino was hacked via its IoT fish tank thermometer
- A major U.S. retailer's payment systems were hacked through their connected HVAC systems

In addition, some specific aspects of IoT infrastructure can amplify vulnerabilities. IoT systems are often:

- **Not designed with security in mind.** Many IoT environments are built piecemeal, grafting new capabilities onto old technology platforms. That makes it impossible to engineer security measures in lockstep with the evolution of your IoT strategy.
- **Unrestricted connected devices.** Attackers often have unrestricted physical access to the end device. In successful attack cases, one device can impersonate another when connecting to the back-end system and use functions not intended for the device or non-standard configurations. Back-end systems often lack mechanisms to detect such situations. Without these mechanisms, risks of sensitive data access and fraud increase.
- **Built using low-cost, outdated software and deprecated hardware.** Evolving to leverage IoT requires a real investment. Many organizations attempt to cut corners with deprecated hardware. However, the trade-off can be important security features.
- **Heterogeneous in software and hardware.** It can be challenging to maintain the life cycle of a huge perimeter of devices. Managing IoT identities and securing an IoT solution is not a one-day job. The system must be updated and maintained for its entire lifetime. Many organizations struggle to stick to consistent update schedules for software and manage different security aspects.
- **Subject to common security pitfalls at the device level.** When IoT doesn't leverage a security by design approach, common vulnerabilities can slip through the cracks. These include weak credential management and the protection of data at rest and in transit.

The IoT Value Chain: Understanding the Risks to Your Ecosystem

Many IoT security issues arise because organizations fail to view their technology ecosystem holistically. Cyberattackers will probe your entire system for weaknesses indiscriminately. That means one weak link can break the entire chain of security.

Organizations must take a systemwide view of IoT threats to understand how to best serve the final customers. It's recommended to conduct a comprehensive evaluation to determine risk levels starting with three critical areas across the IoT value chain.

The suggested approach enables organizations to identify weak links and their potential business impact by applying the following IoT security best practices:

1. Managing Supply Chain Risk

- **Ensure device identity and integrity.** Define the identity management strategy for your physical and virtual assets and ensure the integrity of hardware and software bills of materials (BOMs).
- **Prevent intellectual property (IP) loss.** Complex supply chains could introduce the risk of fake components, which may have various business impacts. Implementing policies and procedures with due diligence activities on first-tier suppliers allows better IP protection and management. Protecting and managing IP is a critical business factor for high-tech companies.
- **Block malware insertion.** Implement technical controls (e.g., Secure Boot) to validate software components' authenticity. These protections prevent unwanted code (malware) or corrupted components from loading when a device boots up.
- **Set and follow robust ecosystem standards.** Security should be a fundamental building block for every link in the value chain. Organizations should maintain quality controls for security throughout their environment. Leveraging standardized processes will ensure the usage of up-to-date credentials and timely software maintenance.
- **Protect your brand reputation.** If implemented correctly, the above best practice helps organizations reduce business risk and strengthen brand reputation. Consumer trust and market standing will rise.

2. Best Practices for Managing Network Service Provider Risk

- **Protect your network from DDoS and botnet attacks.** A thorough risk assessment documents the total costs of a DDoS attack at the network level, including the impact on customers. Codify an incident response plan.
- **Ensure data and consumer privacy.** A privacy audit could help correctly implement governance around sensitive customer data and ensure compliance with privacy regulations.
- **Improve resiliency.** Adopt an IoT connectivity partner that provides resilient service and remote subscription management. These offerings enable customers to fulfill multiple vertical market requirements and use cases.

3. Best Practices for Managing Consumer Risk

- **Build trust and confidence.** Take an approach that ensures total transparency with clients and customers across the IoT value chain to build awareness and trust.
- **Ensure health and safety.** Determine whether a breach compromises personally identifiable data, customers' well-being or records (e.g., financial or medical).
- **Preserve and enhance brand loyalty.** Keep customers returning by assuring them that their transactions and personal information are safe.

A Multilayer IoT Ecosystem Requires Multilayer Security

Organizations should develop a comprehensive security strategy for their IoT infrastructure and processes. It must align corporate decisions with cybersecurity goals and risk appetite. A clear and shared strategy across the organization is crucial to avoid operational errors and maintain coordination between stakeholders and security objectives.

Risk management processes should steer the overall strategy. These aim to identify and address IoT environment cybersecurity threats as they evolve.

The critical aspects of the overall process entail:

The correct cataloging of IoT assets and critical functions across the whole ecosystem

Developing various security strategies identified in the risk management process for all IoT environment layers

For example, what works for smart agriculture may not work for securing electronic medical records.

That means breaking IoT capabilities into discrete layers and identifying overlapping transition points. Setting up these defenses enables you to employ targeted security measures at each juncture point. It mirrors how IoT systems operate, from the edge to the center.

In a typical IoT solution, we have a physical device equipped with sensors, peripherals and controllers at the edge. It collects data from the sensors or acts on the physical world.

This device or the close infrastructure has computing capabilities and edge intelligence to:

- **Process data locally**
- **Reduce latency**
- **Increase autonomy**
- **Decrease the load on the network and cloud**

Once the data is ready, it is transmitted through a network to be collected efficiently and securely by specialized systems. Data is then prepared and rationalized for integration into enterprise IT systems, applications and analytics. These extract insights and value to support and enable business processes and decisions.

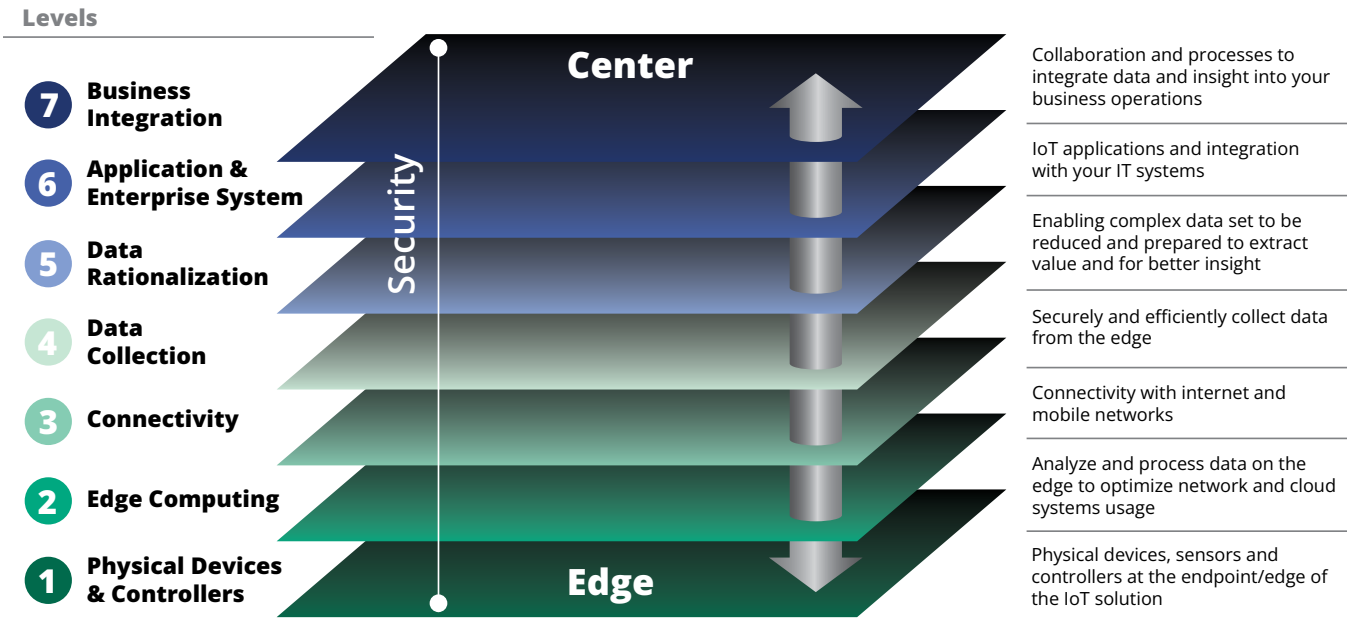


Figure 1: All layers of an IoT environment.

When looking at the setup of an IoT solution, we can identify several attack surfaces that cyberattackers could exploit. In a holistic approach to security, we must make multiple assessments, such as:

- **Secure manufacturing.** Analyze the supply chain processes to verify that the device has not been compromised (e.g., exposing data credentials).
- **Device hardening.** The device should be configured to execute only trusted code. Verify that all the credentials and digital identities are managed correctly and stored securely in a device-protected area.
- **Device management.** The ability to update the software and security patches and monitor the device to spot suspicious behavior.
- **Device digital identities.** Managing digital identities is essential to ensure that the authentication and authorization layers are implemented correctly. This security aspect protects data and access to services.
- **Hyperscalers and third-party service integration.** When adopting and integrating cloud solutions, it's important to understand where the cloud is hosted. You must also know if operations are managed according to best practices and international security frameworks.
- **Connectivity.** Knowing who can manage connectivity configuration or enable or disable the device's SIM card is critical. This can impact security and affect operations.

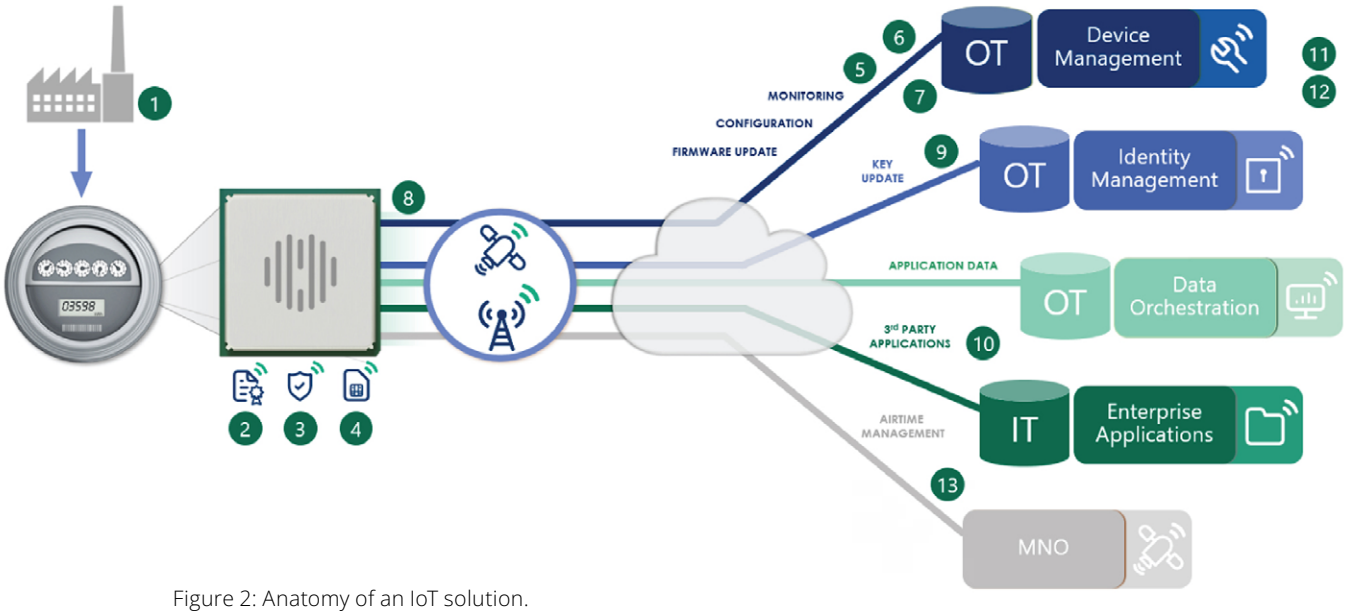


Figure 2: Anatomy of an IoT solution.

13 Questions to Assess IoT Solution Security

1. Has the device been compromised in manufacturing?
2. Can you trust the code running on the device?
3. Who can access and inspect the device?
4. Where is confidential information stored?
5. Can you update the firmware security patches?
6. Who can tamper with device settings?
7. Can you monitor device behavior?
8. Can you detect if your device is under attack?
9. Who manages digital identities and credentials?
10. Are the correct authentication and authorization layers for customer data access implemented?
11. Is the platform operated according to best practices and standards?
12. Where is the cloud platform hosted?
13. Who can manage or disable your SIM card?

Your IoT ecosystem is an overlapping structure, with information moving deeper into your business in discrete layers. Here are examples of layer-specific threats that could impact your IoT solution:

Layer-Specific Cybersecurity Threats and Strategies

Edge Layer

Threat in Action: IoT Malware

Edge devices usually lack hardened physical security protections. In conjunction with other weaknesses, such as device misconfigurations or application vulnerabilities, it could facilitate IoT malware to take control of the edge layer.

For instance, in the consumer market, multiple examples of data breaches and potential malware abuses have been identified on webcams. These breaches allowed a remote third party to spy on end users' private spaces (e.g., baby monitors).

In industrial Internet of Things (IIoT) business environments, there have been multiple malware cases in critical infrastructures. For instance, a major pipeline company suffered a direct impact on service availability.

Connectivity Layer

Threat in Action: IoT Malware

Connectivity vulnerabilities can allow an attacker to take control of a critical device or infiltrate your network. For instance, in 2020, the University of Oklahoma introduced smart clamps for vehicles that violated campus parking laws. Thieves stole SIM cards from these devices and used them to access the network.

Threat in Action: SIM Fraud

SIM cards allow connected devices to send and receive data, making them a tempting target at the edge of IoT systems. For example, criminals in Johannesburg, South Africa, stole hundreds of SIM cards from smart traffic lights.

Cloud Application Layer

Threat in Action: Exploitation of Cloud Vulnerability

Weak device attestation and registration is a cloud application layer vulnerability that can put your applications at risk. Vulnerabilities in the cloud could let remote threat agents access customer data, directly impacting data confidentiality and integrity.

In the case of vehicle assistance services, various vulnerabilities have been highlighted recently. These would have allowed attackers to retrieve the live GPS locations of every device managed by such cloud platforms. In other cases, they could have allowed attackers to:

- **Directly manipulate the engine starter**
- **Lock and unlock the vehicle remotely**
- **Send police and ambulance dispatch locations**

Multiple IoT solutions are strictly interconnected with the real world. Therefore, a weakness in the IoT space could impact our daily lives and global society.

Multilayer Difference for IoT Security

IoT security challenges are problems that stretch across your ecosystem. A systemic approach must be taken to treat security as an essential feature at every layer of your IoT infrastructure from the beginning of the project.

A secure architecture is needed from the endpoints at the edge of your environment toward your central operations, basing the strategy on a set of core principles:

- **Apply security by design by default.** At every layer, build in security from the start rather than adding it later.
- **Secure the manufacturing process.** Look at every process to enforce security, including addressing threats to the supply chain.
- **Create trusted, secure IoT devices.** Ensure that identity and credentials are securely injected and stored into devices during manufacturing. Maintain identities throughout the device's lifetime.
- **Reduce the attack surface.** This approach mitigates whole vulnerability classes by minimizing the target surface and gearing protection toward fewer attackers.
- **Employ defense in depth.** A defense-in-depth methodology combines the newest threat-model approaches with trusted identity and device management.

These principles help build your security level by level. The key points of the security by design approach consider every layer.

Device Security

Focus on protecting your perimeter at the device level, making your system a less attractive target. For solutions based on cellular connectivity, embedded SIM (eSIM) technologies keep your endpoints safely out of malicious actors' reach.

Furthermore, security monitoring and compliance management at the device and fleet deployment level can be complemented by:

- Trusted device identification and authentication
- Secure firmware update processes
- Device and identity life cycle management
- Secure data storage
- Secure communication protocols
- Physical and logical interfaces protection

These protection mechanisms ensure the integrity of your edge at every endpoint.

Network and Connection Security

Robust IoT connectivity management platforms help you:

- Monitor network traffic and usage patterns to identify potential device abuses
- Detect outages and DDoS attacks
- Monitor and detect unauthorized endpoints to avoid fraud
- Address privacy concerns leveraging private APNs, cellular communication encryption and IP secure transport layer

Cloud Application and Data Security

Security at the application level helps build brand trust to guarantee data protection through:

- Adoption of international cybersecurity frameworks for operations and processes
- Business continuity management and resiliency plans
- Multitenancy and physical security using a trusted cloud provider
- Secure end device provisioning into a third-party cloud
- Identity and access management (IAM)
- Encrypted communication links
- Service a data integration for third-party services
- Logging and monitoring

How Our Collaborative, Iterative Approach Works for You

We understand that no other business is quite like yours. We also know that every IoT solution requires a unique, customized approach. Moreover, because the threat landscape evolves along with your business, so do we.

With extensive knowledge and experience in the IoT market, we are uniquely positioned to future-proof your global IoT strategy across the value chain. Our experts collaborate with you to understand your needs and help you build solutions that fit. We offer a comprehensive toolkit to address common risks and vulnerabilities in your IoT ecosystem with the following secure solutions:

IoT Modules Protect Your Edge

Our portfolio of certified, secure cellular IoT modules provides state-of-the-art implementation. They can be used as a stand-alone solution or in a combination. Original equipment manufacturers (OEMs) can create and launch their devices across markets worldwide. Our wireless modules offer security features that include:

- Firmware and code signing
- Secure device credential preloading and identity
- Keystore and critical data protected by hardware building blocks
- State-of-the-art secure socket layer and data encryption
- Security API framework and AT command functions that IoT developers can leverage to create secure applications
- Secured access to serial ports and local interfaces
- Natively equipped with eSIM (iSIM in the future), combined with a service enabling remote subscription management
- Monitor and update your device or your connectivity in the field

NExT™ Protects Your Connections

NExT is an IoT mobile core network. NExT is fully georedundant and provides scalable global connectivity and device management with enterprise-grade security, including:

- Private APN
- VPN
- Access control
- Connectivity management to detect and respond to anomalies
- Network-based security rules and alerts
- Triggers for smart actions on multiple KPIs

deviceWISE® Quickly Connects Plant Floor Devices to Enterprise

A platform that enables easy device and app communication is necessary to build and manage your IIoT solution. deviceWISE, powered by Telit Cinterion, lets you connect your enterprise and apps without writing custom code. In addition, you can set up a closed network for industrial solutions to take advantage of:

- **Policy-based resource access with roles so multiple priority-based policies can be defined and enabled**
- **Access control information is configured for each node**
- **Supports the integration with a centrally managed security service like Active Directory Federation Services (OAuth 2.0)**
- **Security policy control enables or disables a policy defined within a node**
- **Special device drivers support the configuring of individual device variable security**

No matter what IoT solution is best for your business, we have you covered from end to end and strengthen every link in the value chain.

From edge to core to cloud, our security functions give you full life cycle management from fully credentialed experts. We offer industry experience and unique expertise in IoT modules, connectivity, platforms and solutions. This makes us the ideal partner to collaborate on your IoT security strategy.

It's Time to Evolve with Our IoT Solutions

For over 30 years, we have been a leader in global IoT solutions because we believe in the potential of your business. You've done the hard work of digital transformation. IoT will empower the next phase of your future, and security will empower IoT.

Our IoT solutions embrace a 360-degree security by design approach. That means security is built into every layer of your ecosystem, giving you holistic, end-to-end protection. We work with you to find a unique solution and provide the tools and confidence to take the next leap forward.

Build Your Secure IoT Solution with Telit Cinterion

Start Your IoT Journey