The Unique Challenges with Securing Connected Devices

Impacts on manufacturing, regulatory compliance, & documentation

FINITE STATE

Contents

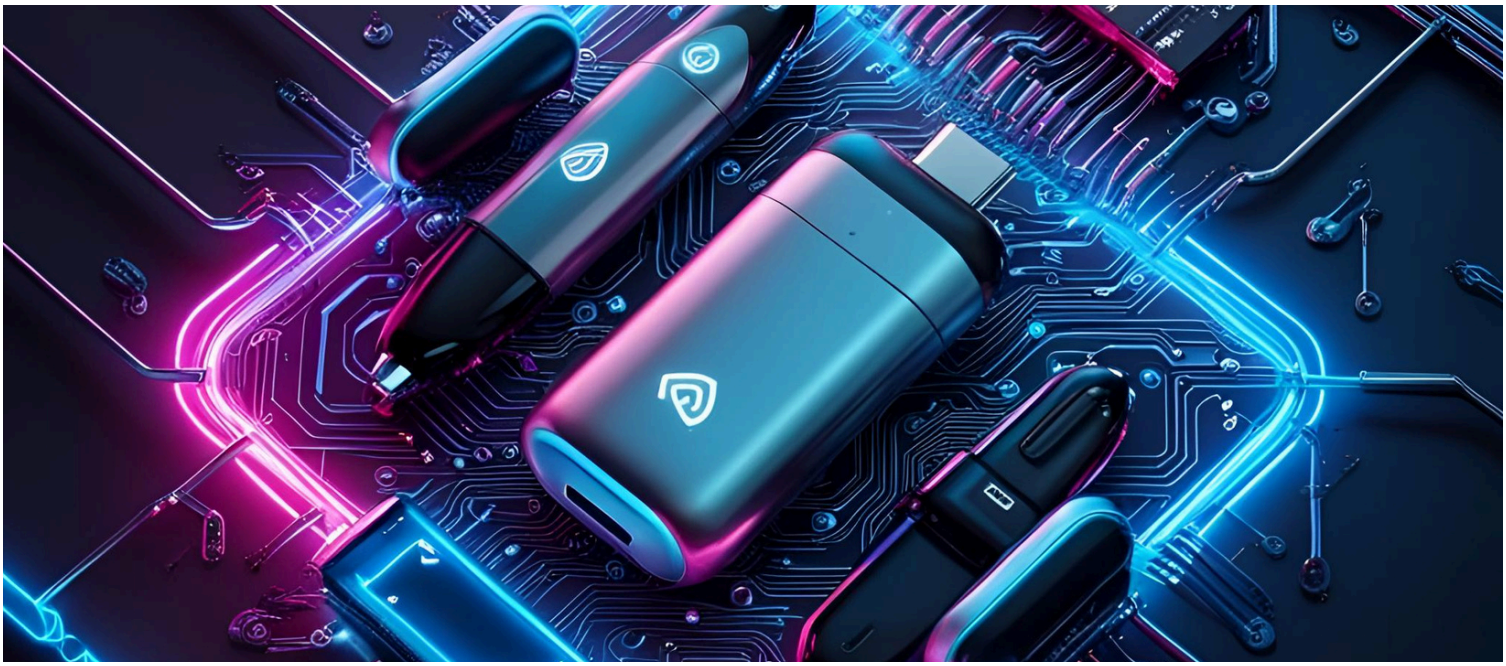
Unique Security Challenges of Connected Devices

Connected devices operate in complex ecosystems that traditional security approaches often fail to protect. This is due, in part, to their unique characteristics — limited resources, extended lifespans, physical accessibility, and intricate supply chains — that create security challenges that are fundamentally different from conventional IT systems.

With explosive growth happening across consumer products, healthcare equipment, industrial systems, and critical infrastructure, the widespread use of interconnected technologies is introducing significant security threats and vulnerabilities.

As security risks escalate, regulatory bodies worldwide have responded with increasingly stringent compliance requirements. For manufacturers and organizations deploying connected devices, understanding these security challenges isn't merely a technical concern — it's becoming a critical regulatory obligation with serious business implications.

> The number of IoT devices worldwide is projected to reach 32 billion by 2030, nearly tripling from the 9.7 billion connected devices in 2020.[1]



Increased Attack Surface & Complexity

Connected devices don't exist in isolation — they form complex ecosystems that interact with multiple networks, cloud services, mobile applications, and other devices. Unlike traditional IT systems, these devices often operate in constrained environments with limited processing power and memory, making them challenging to secure. Each connection point represents a potential entry for attackers.

Examples

Consider smart home environments, where a single vulnerability in a thermostat or doorbell camera could provide access to the entire home network.

In healthcare, connected medical devices like infusion pumps or patient monitors may connect to hospital networks, potentially exposing sensitive systems to compromise if not properly secured.

Industrial control systems face similar challenges, where connectivity between operational technology (OT) and information technology (IT) networks creates new attack pathways.

Supply Chain Vulnerabilty

Modern connected devices rely heavily on a complex web of third-party components, libraries, and open-source software. This reliance on external components introduces significant security gaps that manufacturers may not even be aware of.

The challenge extends beyond software components too. Hardware components sourced from multiple vendors, often with limited transparency into their security practices, further complicate the security picture. When vulnerabilities are discovered in these components, identifying affected devices and coordinating patches becomes tremendously difficult.

> 84% of codebases contain at least one open-source vulnerability, with the average codebase containing 595 dependencies [2]

Lifecycle Management & Patchability

Connected devices like industrial control systems, medical devices, and even some consumer products like smart refrigerators or HVAC systems are designed for extended operation. This extended lifespan creates significant security challenges as new vulnerabilities, threats, and exploits are found in the included software components over time.

Many devices lack automatic update mechanisms, have limited processing power to support new security features, or eventually lose vendor support entirely while actively deployed and operated. The result is a growing population of "legacy" connected devices that cannot be adequately secured against new threats but remain in active use. Each unpatched device represents an expanding security risk over time.

71% of security professionals find patching vulnerable systems overly complex & time-consuming [3]

Default & Hardcoded Credentials

Many connected devices continue to ship with default or hardcoded passwords that users never change. This basic security mistake has led to some of the most devastating cyberattacks targeting connected devices, including the infamous Mirai botnet, which caused widespread internet outages in 2016. More recent botnet variants continue to exploit devices with default passwords, highlighting that this fundamental security issue remains unresolved in many product categories.

Regulatory frameworks, such as the UK's PSTI Act, are now requiring manufacturers to eliminate default passwords and implement stronger authentication mechanisms.

Limited Visibility & Monitoring

Traditional security monitoring tools are designed for conventional IT environments and often cannot effectively monitor connected devices. Without proper monitoring capabilities, silent failures or subtle performance changes that might signal security breaches often go unnoticed until significant damage has occurred.

Data Privacy Considerations

Connected devices often collect vast amounts of sensitive data, from health metrics to behavioral patterns and location information. Securing this data throughout its lifecycle — during collection, transmission, storage, and processing — represents a major challenge that intersects with both security and regulatory compliance.

Physical Security Concerns

Unlike traditional IT assets that typically reside in secured facilities, connected devices are often deployed in physically accessible locations. Smart home devices, public infrastructure sensors, and even medical devices may be accessible to unauthorized individuals.

Physical access to a device can enable attackers to extract firmware, access debug interfaces, or modify hardware in ways that compromise security. These attacks are particularly concerning because they may bypass many software-based security controls.

Insecure Communication Protocols

Many connected devices utilize legacy or proprietary communication protocols that weren't designed with security in mind. For example, Industrial Control Systems often rely on protocols like Modbus or BACnet that lack built-in authentication and encryption.

Even newer devices sometimes prioritize operational functionality and backward compatibility over security, continuing to implement vulnerable communication methods that expose sensitive data and control channels.

98% of IoT device traffic is unencrypted [4]

Limited Encryption Capabilities

Resource constraints often force manufacturers to implement weak encryption or forego it entirely. Many connected devices lack the processing power, memory, or battery capacity to support strong cryptographic algorithms, exposing sensitive data, credentials, and commands to interception.

How Security Challenges Impact Regulatory Compliance

The security challenges of connected devices haven't gone unnoticed by regulatory bodies. In response to growing threats and incidents, governments worldwide have introduced increasingly stringent regulations specifically targeting connected device security. Understanding and complying with these evolving requirements has become a major challenge for manufacturers and deploying organizations.

Key regulations include:

EU Cyber Resilience Act: This landmark regulation introduces mandatory security requirements for products with digital elements. The CRA emphasizes security by design principles, vulnerability management processes, and comprehensive documentation of security measures. To comply, manufacturers will need to perform conformity assessments and maintain security support throughout a product's lifecycle.

NIS2 Directive: Building on the original Network and Information Security Directive, NIS2 expands cybersecurity requirements to additional sectors and imposes stricter risk management measures, incident reporting obligations, and supply chain security requirements. Organizations deploying connected devices in critical infrastructure must ensure these devices meet heightened security expectations.

NIST IoT Cybersecurity Framework: While not a regulation, this framework from the National Institute of Standards and Technology provides guidance that increasingly informs regulatory requirements in the US, like the US Cyber Trust Mark. It emphasizes secure development practices, risk assessment methodologies, and security control implementation for connected devices.

FDA Cybersecurity Requirements: The Food and Drug Administration has strengthened cybersecurity expectations for medical devices through its pre-market submission guidance and post-market security management requirements.

Across these diverse frameworks, common requirements emerge:

- security by design principles
- vulnerability management processes
- transparency about security practices
- ongoing security updates throughout a product's lifecycle.

Compliance Challenges for IoT Manufacturers

Tracking & Securing Third-Party Components

The complex supply chains behind connected devices make compliance documentation extremely challenging. When a single device might incorporate dozens or even hundreds of components from different suppliers, ensuring and documenting the security of each component becomes a massive undertaking.

SBOM Requirements

Software Bills of Materials (SBOMs) are becoming a regulatory expectation. These comprehensive inventories of all software components within a device are essential for vulnerability management but difficult to create and maintain manually.

Continuous Security Assessments

Regulatory frameworks increasingly require ongoing security testing and assessments throughout a product's lifecycle. For resource-constrained manufacturers, conducting regular penetration tests, vulnerability scans, and security audits represents a significant operational burden.

Firmware Vulnerability Management

Regulatory frameworks increasingly expect manufacturers to provide timely security updates for known vulnerabilities, a requirement that can be technically difficult and costly to fulfill without automated vulnerability management.

Authentication & Access Control

Regulatory requirements around strong authentication clash with the reality of many connected devices that still rely on weak access controls. Implementing robust authentication mechanisms while maintaining usability and performance is a significant challenge.

Supply Chain Risk Management

Regulations increasingly hold manufacturers responsible for security throughout their supply chain, requiring formal vendor assessment processes, contractual security requirements, and ongoing monitoring.

Resource Constraints

The technical limitations of many connected devices make implementing certain security controls required by regulations difficult or impossible. Balancing compliance requirements with device capabilities remains a persistent challenge.

45% of companies only do pen-tests once a year. [5]

Outsource this crucial security assessment to Finite State's expert penetration testers & ensure your IoT products are compliant & secure against the threats of tomorrow.

Contact us today to learn more.

Penalties for Non-Compliance

Financial Penalties: Under frameworks like the EU Cyber Resilience Act, non-compliance can result in fines up to €15 million or 2.5% of worldwide annual turnover, whichever is higher. Even smaller regulatory actions can have a significant financial impact.

Market Access Restrictions: Non-compliant products may be prohibited from sale in regulated markets. For example, the UK's PSTI Act enforces compliance by restricting non-compliant devices from the UK market, potentially cutting manufacturers off from millions of customers.

Mandatory Recalls: Regulatory bodies like the FDA have the authority to order recalls of devices with significant security vulnerabilities.

Reputational Damage: Beyond direct regulatory consequences, security failures can devastate brand reputation.

How to Overcome These Challenges

Despite the complexity of connected device security and compliance, organizations can implement effective strategies to address these challenges:

Implementing Security by Design

To protect connected devices, security must be integrated from the earliest stages of product development, not added as an afterthought. This approach aligns with regulatory expectations set out by the EU CRA and produces more secure products.

Security by design includes:

Framework Adoption: Organizations should adopt established security frameworks like NIST's Secure Software Development Framework (SSDF) or IEC 62443 for industrial systems. These frameworks provide structured approaches to incorporating security throughout the development lifecycle.

Threat Modeling: Systematic threat modeling helps identify potential vulnerabilities before implementation begins.

Secure Development Practices: Implementing secure coding standards, automated security testing, and developer security training creates a foundation for secure products. Organizations that integrate security testing throughout development identify vulnerabilities earlier, when the time and cost to resolve them is much lower.

70–89%

of risk vulnerabilities are addressed by threat modeling [6]

Deploying with Secure-by-Default

Secure-by-default deployment of connected devices ensures that security is a fundamental aspect of the device from the moment it is installed. This approach minimizes vulnerabilities and reduces the risk of cyber threats.

Key principles and best practices include:

Secure Configuration from Factory

- Unique Credentials: Devices should ship with unique, strong passwords rather than default credentials.
- Minimal Open Ports: Only necessary ports and services should be enabled by default.

Authentication & Access Control

- Multi-Factor Authentication (MFA): Require additional authentication for critical actions.
- Device Identity Management: Each device should have a unique, cryptographically verifiable identity.
- Monitoring and Alerts: Monitor and automatically alert any suspicious activities.

Only 33% of IoT device users change their default passwords [7]

Secure Communication

- Encryption: Use TLS/SSL for data transmission.
- Mutual Authentication: Require both device and server authentication before data exchange.

Automatic & Verified Updates

- Secure Update Mechanism: Implement signed firmware updates to prevent tampering.
- Automatic Patch Deployment: Devices should automatically receive security patches.
- Rollback Protection: Prevent downgrades to insecure firmware versions.

Privacy & Data Protection

- Minimal Data Collection: Collect only the necessary data and anonymize sensitive information.
- Local Processing: Where possible, process data locally rather than sending it to the cloud.
- Data Encryption: Encrypt data in transit as well as in storage to prevent unauthorized access.

End-of-Life & Secure Disposal

- Secure Decommissioning: Provide mechanisms to wipe data before device disposal.
- User Notification: Notify users when a device reaches end-of-life support

Strengthening Supply Chain Security

Since third-party components introduce security risks, managing security throughout the supply chain is essential for both security and compliance. To better secure connected devices, manufacturers should implement:

Vendor Security Assessment: Implementing formal security assessments for component suppliers helps ensure they meet minimum security standards. These assessments should evaluate security practices, incident response capabilities, and compliance with relevant standards.

Software Composition Analysis (SCA): SCA solutions should be integrated into both development processes and ongoing monitoring to catch newly discovered vulnerabilities in existing components. Using automated tools like Finite State, which can conduct both source code and binary analysis, reduces resource strain and helps security teams identify and track third-party components and their known vulnerabilities, regardless of origin.

Contractual Security Requirements: Establishing formal security requirements in supplier contracts creates clear expectations and accountability. These requirements should address security practices, vulnerability disclosure, and patching responsibilities and timelines for all suppliers.

> Automation cuts time to identify & contain security breaches by 30% [8]

Automate Continuous Security Testing & Vulnerability Management

Regular security testing is essential for identifying vulnerabilities before attackers do:

Penetration Testing: Regular penetration testing by skilled security professionals helps identify vulnerabilities that automated tools might miss. Organizations should conduct penetration tests before major releases and periodically throughout a product's lifetime.

Automated Security Scanning & Real-Time Monitoring: Implementing automated vulnerability scanning tools specifically designed for connected devices, like Finite State, provides continuous visibility into potential security issues. These tools should be incorporated into CI/CD pipelines and deployment processes for complete coverage. Automated scan should cover the following aspects.

- Software Compositions Analysis (SCA)
- Static Application Security testing (SAST)
- Dynamic Application Security testing (DAST)

Proactive Compliance Strategy

Taking a strategic approach to compliance reduces costs and improves outcomes, which is why organizations should prioritize:

Regulatory Monitoring: Establishing processes to track evolving regulations ensures early awareness of new requirements.

Compliance Automation: Implementing tools that automate aspects of compliance reporting and documentation reduces manual effort.

Cross-Functional Collaboration: Creating collaboration mechanisms between engineering, security, legal, and compliance teams ensures regulatory requirements are understood and addressed throughout product development. Regular cross-functional reviews help identify compliance gaps early.

Transparency Through SBOMs & Documentation

Regulatory frameworks increasingly mandate detailed visibility into software components. To stay compliant, manufacturers should implement:

Automated SBOM Generation: Implementing tools that automatically generate and update Software Bills of Materials reduces the manual effort required for compliance. These tools should integrate with development environments to ensure SBOMs remain current as components change.

Vulnerability Management Processes: Establishing clear processes for identifying, tracking, and remediating vulnerabilities in third-party components helps maintain security throughout a product's lifecycle. These processes should include regular component updates and security patches.

Documentation Standards: Creating standardized templates for security documentation ensures consistency and completeness. These templates should align with regulatory requirements to streamline compliance efforts.

Conclusion

Connected devices face unique security challenges that traditional approaches often fail to address. From resource constraints and complex supply chains to lifecycle management and physical security concerns, these challenges create significant security risks that increasingly impact regulatory compliance.

As regulatory frameworks evolve to address these risks, manufacturers and organizations deploying connected devices must adapt their security and compliance strategies. By implementing security by design principles, strengthening supply chain security, automating security testing, maintaining transparent documentation, and adopting proactive compliance approaches, organizations can navigate this complex landscape successfully.

The path forward requires a fundamental shift in how organizations approach connected device security—moving from security as a compliance checkbox to security as a core design principle. Those that make this shift will not only meet regulatory requirements but also build more secure, trustworthy products that stand out in an increasingly security-conscious market.

To learn how Finite State helps manufacturers secure connected devices and meet compliance requirements, contact us today.

Finite State | Purpose-Built for IoT & Embedded Systems

Our platform offers continuous visibility into your entire product portfolio, monitoring for new threats, providing proactive alerts, and developer-friendly remediation guidance that integrates seamlessly into your existing workflows.

✓ Prioritize actions based on exploit availability and severity

✓ Continuous monitoring with real-time vulnerability alerts

✓ Remediate with tailored recommendations and automated fixes

✓ Seamless DevSecOps and product security integrations

- Automatic firmware unpacking and analysis
- Identify vulnerabilities in proprietary code, vendor-supplied code, COTS software, and open source software and their dependencies
- Support for 18+ programming languages, 130+ binary formats, and 30+ architectures

References

1. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
2. https://www.csoonline.com/article/574607/at-least-one-open-source-vulnerability-found-in-84-of-code-bases-report.html
3. https://www.darkreading.com/vulnerabilities-threats/71-of-security-pros-find-patching-to-be-complex-and-time-consuming-ivanti-study-confirms
4. https://www.paloaltonetworks.ca/cybersecurity-perspectives/expanding-iot-visibility
5. https://elitesec.io/blog/limitations-of-pentesting/
6. https://www.securitycompass.com/reports/the-2023-state-of-threat-modeling/#:~:text=Threat%20Modeling%20Tool).-,Challenges,90%25+)%20high%20risk%20vulnerabilities
7. https://patentpc.com/blog/iot-security-challenges-device-vulnerability-attack-stats
8. https://securityintelligence.com/articles/security-automation-save-data-breach/