digicert®

Device Trust: Securing the Future of Smart Technology

EBOOK

Table of Contents

Introduction

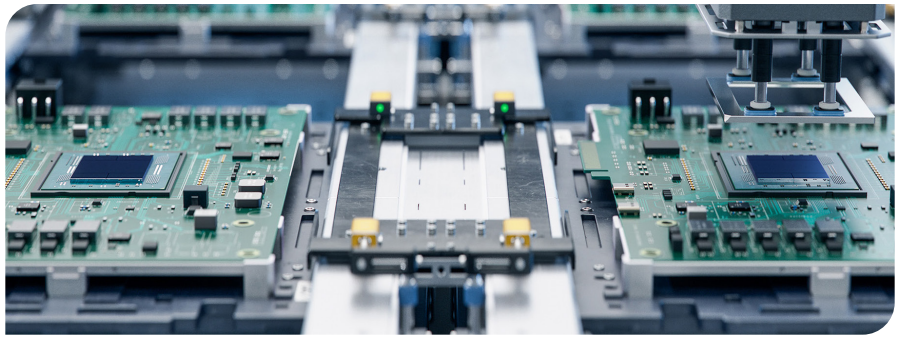
The promise and peril of an increasinlgy Connected World

The world grows more connected every day, creating a landscape rife with opportunities—and vulnerabilities. The dangers facing the connected device market are evolving as rapidly as the technology itself, threatening not just individual users but the integrity of entire networks.

More devices mean more attack vectors. A single breach can trigger the devastating loss of both data and dollars, eroding customer trust and shaking the foundations of organizations large and small.

And as manufacturers and developers capitalize on the public's hunger for connectivity, those that deprioritize security will continue feeding into the booming business of device breaches—a criminal industry that's expected to put $10 trillion in attackers' pockets by 2025.

The question isn't whether you can afford to invest in device security. It's how long can you afford not to. Device trust is a necessity, not a feature. And there are four key ways it can help you stand up to attackers—and stand out in a sea of competitors.



Chapter 1

Security-first Marketing

The manufacturing landscape for connected devices is increasingly security-conscious, recognizing the need for a robust defense against a growing array of threats, which includes identity, tamper-resistance and compliance.

Implementing an Immutable Digital Identity

Device trust secures a device's identity from the moment of its creation, ensuring that its integrity remains unbroken through every phase of its lifecycle. Immutable identities guard against a range of attacks, providing a secure baseline that bolsters the entire manufacturing process.

Engineering Tamper Resistance

The importance of tamper-resistant operations is underscored by the risk of unauthorized modifications, which can compromise not just individual devices but entire networks. With device trust, tamper resistance is engineered into devices via multiple layers of security, including hardware trust anchors and secure boot processes. These features serve as a deterrent to physical tampering and safeguard the device's software integrity, preserving the manufacturer's intellectual property and the user's data.

Adhering to Global Compliance Standards

Device trust manages the complexities of compliance by incorporating features that help manufacturers align with international security protocols through measures like pre-defined compliance templates that map onto regulations, helping manufacturers avoid the pitfalls of non-conformance.

Security-first Marketing in the Real World

We're already seeing the efficacy of these security measures play out in real- world applications like these:

- An electronics company utilized device trust to embed unalterable identities into their smart home products, ensuring that each device's origin and firmware updates remained authenticated and secure from production to customer use.

- A manufacturer of industrial sensors used tamper-resistant features to protect their devices operating in critical infrastructure, reinforcing the resilience of their products.
- Device trust enabled an international home appliance manufacturer to navigate the intricate web of data privacy laws across different regions. Customizing security profiles for various markets ensured that each device met local standards without a complete redesign, saving time and resources.

Device trust provides a comprehensive security framework that starts with the inception of each connected device. By embedding immutable identities, ensuring tamper resistance and facilitating global compliance, device trust not only fortifies the manufacturing process but also enhances the trustworthiness of devices in the field.

Chapter 2

Agile Manufacturing

Flexible deployment options have become a cornerstone of the agility necessitated by the fast-paced world of connected devices, allowing manufacturers to adapt to different environments and requirements swiftly and effectively. The ability to deploy security measures that aren't constrained by a one-size-fits-all approach enables a tailored security posture that fits the unique blueprint of each manufacturing setup. This flexibility isn't just about adapting to different physical environments—it also accommodates the varying technological landscapes that manufacturers face.

Adhering to Diverse Regional Data Protection Laws

One of the biggest challenges for manufacturers aiming to scale globally is maintaining a uniform security standard while adhering to regional data protection laws that can vary greatly from place to place. Scaling operations across borders requires a meticulous orchestration of security practices that align with each region's compliance mandates without impeding the speed and scale of deployment.

The use of a security solution that doesn't enforce a rigid framework but instead provides the tools to scale up operations ensures that manufacturers can grow their global footprint without compromising on the security of their devices.

Taking a Balanced Approach to Device Resource and Memory Availability

The variable nature of device resources and memory in the IoT space necessitates a resource-adaptive security solution. Devices with limited processing power or memory can pose a problem for a resource-intensive security system, but a system that's too lightweight may not offer adequate protection for more capable devices.

A balanced approach that adjusts to the resource profile of each device ensures optimal security without unnecessary overhead. This adaptability is key to ensuring that security can be as robust as needed on high-end devices while remaining lean and efficient on more constrained devices.

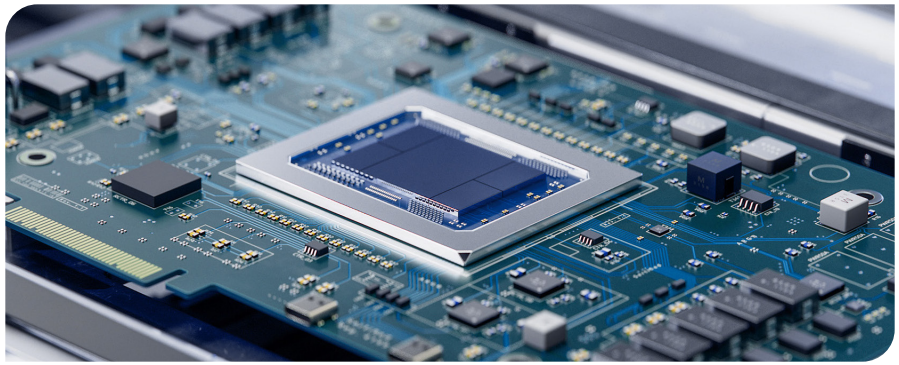
By embedding flexible deployment principles into their manufacturing processes, companies can navigate the complexities of the modern IoT landscape with confidence.

Agile IoT Manufacturing in the Real World

Real-world applications demonstrate the success of manufacturing processes that integrate these principles:

- A consumer electronics company leveraged flexible and scalable security solutions to manage a diverse product line ranging from high-end smart televisions to basic IoT-enabled home gadgets. The ability to adapt security measures to each product's capabilities and market requirements was essential to the company's successful global deployment.
- In an industrial setting, a company producing sensors for smart agriculture utilized these principles to manage devices deployed across different continents, each with its own set of environmental conditions and regulatory requirements. The resource-adaptive nature of the security solution ensured that devices with minimal computing capabilities could still operate securely, even in remote and resource- constrained environments.

By embedding flexible deployment principles into their manufacturing processes, companies can navigate the complexities of the modern IoT landscape with confidence. The agility afforded by flexible deployment, the assurance of global scalability and the precision of resource-adaptive security work together to create a resilient manufacturing ecosystem capable of meeting the demands of the present and anticipating the needs of the future.



Chapter 3

Operational Excellence

In IoT manufacturing, operational excellence hinges on a seamless interplay between automated processes and robust security measures. The heart of this operational strategy is the automated management of the certificates that serve as the bedrock of device identity and security in the IoT space. By automating this lifecycle—from issuing and renewing to revoking certificates—manufacturers can ensure that the identities of the devices they produce are managed with precision and without the risk of human error.

This automated certificate management extends into the realm of device operations in the field. Post-deployment, devices can receive updates and security patches remotely, with minimal downtime and without the need for physical intervention. The implications for operational efficiency are significant. Devices can remain in the field longer, with a reduced need for recalls or manual updates, saving time and resources.

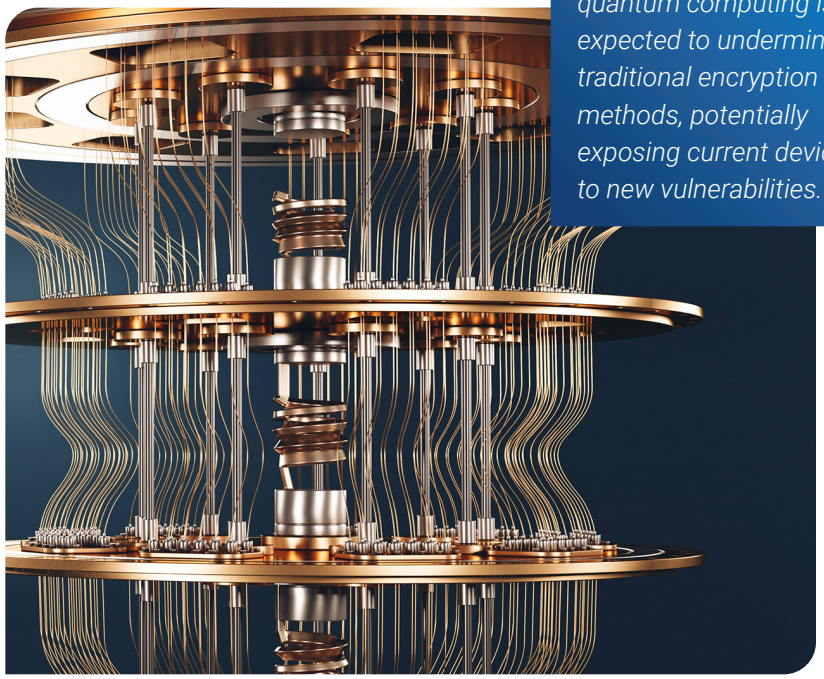
Real-world Applications of Automated Certificate Management

The ubiquity of smart technology means device trust can introduce operational excellence into a wide range of settings:

- In a smart city initiative, thousands of sensors and devices collect and transmit data to manage traffic, energy consumption and public safety. Automated certificate management within these devices ensures that data flows securely and that each device's identity is authenticated, providing assurance that the information relied upon for critical decisions is both accurate and secure.
- In the healthcare sector, where devices range from in-hospital monitoring equipment to wearable health trackers, the need for stringent security and reliable device operation is paramount. Automation in certificate and identity management allows for these devices to be rapidly updated with the latest security credentials, ensuring patient data is protected and that healthcare providers can trust the integrity of the data they receive.

- In manufacturing operations, automated security management translates into devices that can adapt to changing security landscapes. As threats evolve, so too can the security posture of devices in the field, with minimal operational disruption. This adaptability is crucial for maintaining the trust of consumers and the reputation of manufacturers.

The integration of automated certificate lifecycle management and identity management into IoT device operations represents a leap forward in operational excellence. It enhances security, reduces operational risks and improves the overall reliability of IoT ecosystems, ensuring that they can support the demands of modern infrastructure and society.



The emerging threat of quantum computing is expected to undermine traditional encryption methods, potentially exposing current devices to new vulnerabilities.

Chapter 4

Future-Proof Manufacturing

The landscape of IoT security is constantly changing, which means manufacturers can't afford to focus only on present concerns—they must also anticipate future challenges.

Preparing for Quantum Computing

The emerging threat of quantum computing is expected to undermine traditional encryption methods, potentially exposing current devices to new vulnerabilities. The strategic incorporation of post-quantum cryptography (PQC) prepares devices for this eventuality, safeguarding them against the decryption capabilities of quantum computers and ensuring long-term device integrity and data privacy.

Adopting Emerging Technologies

Technologies like MQTT 5.0 provide enhanced features for message queuing in device communication, offering greater levels of security, improved data handling and more efficient device-to-device communication. Similarly, Kubernetes, an open-source system for automating deployment, scaling and management of containerized applications, introduces agility and scalability in device management.

By integrating MQTT 5.0, Kubernetes and other emerging technologies, manufacturers can manage IoT devices more effectively, ensuring that the infrastructure is robust, responsive and adaptable to the rapid pace of technological advancement.

Staying One Step Ahead of Regulatory Changes

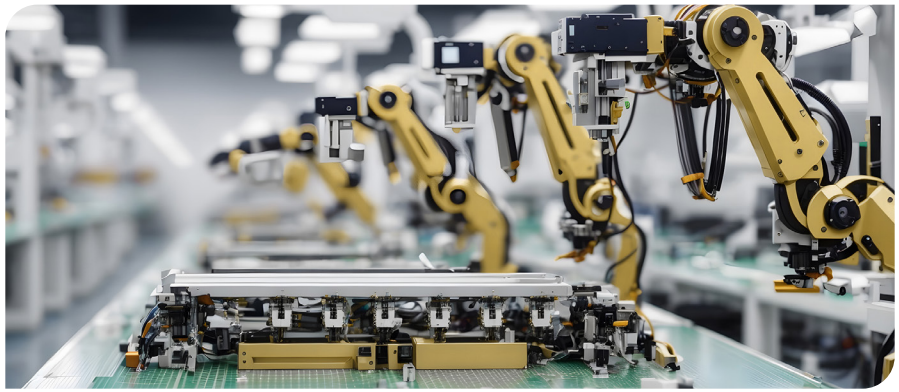
Compliance with industry standards is a moving target, with benchmarks continually shifting as new security threats emerge and regulations evolve. Staying ahead in compliance means not just adhering to the current set of standards but also actively participating in the dialogue that shapes these regulations.

By engaging with standard-setting bodies and technical working groups, manufacturers can gain insights into upcoming changes and prepare their products accordingly. This proactive approach to compliance allows for a smoother transition when new standards come into effect, avoiding costly overhauls and ensuring that products remain on the leading edge of security practices.

The strategic advantage of aligning with evolving standards also positions manufacturers as leaders in the industry, ready to meet the demands of security-conscious customers and to navigate the complexities of global markets with different regulatory requirements. It also serves as a signal to stakeholders that the manufacturer is committed to maintaining the highest security standards, building trust and enhancing the brand's reputation.

The key to future-proofing manufacturing in the IoT domain

Anticipating emerging threats, adopting innovative technologies and taking a proactive stance on compliance will help manufacturers ensure that their products are not only secure for today but also resilient against the challenges of tomorrow. This strategic foresight is what will differentiate the leaders in the IoT space, enabling them to deliver secure, reliable and cutting-edge products that stand the test of time and technology.



Chapter 5

The tangible impacts of Device Trust

There's no better measure of a robust device security framework's impact than real-world customers who have firsthand experience with the transformative power of device trust. The following case studies not only illustrate the practical applications of such a framework but also highlight measurable business impacts, fostering a deeper understanding of the strategic advantages these solutions afford.

Case Study #1

Customer: A leading manufacturer of smart home devices

Solution: Implement a security framework across a full range of products

Result: The customer documented a dramatic reduction in the incidence of security breaches, with an accompanying increase in consumer trust reflected in a significant uptick in market share and a stronger brand reputation. The manufacturer was able to quantify the benefits, with a reported return on investment that far exceeded initial projections.

Case Study #2

Customer: A multinational corporation specializing in industrial IoT devices

Solution: Streamline compliance processes

Result: By integrating a sophisticated device security solution, the company streamlined its compliance processes, resulting in cost savings and a faster time-to-market for new products. The security framework enabled them to automate critical aspects of device security management, reducing the workload on their IT teams and diminishing the risk of human error in certificate management.

Case Study #3

Customer: A major automotive manufacturer

Solution: Develop a custom security solution

Result: The development of custom security solution led to the creation of a highly secure connected car platform. The success of this partnership not only solidified the manufacturer's position as an innovator in automotive technology but also showcased the provider's commitment to and expertise in addressing unique industry challenges.

The ability to demonstrate a proactive and comprehensive approach to security is invaluable in an era where data breaches and security vulnerabilities are high-profile news stories.

Security Solutions that leave a lasting impact

The business impacts of the solutions implemented in these case studies aren't just operational—they have strategic implications that extend into how these companies are perceived in the industry. The ability to demonstrate a proactive and comprehensive approach to security is invaluable in an era where data breaches and security vulnerabilities are high-profile news stories.

Conclusion

Safeguard yor devices to safeguard your business

Safeguard your devices to safeguard your business

The stakes for device security and operational excellence have never been higher. For manufacturers seeking to navigate such a complex security landscape, the choice is clear: Adopt a proactive stance toward device security or risk being left behind.

DigiCert® IoT Trust Manager puts device trust within reach. Visit digicert.com/contact-us to learn more about the ways device trust can safeguard your devices, your data and ultimately your business against the threats of today and tomorrow.

About DigiCert

DigiCert is the leading provider of digital trust, enabling individuals, businesses, governments and consortia to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform OS of digital trust, provides organizations with centralized visibility and control over a broad range of digital trust needs, including securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs our award-winning software with our industry leadership in standards, support and operations, and is the provider of choice for leading companies around the world who put trust to work.