Northern.tech

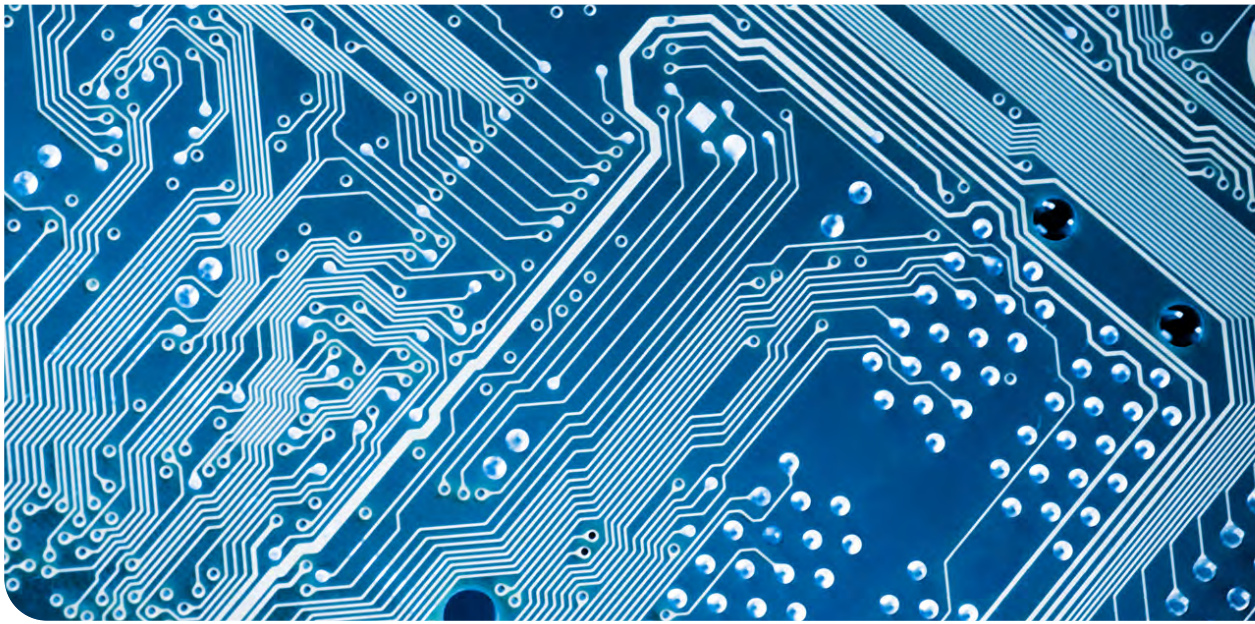
Consulting Services

Device Lifecycle Management

Devices: IoT | IIoT | Embedded | Smart | Connected | Gateways | Sensors | Edge

Key Benefits

- Greater predictability and shortened time to market
- Retain control of your product development
- Mitigate the risk of brand-damaging security incidents
- Avoid costly litigation and ensure cybersecurity compliance

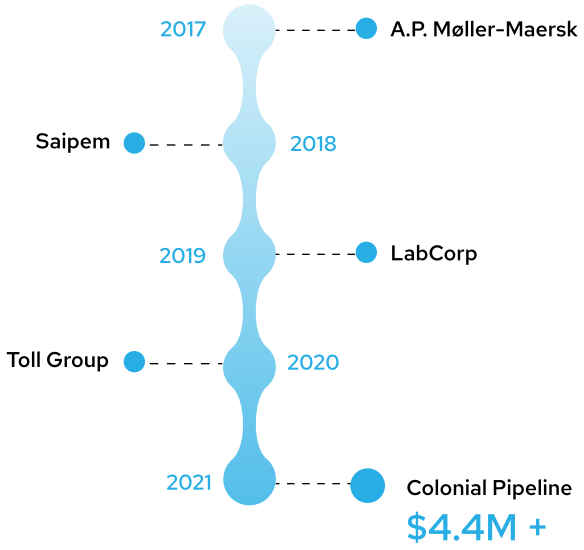


Connected devices are already part of society's critical infrastructure. From automotive, aviation, and defense to energy, smart buildings, and healthcare – devices are becoming smarter, more intelligent, and even autonomous. Despite their purpose, each device is composed of software and hardware – both require continuous management throughout the life of the device.

To continue innovation and stay competitive, organizations must ensure security and robustness at every phase of the device's lifecycle.

Failing to consider DLM best practices in each step of the process – such as credential management, OTA updates, and device registration – risks, product delays, quality issues, and company performance.

Recent Cyber Attacks:



CHALLENGES

The lack of an explicit device lifecycle management process creates several key business challenges.

Delayed and unpredictable product releases

The complex nature of device lifecycle management (DLM) often leads to critical omissions in product development discovered too late in the release process. These surprises can delay the entire product release, or worse, the product is released with known critical weaknesses.

For example, the engineering team may only realize the importance of over-the-air (OTA) updates just before launch. At that point, they won't be able to resolve all quality issues before the initial release and must resolve some issues after the release with OTA updates. Unfortunately, robust and secure over-the-air updates must be included in the design stage due to their implications on how the device boots, its connectivity, and other key design choices. At this time, only two viable options exist: 1) delay the release and redo the product design, or 2) release on time, but greatly risk brand damage and long-tail customer support cost due to poor quality.

Cybersecurity risks

In many cases, products are still released despite critical omissions throughout the devices' lifecycle. In the case of OTA updates, the outcome can be an explicit, yet very risky decision by the business as investors rarely tolerate delays. Since DLM often comes as an afterthought, it is highly probable more unknown gaps and risks exist. These gaps become great exploit opportunities for cybersecurity attackers as weaknesses that may be unknown and never addressed.

For example, the Colonial Pipeline ransomware attack in May 2021 affected over 11,000 gas stations across the US East Coast. The six-day shutdown caused social and economic uncertainty, panic buying, and ultimately, a ransomware payment of $4.4 million USD. Although not all the details of the attack have been published, the attacker exploited an account using a compromised password. In other words, the lack of a key element of device lifecycle management – credential management – resulted in high-profile damage to critical infrastructure.

Although not all infrastructure will create this level of public awareness if compromised, brand damage created by security breaches can be devastating to any business. Even products that seem to have a small impact if breached, such as a camera, can create headlines if an attacker publishes sensitive images captured. On the other hand, the mechanisms for mitigating the risk of this happening are similar for all connected device products.

The unknown nature and limitless liability of cybersecurity risk makes the insurance industry unwilling to underwrite meaningful cybersecurity insurance policies. The risk of compromise falls on the business. Thus, businesses must **take ownership of and mitigate** their cyber risk.

Governments worldwide now realize the need to regulate connected devices to make them more secure against misuse or abuse. Increasingly, businesses need to comply with new security standards or regulations. For example, it would be impossible to comply with the newly proposed European Union Cyber Resilience Act without first having a secure and documented device lifecycle management in place. Similar legislation is likely to come into force both in North America and Asia in the coming years.

To continue to operate in the long run without intolerable risk of brand damage and costly litigation, businesses must take ownership of and implement a baseline cybersecurity policy. Device lifecycle management is a core element.

Effectively deciding what to build or buy

Ensuring the development of smart connected products actually meets market needs is a complex endeavor. Many pieces need to fit together, such as hardware, security, operating systems (OS), software development efficiency, among many others. Complicating matters further, if the initial product revision is successful, then new revisions and products will be released. Starting again from scratch wastes valuable time and increases costs.

No company can fully build everything in-house – even if it were feasible, it would not be cost-effective. However, conversely, fully outsourcing everything around product development is inefficient and risky, too – as it lacks re-use and leaves the OEM hostage to supplier lock-in.

Inevitably, the long-term winners in connected device products are the companies who do acquire sufficient technical knowledge in-house to understand, reuse, and control their own technology development, including DLM and components to IoT platforms.

Armed with technical in-house knowledge, companies can be effective by controlling their own product development and focusing on market differentiators, while increasing efficiency through outsourcing commodity components that may be exchanged in the future. Technology is quickly becoming a necessary core competence in any business, regardless of the legacy of that industry.

Best Practices for Device Lifecycle Management

Device lifecycle management (DLM) consists of five stages for managing and securing a device.

Design

Determine product requirements, select security level, identify DLM mechanisms, and plan overall interactions, including:

- Hardware requirements
- Storage layout
- Boot-time integrations

Commission

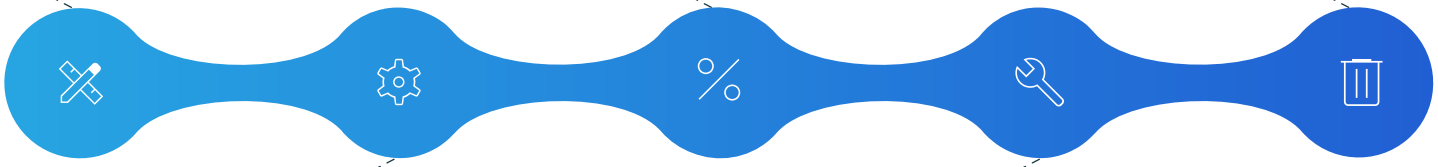
The product starts generating value for the customer. Activate the product in the field and prepare for initial use, including:

- Registration
- First-boot OTA update
- Unique configuration

Decommission

Hardware failure or replacement or end of support or warranty period causes the product to be taken out of service, including:

- De-registration
- Credential revocation
- Secure erase of secrets or IP



Manufacture

In-factory assembly of the physical product, hardware, initial software provisioning, and quality assurance (QA), including:

- Initial software provisioning
- Unique credential provisioning

Maintain

Increase product value and ensure security issues are discovered and remediated. Continuously improve product, including:

- Software build (CI) workflow
- OTA update (CD) workflow
- Vulnerability management
- Credential management

Top considerations based on industry experience:

- What is your risk tolerance?
- What are your weakest links in DLM, and what would be the impact of their failure?
- How does your company compare to competitors and peers in the market?
- Do you have a device lifecycle management strategy and continuous improvement process in place already?

Strengthening device lifecycle management requires a strategy. Once implemented, the numerous benefits ensure your organization's success today and into the future.

Overcoming the challenges around device lifecycle management starts with knowledge. From design to decommission, there are six critical elements to ensure superior device lifecycle management that drives business results.

Over-the-air (OTA) updates: Continuously improve product post-release by delivering new software to connected devices in a robust, secure and scalable way.

Secure boot, software integrity, and chain of trust: Protect against malware, taking control of foundational components of the device and verifying software signatures during the boot process.

Storage encryption and IP protection: Defend against industrial espionage and avoid competitors copying your solution, while safeguarding the company brand from adverse publicity on data privacy.

Vulnerability management: Secure against avoidable attacks and brand damage by detecting and remediating new software vulnerabilities as they become known – on a continuous basis.

Credentials management and public key infrastructure (PKI): Limit the impact of compromised access credentials by ensuring uniqueness and adhering to the principle of least privilege. Manage credentials revocation during a security incident or decommissioning to avoid future exploitation.

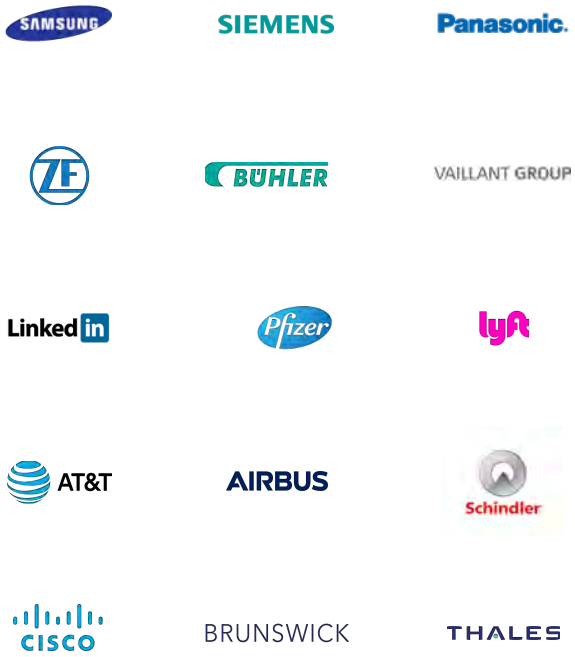
Source of truth: To control and secure, all connected devices must be defined in one, central place where the lifecycle stage and other key DLM information, like connectivity status, installed software version, and owner, are maintained. A source of truth also serves as the point for synchronization to other systems like ERP.

These elements must be adequately implemented across the five stages of device lifecycle management.

It is difficult to objectively judge the state of your own device lifecycle management. But understanding your current practices directly impacts your organization's ability to thrive. How do you decide the level of effort and priorities in improving your current device lifecycle management?

Northern.tech

Consulting Services



Trusted Consulting Services

The leader in device lifecycle management (DLM), Northern.tech provides deep expertise on connected device environments and device management best practices. Northern.tech has partnered with hundreds of companies, helping them transform into the most efficient and secure device producer in their industries.

Produce faster with confidence and compete better in the market.

Learn more about our device lifecycle management consulting, including:

- **Tailored DLM Evaluation:** Our most experienced DLM experts come on-site for three days and evaluate your environment.
- **Technical Training:** Learn about best practices, ideal process, and overall architecture around DLM.
- **DLM Gap Report:** Receive an extensive report of gaps and recommended improvements for your environment.
- **Industry Rating:** Get your DLM rating in your industry against your peers, including your strengths and weaknesses.
- **Ecosystem Access:** Gain access to Northern.tech's network of trusted partners for any follow-up expert service or solution requirements.

Northern.tech

About Northern.tech

Northern.tech is the leader in device lifecycle management with a mission to secure the world's connected devices. Established in 2008, Northern.tech showcases a long history of enterprise technology management before IIoT and IoT became buzzwords. Northern.tech is the company behind CFEngine, the pioneer in server configuration management, to automate large-scale IT operations and compliance. In 2015, Northern.tech released the first version of Mender, the market leader in over-the-air (OTA) software update management.

Learn more about device lifecycle management at Northern.tech

contact@northern.tech