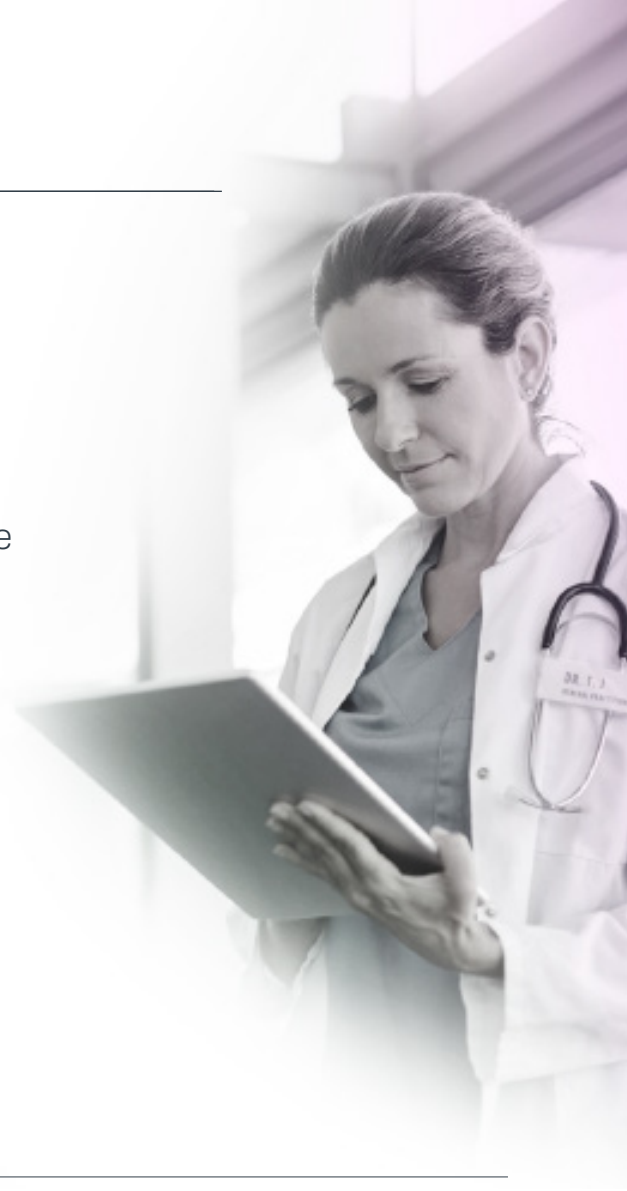
revenera™

EBOOK

How to Manage, Monetize, and Secure **IoT Medical Devices**

Best Practices
for Medical Device Manufacturers

Protect Your Devices to Protect Your Patients

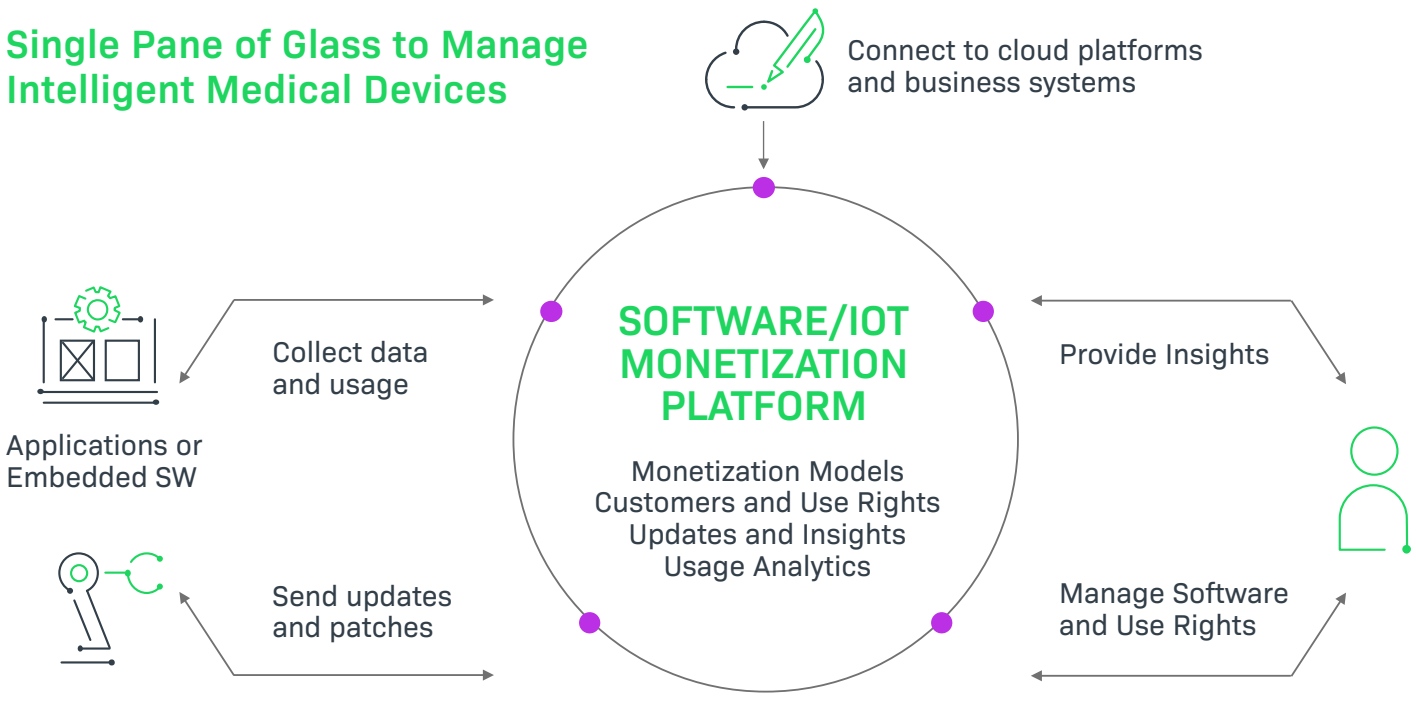


The quality of patient care is central to healthcare. In the fast moving world of medical devices, software is at the heart of innovation, with producers shifting from hardware-focused to subscription-based business models. Today embedded software is integral to these medical devices. It's critical that device manufacturers prescribe success by having appropriate processes and systems in place.

Medical device companies need business solutions that:

- ***Deliver a secure product.***
- ***Manage software and streamline updates.***
- ***Increase the profitability of devices.***

Single Pane of Glass to Manage Intelligent Medical Devices



Healthcare Security is Business Critical

The Internet of Things (IoT) is changing the way technology is consumed, driving a transformation in the healthcare industry. These are part of what VDC Research highlights as the *"changing device functionality requirements"* impacting traditional embedded or industrial markets. Healthcare and medical device manufacturing are addressing compliance, cost pressures, consolidation, continuous management, commoditization, and business model changes.

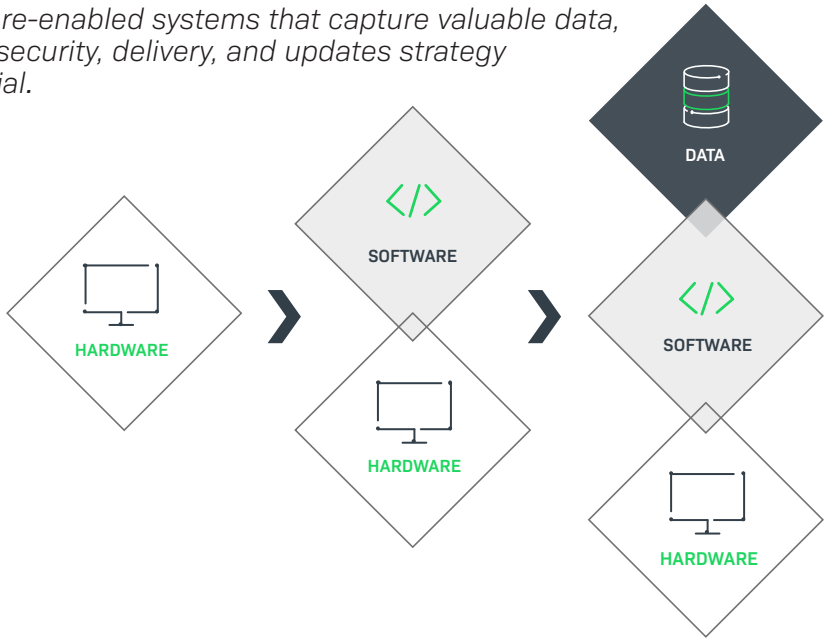
The industry's transformation and the shift to IoT medical devices represent:

- A focus on **value-based healthcare**, improving clinical outcomes while lowering overall costs.
- Incorporation of **technology in the diagnostic and post-procedural phase** to improve value across the continuum of care.
- Reliance on **technology services and insights** to deliver operational efficiencies and better patient care management.
- A need to **secure IoT devices** to ensure increased profitability.
- Use of r**eal-time insights to deliver personalized patient care**.

Medical Device Value Shift

Innovate and Differentiate

As medical devices evolve from conventional hardware to software-enabled systems that capture valuable data, a robust security, delivery, and updates strategy is essential.



Big Tip

Device manufacturers are responsible for everything they distribute or host. You must have the tools and processes in place to identify, mitigate, and remediate security flaws.

The Medical Industry's Specific Challenges & Needs

The medical industry now faces unique challenges in protecting their software supply chain. While undocumented open source code is in virtually all software, unique precautions apply in healthcare, where HIPAA requires device manufacturers to minimize the risk of shipping products to customers with unpatched vulnerabilities. Specific needs in this field have often meant that:

- More complex devices require compatibility or dependency checks before a software update,
- Technicians have needed to manually verify hardware compatibilities before starting updates, and
- That there was no visibility or insight into software or firmware versions on devices.

A better approach is possible. Autonomous updates can replace costly, time-consuming manual processes. This allows the supplier or device manufacturer to be prepared for regulatory compliance, with a complete track record of what software is running where. This is particularly necessary as the frequency and sophistication of security exploits increases.

The Medical Industry Has an Action Plan. Do You?

The medical industry has detailed an action plan to secure medical devices, with clearly defined responsibilities for manufacturers. Medical cybersecurity regulations emphasize managing cybersecurity risks throughout a medical device's entire lifecycle.

The **U.S. Food & Drug Administration** has a Medical Device Safety Action Plan, with the goals of reducing attack surfaces, controlling access to software and data, and keeping software and firmware up to date. The FDA's cyber regulations are primarily focused on medical devices with cybersecurity risks (networked, containing software, etc.).

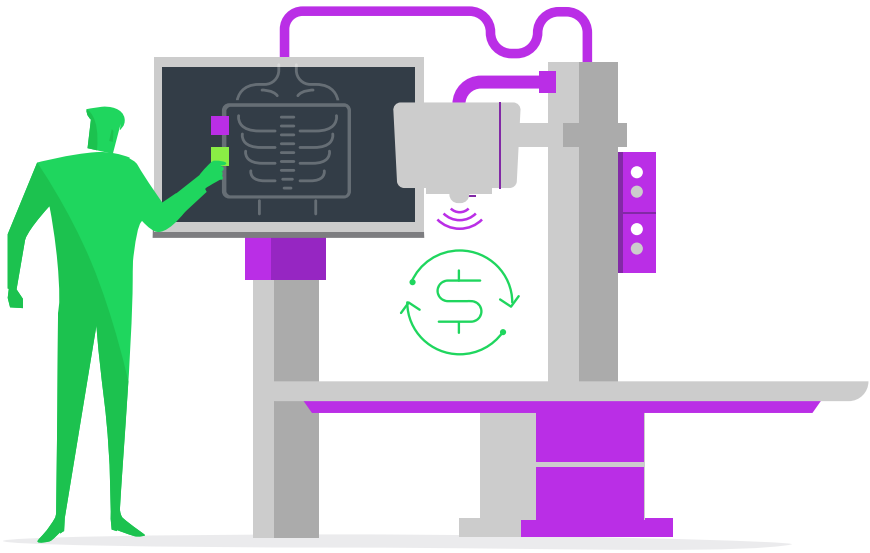
- Medical device manufacturers must build the capability to patch device security into a product's design and to provide appropriate data regarding this capability to the FDA as part of the device's **pre-market submission** to demonstrate reasonable assurance cybersecurity procedures and testing (including SBOMs).
- **Post-market requirements** include the need to monitor, identify, and address cybersecurity vulnerabilities and exploits; this relies on maintaining SBOMs as part of an SCA program.

Similarly, the **EU Medical Device Regulation** (MDR) applies to manufacturers, authorized representatives, importers or distributors of medical devices in the EU. These parties must identify vulnerabilities and potential exploits in their devices; design, develop, and maintain medical devices with robust cybersecurity features, and provide timely software updates and security patches.

WHAT IS...?

SBOM
software bill of materials

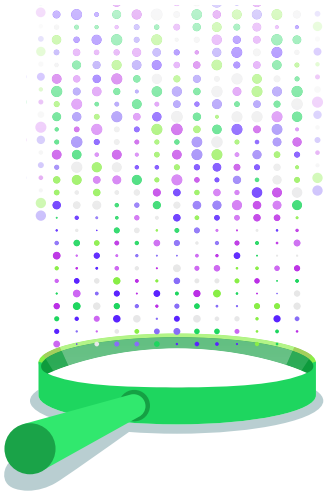
SCA
software composition analysis



A Closer Look at SBOMs

A software bill of materials is a formal and queryable record containing the details and relationships of various components used in building software. Think of it as an ingredients label for your software application.

The multiple uses of SBOMs include automating the inventory processes for open source software and third-party components, enabling transparency for customers and authorities, and tracking vulnerabilities for the components in use. Taken together, these allow device manufacturers to understand the risk present in their devices and act accordingly to secure them.



Medical device manufacturers can use SBOMs to address **five critical questions** to stay in control of OSS usage:

1. **Do we know what components are in our applications?**
2. **Do we have any legal and/or security compliance issues per our policy?**
3. **Are we exposed to a specific vulnerability?**
4. **Are our components up to date?**
5. **Where is the risk and how do we mitigate it?**

SBOM | *A Software Bill of Materials (SBOM) is a formal and queryable record containing the details and relationships of various components used in building software.*

WHAT GETS SCANNED

- EXECUTABLES
- COMMERCIAL LIBRARIES
- PROPRIETARY SOFTWARE
- OSS COMPONENTS

→

INFORMATION RECORDED

- SUPPLIER INFORMATION
- SOFTWARE COMPONENTS + VERSIONS
- DEPENDENCIES
- AUTHOR NAMES
- LICENSES
- SECURITY VULNERABILITIES

Monetization Opportunities for the Medical Industry

The pathway to a modern, secure, and profitable business model for medical devices centers on helping customers stay current and secure, knowing what customers are using, and learning from software and device insights. To achieve this, medical device manufacturers must evaluate how to implement new business models, grow recurring revenue, stay in compliance with industry regulations, and ship secure software products that are free of vulnerabilities.

Depending on the application and the industry, updates may need to be delivered quarterly, monthly, weekly, or even continuously. The process of managing software updates needs to scale. Manual processes will break, particularly as the number of devices (including tablets and sensitive machines) grows.

An automated, comprehensive IoT monetization platform:

- Securely and accurately provides entitlement-driven delivery of updates and security patches,
- Increases security and vulnerability mitigation with an end-to-end process,
- Stops revenue leakage from updates delivered to non-eligible customers, thereby protecting intellectual property,
- Implements end-to-end process automation based on subscriptions and other entitlement information,
- Offers the usage data and analytics to help businesses grow, and
- Helps medical device manufacturers offer the right monetization models for the right products at the right price.

Monetize with Compliant Medical Software Licensing

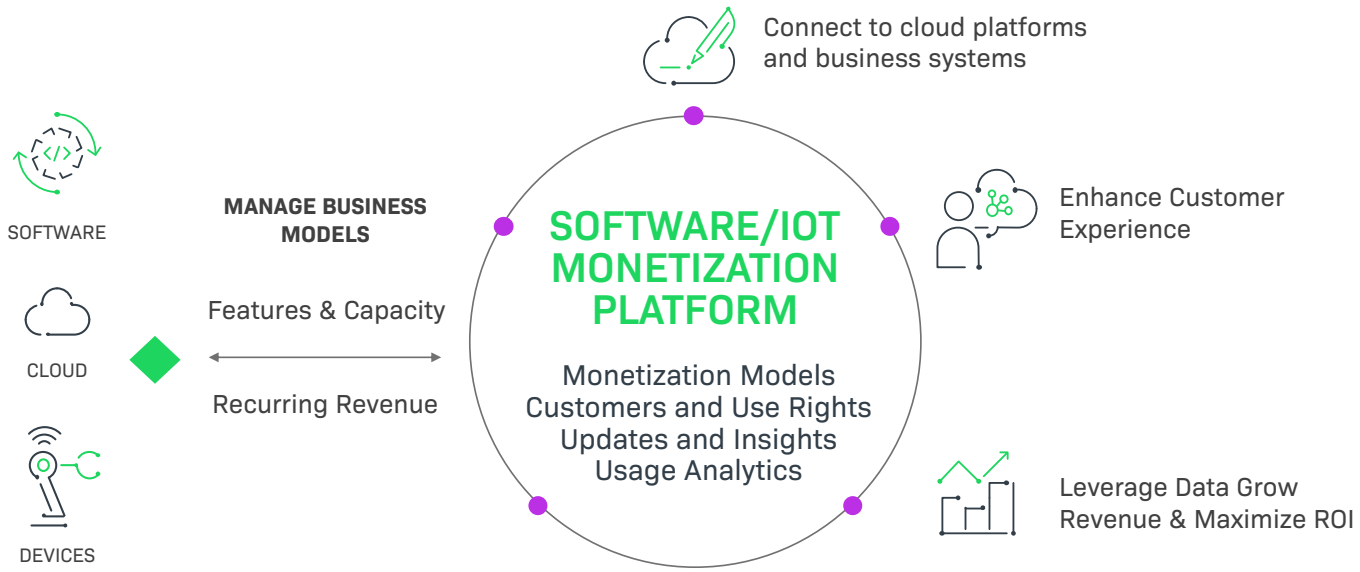
LEARN MORE >

Increase top line revenue

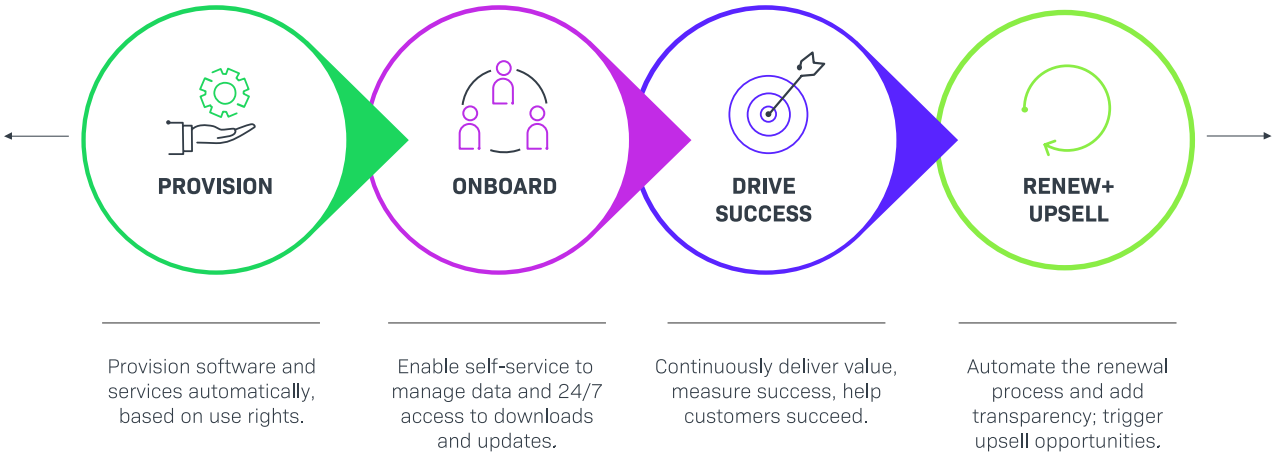
Improve the customer experience

Drive operational efficiencies

Dynamic & Agile Business Transformation Unlock New Business Models



Keep your Customers Front and Center



Keep your customers—and their patients—front and center.

Medical device manufacturers should turn to software monetization and software composition analysis solutions that enable implementation of new business models, grow recurring revenue, stay in compliance with FDA/MDR regulations and ship secure software products that are free of vulnerabilities. Adhering to industry best practices—operating within a security framework, developing and maintaining an OSS policy, and generating SBOMs—can help drive digital transformation and meet industry requirements efficiently. The end result is that your code, your customers, and your reputation all remain healthy.

NEXT STEPS

Download Revenera's IoT Monetization Toolbox for Medical Device Manufacturers.

ACCESS NOW >

Revenera helps product executives build better products, accelerate time to value and monetize what matters. Revenera's leading solutions help software and technology companies drive top line revenue with modern software monetization, understand usage and compliance with software usage analytics, empower the use of open source with software composition analysis and deliver an excellent user experience—for embedded, on-premises, cloud and SaaS products. To learn more, visit **www.revenera.com**