
SBOM and
Connected Device
Security
FINITE STATE

FINITE STATE

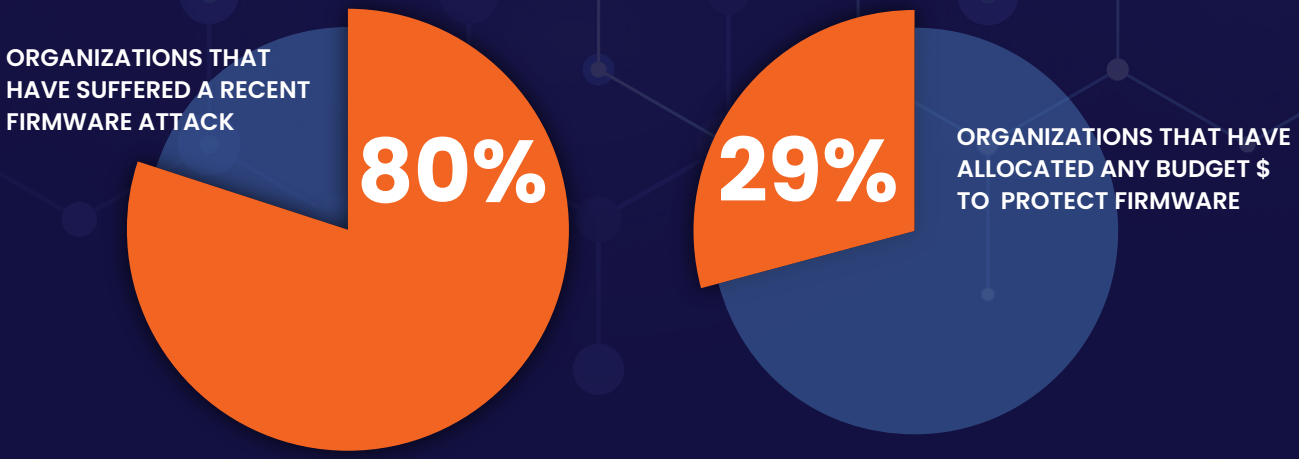
Microsoft reports that 80 percent of organizations have suffered at least one firmware attack in the last 24 months.

When it comes to device firmware and connected device security, where does a manufacturer or buyer start? Here's the good news: you can find everything you need to know to mitigate your device risk within the firmware itself.

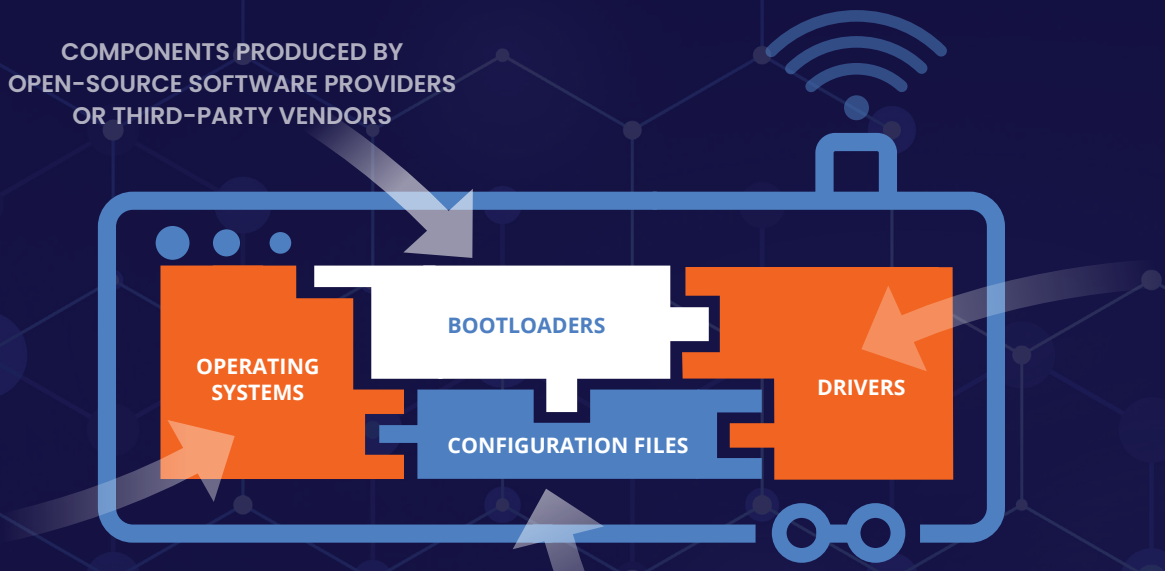
What you need is a Software Bill of Materials (SBOM).

For manufacturers, their ability to keep their new connected devices secure has not kept pace with their ability to scale their production capabilities or the overall growth of the Internet of Things (IoT), Operational Technology (OT), and other embedded systems. Their buyers struggle with grasping the risks inherent in embedded technology. Nearly two-thirds of respondents to the PwC 2022 Global Digital Trust Insights Survey claim limited to no knowledge of IoT-related risks.

Since 2017, attacks against firmware have spiked 500 percent according to NIST data compiled by Microsoft. This spike in firmware attacks comes at a time when just 29 percent of companies have any budget allocated to protect firmware even though 73 percent of respondents to a 2021 Ponemon Institute Study are committed (33 percent) or very committed (40 percent) to securing their supply chain.



But protecting firmware is not as easy as it may sound. Like a car is assembled from parts, manufacturers create firmware from parts as well. These include operating systems, bootloaders, drivers, and configuration files. Nearly all of these parts come from other manufacturers—open-source software providers or third-party vendors.



Just like faulty tires may expose a vehicle to a serious, or even fatal flaw, a security flaw in a device's firmware can be integrated into a finished product, most often unintentionally.

As these realities become clearer to manufacturers and their customers, worry grows about rising cyberattacks against products and critical networks. While many organizations have invested in application security and network monitoring, much fewer have implemented product security programs that can identify and mitigate connected device risk.

Starting with a Software Bill of Materials can help.

Supporting content

The Importance of Securing Connected and Embedded Devices In the Supply Chain

What is a Software Bill of Materials? (SBOM)

Many firms first learn how to define SBOMs when they realize that they need one. The headlines announce the discovery of a zero-day vulnerability in an open-source library. Huddled around a conference table, stakeholders ask questions about where they face risk. The answers eventually coalesce around device firmware.

But, no one has a clear answer about the composition of that device firmware or the location or extent of the zero-day vulnerability.

Many Original Equipment Manufacturers (OEMs) do not know what software or which software versions are in their product because they source a lot of their components from third-party vendors. While OEMs may know what software (and which versions) they have used in the components they have created, this becomes much less so in components that have been sourced from third parties.

If you have a Software Bill of Materials, and you know that a vulnerability affects certain versions of a specific software, a simple search on that SBOM can tell you if you're at risk, and where.

Supporting content

Nearly 60% of Organizations Say Connected Product Security Concerns Have Cost Them Sales, Finite State Research Finds

Simply put, an SBOM provides the foundation for product and supply chain security for device manufacturers and their customers. But, that's where the simplicity in defining SBOMs ends.

Even though standardization is coming—through new regulations—to define what an SBOM is and what it contains, today, SBOMs can go to any level of granularity. There's no standard SBOM and every vendor offers its own version.

Today, many organizations scan first-party, and not third-party, code. Many organizations know that the level of detail in their SBOMs—if they even have SBOMs—creates security gaps, but many don't know how to confront this risk or simply do not have the resources. So they do nothing.

Without the right tool, constructing an SBOM is hard to do. It requires manual processes, which are not scalable. Building an SBOM means defining the components within your components—breaking down those compound parts into their atomic parts. The challenge is reaching supply chain transparency where we can get to the list of atomic parts we have—software and its versions—so we can understand if we have vulnerabilities before we can decide how to address them.

Why would you need an SBOM?

What happens when your product experiences a security breach? What if you didn't even know your product was vulnerable?

SBOMs can serve as valuable tools in determining if, and where, you face exposure to security breaches and vulnerabilities. They can also help you fulfill your obligations under current and developing regulations.

With the recent publication from the U.S. Department of Commerce on what a SBOM should minimally include, the NTIA advises software vendors that SBOMs should be machine-readable—so their details can be uploaded into a larger database.

With these new regulations, organizations are searching to find an SBOM solution, and a solution that is scalable.

But, it's not just regulations and compliance. Device firmware now performs many of the functions that were once controlled by physical systems. Residing in the memory of connected devices, firmware is ubiquitous in our IoT-enabled world. Many users and even manufacturers don't know or understand all the components—and risks—that come with their device firmware. That doesn't mean that these risks shouldn't be identified and mitigated.

When your work product experiences a security breach, this creates a problem with trust in the brand. It also creates problems in revenue.

According to a Ponemon Institute Study, 59 percent of organizations have lost sales following product security concerns. That can affect public company stock prices, reputation risk, and can even result in governments banning the sale of devices within their territories.

Six of every ten product security leaders say that their organization finds it difficult to respond to new vulnerability disclosures...

Six of every ten product security leaders say that their organization finds it difficult to respond rapidly to new vulnerability disclosures that may impact their devices. SBOMs represent an effective first step to gaining an understanding of your connected device exposures by providing a map showing where those risks lie. But SBOMs also help to protect against other risks like:

- Security breaches or exploits, and associated losses of revenue, impacts on reputation, and resources spent on customer support and mitigation
- Loss of sales and revenue to competitors who offer SBOMs with their products
- Complications during mergers and acquisitions (inheriting security issues when acquiring a company OR not being able to provide proof of your product security when being acquired)
- Compliance and regulatory issues such as fines, black lists, etc.
- Not knowing when your products are impacted by new vulnerabilities
- Opaque supply chains

Why are SBOMs for connected devices more difficult to create and procure?

You cannot protect what you cannot see. Seeing into the firmware of connected devices is harder to do than, say, detailing the components of a web application. Web applications are singular programs, whereas a device firmware is a complex system of programs that can contain libraries, operating systems, boot loaders, configuration files, and numerous other components and component clusters that can be broken down even further. So, **SBOMs for firmware and connected devices are more complex than SBOMs for web applications and other singular programs** where traditional AppSec tooling might suffice to create an SBOM.

So, what happens when you try to use traditional AppSec tooling to create an SBOM for your embedded products?

Traditional AppSec tooling will create an incomplete SBOM for an IoT device or other embedded product. It won't find libraries that were recompiled or modified and will only focus on visible source packages. It misses out on vulnerabilities, which end up in the binary files. A product security tool purpose-built for connected products will create a comprehensive SBOM of open source, custom/first-party, and third-party/COTS components.

Supporting content

Five New Challenges Facing Connected Device Manufacturers

Detecting and Verifying New Vulnerabilities Across Your Product Portfolio

That's important when you consider that, based on Ponemon Institute research, some 60 percent of respondents report that their organizations have trouble responding quickly when new vulnerabilities that may impact their devices are disclosed. That's a problem for manufacturers, vendors, and buyers of those devices.

You can't protect what you can't see—unpacking the supply chain and third-party components

Today, supply chains have grown increasingly opaque, complex, and vulnerable to attack. It's one of the most common challenges facing connected device manufacturers. When different manufacturers provide both hardware and software components—and these providers interweave with each other—risks and vulnerabilities abound. Even though these exposures may be confusing and difficult to identify, they must still be managed. Even if your vendors are running their DevSecOps processes, they likely still won't know what's in their software if they don't have the right tool that can produce an SBOM with device-level detail. To fully control the process, even if your vendors won't, you can detect and mitigate vulnerabilities if you can analyze the binary files within your device firmware.

In the market today, you've likely experienced the limitations of tools for secure embedded development. Maybe you've overcome them by creating your own toolset. But that requires time, resources, and expertise that's hard to find and even harder to hire.

Challenges in product security that device manufacturers face

With the emerging technologies inherent in connected devices, we all face new challenges, regardless of whether we manufacture or use:

- Medical devices (IoMT)
- Industrial Control Systems devices (ICS)
- Operational Technology devices (OT)
- Consumer and enterprise Internet of Things devices (IoT)

You're here because you're considering upping your investment in product security. But, some questions remain:

- What challenges will you face as you work to instill confidence in your product?
- How will you stay ahead of cyber criminals who may target your connected devices?

With SBOMs, you can take some control back from your supply chain. With the emergence of new connected-device technologies, our supply chains are growing more opaque. Increasing complexity leads to more vulnerabilities, which require more time and expertise to identify and manage. CVEs and CWEs can exist, undetected, in your firmware code for years and expose you to potential backdoors.

You have some suppliers who provide hardware for your connected devices. Others provide software. Often, these components are tightly coupled with each other. This growing number of vendors means you need to get a handle on the vulnerabilities in your product.

Your vendors probably have their own security processes, but relying on that means blindly trusting that their processes are airtight. You need to be able to validate what's inside the components you're putting into your connected devices.

You need the right tools, and the current tools available for secure embedded development are lacking.

Finite State's robust Software Bill of Materials can help. Using Device Composition Analysis (DCA), our automated platform creates a comprehensive SBOM that can help you identify vulnerabilities in your products and provide actionable guidance.

Supporting content

Security Processes for Connected Devices – Revisiting AppSec

What makes Finite State a better fit than traditional SCA tools?

Executive Order 14028 and supply chain security

In May 2021, President Biden released his Executive Order on Improving the Nation's Cybersecurity. The intent, captured in its name, was to improve the country's cybersecurity in the wake of a growing number of breaches and attacks. The EO instructed government agencies to establish new security requirements designed to improve the secure functioning of technology products sold to the US government. President Biden's executive order also established robust new expectations for supply chain security.

The US Department of Commerce responded to the Executive Order on Improving the Nation's Cybersecurity by establishing new requirements for Software Bills of Materials (SBOMs). Through the National Telecommunications and Information Administration (NTIA), the Department of Commerce sought to strengthen the SBOM's role in supply chain security. The new NTIA guidance set requirements for what SBOMs must include.

Through establishing new SBOM requirements, NTIA's guidance requires product software and connected device manufacturers to provide more proof around vulnerabilities that impact their products. These manufacturers will now need to check for vulnerabilities not just in their own software, but in the software from third parties that gets integrated into their products.

Federal entities will now require SBOMs as part of the products they buy. Software and connected device manufacturers will have to attest that their SBOMs are accurate... and complete.

Specific to SBOMs, this new guidance established new Minimum Elements, such as:

- Minimum informational requirements for each software component
- Minimum informational requirements about the SBOM
- Automatic generation and machine readability capability
- Expectations regarding the frequency of SBOM generation
- Depth of reporting, e.g., how many levels down to dive for relationships
- Expanded clarity on the existence of dependencies, or lack thereof

President Biden's Executive Order on Improving the Nation's Cybersecurity targets federal procurement. However, Finite State anticipates that the requirements established by NTIA and other federal government agencies will become industry best practices, in contracts, RFP questionnaires, or even in requirements set by cyber insurance carriers. We expect the EO will impact all device manufacturers and software companies.

Supporting content

NTIA & SBOM: Review of the U.S. Department of Commerce Minimum Elements For a Software Bill of Materials

How does an SBOM improve connected device security?

Not all SBOMs are created equal. Your cybersecurity effort needs a comprehensive SBOM that lists your open-source, custom/first-party, third-party and COTS components.

The market abounds with incomplete SBOMs. Incomplete SBOMs miss libraries that have been recompiled or modified, and often only focus on visible source packages and miss out on vulnerabilities, which end up in the binary.

The right SBOM can help you identify security issues and determine the vulnerabilities in your connected devices and embedded systems. It can mean the difference between a conference room full of head-scratching and effective discourse leading to actionable insights and swift action.

SBOMs can help you:

- **Improve your product's cyber resilience**
- **Determine exposure in your supply chain**
- **Confront security issues head-on**
- **Comply with standards as they come online**
- **Show evidence of your development due diligence**

A comprehensive, machine-readable Software Bill of Materials provides full visibility into every component of your software, including binaries, open-source software, embedded software, and more.

Supporting content

Finite State Boosts Velocity And Depth Of IoT Vulnerability Discovery Through New Advanced Search

Debunking the common misconceptions of SBOMs

Myth #1: I'll have to reveal my source code to create an SBOM.

Reality: The Finite State platform can create an SBOM based solely on a final firmware image. By unpacking that, we can automatically uncover security issues throughout your product portfolio and supply chains.

Myth #2: I can use an existing application security tool to create an SBOM.

Reality: Existing AppSec tools don't translate over to embedded systems. Where an application is one program, firmware can represent hundreds. Existing tools struggle to unpack that, and often aren't up to the task.

Myth #3: Isn't creating this list of components and vulnerabilities like handing a roadmap to a hacker?

Reality: No—while an attacker could use an SBOM to determine which components of your device firmware may be susceptible to attack, many attackers use a "buckshot" approach to launching attacks. Their mass attacks are often indiscriminate. They keep trying until they hit pay dirt.

However, if you use your SBOM as a preventative control, you can direct your resources toward mitigating your vulnerabilities and exposures instead of struggling to identify them. You can resolve your connected device risks before hackers can land upon them. SBOMs level the playing field for those defending against cyberattacks.

Myth #4: I'll expose my trade secrets and IP if I create an SBOM.

Reality: SBOMs don't expose intellectual property rights and do not have to be made public. SBOMs don't include code, patents, and algorithms, for example. Where you may have a recipe to replicate IP, an SBOM is more like a list of ingredients.

See Finite State in action. Schedule a demo.

Finite State brings visibility and control to the supply chains of your connected devices and embedded systems. The Finite State Platform unpacks and analyzes every file, configuration, and setting in a firmware build and creates a comprehensive SBOM.

Finite State's SBOM identifies known and zero-day vulnerabilities, assigns a score that reflects your risk level, and delivers insights you can act on now to secure your software before it's too late.

Let's look at your firmware and its supply chain, using our intuitive platform. We'll help you ship secure products faster and help your users trust their connected devices more.

Schedule a demo today

FINITE STATE

finitestate.io