OMDIA MARKET RADAR

Publication date:
12 May 2025

Author(s):
Hollie Hennessy, Principal Analyst
Rik Turner, Chief Analyst, Cybersecurity

Omdia Market Radar: Firmware and Software Supply Chain Security, 2025

OMDIA

Summary

Catalyst

In this Market Radar, Omdia explores the firmware and software supply chain security (SSCS) market, comparing different vendor capabilities in the category. As government focus increases regarding product security for the Internet of Things (IoT) and the wider ecosystem of connected devices alongside software bill of materials (SBOM) requirements, demand for technology to generate, manage, and analyze SBOMs and vulnerabilities within firmware and software rises.

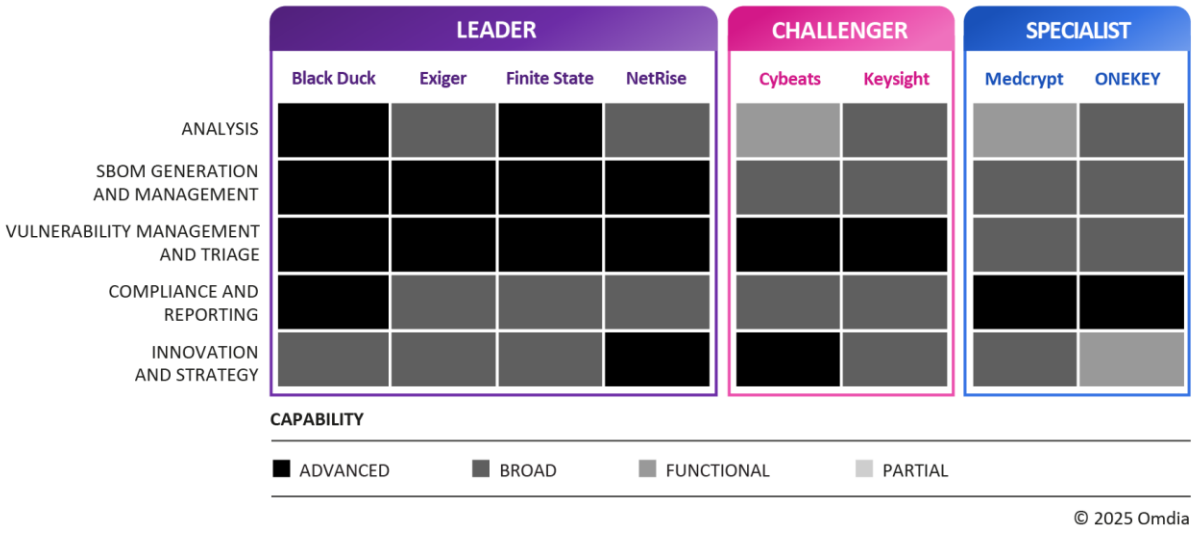
While SSCS is a broader category that encompasses tools designed to ensure the security of all application software (and even operating systems), firmware security is a smaller but increasingly important segment that focuses specifically on the software that ships within devices. This comprises products in the worlds of IoT, operational technology (OT), and enterprise IT, but for the purposes of this report, Omdia has narrowed its analysis to vendors of security tools for OT/IoT firmware. This is why we provide only an honorable mention for Eclypsium, whose target market is more focused on enterprise IT devices and so falls slightly out of scope here.

While automotive is a key vertical for a number of the vendors profiled in this report, we have not included the automotive security specialists, as they tend to have capabilities over and above firmware/software supply chain security, relating to the broader cybersecurity of the connected vehicle. This market and the players within are profiled in our *Market Landscape: Automotive Cybersecurity*.

Market snapshot

Figure 1 illustrates the solutions Omdia explored as part of this research and highlights the capability categories that were analyzed. The definitions, assessment process, and vendor information are described in more detail later in this report.

1. Figure 1: Omdia heatmap for firmware and software supply chain security



Note: Vendors are listed in alphabetical order
Source: Omdia

Key messages

- **The firmware security market has evolved:** The firmware security space is receiving significant attention, driven by an increased awareness of security vulnerabilities within IoT and connected devices—on the part of governments and enterprises. A number of startup vendors have entered this space alongside a handful of more established players. Many of these have evolved from solely firmware security for the IoT to platform-based approaches combining firmware security with wider software supply chain security (SSCS) capabilities. There has also been a notable expansion of coverage beyond IoT and firmware to broader IT assets and software, thus factoring into this shift.
- **Firmware security is at least partly compliance-driven:** Government regulation and legislation are key drivers of firmware security, so compliance and reporting are capabilities Omdia has looked at in this study. Manufacturers must adhere to product security requirements, while asset owners are increasingly required to understand their device and supply chain security landscape. This is especially true for critical infrastructure organizations.
- **We will see a combination of technical approaches:** The technology on the market can be categorized into two approaches: binary analysis and source code analysis (SCA). Binary examines compiled firmware, making it accessible to both asset owners and manufacturers, while source code analysis focuses on assessment earlier in the software development lifecycle; that is, it inspects the uncompiled code, which in turn limits its use to device manufacturers with access to original code unless they are willing to share that source code with their customers (which is not the norm).

Some vendors combine both approaches, and Omdia expects this trend to continue in an effort to deliver a more comprehensive offering throughout the development and device lifecycle and to open up a wider market opportunity.

- **Buyers need SBOM management, analysis, and automation:** The requirements around SBOM have evolved from generation toward management and security analysis. Given the noise that

can be created by scanning tools, understanding and contextualizing the vulnerabilities and issues found are key for organizations and manufacturers to remediate and mitigate risk.

Automation is key here as it can alleviate challenges for product and cybersecurity teams, improving the speed at which they can remediate issues and their ability to meet compliance requirements. For device manufacturers, integration into the existing development lifecycle is becoming increasingly important.

- **Expect further BOM requirements going forward:** Two other flavors of SBOM, cryptographic bill of materials (CBOM) and artificial intelligence bill of materials (AIBOM), are emerging at this point. They will likely become requirements soon.

As quantum computing becomes a technical and then a commercial reality, CBOMs will help organizations understand their encryption estate and determine which encrypted data needs to be migrated to quantum-safe cryptography first.

Meanwhile, companies using third-party models and applications will need to know what vulnerabilities these pieces of code may contain and will ask for AIBOMs.

- **AI is on the roadmap:** It is no surprise that one of the most common roadmap items and components of recent releases is AI-powered technology. Many vendors offer, or are planning to offer, AI-powered analysis to aid in remediation suggestions and pinpoint exactly which vulnerabilities need addressing and in what order. This is a trend that will only intensify.

Omdia view

Firmware security fits within the spectrum of proactive technologies that have been sweeping through the cybersecurity world since the late 2010s. It seeks to find issues in a given area of infrastructure, which may be enterprise IT, IoT, or OT, and address them before they become the object of an exploit against the organization that owns the assets. Indeed, in as much as firmware security is sold to and used by device makers, it can also be thought of as a manifestation of the Secure by Design mantra of getting things right before they ever leave the manufacturer's premises.

The other community of users is the asset owners, who have a vested interest in guaranteeing the integrity of the firmware on the devices they buy on the day they receive these devices from the manufacturer, as well as its continuing integrity through the device's lifecycle.

Is this a big enough market in its own right to sustain a bevy of technology vendors? Perhaps not at the moment, but as the IoT continues to expand and ever more OT devices gain a connection to the IT side of an organization, we forecast that it will grow. Meanwhile, the vendors in this quite specialized corner of the SSCS market could do worse than to spread their wings into the broader, more mainstream segments, which should not be too great a leap, given that the same underlying skills pertain in firmware security and the broader SSCS.

Recommendations

Defining the firmware security market

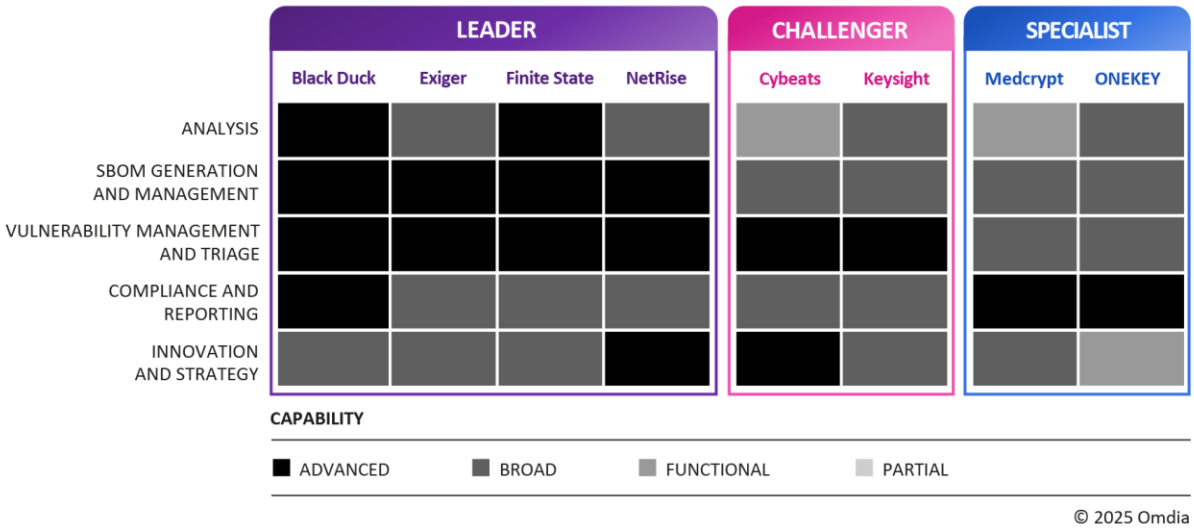
Key capabilities

Vendor landscape

Figure 2: Firmware and software supply chain security market radar capabilities

Source: Omdia

2. Figure 3: Omdia heatmap for firmware and software supply chain security



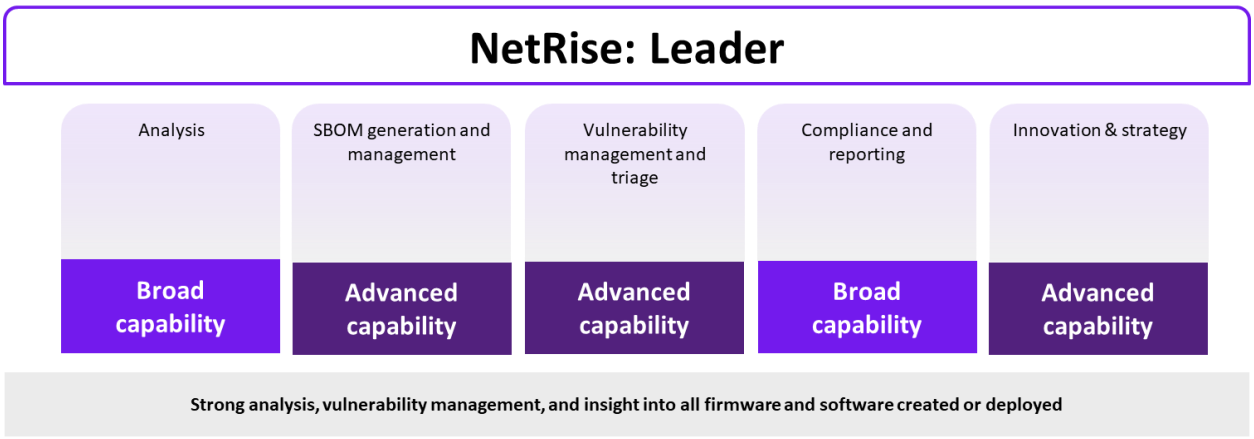
Note: Vendors are listed in alphabetical order
Source: Omdia

Honorable mentions

Vendor analysis

NetRise

Figure 10: Omdia Market Radar recommendation—NetRise



Source: Omdia

Why consider NetRise?

- NetRise offers software supply chain security for a wide range of assets and specializes in IoT and firmware, given its origins in the device security space and its advanced binary analysis capabilities.
- The vendor has expanded its offering to appeal to those looking to secure IT-focused assets and software, for which reason it provides an interface that highlights and prioritizes the risks for these assets. In addition, the platform can create Vulnerability Exploitability Exchange (VEX) documents that help track and explain risks associated with software.
- Beyond its capabilities in product security, NetRise can also offer enrichment and visibility for enterprise security teams. This is particularly useful for operators of critical national infrastructure (CNI) given the heavy use of OT and IoT alongside IT assets—all of which NetRise can cover.
- Additionally, recently enforced and upcoming legislation puts emphasis on supply chain security and risk assessment for many of these CNI organizations.
- NetRise's product is increasingly viewed as one that assesses risk in the software running in devices deployed by enterprises—complementing the hardware asset inventory they currently maintain with the creation of a software asset inventory.
- The platform is also useful for security consultant buyers, who can use it in penetration testing, vulnerability research, and other offensive activities.

Roadmap and areas of future focus

- In the three years since the platform's initial release, NetRise has added a number of capabilities, adding CISA KEV support in 2023 and its AI-powered search in November 2024. This search is designed to reduce the manual and time-consuming task of detecting known and hidden threats across the firmware/software supply chain.
- NetRise's focus areas for the future around innovation include the ability to identify software in all environments and to extract and analyze a wide range of compiled artifacts. Another area of focus is making the SBOM more useful for manufacturers, especially developers (e.g., for merging, as well as for comparing and assessing risk). It also plans to build out OEM and partner integrations, enriching third-party products with firmware and software supply chain security insights.
- Its roadmap further looks to expand capabilities around vulnerability management—being able to find zero-day vulnerabilities such as undiscovered weaknesses (e.g., CWEs that can manifest as exploitable vulnerabilities), looking more into vulnerability reachability, and automating triage (thus adding context to any recommendations and risk prioritization).
- Further planned capabilities include agent-based analysis, allowing for ongoing monitoring at runtime. This adds further value to its enterprise customers and is useful for cloud workloads and endpoints.

Market impact

- NetRise analyzes software and firmware security through the prism of binary code inspection. This allows it to serve enterprise customers and device manufacturers that want to analyze their already compiled code. Although binary analysis opens up these avenues of opportunity, it does not offer SCA. While there are pros and cons to each approach, few vendors in the space can do both. Arguably, those that do may have more opportunities.
- Netrise has successfully expanded from device manufacturer clients to the wider segment of enterprise clients, with a number of partnerships to aid its expansion. It has a strong, focused strategy to develop its capabilities tailored for the enterprise, with different views and capabilities for both buying personas, which bodes well for its future.
- NetRise offers vulnerability management and querying capabilities to allow users to uncover software and firmware vulnerabilities at speed. However, with the move to the proactive approach to cybersecurity and product security, enhancing this capability with actionable insight will be key, in Omdia's view. NetRise has already made improvements in this space and has roadmap items for further development.
- Netrise has been bold in its strategy to cover more than just IoT—effectively offering SSCS for all manner of assets, unlike many of its competitors in the space. While software and firmware security are key in the IoT and OT space, the need for supply chain security is important in the broader IT context. This is especially true for industries such as automotive that are heavily software-driven and with OT in the midst of the digital transformation termed Industry 4.0, resulting in further connectivity in operational environments.

Appendix

Further reading

Market Landscape: Automotive Cybersecurity (June 2024)

On the Radar: Eclypsium secures the IT infrastructure supply chain (February 2025)

On the Radar: Sternum brings runtime protection and continuous monitoring to IoT devices (December 2024)

Market Landscape: Embedded Security for IoT (March 2024)

Market Landscape: Application Security Posture Management (ASPM) – An Update (August 2024)

Author

Hollie Hennessy, Principal Analyst, OT & IoT Cybersecurity

Rik Turner, Chief Analyst, Emerging Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com