Publication Date: 2025-04-24

OpenEoX

A Standardized Framework for Managing End of Life and other Product Lifecycle Information

Omar Santos
Cisco
USA
osantos@cisco.com

Thomas Schmidt
BSI
Germany
thomas.schmidt@bsi.bund.de

Przemyslaw Roguski
Red Hat
Poland
proguski@redhat.com

Art Middlekauff
Flexera
USA
amiddlekauff@flexera.com

Sergii Demianchuk
Cisco
USA
ndemianc@cisco.com

Justin Murphy
CISA
USA
justin.murphy@mail.cisa.dhs.gov

Feng Cao
Oracle
USA
feng.cao@oracle.com

Langley Rock
Dell
USA
Langley.Rock@Dell.com

Stefan Hagen
Individual
Switzerland
stefan@hagen.link

Shridhar Chari
Cisco
USA
shridarc@cisco.com

Thomas Schaffer
Cisco
Germany
thschaff@cisco.com

Abstract

The accelerating evolution of technology underscores the critical need for clear, consistent communication regarding product life cycles. Currently, information about End-of-Life (EoL), End-of-Security-Support (EoSSec), and other states for software, hardware, services and specifications is often fragmented and inconsistently defined across the industry.

OpenEoX is a very important initiative designed to address this challenge by standardizing the exchange of this information. Encompassing both commercial vendors and open-source maintainers, OpenEoX provides a transparent, efficient, and unified framework. OpenEoX can also apply to AI models. This white paper provides a detailed explanation of OpenEoX core concepts and taxonomy, based on its foundational definitions.

Keywords

OpenEoX, End-of-Life, End-of-Security-Support, End-of-Sales, product lifecycle

1. Introduction: The Need for Standardization

Understanding the lifecycle status of these components (particularly when they will cease to receive updates or be supported) is crucial for security posture, operational stability, regulatory compliance, and strategic planning. However, the lack of a common standard for defining and

communicating EoL and other product lifecycle information creates significant hurdles. Different vendors and open source maintainers use varying terminology, timelines, and communication methods, leading to potential confusion, increased operational risk from unsupported products, and inefficient resource allocation for tracking and migration. This is why OpenEoX aims to bring clarity and consistency to product lifecycle management. The core objectives include:

- Transparency: Making lifecycle information readily accessible and understandable.
- Efficiency: Streamlining the process for both information providers (vendors, maintainers) and consumers (users, organizations).
- Unification: Establishing a common language and data structure for lifecycle stages such as EoL, EoSSec, and EoS information.

2. Core OpenEoX Concepts and Taxonomy

A shared understanding requires precise definitions. All of the definitions are available at the OpenEoX GitHub repository at: https://github.com/oasis-tcs/openeox

OpenEoX establishes a core taxonomy built upon the following definitions:

2.1 Vendor

- Definition: Vendor refers to the community, individual, or organization which created or maintains a product (software, hardware, managed service and other deliverables). This includes, but is not limited to open-source software and hardware providers.
- Informative Note: This definition deliberately casts a wide net. It clarifies that the entity responsible for a product's lifecycle and its communication is not limited to traditional commercial software or hardware companies. It explicitly includes open-source projects, communities, and even individual maintainers. In the OpenEoX context, any such entity is considered the 'vendor' responsible for declaring and sharing lifecycle milestones according to the standard.

2.2 Product

- Definition: Product is any deliverable (e.g. software, hardware, specification, services, etc.) which can be referred to with a name. This applies regardless of the origin, the license model, or the mode of distribution of the deliverable.
- Informative Note: This definition deliberately casts a wide net. It clarifies that OpenEoX can be used on any type of deliverable. Also the scope can be adapted to the needs of the information that should be communicated, i.e. describing the product with or without version.

2.3 Product Lifecycle

- Definition: Every product type (software, hardware, managed service and other deliverables) can be associated with a lifecycle model. It can contain definitions of various support models (different levels of maintenance) in association to the product versioning convention. The lifecycle support model can be dynamic and might change over time, from the product's initial release (General Availability) to its discontinuation (End-of-Life). During the product lifecycle, support models may switch from one state to another and may even run in parallel to meet individual requirements. Those requirements may depend on the product type, the vendor offerings, as well as geographical related regulations.
- Informative Note: This concept frames the entire journey of a product from its introduction (General Availability or GA) to its final retirement (End-of-Life). It highlights several key characteristics:
  - Phased Approach: Lifecycles consist of different stages, often with varying levels of support (e.g., full support, maintenance, security-only).
  - Version Specificity: Lifecycle milestones are typically tied to specific versions or releases of a product.
  - Dynamic Nature: The level of support and the product's status evolve over time. It's not uncommon for different support levels (e.g., standard vs. extended) to exist concurrently for different customer needs.

- Contextual Variation: The exact structure of a lifecycle can differ based on the type of product, the vendor's specific policies, and potentially external factors like regional laws. The specific milestones like EoS, EoSSec, and EoL are key events within this overarching Product Lifecycle.

2.4 End-of-Sales (EoS)

- Definition: The End-of-Sales (EoS) indicates the last day when a particular product (or the product version/release) may be ordered by customers from vendor sales channels. After this date, the product is no longer for sale. However, there might be other sources where the product is still available. Once the product reaches the End-of-Sales (EoS) lifecycle stage, it may still be supported by the vendor, based on the official or dedicated vendor lifecycle model for this product, for existing customers. The implications for existing customers regarding license renewals, updates, upgrades to newer versions or ongoing technical support can vary depending on the vendor's specific policies.
- Informative Note: EoS marks a specific commercial transition point. It is the date after which a vendor will no longer accept new orders for a specific product or version through its primary sales channels. It's critical to understand that:
  - EoS does not automatically mean the end of technical support or updates.
  - Existing customers who have already purchased the product may continue to receive support according to their agreements and the vendor's stated lifecycle policy.
  - The product might still be available through resellers or other secondary channels.
  - Vendor policies dictate the specifics regarding license renewals, access to updates, and ongoing support for existing customers after the EoS date. EoS is distinct from the cessation of technical or security support (EoL and EoSSec).
  - End of Sales won't be added yet to the MVP (minimum viable product) of the OpenEoX, but it can be added in the future.

2.5 End-of-Security-Support (EoSSec)

- Definition: End-of-Security-Support (EoSSec) indicates the last day when the vendor has committed to providing security remediations for the particular product (or the product version/release).
- Informative Note: EoSSec is a critical security milestone. It defines the date until which the vendor commits to releasing fixes or patches for security vulnerabilities discovered in the specified product or version. The key implications are:
  - Operating a product beyond its EoSSec date carries significant security risks, as new vulnerabilities will not be addressed by the vendor.
  - This date is essential for risk assessment and compliance management.
  - EoSSec applies specifically to security-related support, which may end before general EoL. Clear communication of the EoSSec date is a primary goal of OpenEoX to enable users to maintain a secure environment.

2.6 End-of-Life (EoL)

- Definition: The End-of-Life (EoL) indicates the last day when the particular product (or the product version/release) is officially supported in any way by the vendor. After this date there shouldn't be more development, updates or any type of support expected from the vendor. The existing customers are also impacted by this product lifecycle stage and should consider migration to the still supported product version or release.
- Informative Note: EoL marks the definitive conclusion of the vendor's commitment to a product or version. It signifies the cessation of all forms of official support, including:
  - Development of new features.
  - Provision of updates (including bug fixes, performance enhancements, and security patches unless covered by a separate, extended security support agreement which itself would have an end date).

- Access to technical support or assistance from the vendor.
  The EoL date signals that the product has reached the end of its vendor-supported lifespan. As the definition states, customers using the product should actively plan and execute migrations to supported alternatives before or upon reaching the EoL date to ensure continued functionality, security, and access to support. EoL typically occurs after EoS and may coincide with or occur after EoSSec.

Figure 1 is a simple timeline of a product's lifecycle, marked by four key milestones:

- General Availability (GA)
- End of Sale (EoS)
- End of Security Support (EoSSec)
- End of Life (EoL)

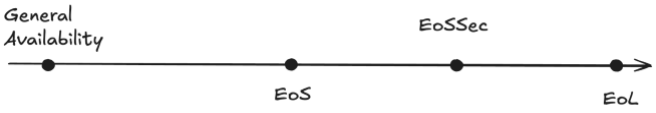

Fig. 1. OpenEoX Timeline

3 Benefits of Adopting OpenEoX

The standardization provided by OpenEoX offers tangible benefits across the technology ecosystem:

- For Users and Organizations:
  - Reduced Risk: Clear EoSSec and EoL dates enable proactive mitigation of security vulnerabilities and operational disruptions associated with unsupported products.
  - Simplified Planning: Consistent information facilitates easier asset management, budget forecasting, and migration planning.
  - Improved Compliance: Helps organizations meet compliance requirements related to using supported software/hardware.
  - Informed Procurement: Better visibility into product lifecycles aids purchasing decisions.
- For Vendors and Maintainers:
  - Clear Communication: Provides a standard way to communicate lifecycle information, reducing customer confusion and support queries.
  - Streamlined Processes: Enables easier integration with industry tools and platforms that consume lifecycle data.
- For the Industry:
  - Increased Transparency: Fosters a more open and predictable environment regarding product support.
  - Enhanced Efficiency: Increases the efficiency handling disparate lifecycle policies.

4 OpenEoX vs. SBOMs vs. CSAF

OpenEoX does not compete or replace Software Bill of Materials (SBOMs) or the Common Security Advisory Framework (CSAF). OpenEoX compliments and can potentially be integrated with SBOMs and CSAF/VEX documents, OpenEoX can enable organizations to incorporate EoL and EoSSec information into existing security and compliance workflows. In order to do this, OpenEoX provides a core schema containing just the OpenEoX statement. The product is identified by the context of the incorporating standard.

A standalone schema, consisting of the core schema and the shell schema which provides the product identification, also makes it flexible and adaptable to a variety of environments.

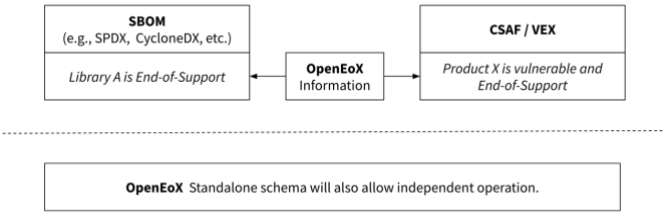

Fig. 2. OpenEoX Integrations

OpenEoX can be adopted widely without requiring extensive system overhauls.

5 Conclusion and What's Next

Effective management of product lifecycles is indispensable in the rapidly evolving technology sector. OpenEoX offers a solution by establishing a standardized framework and taxonomy for product lifecycle information, like EoL or EoSSect. The OpenEoX Technical Committee (TC) will continue to work on defining additional elements, as well as providing a distribution and discovery scheme.

6 Feedback

This work is ongoing in the OpenEoX TC at OASIS Open. Current members include:

- Cisco Systems
- Dell
- DHS Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Office for Information Security (BSI) Germany
- Flexera
- Huawei Technologies Co., Ltd.
- IBM
- Microsoft
- National Security Agency
- Oracle
- Red Hat
- sFractal Consulting LLC
- Siemens

Please provide feedback through the comment mailing list of the OpenEoX TC.

Notices

This document was approved for publication by the OASIS OpenEoX Technical Committee and is the work of the Authors, and is offered for informational purposes. It has not been adopted or licensed under the OASIS rules for approving standards and specifications. OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to its subject matter, nor has it made any effort to identify any such rights.