LYNX

Strengthen Your Software Security and Compliance with LYNX MOSA.ic™ SCA

Prevent up to 70% of security incidents with robust Software Bill of Materials implementation. Ensure compliance, reduce vulnerabilities, and safeguard your mission-critical systems.

A Clear View of Your Software's Security and Compliance

With over 40,000 new Common Vulnerabilities and Exposures (CVEs) published in 2024 alone—an average of more than 760 per week6—companies are increasingly making headlines worldwide for the wrong reasons. The rapid proliferation of vulnerabilities highlights the urgent need for proactive software security and compliance measures.

Modern software development increasingly relies on open-source components and third-party libraries. While these resources accelerate innovation, they also introduce risks—vulnerabilities, licensing issues, and outdated dependencies—that can threaten security and compliance.

LYNX MOSA.ic.SCA is a comprehensive solution for Software Composition Analysis (SCA), designed to help you identify, analyze, and manage both proprietary and third-party open-source libraries across your entire software project. Integrating automated monitoring, policy enforcement, and risk mitigation tools ensures your software supply chain meets internal standards and external regulations.

With MOSA.ic.SCA, you can:

Enhance Visibility - Gain a comprehensive view of your software components through detailed Software Bill of Materials (SBOM) management.

Ensure Compliance - Follow government mandates, such as the White House EO 14028 and the EU Cyber Resilience Act (CRA).

Minimize Risk - Address vulnerabilities swiftly and effectively, keeping your engineers focused on delivering cutting-edge products.

Supply chain disruptions can cost over $1 million per day, depending on severity, in industries ranging from aerospace to defense. LYNX MOSA.ic.SCA empowers you to reduce risks, cut through the noise of irrelevant vulnerabilities, and focus on what matters most: mission success. With Lynx, you gain the tools to Seize the Edge™ in securing and optimizing your software supply chain.

12.7%

In 2022, the average cost of a data breach was $4.35 million, which is a 12.7% increase from 2020[4]

IBM Cost of a Data Breach Report 2022

46%

A 2022 government study found that 46% of large businesses say they have had to take up new measures to save them time and protect their assets.[3]

Cyber Security Breaches Survey 2022

10,000

In 2021 alone, nearly 10,000 known security vulnerabilities were detected in open source components.[5]

All About Mend's 2021 Open Source Security Vulnerabilities Report

LYNX

Addressing the Complexities of Software Security and Compliance

The rapid growth of open-source adoption and evolving cybersecurity mandates have made managing software vulnerabilities and compliance a formidable challenge. Organizations face significant risks and obstacles in ensuring their software supply chain remains secure and compliant.

Key Challenges in Software Security and Compliance:

Rising Volume of Vulnerabilities
Over 760 new Common Vulnerabilities and Exposures (CVEs) are identified each week, leaving organizations struggling to keep pace.[6]

High Costs of Supply Chain Disruptions
In industries like aerospace, disruptions can result in costs ranging from $100,000 to over $1 million per day.[2]

Complexity of Compliance Standards
Navigating mandates such as White House EO 14028, FDA Cybersecurity, and the EU Cyber Resilience Act (CRA) demands a comprehensive and proactive approach to software management.

Inefficient Vulnerability Management
Manually triaging and analyzing CVEs leads to wasted resources, with up to 95% of alerts being false positives.[3]

Delayed Remediation
Vulnerabilities often remain unaddressed due to publication delays of up to four weeks.[4]

At Lynx, we understand these challenges and have designed LYNX MOSA.ic.SCA to help you overcome them with confidence. By streamlining vulnerability tracking, automating compliance processes, and reducing workload inefficiencies, we empower your team to focus on innovation while maintaining security and compliance. Seize the Edge with Lynx by transforming challenges into opportunities for innovation and resilience.

Why Organizations Choose LYNX MOSA.ic.SCA

At Lynx, we empower organizations to strengthen their software supply chains with efficient, scalable, and secure solutions. With LYNX MOSA.ic.SCA, your team gains the tools to manage vulnerabilities, ensure compliance, and reduce costs—all while focusing on what matters most: delivering mission-critical solutions.

Manage vulnterabilities

Ensure compliance

Reduce costs

Learn more customer benefits enabled by LYNX MOSA.ic.SCA on the next page.

Customer Benefits	Capability Enabled by LYNX MOSA.ic.SCA
Efficient Vulnerability Tracking	• Minimize irrelevant CVEs, providing 85% fewer CVEs to analyze and 95% fewer false positives.[3] • Streamline SBOM management with support for multiple industry-standard formats. • Automated, real-time CVE tracking with intelligent filtering and a curated database. • Improve team collaboration and workflows across multiple SBOMs.
Faster Remediation	• Cut through delays of up to four weeks by mapping package names to CVE identifiers, versions, and patches.[4] • Parse kernel and boot configurations to identify CVEs. • Resolve issues faster with detailed fix recommendations and direct patch links.
Scalable for Large Projects	• Avoid the additional $100,000–$300,000 in engineering costs associated with DIY solutions.[2] • Leverage patch notifications and management tools to accelerate issue resolution. • Use powerful triage and collaboration tools to prioritize, assess, and resolve security issues effectively.
Reduced Workload	• Avoid the 3–5x labor costs of DIY solutions with the cost-effective MOSA.ic.SCA license. [7] • Simplify processes with a user-friendly interface for SBOM visualization and analysis. • Seamlessly integrate with CI/CD pipelines and Jira.
Risk mitigation	• Prevent $1M–$4M data breaches with automated tracking, regular updates, and professional support.[5] • Track changes between builds and releases, and simplify compliance reporting with automated summary reports.
Lower Compliance and Audit Costs	• Save up to $200,000 annually with professional support.[7] • Ensure compliance with a robust audit trail and streamlined cybersecurity documentation. • Deploy on-premises with SSO, role-based access, and project-specific permissions.

SBOM Management and Compliance: Simplify Security and Regulatory Alignment

In today's highly regulated industries, such as aerospace and defense, long-term security and compliance are critical to success. LYNX MOSA.ic.SCA simplifies Software Bill of Materials (SBOM) management with the powerful Vigiles™ suite, ensuring transparency, security, and alignment with key government mandates and industry standards. This is particularly valuable for highly regulated industries such as aerospace and defense, where long-term security and ongoing regulatory compliance are essential.

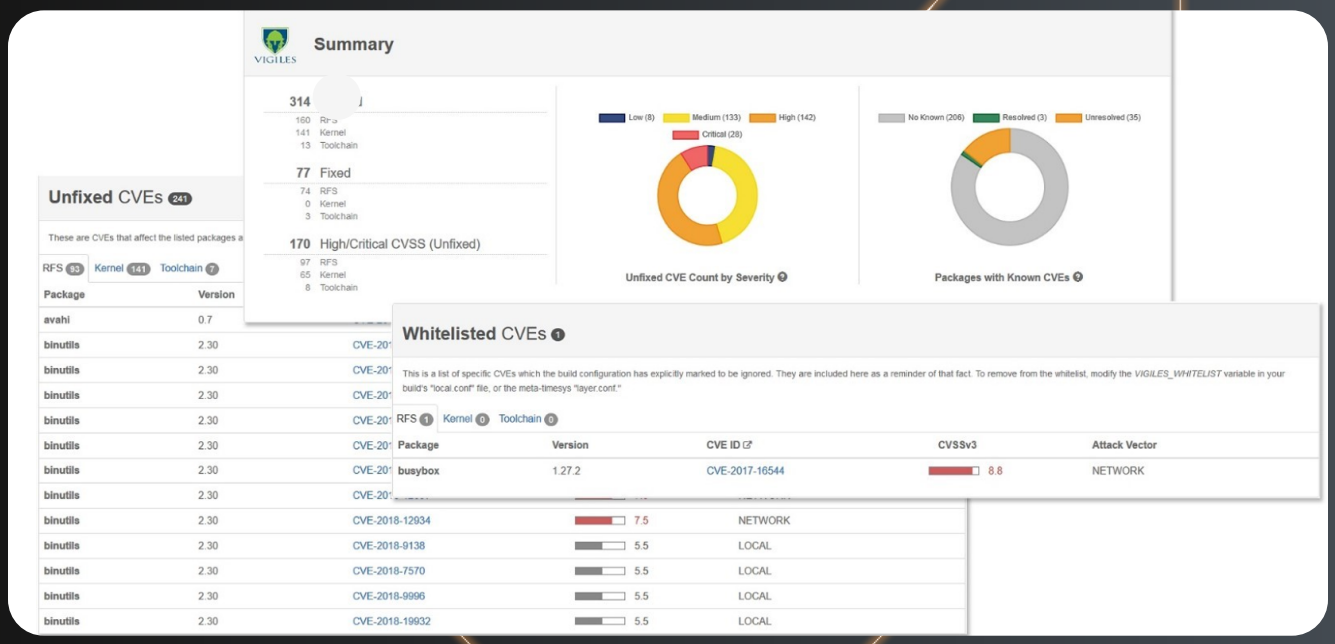
How MOSA.ic.SCA Supports Compliance

- **Automated SBOM Management** - Streamline the generation and management of SBOMs, keeping your software supply chain secure and auditable.
- **Comprehensive Mandate Alignment** - Comply with essential regulations, including:
  - White House EO 14028 for enhanced cybersecurity standards.
  - FDA Cybersecurity guidelines for medical devices.
  - EU Cyber Resilience Act (CRA) for robust system security.

Powerful Tools for Continuous Monitoring

- **Vigiles Dashboard -** Provides a centralized view of all projects, SBOMs, and teams, empowering your organization to easily manage complexity.
- **API-Driven Integration -** Seamlessly integrate Vigiles into CI/CD pipelines for continuous vulnerability monitoring and real-time updates.

By automating SBOM management and ensuring ongoing compliance, LYNX MOSA.ic.SCA equips your team to Seize the Edge in securing critical software systems while focusing on innovation.



Vigiles Key Capabilities: Targeted Tools for Embedded Systems Security

With more than 20 years of secure embedded software design expertise, Vigiles is purpose-built to address the unique challenges of managing vulnerabilities and maintaining compliance in mission-critical systems. By combining speed, accuracy, and embedded system optimization, Vigiles empowers your team to strengthen software security and Seize the Edge.

How Vigiles Delivers Value

- **Faster Reporting -** Reduce reporting delays by up to four weeks by aggregating data from multiple sources, providing your team with timely access to critical information.
- **Relevant CVE Filtering -** Focus on what matters most with intelligent filtering that reduces unnecessary analysis:
  - 85% fewer CVEs to review, cutting down on irrelevant alerts.
  - 95% fewer false positives.
- **Improved Accuracy -** A curated CVE database ensures up to 40% greater accuracy than the National Vulnerability Database (NVD). Security experts continuously update and validate CVEs, referencing the Common Platform Enumeration (CPE) to ensure relevance to your system.
- **Optimized for Embedded Systems -** Explicitly tailored for embedded environments, Vigiles understands kernel and U-Boot configurations, enabling precise daily monitoring. This is critical for aviation and defense systems requiring stringent, ongoing surveillance.
- **Streamlined Remediation -** For each vulnerability, Vigiles provides detailed fixes, patches, and configuration recommendations. With links to patches, workarounds, and testing resources, your team can resolve issues faster and more efficiently.

Vigiles Ecosystem: Support for Modern Development Environments

The Vigiles ecosystem is built to adapt to the diverse needs of today's embedded systems, providing seamless integration with a wide range of programming languages, build systems, and operating environments. With Vigiles, your team can intuitively track and manage Software Bill of Materials (SBOMs) across products and releases, ensuring compliance and security at every stage of development.

Extensive Language and Platform Support

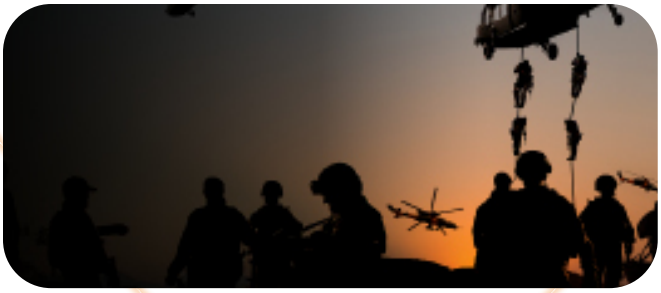
Vigiles supports a growing list of ecosystems, enabling broad compatibility for your development workflows, including:

- **Programming Languages**
  Rust, Go, Haskell, Erlang, Kotlin, Java, .NET, Node.js, Python, Ruby, Dart, and C/C++.
- **Package Managers**
  Crates.io, Hackage, Hex, Maven, NuGet, NPM, PyPI, RubyGems, and Pub.
- **Operating Systems**
  Debian.
- **Containers**
  Debian Containers.
- **RunSafe Integration**
  Enhanced security for embedded systems.
- **LYNX MOSA.ic**
  Fully optimized for seamless integration within Lynx environments.

Linux Build System Compatibility

Vigiles works effortlessly with all significant Linux build systems, ensuring flexibility for your embedded projects:

- Yocto
- Buildroot
- PetaLinux



SBOM Management Made Simple

Vigiles supports industry-standard SBOM formats to streamline compliance and collaboration:

- CycloneDX
- SPDX
- SPDX Lite

By supporting multiple development environments and standards, Vigiles ensures you has the tools to Seize the Edge with comprehensive, secure, and efficient workflows. These standards enable seamless workflows, regardless of the other tools your team uses, ensuring interoperability and flexibility across your entire ecosystem.

Eliminate Vulnerabilities and Future-Proof Your System with RunSafe™

Protecting embedded systems from cyber threats requires proactive, targeted solutions. RunSafe™ Security, integrated with LYNX MOSA.ic.SCA, addresses one of the most common attack vectors—memory corruption vulnerabilities—while ensuring your systems remain resilient and performant.

How RunSafe Enhances Security

- **Memory Corruption Mitigation -** RunSafe Security targets vulnerabilities that account for over 40% of exploited attacks and more than 60% of high and critical CVEs. By mitigating these vulnerabilities, your systems gain robust protection against zero-day threats and known memory-related bugs.
- **Seamless Workflow Integration -** Fine-grained Address Space Layout Randomization (ASLR) integrates directly into your existing development workflows, providing advanced protection without impacting performance.
- **Focused Feature Development -** The RunSafe Code™ Vulnerability Mitigation Visualizer works with Vigiles to identify mitigated vulnerabilities, enabling your team to prioritize innovation and feature development.

A Comprehensive Security Solution

Combining RunSafe Security with Vigiles gives you a multi-layered approach to vulnerability management and risk reduction. Together, these tools empower your team to Seize the Edge by addressing today's threats while preparing your systems for tomorrow's challenges.

Education and Services: Supporting Your Success Every Step of the Way

At Lynx, we're committed to ensuring your Software Composition Analysis (SCA) strategy is deployed effectively and delivers maximum value. Our services are designed to streamline your workflows, enhance your team's capabilities, and provide expert guidance tailored to your mission-critical needs.

Our Services Include

Quick Start Training- Equip your team to quickly identify vulnerabilities in your project's SBOM and confidently take action.

Self-Help and Education - Access a robust library of documents, videos, demos, and webinars catering to all skill levels.

Deployment Service - Receive on-site or remote assistance to integrate LYNX MOSA.ic.SCA seamlessly into your infrastructure.

Managed Services - Let Lynx handle end-to-end vulnerability management, from detection to remediation, allowing your team to focus on innovation.

With a team of experienced professionals holding security clearances, we provide support in controlled environments, ensuring your sensitive projects are handled with the highest level of security and expertise.

Seize the Edge in Software Security and Compliance

Take the next step in safeguarding your software supply chain. With LYNX MOSA.ic.SCA, you'll gain the tools, expertise, and support needed to navigate complex vulnerabilities and compliance challenges with confidence.

Proactive Vulnerability Management

Streamlined Compliance

Comprehensive Support

Sources

1. Source: Gartner, referenced in the datasheet regarding SBOM implementation preventing up to 70% of security incidents.
2. Source: Deloitte, “Annual Cyber Threat Trends report: Insights, emerging threats, and their potential impact,” 2024.
3. Source: Cyber Security Breaches Survey 2022, highlighting vulnerability triage inefficiencies.
4. Source: IBM Cost of a Data Breach Report 2022, citing delays in CVE publication.
5. Source: All About Mend’s 2021 Open Source Security Vulnerabilities Report.
6. Source: Cybersecurity News, ‘40,000 CVEs Published in 2024,’ https://cybersecuritynews.com/40000-cves-published-in-2024/. Source:
7. Lynx internal report.

Copyright

LYNX

Ready to revolutionize your mission-critical systems?

Contact Lynx today to learn more about how LYNX MOSA.ic.SCA can empower your success and help you Seize the Edge in every mission-critical endeavor.

edge@lynx.com
US: 408-979-3900
www.lynx.com