

Open Source Compliance and Security

Revenaera uses FlexNet Code Insight to manage Open Source Risk



Revenaera has been in business for over 30 years. Revenaera runs seven different lines of software products and serves more than 80,000 customers. Strong brands like InstallShield and AdminStudio are part of Revenaera's portfolio, as well as business-critical solutions for Software Asset Management, Software Monetization, and security products for Software Vulnerability Management and Software Composition Analysis.



CHALLENGE

- Utilize automation to create efficiencies and accuracy in open source management
- Free up engineers for business-critical work
- Create accurate software Bill of Materials (BOM)
- Single source of truth for the use of open source software across all products



SOLUTION

- FlexNet Code Insight leveraged for OSS scans of all Revenaera products
- Revenaera Audit Services leveraged for code audits and M&A activity
- Robust approach to Software Composition Analysis supported by consistent processes and policies



BENEFITS

- Creation of a "get clean, stay clean" strategy
- Automated, alert-based solution to manage priority issues
- Improved resource and process management
- Immediate action against identified OS risks and vulnerabilities

The Challenges of Open Source Security

When Revenera acquired Palamida in 2016, it was with the intent to extend their security and software management solution offerings. A Software Composition Analysis solution would help Revenera customers manage the compliance and security risks inherent in under-managed Open Source Software (OSS) components. Security, development and executive teams at Revenera also fully understood how important OS analysis of their own applications was for the company. Scanning and remediation of identified risks always was a priority for the business and Revenera was looking to add more automation to it.

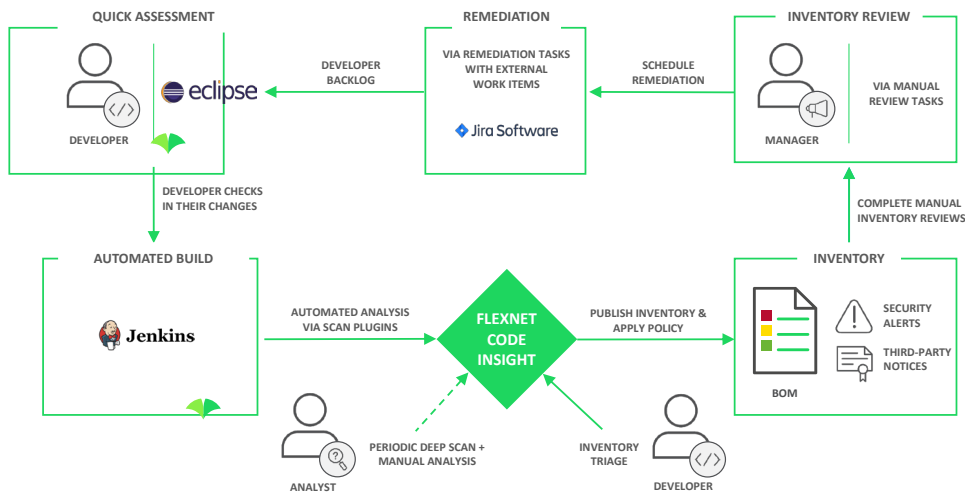
Revenera at one time—like many companies—followed a manual process for identifying known vulnerabilities within open source code being used internally and across solutions. It was a manual process to make sure that open source components and related license and vulnerability information was shared and kept up-to-date by teams across the company. This made for an inefficient method to create and update Bills of Material (BOMs).

But Revenera understood that a manual process for OSS tracking is not ideal, especially since the use of open source was on the rise, the software supply chain was growing and becoming more complex, and with the increase in number of possible threats being reported, the company needed to get ahead of any potential vulnerabilities that could threaten the supply chain. The manual process was not a good use of time for developers and it didn't fully deliver on the high standard Revenera set for the management of open source components.

The Get Clean, Stay Clean Solution

Revenera implemented its own Software Composition Analysis Solution, FlexNet Code Insight. Working with Code Insight, engineers and developers take advantage of this automated, purpose-built solution that scans applications, identifies any open source, sends out alerts about license and security risks, prioritizes issues for remediation, and recommends remediation steps.

REVENERA'S PROCESS FLOW USING INSIGHT



"In providing Software Composition Analysis and vulnerability management solutions to our customers, we need to lead the way in exemplifying how to get clean and stay clean. FlexNet Code Insight is our comprehensive approach to managing risk and staying ahead of open source license compliance and security issues."

ALEX RYBAK
—DIRECTOR, PRODUCT MANAGEMENT, REVENERA



CASE STUDY

FlexNet Code Insight enables the company to:

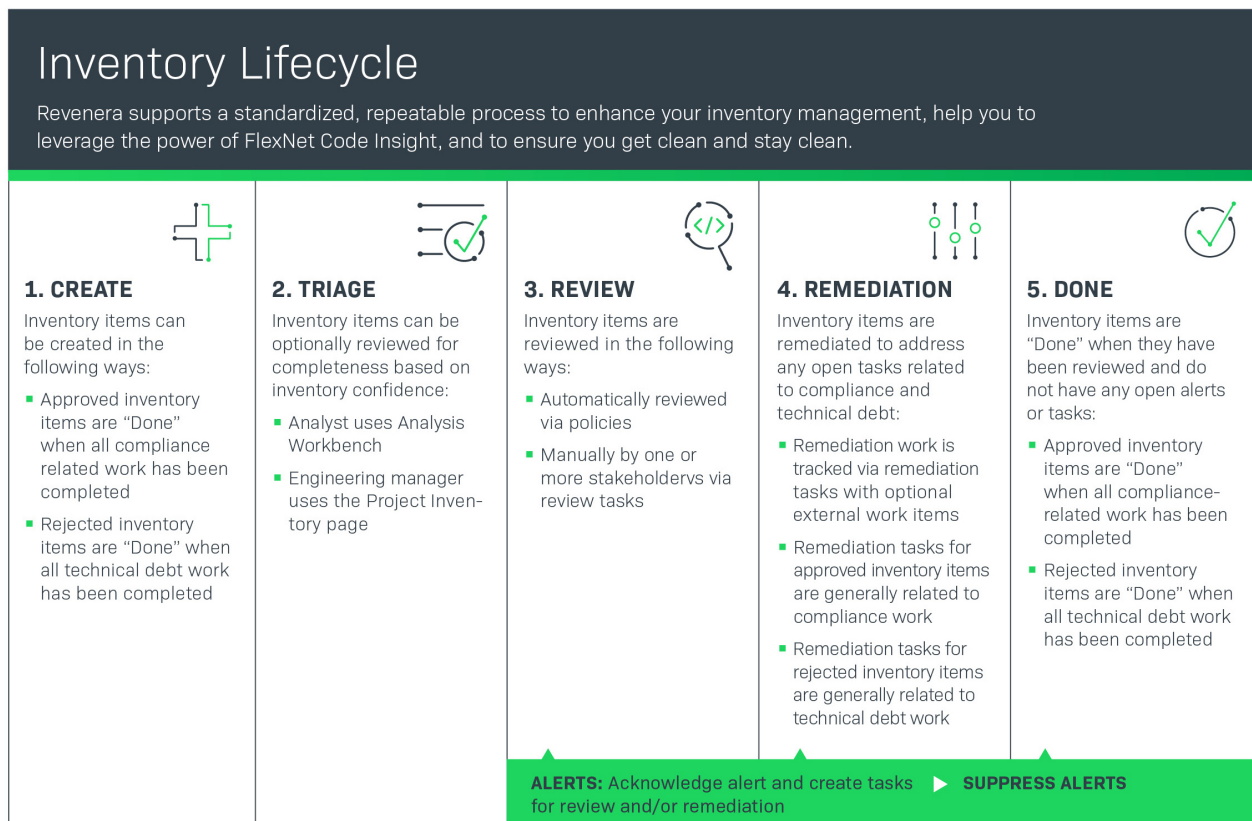
- Establish a single source of truth about all Open Source Software use across the organization
- Create an accurate BOM
- Free up engineers and developers to focus on mission-critical programs
- Get accurate, deep scans of applications, ensuring compliance with open source licenses
- Take immediate action against identified vulnerabilities

Reverera understands that, although FlexNet Code Insight offers a completely automated workflow, there are manual checks needed to support the overall strategy. To help keep their efforts seamless, Reverera created a “Get Clean, Stay Clean” approach to OSS security and compliance management. The “Get Clean” step was to implement FlexNet Code Insight for all product lines, build a complete inventory and remediate priority issues. This stage is critical to creating the foundational BOM. “Stay Clean” involves a long-term strategy where the company reaps the benefits of

regular scans and initiates ongoing maintenance of its software composition analysis process. “Stay Clean” includes:

- A shift of ownership from auditors to the Engineering Manager
- Management of newly added components, new vulnerability alerts, and creation of remediation tasks
- Weekly review of new vulnerabilities, actions, and results with the engineering team
- Regular triage of issues and change management of policies to support business needs

The Reverera team uses a five-step inventory lifecycle process. The process manages inventory end-to-end, from how inventory items get created and triaged through to remediation and notice of issue completion—meaning inventory items are “Done” because they have no open alerts or tasks assigned to them. From start to finish, Reverera has created a standardized, repeatable process across the organization to enhance inventory management, leverage the power of FlexNet Code Insight, and ensure they adhere to their “Get Clean, Stay Clean” strategy.



Enhanced Analysis Leads to More Secure Outcomes

Using FlexNet Code Insight to manage OSS compliance and security has enabled Revenera to better manage resources, to quickly and efficiently seek out, find and remediate risk issues, and to greatly improve processes for ensuring continued company-wide policy adherence of open source use.

Additionally, if there is a news-worthy event such as the case with Apache Struts 2, Revenera can react quickly because they know what's in their code and what may be vulnerable. Queries are fast and immediate at a time when hours can mean the difference between bottom-line impact and loss of reputation. FlexNet Code Insight gives Revenera development, security, and legal teams complete peace of mind.

What the Future Holds

Revenera understands that open source use is on the rise for its customers as well as for its own purposes, and intends to continue to push its Software Composition Analysis efforts forward. The company has a plan to add functionality to its system in order to uplift its software license compliance and vulnerability management. Next steps include:

- Tighten the step-by-step process for onboarding internal teams to use FlexNet Code Insight
- Expand proactive use of the OSRB to review developer requests to use ODD in their development
- Refine/expand corporate policies for automated review, usage, and remediation guidance
- Enhanced reporting capabilities for publication of third-party notices and other disclosures
- Usability improvements to make the inventory clearing process more efficient
- Expand guidance for common remediation scenarios

"Open source scanning and analysis should be a priority for any company that is building software. As the provider of Software Composition Analysis solutions for global companies, Revenera should lead by example. FlexNet Code Insight is the foundation of our open source security and compliance efforts. Our teams trust it and we know it allows us to make better decisions faster."

SAI VENDANTAM

—DIRECTOR, SOFTWARE DEVELOPMENT, REVERERA



NEXT STEPS

Take control of your open source software license compliance and security.

[LEARN MORE >](#)

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. www.revenera.com