BLACK DUCK®

TAS Group Improves Security Posture and Streamlines Compliance with Black Duck SCA and Coverity

ABOUT TAS GROUP

Industry: Fintech, digital payments, financial software

Headquarters: Rome, Italy

Customer footprint

- Major commercial and central banks
- European financial services centers
- Global Fortune 500 broker/dealers

Core business areas

- Digital payment and card management
- Financial messaging and market infrastructure
- Capital markets and treasury software
- Open banking and banking-as-a-service
- Fraud prevention and regulatory compliance

Challenges

- Vulnerability management
- Slow and manual processes
- False positives
- Obscured risk exposure

Requirements

- Open source license risk management
- Software supply chain visibility
- Software Bill of Materials
- Continuous vulnerability monitoring
- Application security posture management
- PCI DSS, GDPR, PSD2, NIS2, and DORA compliance

Solutions

- Black Duck SCA
- Coverity

TAS Group is a recognized fintech leader across Europe, shaping the future of digital payments, card management, and financial markets with advanced software solutions. It's motto, "Agile, flexible, and scalable technologies are our starting point; fast, customized, and reliable services are our destination," is also the company's foundational philosophy.

TAS Group helps its clients modernize complex payment systems, efficiently manage liquidity, and navigate the intricate web of international compliance standards, including PCI DSS, GDPR, PSD2, NIS2, and the Digital Operational Resilience Act (DORA).

While many in the financial sector are still grappling with the implications of these regulations, TAS Group's proactive and forward-thinking approach gives it a competitive advantage. Its leadership in handling these regulations underscores its understanding that cybersecurity and cyber-resilience are not just checkboxes but fundamental pillars of trust and continuous service delivery.

TAS Group has a deep commitment to operational resilience, business continuity, and robust cybersecurity practices. To deliver on its vision and maintain its leadership in compliance and innovation, TAS Group recognized the critical need to integrate security into its agile software development life cycle and gain continuous, comprehensive visibility.

CHALLENGES

Maintaining a competitive edge in a rapidly evolving threat landscape presents challenges, even for an innovator like TAS Group. According to Chief Information Security Officer Fabrizio Brintazzoli, vulnerability management issues plagued the development team before partnering with Black Duck. The vulnerability management processes were slow, manual, and prone to false positives, creating a bottleneck for his team. This hindered its agility and obscured the company's true risk profile across its extensive software portfolio, threatening to slow down its fast, customized, and reliable services.

"We really needed to create a continuous compliance program, not just a one-off implementation."

–Fabrizio Brintazzoli

"The ability to generate comprehensive Software Bills of Materials (SBOMs) and streamline third-party risk management is particularly critical for meeting stringent DORA requirements."

–Fabrizio Brintazzoli

SOLUTION

The team chose Black Duck® SCA and Coverity® Static Analysis, and the solutions quickly became indispensable. Black Duck's automated open source license risk management, unparalleled software supply chain visibility, and continuous vulnerability monitoring directly support TAS Group's agile development practices, ensuring that security is built-in, not bolted on.

With Black Duck, TAS Group could not only address immediate security challenges but also reinforce its foundational commitment to agile, flexible, and scalable technologies, ensuring it could continue to deliver the secure, reliable, and compliant services its customers depend on, now and in the future.

BLACK DUCK SCA

TAS implemented Black Duck SCA to gain better visibility into its software supply chain, improve the overall security posture of its software, and automate open source license risk management. Black Duck SCA combines file system scanning and source code analysis to deliver a complete and accurate view into the software supply chain, including

- **Dependency analysis** to identify direct and transitive dependencies declared by package managers
- **Binary analysis** to detect dependencies in post-build artifacts like firmware and container images, without access to source code
- **Snippet analysis** to find and match code snippets, such as those introduced by AI coding tools, back to their original open source projects
- **CodePrint analysis** to identify dependencies in source files and directories, even when they're not declared by package managers
- **Container scanning**, which is a combination of binary and CodePrint analysis that identifies open source dependencies in container images, layer by layer
- **C/C++ scanning** to accurately identify open source dependencies and libraries in C/C++ applications, even when there are no package managers

"Black Duck SCA has significantly improved our ability to generate a comprehensive SBOM for our applications," Brintazzoli said. "The reports are easily exportable and integrate well with our existing compliance and security workflows, streamlining audits and reducing manual effort, as well."

Improved security posture

Black Duck SCA provides detailed dependency identification, early vulnerability detection, and automated security testing integrated into development workflows, significantly improving security posture.

"Most notably, the automated identification and continuous monitoring of open source components has drastically reduced our exposure to known vulnerabilities," said Brintazzoli. "We have seen a clear decrease in the number of security issues related to third-party libraries, thanks to timely alerts and remediation guidance."

Additionally, Black Duck's license compliance features have minimized the legal risks associated with open source use.

Automated license risk management

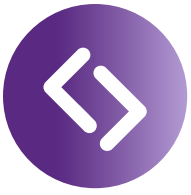
Black Duck allows organizations to set license policies in advance, so developers can implement open source without the additional work required to evaluate license obligations.

"Black Duck SCA accurately detects the licenses associated with each component and flags any potential conflicts or obligations in real time," Brintazzoli said. "This significantly reduces the manual effort required to track license compliance."

Black Duck SCA also finds explicitly declared licenses, sublicenses, and embedded licenses, and presents the requirements and restrictions in a simplified view, along with complete license text and copyright information.

"Black Duck SCA's detailed reports and alerts enable our legal and development teams to collaborate efficiently, ensuring that any incompatible or risky licenses are identified early in the development cycle, preventing costly compliance issues down the line."

–Fabrizio Brintazzoli



COVERITY STATIC ANALYSIS

TAS integrated Coverity into its CI/CD pipeline for seamless, continuous static analysis without a significant impact on build times. "After each build, the analysis results are uploaded to the Coverity server for processing and review," Brintazzoli said. "We configured the pipeline to fail or send alerts if critical issues are detected, ensuring early feedback to developers."

Coverity scans can be performed throughout the early stages of the SDLC to uncover security and quality issues when they're least disruptive and easiest to resolve.

“Overall, the integration of Black Duck SCA and Coverity into our development life cycle has accelerated our vulnerability management process, improved risk visibility for our security and development teams, and helped us maintain a more secure and compliant software supply chain.”

–Fabrizio Brintazzoli

RESULTS

Since implementing Coverity and Black Duck SCA, TAS Group has seen several significant improvements.

Streamlined identification and prioritization of security vulnerabilities

“From a development perspective, integrating Coverity into the CI/CD pipeline has had a positive impact on productivity and release velocity,” said Brintazzoli. Now, TAS’s developers are notified about security and quality issues in the early stages of the SDLC, when they are least disruptive and easiest to resolve. This has transformed TAS’s previously slow and manual process. This, combined with the accuracy of Coverity scans, has significantly reduced false positives and accelerated the previously slow and manual process of finding and resolving issues.

Black Duck SCA’s continuous monitoring and accurate vulnerability identification capabilities have drastically reduced exposure to known vulnerabilities, as well. The combination of Black Duck SCA and Coverity helps TAS maintain its compliance with regulatory frameworks like PCI DSS, GDPR, PSD2, NIS2, and DORA without duplicating efforts or introducing inconsistencies.

Improved third-party and vendor risk management

Black Duck SCA generates SBOMs in SPDX and CycloneDX formats, so exporting and sharing them with customers is easy. This streamlines audits and reduces manual effort, significantly improving the management of data processors and critical ICT third parties. And providing clear visibility into software components and their associated risks aligns with regulatory requirements for vendor assessments and contractual controls.

Minimized legal and operational risks

Black Duck SCA’s open source license management minimizes the legal risks associated with open source use and ensures compliance with regulations. It accurately detects licenses and flags potential conflicts or obligations in real time, significantly reducing the manual effort required for license compliance—crucial for managing third-party components and avoiding costly compliance issues.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.