nuaware
An Exclusive Networks Company

Solution Brief

Better together: Black Duck Application Security and Docker Desktop

Secure your containers with Black Duck and Docker—because security and speed should go hand in hand.

Nuaware | © 2021 Nuaware All Rights Reserved

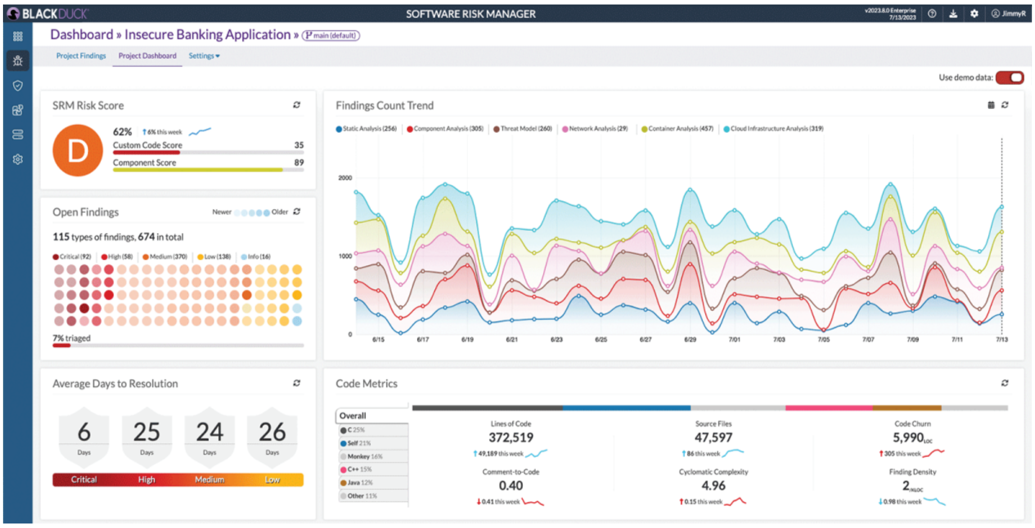
Securing Containerized Applications with Confidence

As organizations embrace containerized applications and microservices, securing these environments becomes a critical priority.

Containers simplify application deployment and management, but it also introduces unique security risks, including vulnerabilities in container images, open-source dependencies, and misconfigurations.

Black Duck Application Security provides a comprehensive solution for identifying and mitigating risks before they undergo their way into Q/A and then production.

Software supply chain risk management is critical when using open source since 86% of code bases globally contain vulnerable software according to OSSRA, this is related to Software Licenses as well where 56% of the code bases have license conflicts.



Software supply chain management

86% of code bases globally contain vulnerable software*

56% of the code bases have license conflicts*"

*according to OSSRA

Nuaware | © 2021 Nuaware All Rights Reserved

Why a Black Duck and Docker are better together?

Automated Security at the Speed of DevOps

Containers enable rapid development and deployment, but security must keep pace.

Black Duck seamlessly integrates with Docker to scan container images, ensuring that vulnerabilities and licenses in open-source components are detected early in the software development lifecycle (SDLC).

By embedding security into DevOps workflows (DevSecOps), teams can catch and fix issues before they become costly problems.

Deep Visibility into Open-Source Risks

Docker images contain multiple layers, including open-source libraries and dependencies.

Black Duck provides deep visibility into these components, identifying known vulnerabilities (CVEs and BDSAs), license compliance risks, and outdated packages.

This level of insight allows developers to make informed decisions about the security posture of their containers.

Continuous Monitoring to Secure Operations

Security requires continuous monitoring.

Black Duck helps maintain the security of running containers by regularly scanning for newly discovered vulnerabilities, even after deployment.

This ensures applications remain secure throughout their lifecycle, reducing the risk of exposure to new threats.

Secure your containers with Black Duck and Docker— because security and speed should go hand in hand.

Seamless Integration across the CI/CD Pipeline

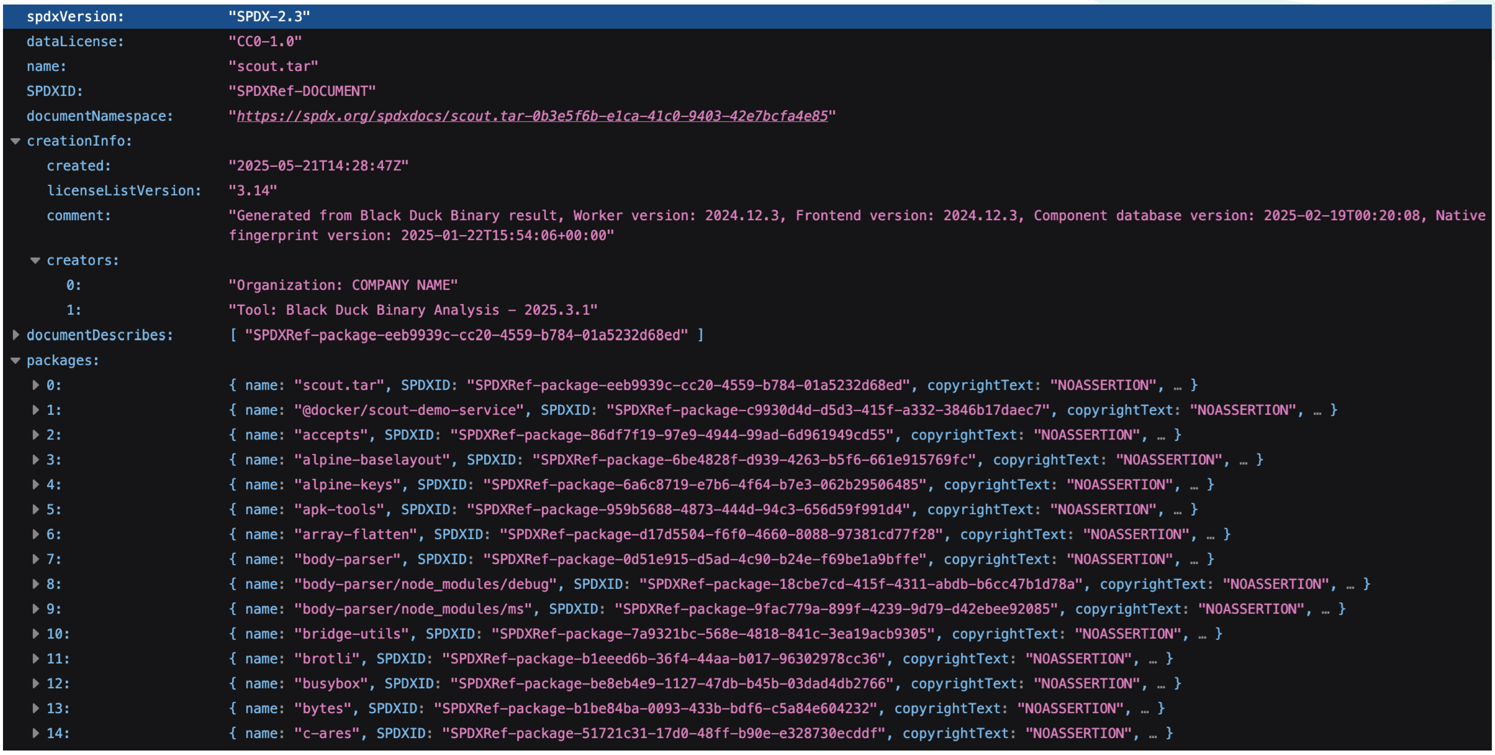
Black Duck integrated to any CI/CD tools and provides plug-ins to most popular environments (GitHub, GitLab, ADO, Jenkins), it also exposes AppSec value to developers using it's Code Sight IDE plug-in (supported in Visual Studio, Visual Studio Code, Jenkins and Jetbrains).

These integrations increase the efficiency of the SSDLC preventing vulnerable containers to hit production environments.

Actionable Remediation and Policy Enforcement

Black Duck doesn't just identify vulnerabilities it helps teams prioritize and remediate them effectively.

With policy-driven security controls, organizations can enforce security best practices, blocking non-compliant images from deployment and reducing the attack surface of their containerized environments.



```
  spdxVersion:            "SPDX-2.3"
  dataLicense:            "CC0-1.0"
  name:                   "scout.tar"
  SPDXID:                 "SPDXRef-DOCUMENT"
  documentNamespace:      "https://spdx.org/spdxdocs/scout.tar-0b3e5f6b-e1ca-41c0-9403-42e7bcfa4e85"
▼ creationInfo:
    created:              "2025-05-21T14:28:47Z"
    licenseListVersion:   "3.14"
    comment:              "Generated from Black Duck Binary result, Worker version: 2024.12.3, Frontend version: 2024.12.3, Component database version: 2025-02-19T00:20:08, Native
                          fingerprint version: 2025-01-22T15:54:06+00:00"
  ▼ creators:
      0:                  "Organization: COMPANY NAME"
      1:                  "Tool: Black Duck Binary Analysis - 2025.3.1"
▶ documentDescribes:      [ "SPDXRef-package-eeb9939c-cc20-4559-b784-01a5232d68ed" ]
▼ packages:
  ▶ 0:                    { name: "scout.tar", SPDXID: "SPDXRef-package-eeb9939c-cc20-4559-b784-01a5232d68ed", copyrightText: "NOASSERTION", … }
  ▶ 1:                    { name: "@docker/scout-demo-service", SPDXID: "SPDXRef-package-c9930d4d-d5d3-415f-a332-3846b17daec7", copyrightText: "NOASSERTION", … }
  ▶ 2:                    { name: "accepts", SPDXID: "SPDXRef-package-86df7f19-97e9-4944-99ad-6d961949cd55", copyrightText: "NOASSERTION", … }
  ▶ 3:                    { name: "alpine-baselayout", SPDXID: "SPDXRef-package-6be4828f-d939-4263-b5f6-661e915769fc", copyrightText: "NOASSERTION", … }
  ▶ 4:                    { name: "alpine-keys", SPDXID: "SPDXRef-package-6a6c8719-e7b6-4f64-b7e3-062b29506485", copyrightText: "NOASSERTION", … }
  ▶ 5:                    { name: "apk-tools", SPDXID: "SPDXRef-package-959b5688-4873-444d-94c3-656d59f991d4", copyrightText: "NOASSERTION", … }
  ▶ 6:                    { name: "array-flatten", SPDXID: "SPDXRef-package-d17d5504-f6f0-4660-8088-97381cd77f28", copyrightText: "NOASSERTION", … }
  ▶ 7:                    { name: "body-parser", SPDXID: "SPDXRef-package-0d51e915-d5ad-4c90-b24e-f69be1a9bffe", copyrightText: "NOASSERTION", … }
  ▶ 8:                    { name: "body-parser/node_modules/debug", SPDXID: "SPDXRef-package-18cbe7cd-415f-4311-abdb-b6cc47b1d78a", copyrightText: "NOASSERTION", … }
  ▶ 9:                    { name: "body-parser/node_modules/ms", SPDXID: "SPDXRef-package-9fac779a-899f-4239-9d79-d42ebee92085", copyrightText: "NOASSERTION", … }
  ▶ 10:                   { name: "bridge-utils", SPDXID: "SPDXRef-package-7a9321bc-568e-4818-841c-3ea19acb9305", copyrightText: "NOASSERTION", … }
  ▶ 11:                   { name: "brotli", SPDXID: "SPDXRef-package-b1eeed6b-36f4-44aa-b017-96302978cc36", copyrightText: "NOASSERTION", … }
  ▶ 12:                   { name: "busybox", SPDXID: "SPDXRef-package-be8eb4e9-1127-47db-b45b-03dad4db2766", copyrightText: "NOASSERTION", … }
  ▶ 13:                   { name: "bytes", SPDXID: "SPDXRef-package-b1be84ba-0093-433b-bdf6-c5a84e604232", copyrightText: "NOASSERTION", … }
  ▶ 14:                   { name: "c-ares", SPDXID: "SPDXRef-package-51721c31-17d0-48ff-b90e-e328730ecddf", copyrightText: "NOASSERTION", … }
```

Nuaware | © 2021 Nuaware All Rights Reserved

nuaware
An Exclusive Networks Company

Use Case: Secure Containerized Development Pipeline

Imagine a development team building an application with Docker. As they create and push Docker images to their registry, Black Duck automatically scans these images, identifying security risks in open-source libraries.

If a high-severity vulnerability is detected, the pipeline can be configured to fail, preventing insecure images from being deployed.
Developers receive detailed remediation guidance, allowing them to update affected dependencies quickly.

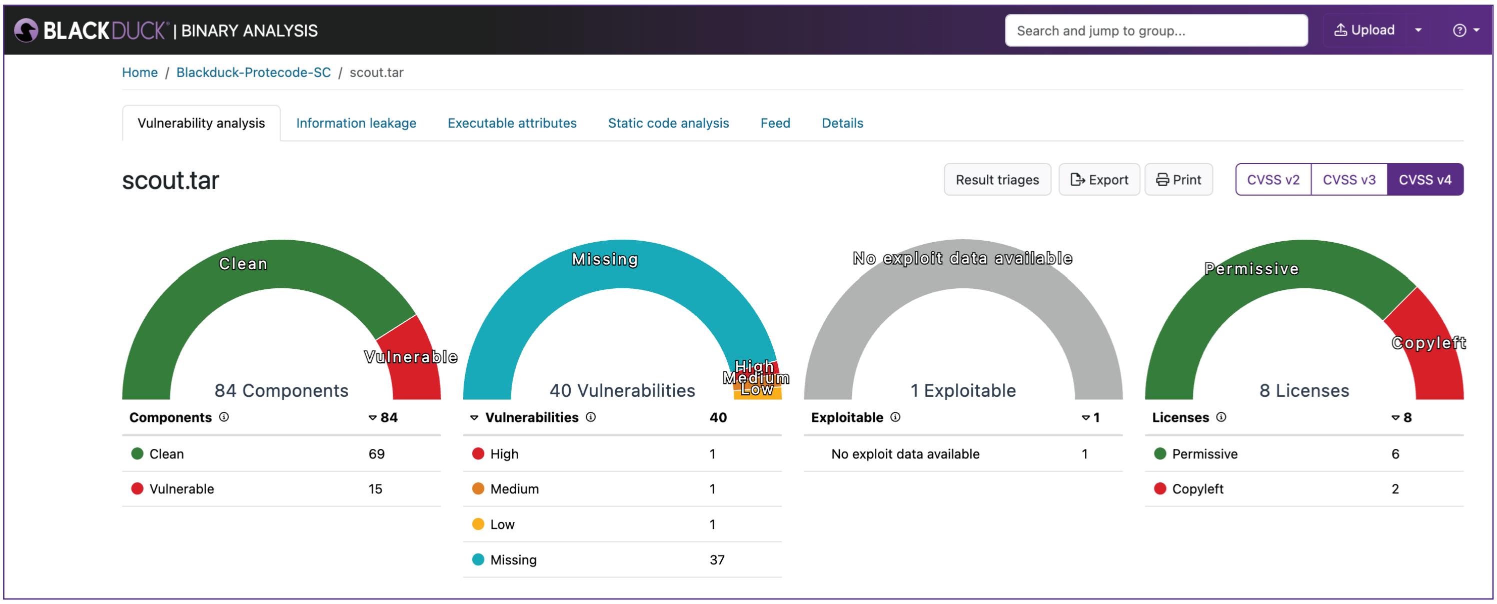
By integrating Black Duck with Docker, organizations can confidently deploy secure applications while maintaining the speed and agility of containerized development.

Docker revolutionizes application deployment and security must be a top priority.

Black Duck is the perfect security add-on for Docker which provides true scale and automated vulnerability scanning, deep open-source visibility, continuous monitoring, and seamless CI/CD integration.

Allowing organizations to manage their risk, conform to industry and legislation specific requirements around application security testing and supply chain risk management (SBOM).

Together, Black Duck and Docker empower teams to build and deploy secure, compliant, and resilient containerized applications.



scout.tar

84 Components

Components	84
● Clean	69
● Vulnerable	15

40 Vulnerabilities

Vulnerabilities	40
● High	1
● Medium	1
● Low	1
● Missing	37

1 Exploitable

Exploitable	1
No exploit data available	1

8 Licenses

Licenses	8
● Permissive	6
● Copyleft	2

Nuaware | © 2021 Nuaware All Rights Reserved

About us

About Nuaware

Nuaware, an Exclusive Networks company, specializes in DevSecOps, providing seamless access to best-in-class technologies. As a value-added distributor, Nuaware enables organizations to adopt modern security architectures with a shift-left security approach and managed cloud security, supported by the appropriate technologies, training, and a robust partner ecosystem

About Exclusive Networks

Exclusive Networks (EXN) is a global cybersecurity specialist that provides partners and end-customers with a wide range of services and product portfolios via proven routes to market. With offices in over 45 countries and the ability to serve customers in over 170 countries, we combine a local perspective with the scale and delivery of a single global organisation.

About Black Duck

Black Duck provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk.

We partner with Black Duck to offer you an industry-leading portfolio of software security products and services.

Black Duck solutions interoperate with third-party and open source tools, allowing you to leverage existing investments to build the security program that's best for your business. Only Black Duck offers everything you need to build trust in your software.

About Docker

Developers can create and deploy secure applications to any cloud or on-premises infrastructure using Docker Desktop, resulting in faster delivery times. The Pro, Team, and Business subscriptions provide companies with additional features that enhance the value of Docker Desktop. These features include the ability to manage secure software supply chains, centralise policy visibility and control, and manage users and access.

Docker Desktop requires a paid subscription (Pro, Team, or Business), available for as little as $5 per month for larger enterprises (over 250 employees or over $10 million in annual revenue).

Nuaware | © 2021 Nuaware All Rights Reserved

nuaware
An Exclusive Networks Company

🔗 nuaware.com

✉ info@nuaware.com

☎ +44 (0) 203 488 0530

Nuaware | © 2021 Nuaware All Rights Reserved