rezilion

SOLUTION OVERVIEW

Dynamic SBOM

A Software Bill of Material is not enough. True risk mitigation of the software attack surface requires a Dynamic SBOM.

With a Dynamic SBOM you can

- ✔ **Get a complete, comprehensive, and continuous view into all of your software components**
- ✔ **Understand your true software attack surface at all times with real time updates**
- ✔ **Quickly search for known vulnerabilities and components and find out if they are present in your environment**
- ✔ **Know which vulnerabilities are exploitable in your environment, so you can focus on what matters most**
- ✔ **Understand your open source, third party and supply chain risk**
- ✔ **Make sure you are compliant with requirements to provide an SBOM**

THE CHALLENGES

Businesses need complete and real-time transparency across the entire software lifecycle and stack.

Organizations have two massive security challenges in today's software-driven world:

- The software attack surface keeps growing through software innovation. Translation: millions of lines of code, and an equal amount of components means elevated risk.

- Threat actors leverage the growing software attack surface and find new threat vectors. Recent attacks, like a Solarwinds, and vulnerabilities like Log4j, Spring4Shell reveal how vulnerable the software supply chain is today.

Developers and product security teams must release products quickly and securely, every day.

But today's software environment includes many software components from a broad range of sources. These software components range from packages, images, libraries, and files, including third party, Commercial Off the Shelf (COTS), and Open Source Components (OSS). It's a very complex environment to manage.

To mitigate software security threats, security leaders must:

- ✔ Truly understand their attack surface at any given time
- ✔ Know which components of the attack surface are vulnerable and exploitable
- ✔ Understand their supply chain risk
- ✔ Have the critical information needed to prioritize software risks
- ✔ Be positioned to mitigation and remediate risks quickly

With little to no understanding of their true attack surface, its composition and exploitability in real time, it is not possible for developers and product security teams to prioritize and remediate effectively.

SBOMs

Software Bill of Materials or SBOMs are a must-have tool to ensure the software is developed, sold, and purchased securely. But an SBOM is a static, point-in time machine readable artifact with an inventory of everything present in a software environment. SBOMs provide greater transparency on composition of software, their dependencies, provenance, as well as potential risk associated with such components. But, they have serious limitations.

Why an SBOM is not enough

The current SBOMs have a few challenges associated with them:

1. **Today's SBOMs are static,** while software is dynamic. Software is constantly changing, be it in development or production, and SBOMs need to reflect these changes in real time. If SBOMs cannot be easily updated, their value is greatly diminished.

SBOMs provide greater transparency on composition of software, their dependencies, provenance, as well as potential risk associated with such components. But, they have serious limitations.

2. **SBOMs are not fully automated,** which diminishes effectiveness. Without automation, it is easy to miss risks caused by updates SBOMs are only truly effective as a security tool if their management is automated.
3. **SBOMs are specific to certain software or applications** — Current SBOMs are related to a specific software and/or application/stack and do not provide complete third party components information, which makes their use limited. Modern software environments have multiple software/ applications in development and production. This requires creating multiple SBOMs, which makes management even more complex.
4. **SBOMs require an additional artifact for context** — SBOMs by themselves offer limited value when understanding the exploitability of a specific vulnerability unless they provide the additional context needed to understand if the components and vulnerabilities are actually exploitable. This document is called VEX (vulnerability exploitability exchange) which is a machine readable companion to the SBOM, adding to further management complexity.
5. **Current SBOM outputs are very large and noisy,** which makes them difficult to understand and adds extra work for the users — developers, product security teams, CISOs, legal, and compliance officers that maintain them.

The current manual and static approach to SBOMs, though valid, will not offer enhanced security of the software supply chain.

SOLUTION: DYNAMIC SBOM

Rezilion Inc, offers an SBOM that is just not a static point in time artifact, but a continuous and real-time dashboard that updates whenever there is a change in the software. In other words, it is a dynamic SBOM.

With Rezilon's Dynamic SBOM, customers know their real attack surface as it changes dynamically. The Dynamic SBOM allows customers to understand true risk with built-in vulnerability context and VEX. It enables organizations to search for vulnerable components and use that information to take appropriate remediation action throughout the development lifecycle — all in real time. Additionally customers can control their supply chain risk, achieve compliance, and share the Dynamic SBOM by exporting it as a CycloneDX artifact.

Rezilion's Dynamic SBOM seamlessly plugs to all software environments, from development to production, and provides real-time visibility to all software components. It provides full-stack coverage of third-party and home-grown software across hosts, containers, and application layers. Unlike static SBOMs, Rezilion's Dynamic SBOM does more than just uncover what software components are there: it reveals if and where they're being executed in runtime (if loaded to memory, they are exploitable, if not loaded, they don't pose a risk), providing organizations with an unparalleled solution to understand where bugs exist — but also whether or not they could be exploited by attackers.

The Dynamic Software Bill of Materials (SBOM) is essential to truly see into, discover, and understand your true software attack surface.

Key Features of the Dynamic SBOM

✔ **Continuous**

- SBOM reflects changes as your environment changes
- No need to maintain multiple versions
- Offers continuous risk assessment

✔ **Dynamic**

- Know component state to triage active versus latent threats
- Provides context on what is exploitable or not exploitable in your environment and reveals what is loaded, or not loaded to memory
- Run time context tells you where to focus your remediation efforts

✔ **End-to-End — Full Stack/Full Cycle and Comprehensive**

- Provides visibility into your entire software environment from dev to production
- Covers a broad range of software component types such as containers, applications, hosts, packages, and files

✔ **Searchable and Customizable Results**

- Customize using filters to define acceptable risk thresholds
- Search by every identifier of the component
- Drill down

✔ **Contextualized**

- VEX — built in dashboard as well exportable as a separate artifact.

✔ **Exportable**

- As a standard CycloneDX format.

Key Benefits of the Dynamic SBOM

✔ **Dynamic Visibility** — Continuous tracking and management of the software environment and components as changes are being introduced for a clear understanding of your attack surface. Instantly view which components are actually being used and whether they impact your attack surface.

✔ **Dynamic Identification** — Instantly search and pinpoint vulnerabilities and components (such as Log4j) across billions of files and instantly determine whether or not they are exploitable in your environment.

✔ **Dynamic Context** — Know down to the function level what every component is doing in runtime to triage active versus latent threats.

✔ **Full Stack, Full Cycle Coverage** — See all software components across dev and prod, on-prem and cloud, hosts, and containers.

✔ **Share your SBOM with Exportable Formats** — Share important information with customers using a formal VEX (vulnerability exchange) or Cyclone DX document to facilitate transparency and compliance.

- ✔ **Assure your customers** — Communicate important vulnerability information with your customers with built validation in your dashboard or using a formal VEX (vulnerability exchange) document to outline the actual impact of vulnerabilities they may detect in your product.
- ✔ **Manage your supply chain risk** — Know where everything came from and risks associated with it.

What's in Your Dynamic SBOM

An SBOM is only as good as the details it contains. And static SBOMs do not contain enough updated, real-time details to offer better security in the software supply chain. Rezilion's Dynamic SBOM is detailed, comprehensive, and continuously updated. It covers software components ranging from container images to packages, hosts, and files, etc.

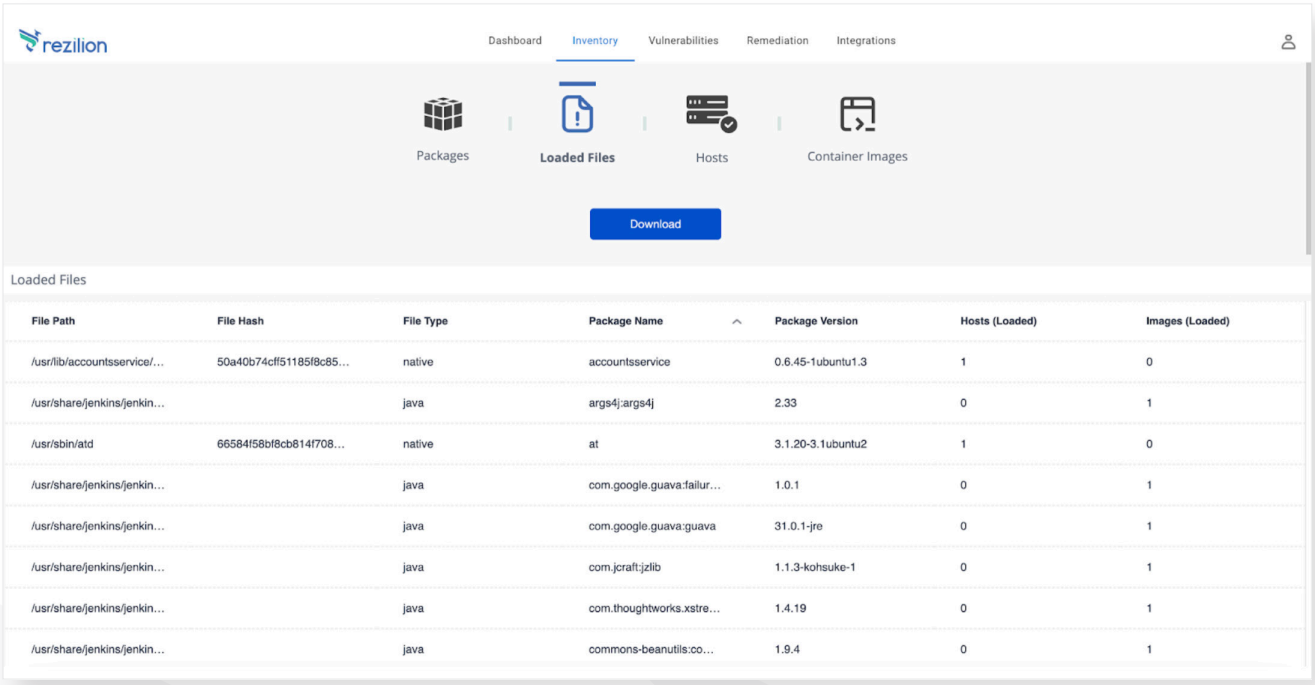

Fig 1: Inventory of all loaded files with details

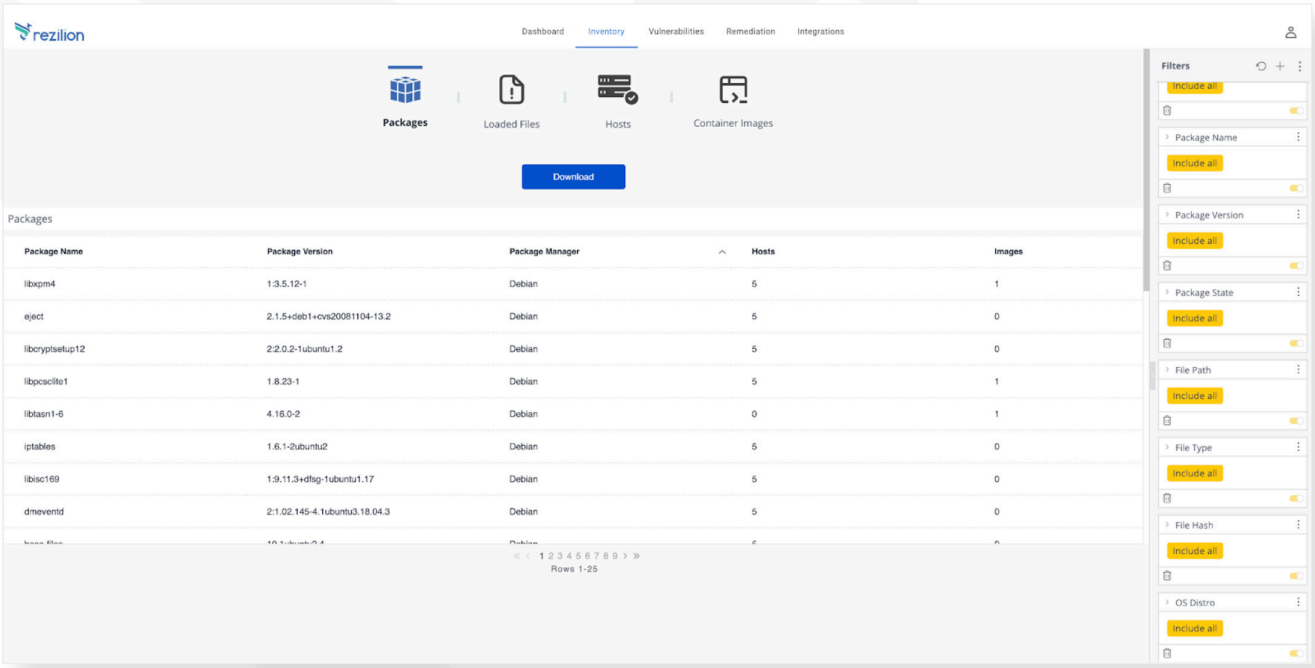

Fig 2: Inventory of all the packages and available filters

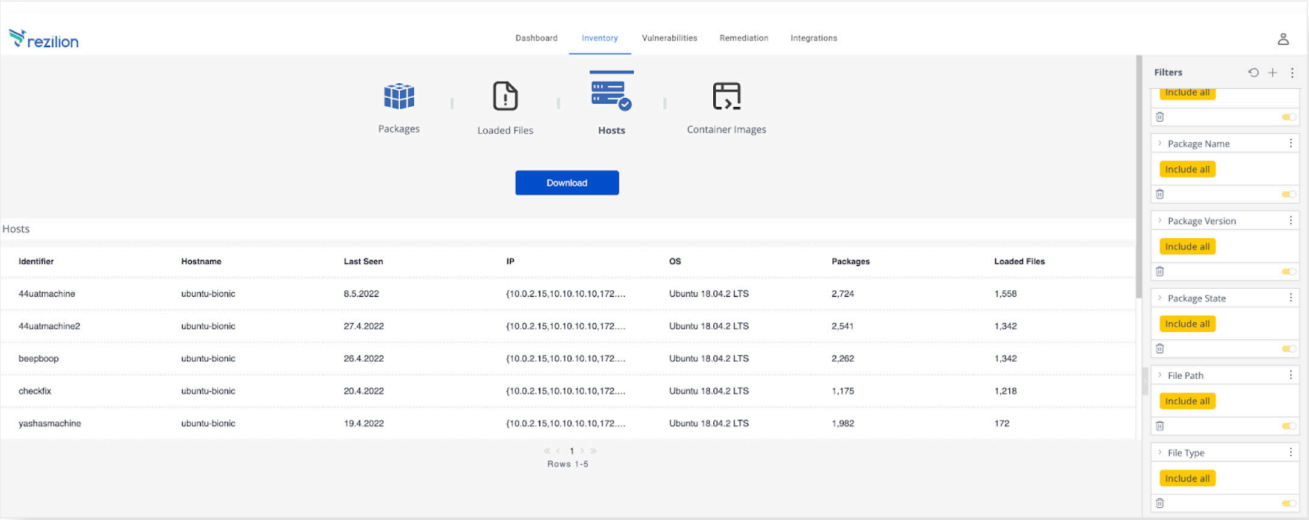

Fig 3: Inventory of hosts and associated packages and loaded files

Rezilion's Dynamic SBOM will be available in CycloneDX format and covers comprehensive details about the components and is continuously updated to reflect the real software bill of materials at all times.

Why Security Teams Need a Dynamic SBOM Now

With a growing software attack surface - developers and product security teams must ensure that the products are released quickly and also secured quickly. The need to reduce the time-to-fix window is underscored by the need to shorten the attack window. A Dynamic SBOM is one such tool that allows security teams to secure and release quickly. A few of the most important use cases are:

- **Understand Supply Chain Risk:** Quickly identify and search specific software components for vulnerabilities within your environment.
- **Understand Security Risk:** Immediately identify which components of your SBOM are exploitable and which are not using run time analysis.
- **Track Changes:** Get a real time and updated view of your software attack surface whenever there is any change.
- **Achieve Compliance:** Instantly create and share the inventory.documentation necessary to comply with government SBOM requirements including licensing obligations.
- **Search and Analyze:** Instantly search for vulnerable components and understand the impact of specific components or threats (like Log4j) and trigger Dev/Ops to fix them.

Rezilion's Dynamic SBOM is available now, free-of-charge for use, in CI environments such as Jenkins and Gitlab. For more information, visit **www.rezilion.com/platform/dynamic-sbom/** and to sign up for a free 30-day trial at **www.rezilion.com/sign-up-for-30day-free-trial/**.

About Rezilion

Rezilion is an automated software attack surface management platform that allows organizations to effortlessly reduce and mitigate software vulnerabilities from dev to prod and across cloud workloads, applications, and IoT devices. Rezilion eliminates more than 70% of the manual work security and engineering teams have to do, harmonizing previously oppositional efforts, and empowering organizations to innovate faster. With operations in Israel and the United States, Rezilion is swiftly attracting a growing client base of Fortune 100 companies and leading industry partners. For more information, visit **www.rezilion.com**.

Updated May 2022