Rezilion

Rezilion's Holistic Approach to Software Attack Surface Management

BAKSHEESH SINGH GHUMAN

The Modern Software Attack Surface

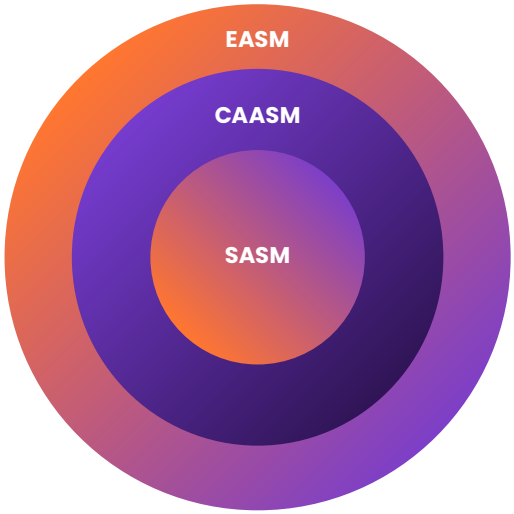
THE MODERN SOFTWARE ENTERPRISE has spawned the modern attack surface. It is constantly growing in size and type. From hosts, servers, cloud workloads, and mobile; to applications, development pipelines, and production environments encompassing files, libraries, code, operating systems, etc. there is no shortage of attack vectors. The modern attack surface is anything and everything that you are connected to, directly or indirectly. Along with the modern attack surface comes a range of benefits that include flexibility, efficiency, cost savings, and innovation. But these benefits also open the door to potential threats, weaknesses, and vulnerabilities.

WHAT IS AN ATTACK SURFACE AND SOFTWARE ATTACK SURFACE

The attack surface is the entire area of an organization or system that is susceptible to hacking (TechTarget). It can be divided into a few main sub-categories:

- **Network/External Attack Surface (EASM) —** includes all potential entry points available for an external attacker through enterprise networks.
- **Cyber-Assets Attack Surface (CAASM) —** this includes all the physical and virtual assets (servers, databases, devices, and cloud services) inside enterprise networks.

While these two categories have to do with physical assets, there is a third category of the attack surface which deals primarily with software.



- **Software Attack Surface (SASM) —** includes all software components that are deployed across cyber assets and could be exploited by an attacker. *Software attack surface includes the complete profile of all code running in a given system… The more surface there is, the better the chance an attacker or a piece of malware can use various exploits to gain access and run code on the target machine.* (TechTarget). Characteristics of the software attack surface include:
  - The software attack surface is the attack surface associated with all software components that are deployed across assets (servers, devices, cloud infrastructure, etc.) that could be exploited by an attacker.
  - The software attack surface includes proprietary code, third-party, and open-source code across all layers of the stack (OS, containers, hosts, container images, libraries, and applications) that make up the enterprise's Software Bill of Materials (SBOM).
  - A software attack surface does not include the configuration of cyber assets, cloud services, physical devices, or networks on which software is deployed.

Software Vulnerability Management Has A Lot of Ground to Cover

AS THE SOFTWARE ATTACK SURFACE GROWS, so does the potential for threat actors to exploit vulnerabilities. Particularly in the world of software, the attack surface encompasses code, binaries, operating systems, firmware, libraries, etc., which adds to the complexity and sheer volume of vulnerabilities. Enterprises do not have enough people or time to fix these vulnerabilities, leaving them in a fragile state, and open to being exploited.

As we have seen with the recent Log4j zero-day vulnerability, the connected and massive attack surface is collectively at risk. Traditional vulnerability management (VM) tools were not able to detect this zero-day vulnerability and it quickly took over the entire attack surface, putting thousands of enterprises and millions of devices at risk. Traditional VM tools need to evolve to account for the ever-changing attack surface. There are three key limitations of existing software vulnerability management tools that need to be addressed.

1. **Lack of dynamic and holistic visibility:** There is an old saying, you cannot protect what you cannot see. The dynamic nature of the modern software attack surface needs to be continually protected and you cannot do that unless you can see the changes in real-time. Traditional VM tools work on scheduled scans or compliance-based scans, rarely continuous. They provide an inventory of assets if they can find all of them, most often they don't. There are coverage gaps, insufficient data points, and to top it off — too many vulnerabilities. The Software Bill of Materials (SBOM) is emerging to be the de facto approach to software visibility. Current SBOMs are static, point-in-time lists that are not continually updated and are out of date as soon as there is a change in the environment, providing you with an incomplete view of your environment. The modern software attack surface is not static, so why should your discovery tool be static?

2. **Manual prioritization:** There are two major challenges with how traditional VM tools approach vulnerability prioritization. First, they are heavily focused on infrastructure vulnerabilities and not as much on software, and second, they lack the exploitability context of your environment. This leaves you, the user, with coverage gaps and the daunting task of figuring out what to fix first. Most organizations resort to manual approaches which are not practical or effective as there are too many vulnerabilities, too little time, and often, not enough people.

3. **Incomplete remediation:** Remediation is the holy grail of VM. What do you do when you know that you have vulnerabilities in your environment? Fix them. However, it is important to remember that remediation is not just patching. Traditional VM tools have some drawbacks.
   - They do not clearly specify what is the most optimal fix available, rather they focus on available patches, which may or may not be the best solution.
   - They are not automated.
   - They are not integrated into existing workflows allowing you to create, track, and resolve issues.

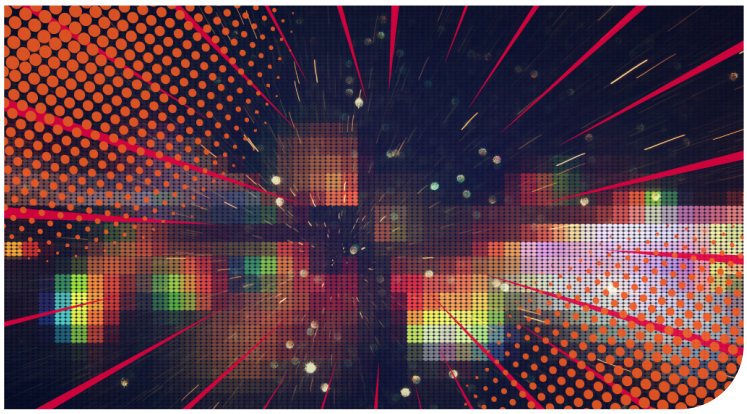
It is quite evident that the modern software attack surface needs a different approach to vulnerability management, one rooted in its expanding, dynamic, and complex nature.

Software Attack Surface Management Emerges as the Next-Generation Approach to Software Vulnerability Management

SOFTWARE ATTACK SURFACE MANAGEMENT (SASM) includes identifying, prioritizing, and mitigating all security risks and vulnerabilities associated with software components that could be exploited by an attacker across servers, devices, cloud infrastructure, operating systems, and applications.

Ideally, SASM solutions merge three capabilities traditionally delivered by multiple tools in order to provide a holistic way to identify, prioritize, and mitigate software vulnerabilities:

- ✓ **Dynamic SBOM —** SASM solutions identify and continuously maintain a comprehensive SBOM) which is continuous and updated in real-time. Dynamic SBOMs detail all software components that are deployed across infrastructure and applications and the vulnerabilities (CVEs) associated with them, and their exploitability.
- ✓ **Risk-Based Vulnerability Management (RBVM) —** SASM solutions help customers aggregate, prioritize, and navigate through the plethora of vulnerabilities in their SBOM, assessing their true risk with the goal of reducing long backlogs to a manageable size.
- ✓ **Mitigation Intelligence and Automation —** SASM solutions help customers remediate prioritized vulnerabilities by:
  - Automatically remediating vulnerabilities.
  - Providing intelligence on how to fix or contain these vulnerabilities with minimal impact on software functionality and operational risk.
  - Informing relevant stakeholders across engineering teams and automating the workflow of mitigating these vulnerabilities. SASM solutions do this by integrating tightly with developers and IT Service Management (ITSM) tools.



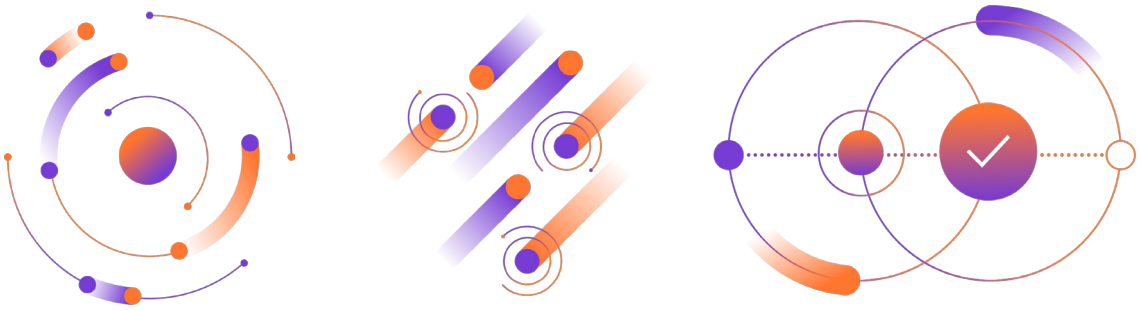
The Rezilion Approach to Software Attack Surface Management

REZILION HAS TAKEN AN APPROACH TO SOFTWARE ATTACK SURFACE MANAGEMENT that can be underscored by one adjective — automated. Our holistic approach aims to address coverage gaps by providing automated end-to-end visibility, an improved focus by providing insights on what vulnerability is the most exploitable, additional dynamic views so you are continuously on top of your risk, and the ability to automatically remediate to ensure security posture.

- **End-to-end visibility with Dynamic SBOM —** Rezilion's holistic platform gives you visibility into your entire Software Development Life Cycle (SDLC) from development to production, as well as the entire technology stack providing a comprehensive and continuous view of all the software components present in the software ecosystem via a *Dynamic SBOM*. Consequently, Rezilion is able to discover all vulnerabilities associated with each component, and group the components together by category, making it easier for security practitioners to focus on highly vulnerable components.
- **Vulnerability Prioritization with Granular Run-Time Context —** Just because vulnerabilities are present in your environment, it does not mean they are exploitable. Using Rezilion's Next-Generation Vulnerability Database (NGVDB) the Rezilion platform identifies the components that are loaded into memory down to function and class level, as well as all their nested dependencies so that you can determine your exposure. This is very important as it empowers you to:
  - Reduce your vulnerability backlog by up to 95%
  - Focus on components that are vulnerable in your environment
  - Prioritize remediation and mitigation for components that are exploitable and not just for every vulnerability
  - Save thousands of hours and dollars on patching
- **Automated remediation with workflow integration —** Rezilion's automated approach to remediation is underscored by the following features:
  - Easily integrates with your existing ITSM tools
  - Know the lowest-cost fix for each vulnerability
  - Understand operational risk before applying a patch with Rezilion's Next Generation Vulnerability Database (NGVDB).
  - Create smart remediation plans by instantly grouping thousands of vulnerabilities into a handful of low-impact software updates.
  - Automate the next remediation steps in CI and production to speed up remediation and save time.
  - Track your team's remediation efforts and SLAs to ensure that you are not out of compliance.
  - Automatically resolve issues that have been fixed
- **Security Policy Compliance —** Rezilion's platform makes sure that your development and production environments all *comply with the security posture and policies of your organization* at all stages of your SDLC. Additionally, the Rezilion platform also helps customers validate the security posture of software components (such as executable files and packages) that make their way into production, by using several criteria such as risk and provenance. These components only make it to production if they meet the predefined criteria. This end-to-end approach to security compliance provides two key benefits:
  - Minimizes the potential of vulnerabilities being exploited by adding an additional layer of security.
  - Automates the process of security compliance by smart gating between pipeline and production.

This dynamic, end-to-end, modern approach to software attack surface management enables Rezilion to cover the entire software ecosystem, making it easier for customers to have a unified view of their software attack surface and associated risk at all times.

Key Benefits of Using the Rezilion Approach



REZILION'S PLATFORM IS NOT A POINT-IN-TIME ASSESSMENT and analysis cybersecurity tool. It is a full-stack, full-cycle dynamic platform that continually scans your environment and provides you with an accurate and real-time view/assessment of your actual software attack surface and vulnerabilities and automatically takes the necessary steps to safeguard your security. By using a continuous approach, the Rezilion platform helps customers to stay on top of their security posture. Some key benefits include:

- **A unified view of your software environment** across the entire tech stack and DevOps lifecycle of all scans, software components, vulnerabilities, and supply chain security issues.
- **85% or more reduction in patching efforts** eliminating unexploitable vulnerabilities and fixing what matters most in your environment.
- **A Dynamic SBOM** that creates a dynamic inventory of all the software components, including open source components and their loaded/unloaded status for a quick risk view. Track in real-time where every piece of code came from, what its function is, what it depends on, and whether it's executing or not, eliminating any coverage gaps.
- **Know your true software attack surface** after filtering out unloaded software components, thus identifying components that are truly exploitable. This allows you to really understand all the controls and mitigation strategies you need to implement as well as decrease your scope for audits and be compliant.
- **Reduction of remediation timelines from months to hours** by focusing on only exploitable risks and greatly improving the efficiency and accuracy of security workflows.
- **Workflow integration with out-of-the-box integrations** can be deployed as part of your security workflow.
- **End-to-end vulnerability management** that not only shifts left but also right. Rezilion provides holistic vulnerability management through the entire SDLC from development to production.
- **Actionable insights** and easy-to-interpret metrics and reports that allow you to identify and analyze issues for appropriate remediation.

Log4j: A Case Study of Modern Software Attack Surface Management

THE FOLLOWING TABLE SUMMARIZES the differences between traditional approaches to software vulnerability management vs Rezilion's approach and how we can quickly help identify, prioritize, and remediate critical vulnerabilities like Log4j.

	SCA SCANNERS	INFRASTRUCTURE SCANNERS	REZILION
Discovers un-nested instances of Log4j	Yes	Yes	**Yes**
Discovers nested instances of Log4j	Yes	No	**Yes**
Provides end-to-end visibility (Dev and Production)	No	No	**Yes**
Determines if Log4j instances are actually exploitable	No	No	**Yes**
Provides real-time continuous updates	No	No	**Yes**
Discovers in seconds	No	No	**Yes**

For more information, visit www.rezilion.com/platform/dynamic-sbom/ and see it in action and book a demo at www.rezilion.com/request-a-demo/.

About Rezilion

Rezilion's platform automatically secures the software you deliver to customers. Rezilion's continuous runtime analysis detects vulnerable software components on any layer of the software stack and determines their exploitability, filtering out up to 95% of identified vulnerabilities. Rezilion then automatically mitigates exploitable vulnerabilities across the SDLC, reducing vulnerability backlogs and remediation timelines from months to hours, while giving DevOps teams time back to build.

Learn more about Rezilion's software attack surface management platform at https://www.rezilion.com/why-rezilion/ and get your 30-day free trial.