SOLUTION BRIEF

rezilion | aws

Rezilion for AWS

CHALLENGES: **Volume, Complexity and Speed Create Vulnerabilities**

As pressure rises for organizations to release products faster, cloud environments and DevOps cycles bring significant amounts of complexity and code to production workloads and applications, creating an increasing number of security issues and risks. For security teams, keeping up with this activity and technical debt is equally complex. Armed with traditional vulnerability management tools that detect and sort vulnerabilities according to their risk scores, Security teams apply manual workflows to validate and remediate detected risks, lengthening time-to-remediate and eroding trust between Security and DevOps teams. New strategies — and new tools — are required to more holistically manage risk across the entire attack surface and restore balance between all teams supporting the SDLC.

Rezilion + Amazon Inspector

Amazon Inspector is the premier security assessment tool for Amazon Web Services (AWS) environments. It is purpose-built to ensure users understand and uphold their end of the shared responsibility model for security in the cloud. Inspector is especially adept at identifying vulnerabilities in AWS environments. It continuously assesses Amazon Elastic Compute Cloud (Amazon EC2) instances and container images pushed to the Elastic Container Registry (ECR) for software vulnerabilities, providing automated recommendations for the most efficient paths to remediation based on aggregated and validated data to make informed decisions and take action faster. Rezilion's runtime visibility feature, which works in harmony with Amazon Inspector, helps to focus remediation efforts on exploitable vulnerabilities, helping teams to avoid patching vulnerabilities that manifest as false-positives when they are not loaded into memory and therefore pose no actual risk. By using Rezilion, customers can reduce their patching efforts by at least 70%, get a dynamic Software Bill of Materials (SBOM), measure their actual attack surface, and reduce remediation timelines from months to days without sacrificing security or productivity.

Proprietary Platform

Rezilion is powered by an automated analysis technology that reverse-engineers workloads and applications. It automatically creates an inventory of all artifacts and processes and maps dependencies, connections, code provenance, memory, and runtime execution flows in a dynamic SBOM. Rezilion then applies this SBOM to your scan results, providing a new dimension of understanding that helps teams identify exploitable vulnerabilities in code loaded to memory.

Benefits of Rezilion

As the pressure to accelerate time-to-market increases, security teams need solutions that help them release products without compromising speed and security. Rezilion and Inspector offer a unique value proposition: automated detection, prioritization and management of risk — to support a fast-moving product release environment with both precision and agility without sacrificing security.

Some of the many benefits of Rezilion include:

Vulnerability Validation

Decrease your vulnerability patching efforts by at least 70% by focusing on vulnerabilities that are loaded to memory. By focusing on only exploitable risks, teams can reduce the average time to remediate from months to days, greatly improving the efficiency and accuracy of security workflows.

Accurate Attack Surface

Get a view of your environment's actual attack surface after filtering out unloaded packages. This allows you to decrease your scope for audits and be compliant.

Package Level Patch Details

Eliminate the guesswork in patching with specific package-level detail, including nested Java Archives (JAR) within Java.

SBOM

Create a dynamic inventory of your environment, including OSS and other elements present in your software package. 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.

CASE STUDY: AppsFlyer

As pressure rises for organizations to release products faster, cloud environments and DevOps cycles bring significant amounts of complexity and code to production workloads and applications, creating an increasing number of security issues and risks. For security teams, keeping up with this activity and technical debt is equally complex. Armed with traditional vulnerability management tools that detect and sort vulnerabilities according to their risk scores, Security teams apply manual workflows to validate and remediate detected risks, lengthening time-to-remediate and eroding trust between Security and DevOps teams. New strategies — and new tools — are required to more holistically manage risk across the entire attack surface and restore balance between all teams supporting the SDLC.

Challenges

AppsFlyer is a cloud-native company that's embraced DevOps and regularly deploys to a containerized AWS environment. Their security tools and practices were very manual and couldn't keep pace with their deployments.

Solution

AppsFlyer implemented Rezilion to ease the security burden on engineering by allowing them to focus on a small subset of vulnerabilities that are loaded into memory and actually exploitable.

Results

Rezilion greatly cut down on false positives from other vulnerability sources and acted as a source of attestation that only some vulnerabilities are actually exploitable. As an added benefit, engineering could remove bloated code from their images.

Get Started with Rezilion Solutions on AWS

Visit us on AWS Marketplace or www.Rezilion.com/AWS-Microsite to request a demo or purchase today.

Last Updated: December 2021