Rezilion on AWS

Rezilion for AWS

Challenges
Speed and complexity create vulnerabilities

Cloud environments and DevOps bring significant amounts of complexity and code to production workloads and applications that creates security issues and vulnerabilities. This complexity combined with increased deployment velocity means that security teams are constantly trying to dig out of a mountain of vulnerabilities and tech debt. Traditional vulnerability prioritization isn't enough because it only reorganizes a list of thousands of vulnerabilities, it doesn't change the work required to decrease risk across the attack surface.

Rezilion Validate + Amazon Inspector

Amazon Inspector is the premier security assessment tool for AWS environments. It's 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 assess 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 Validate helps focus remediation efforts on exploitable vulnerabilities and helps avoid patching vulnerabilities that manifest as false-positives when they are not loaded into memory and therefore pose no actual risk.

Proprietary Unison Platform
Unison is an automated analysis 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 Software Bill of Materials (DBOM). Validate compares this DBOM to your scan results and reduces patching efforts by 70% by identifying exploitable vulnerabilities in code loaded to memory.

Benefits of Rezilion Validate

Security teams get a better understanding of their actual attack surface, waste less time patching vulnerabilities that don't pose risk, and buy time to patch production vulnerabilities. Having an accurate view of the attack surface also limits the scope for audits and allows you to focus on vulnerabilities that need to be patched in order to meet compliance requirements.

Vulnerability Validation
Decrease your vulnerability patching work by up to 70% by focusing on vulnerabilities loaded to memory.

Autonomous Mitigation
Automatically take action from alerting to safely redeploying an asset in the event of a breach. Demonstrate that mitigating controls in place are operating effectively to reduce risk.

Accurate Attack Surface
Get a view of the environment's actual attack surface after filtering out unloaded packages. Decrease your scope for audits.

Package Level Patch Details
Eliminate the guesswork in patching with specific package level detail including nested JARs in java.

Case Study: AppsFlyer

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 actually exploitable.

Results

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

Get started with Rezilion solutions on AWS

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