Rezilion Validate Datasheet

Security is a difficult balancing act in a DevOps environment, apply it too strictly and nothing gets released, too passively and risk quickly accumulates. This leads to constant back and forth between v and security - identifying vulnerabilities, prioritizing patches, and finally passing builds for production release. Worse yet, oftentimes vulnerabilities are flagged in components that will never be loaded to memory and therefore pose no risk.

Additionally, production environments are full of legacy code and backlogs of vulnerabilities that would take years to patch. Security and DevOps teams need an understanding of their actual attack surface consisting only of exploitable vulnerabilities.

Rezilion Validate allows Security teams to keep pace with DevOps and reduces work for both teams in the process. Traditional scanning solutions create work, Validate reduces it by allowing users to focus solely on exploitable vulnerabilities. Leveraging existing Security and DevOps tools and processes, Rezilion Validate eliminates the manual work required to protect applications from vulnerabilities and threats.

Key Benefits:

- **Patch Up to 70% Less**
  Save countless hours and dollars by focusing time and resources on vulnerabilities that actually pose a risk.
- **Release Faster**
  Help DevOps maintain release velocity with less false positives and failed builds by automating vulnerability analysis and triage
- **Improve Relationships Between Security and DevOps**
  Unplanned work and false positives strain relationships, Validate eliminates both and brings teams together.
- **Remove Code Bloat**
  Unloaded packages can be removed from images for more maintainable code. This also allows you to harden images for security and compliance requirements.
- **Single Pane of Glass**
  Aggregate scan data from any type or number of scanning tools to accurately report on the effectiveness of your vulnerability management program.
- **Measure the Actual Attack Surface**
  Focus your efforts on exploitable vulnerabilities and avoid patching false-positives that are not loaded into memory and therefore pose no risk.

Key Features:

- **Patent Pending Unison Analysis Technology**
  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.

- **Full Stack Visibility**
  Validate aggregates scan data from any type or number of scanning tools to accurately report on the effectiveness of your vulnerability management program. Vulnerabilities in the application, container, and the infrastructure layers are displayed in a single pane of glass view that can be customized based on the user's needs.

- **Package Level Remediation Information**
  DevOps practitioners don't speak in CVEs and Validate doesn't require them to. Validate captures package level information and ranks them in order of risk so teams understand the assets that are impacted by each unique vulnerability to manage with both telescopic vision and microscopic precision.

- **Recommended Remediation Actions**
  Validate provides automated recommendations for the most efficient paths to remediation based on aggregated and validated data, to make informed decisions and take action faster

- **Flexible Deployment in as Little as 15 Minutes**
  Validate can be deployed in CI, Staging, or Production environments in a variety of architectures including on-premise, hybrid, cloud, containers, and kubernetes. Deployment options include a CI plugin, sidecar container, YAML, or a continuously running script.

- **Seamless Integration with Existing Scanning Technologies**
  Validate is not a scanner but it's also not meant to disrupt existing workflows or displace existing technology. Highly extensible APIs allow Validate to integrate with any of the leading SCA, and infrastructure scanning tools. Alternatively, Validate can be packaged with an open source scanning solution in environments that don't currently have tools in place.