RAPIDFORT

Optimize & Secure Your Cloud

Introduction

Modern cloud workloads include a large number of unused or seldom used components. These components are present either because they might be needed in an emergency or because engineers aren't sure if they are needed or not. Attackers frequently use these same components to help them "live off the land" and avoid detection once they have compromised a system or, in some cases, facilitate an initial compromise.

Many organizations have implemented patching policies and scanning tools to detect these potentially vulnerable components and ensure they are patched, but software patching remains one of the most time consuming and potentially dangerous activities in most organizations. Ensuring software components are truly unused and removing them, a process also known as software attack surface management, takes valuable developer time away from building the next new product and focuses it on maintaining existing products.

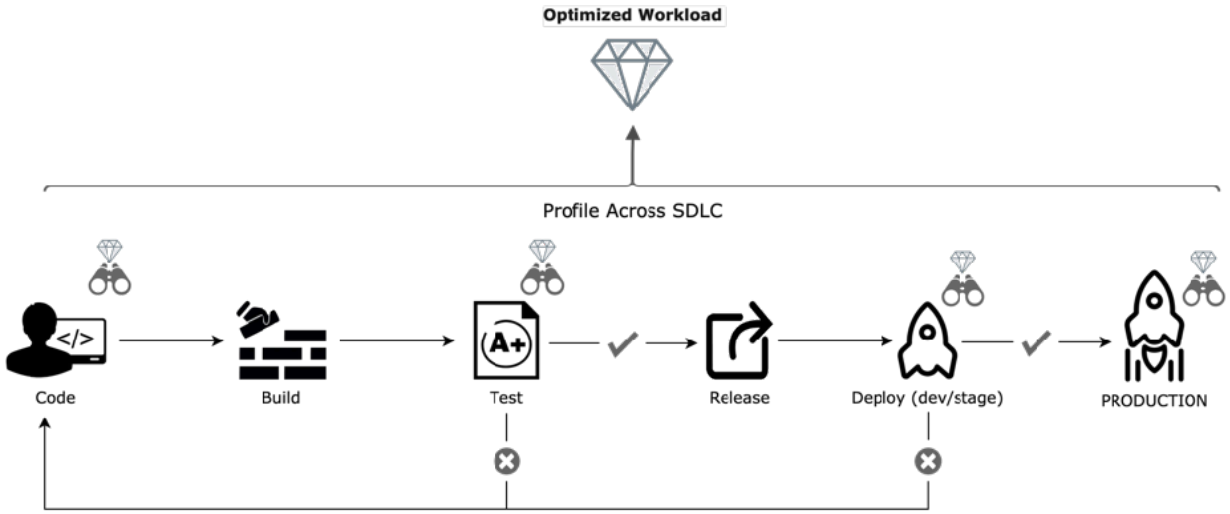
Software attack surface is the sum of all software opportunities that unauthorized parties can exploit to access a system. Reducing your software attack surface is an essential security measure. The larger the software attack surface, the larger the number of known and unknown vulnerabilities. Unknown vulnerabilities are the source of zero-day attacks. The most crucial — and perhaps the only — measure that an organization can take to reduce their exposure to zero-day attacks is to reduce their software attack surface. While there are well-established practices for reducing network attack surface, there has not been as much progress in managing and optimizing your software attack surface.

RAPIDFORT solves this problem by providing organizations with a platform to continuously monitor and minimize their software attack surface.

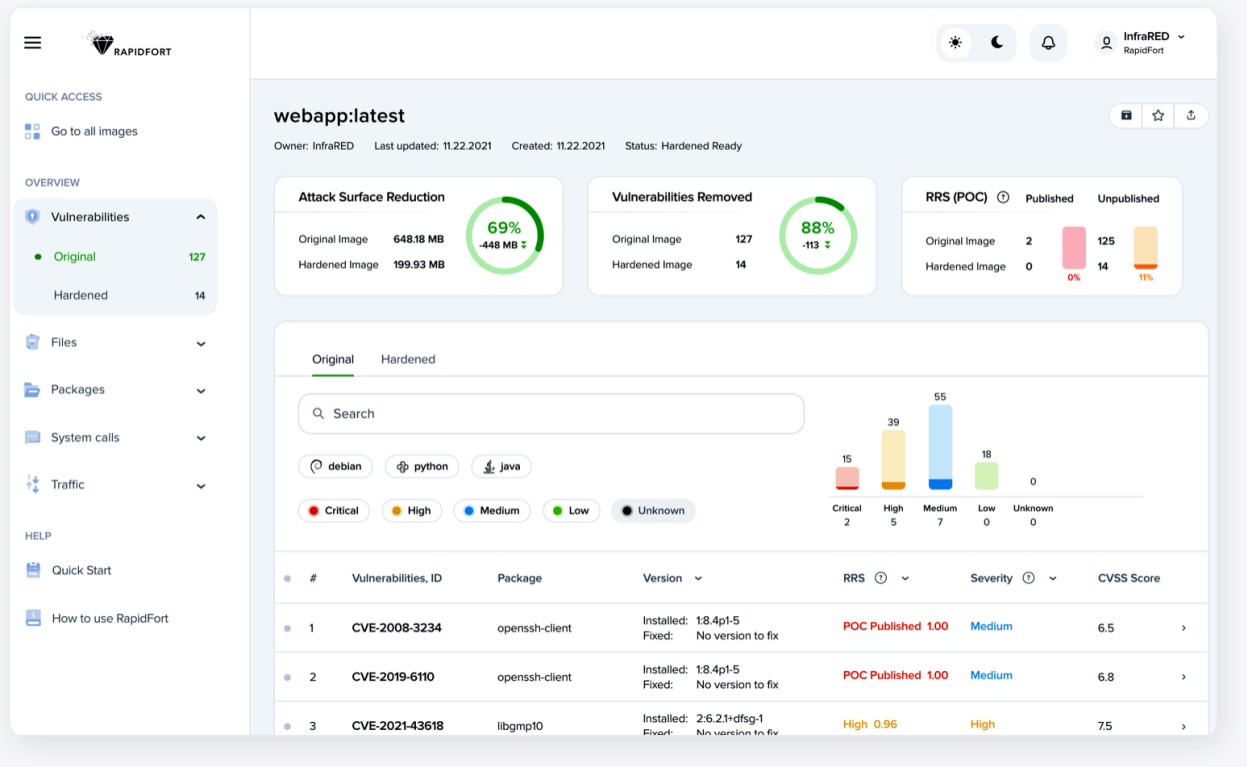
What Does RAPIDFORT Do?

RAPIDFORT is the first software attack surface optimization platform. To effectively manage software attack surfaces, one must first deeply understand that software. RAPIDFORT helps teams develop a deep understanding of the behavior of their workloads at the deepest level while they run in their "natural" runtime environments.

RAPIDFORT collects behavioral information at all points of the SDLC: During development, unit tests, integration tests, manual QA tests, staging, and production. It correlates and merges that information across all instances, runs, and builds of a workload. As a result, it creates a complete and accurate picture of what a workload needs to function and how it interacts with other components. It uses simple and intuitive workflows that are easy to integrate into the existing build and release tools.



This information is presented via a UI and an API, providing deep insights and tools to act upon them:



Reducing Vulnerability & Patch Management Backlog With RAPIDFORT

An immediate benefit of RAPIDFORT's solution is that, even before the workload arrives for production deployment, there is a clear understanding of which packages and vulnerabilities are in use by the workload, reducing vulnerability remediation and patch management backlog by 50%-90%.

Without any change to your production software, RAPIDFORT identifies the unused packages and their associated vulnerabilities and presents them for easy integration to your upstream and downstream processes.

Optimizing and Hardening Your Workloads

However, unused software components left in the workload still present a significant risk as attackers can use them for lateral movement or privilege escalation within your infrastructure. The best practice is to remove or disable them altogether.

RAPIDFORT provides a complete set of tools to help your organization achieve a fully automated process to remove unused components. Every workload can be automatically optimized and hardened, improving your processes and tooling incrementally to achieve a fully optimized build/release cycle.

RAPIDFORT can produce a repackaged, hardened version of the application upon request or based on a policy at any given point in the process. This action can be repeated as many times as desired and can include profile information from different versions of a container from previous builds using RAPIDFORT's workload tags.

In some environments, there can be many instances of a workload running simultaneously (as in a Kubernetes deployment, for example), and it can run multiple times across any number of invocations. RAPIDFORT supports all deployment environments including managed services such as AWS Fargate and Amazon EKS.

Improving Your Test Coverage

RAPIDFORT provides tools to "snapshot" the application's profile at various stages in the SDLC, allowing a comparison of its behavior as it moves through its lifecycle. This yields insights into what testing coverage might be missing from automated versus manual tests or production versus previous steps.

Engineering and QA teams can quickly identify test coverage gaps and improve test suites and enhance coverage for future releases.

How Does RAPIDFORT Work?

Below are the high-level steps in a RAPIDFORT workflow. For simplicity, we discuss a containerized application here:

1. Instrument the application - referred to as stub in RAPIDFORT.
2. Run the instrumented application instead of the original application through test, QA, release cycles. You can optionally run the application in production as well for any length of time to get exposure to production traffic.
3. Get a report of components actively being used at any stage.
4. Create a hardened version of the application at any point or multiple points in the process.

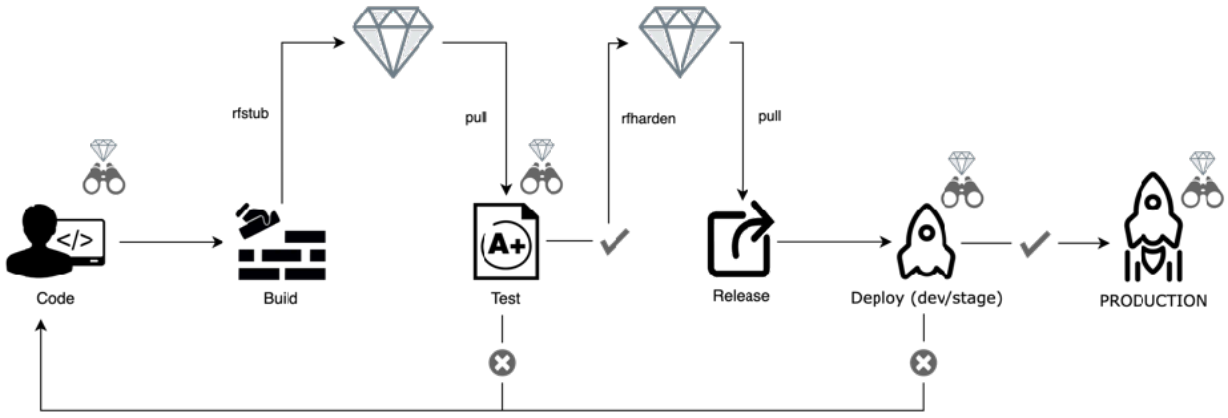
Once an application is built, RAPIDFORT instruments it. Instrumentation captures all activities of an application and its processes "*completely*" and "*efficiently*":

- Completely: There are no activities that are untracked by RAPIDFORT's instrumentation modules.

- Efficiently: The overhead of instrumentation is negligible. Currently, the overhead is ~10%-20% in CPU usage, although the clock-time overhead can be a lot more. Before the end of this year, RAPIDFORT's new instrumentation methods target CPU overhead of < 1% with no noticeable overhead on clock-time.

When the container image is ready, it is delivered to the RAPIDFORT system via a simple CLI command or automatically by the RAPIDFORT ***runner*** service, which continuously pulls images from a registry or upon invocation.

RAPIDFORT analyzes the application for structure, instruments the image using proprietary techniques, scans it for packages, looks up all the known vulnerabilities for the discovered packages, and produces a Software Bill of Materials (SBOM) and a vulnerability report as well as a repackaged instrumented container, referred to as a stub container. In the case of a runner, the instrumented container's image is automatically pushed back to the registry.



The instrumented container is deployed for testing, verification, staging, or production in any way the original container would be. While the container is running, RAPIDFORT collects profile information about the application.

The diagram above demonstrates one such hardening scenario, where RAPIDFORT generates a hardened image after all tests are done. Note that hardening can be performed at any point and multiple times.

Starting and Scaling With RAPIDFORT

Organizations use RAPIDFORT to automate their workload optimization processes, remediate vulnerabilities efficiently, reduce their patch management overhead significantly, reduce their attack risk exposure, and minimize their attack surface continuously. One of our customers refers to RAPIDFORT as "*a diet pill for your infrastructure*": Smaller, safer, faster, cheaper workloads delivered automatically and continuously.

RAPIDFORT provides immediate benefits when your first workload is instrumented. It then provides your infrastructure and development teams with the tools to gradually achieve The Holy Grail: Fully Automated Workload Optimization On Every Single Build.

It's easy to start with RAPIDFORT and see for yourself. Sign up and use our free scanning tool to scan your containerized and VM workloads, and use the free tier offering to harden your containerized applications. It's easy; it's magical! Visit us at www.rapidfort.com, and let us help you run free and stay secure.

RAPIDFORT

Optimize & Secure Your Cloud