RAPIDFORT

DISA

RapidFort Capabilities Overview DISA

12 Dec 2023

📝 Provocative Ask

RapidFort can solve the majority of DISA's SBOM and Software Supply Chain challenges by being seamlessly inserted in every single DISA cloud based system.

How do we get the opportunity to prove we can perform as advertised?

How do we get connected to a resource that can lay out a plan for our engagement?

Presentation Agenda: Solving the DoD's Software Supply Risk Compliance Challenges

- RapidFort Introduction
- Introducing Software Supply Chain Risk
- DISAs need for enhanced software supply chain tooling
- Increasing compliance, security, and espionage software supply chain attacks
- Toolset to meet Evolving SBOM Needs
- How RapidFort Works: Reducing the Amount of Software to Defend
- A Comprehensive Software Supply Chain Platform: Build-Time and Run-Time SBOM Scanning & Profiling
- Demo
- Seeking Next Steps: How can we engage with DISA and validate
- Plenty of time for Q&A

RapidFort should be installed in every DISA cloud because it provides game changing foundational risk reduction capabilities typically by as much as 80%

RapidFort Overview

- Founded late 2020, team of 37
- $8.5M Seed (March 2022), backed by Felicis, Forgepoint, Bloomberg Beta and cloud-native / cybersecurity pioneers
- Deep technology, defensible platform, technical leadership
- Solid traction within the DoD moving into regulated industries
- Formal enterprise product launch in Sept

Felicis

FORGEPOINT

Bloomberg BETA

AFWERX

AFWERX PRIME

📝 Defining Software Supply Chain Risk

"Security issues introduced by the third-party components and technologies used to write, build, and distribute software*" *(Linux Foundation Definition)*

"Systemic risk that arises from using software components or applications not developed internally." *(RapidFort definition)*

* From Linux Foundation Course, "Securing Your Software Supply Chain with Sigstore," LFS182x.

Overview: The New Need for Improved Software Supply Chain Risk Tooling

- Historically, defense and aerospace industries used relatively simple software frameworks focussed on **HERITAGE SOFTWARE** (proven/had considerable flight time). Memory safe/secure/not networked but had limited capabilities.
- It was **CLOSED SOURCE**.
- Legacy software is **NOT SOPHISTICATED** enough to provide the advanced capabilities for complex DoD missions.
- **ADVANCED MISSION** capabilities, require **ADVANCED SOFTWARE**. The DoD is embracing “cloud native technologies” using new frameworks, software containers, and kubernetes.
- **NEXT GENERATION SOFTWARE PERFORMS BETTER**: improved capabilities, performance advantages, cheaper, faster to develop, easier to maintain, easier to future proof, and has performance and feature benefits.
- However, this software is bloated and has considerable open source components so is **NOT INNATELY SECURE** so must be secured and rapidly ATO’d.
- RapidFort has developed **GAME CHANGING TOOLING** to secure this next generation software providing security, developer, ATO speed, and cost advantages.

📝 The Source of Software Supply Chain Risk: Complexity!

- Compounded Risks: 20 components 2% of breach in next year, 98% "safe" BUT! = 33% chance of breach this year. (1-0.98^20)
- Only as strong as the weakest link: 20 component system: 19 100% safe, 1 30% = 30% (Think of Uber and # of employees, only takes one failure to result in a breach)
- Component Chains are growing longer: attack surface is increasing (Working from Home, devices, open source, SAAS, IAAS and PAAS, third-party APIs, CSPs etc etc etc etc.).
- This is challenging because with OpenSource we don't own the doors
- Maybe we should remove the doors altogether!

"It's often not our software, there is a lot of it, it's risky, we are not sure where the risks are, and we rely on third parties to remediate said risks"

Software Supply Chain Management Today Is Messy

MEDIUM ENTERPRISE

1-3M

Vulnerabilities

LARGE ENTERPRISE

10-20M

Vulnerabilities

SMALL ENTERPRISE

50-200K

Vulnerabilities

Expensive, Wasteful, Small Sent in Risk, Suboptimal

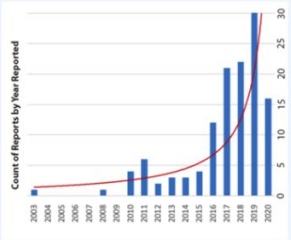
DISA's Need for Improved Software Supply Chain CyberSecurity

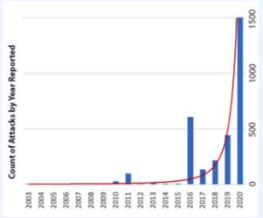
- Software Supply Chain Risk refers to the risk from using these next generation software frameworks.
- Software Supply Chain Risk is gaining attention because of compliance and security concerns:
  - **COMPLIANCE** regulation is growing meaning USSF must ensure this software meets new cybersecurity policy and requirements so it can be ATO'd
  - **SECURITY** risks are increasing because the volume, frequency and intensity of attacks is exploding
  - **ESPIONAGE** Risks are growing especially with encrypted harvesting techniques that quantum technologies can potentially break
- The DoD must secure all their next gen software so that:
  - They can support their new mission capabilities
  - They are compliant with new regulation & policy
  - They can get ATOs for the systems rapidly
  - They are secure from foreign threat-actors

SBOM Drivers: Compliance and Risk

- Compliance Need: Numerous regulation need to start generating SBOMs
- 

NIST, NSA, CISA, NTIA …
- Security Need: Software supply chain attacks growing bu ~650% YoY





Geer et al, "Counting Broken Links," *USENIX ;login:*, 2020

DoD Software MUST to be Secured Against National State Threat Actors

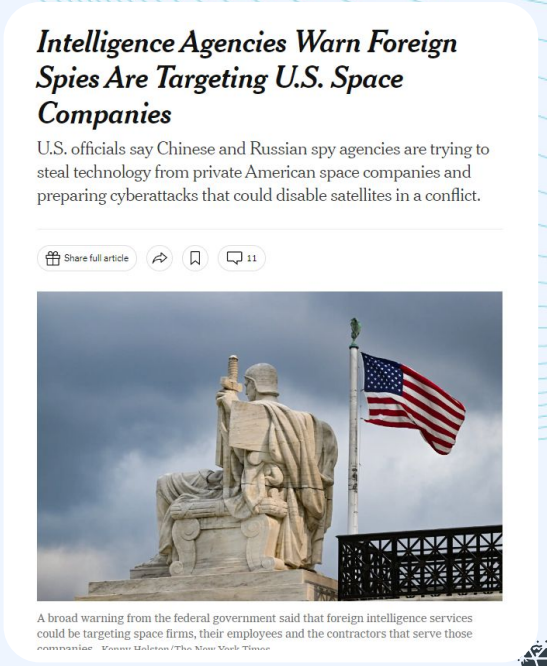
***Dec 8 2023:** "A top White House national security official said recent cyber attacks by Iranian hackers on U.S. water authorities — as well as a separate spate of ransomware attacks on the healthcare industry — should be seen as a call to action by utilities and industry to tighten cybersecurity."*

- Cybersecurity attacks creates asymmetrical opportunities to attack without retalitorory risk
- Typically not attributable
- Potentially extensively damaging in nature … literally turn off the lights
- Inexpensive to produce and weaponize … excellent ROI
- Not geographically bounded
- Limited repercussions
- Extremely leveraged, one breach can render an entire ecosystem: Solarwinds had 37 DIB companies effected

DoD Software MUST to be Secured Against Chinese Espionage Attacks NOW

Friday: 18 August 2023: ***"Chinese and Russian intelligence agencies are targeting American private space companies, attempting to steal critical technologies and preparing cyber attacks aimed at degrading U.S. satellite capabilities during a conflict or emergency, according to a new warning by American intelligence agencies." USAF, USSF, FBI, National Counterintelligence and Security Center***

- China poses a significant national security threat because of vast numerical and manufacturing advantages (China graduates 30x more engineers than we do)
- A wave of Chinese cyber espionage attacks appears to be be underway stealing IP and discovering vulnerabilities that can be exploited in the future
- There is considerable evidence that China has breached a large number of DoD networks as recently as 30 August.
- One of the most effective ways to secure cloud technology it so reduce the software attack surface one has to defend
- RapidFort has developed an automated toolset to harden space software:
    - By improving the ability to detect vulnerabilities through advanced scanning
    - By reducing the amount of software to defend through software attack surface reduction
- This will free up security teams to focus on other types of espionage and security threats



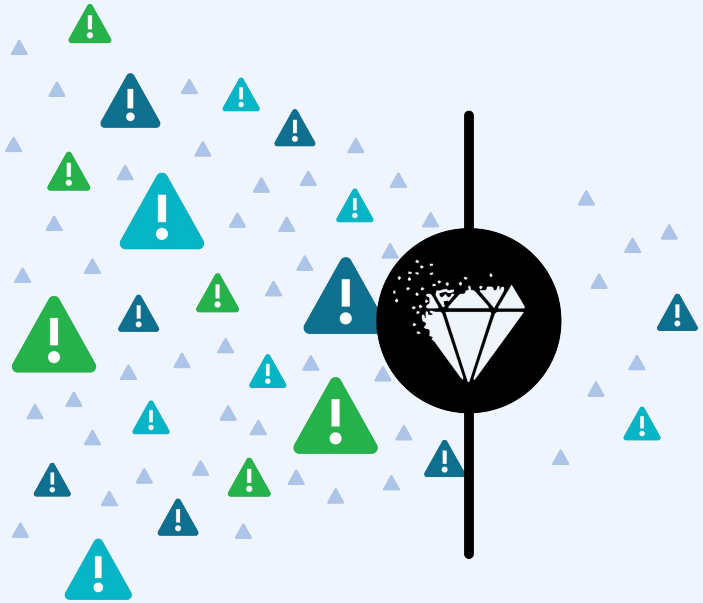
Intelligence Agencies Warn Foreign Spies Are Targeting U.S. Space Companies

U.S. officials say Chinese and Russian spy agencies are trying to steal technology from private American space companies and preparing cyberattacks that could disable satellites in a conflict.

Share full article 11

A broad warning from the federal government said that foreign intelligence services could be targeting space firms, their employees and the contractors that serve those companies. Kenny Holston/The New York Times

Key Insight: When modern software is built it becomes “bloated”: 50-90% of software in modern workloads **is not used** in production

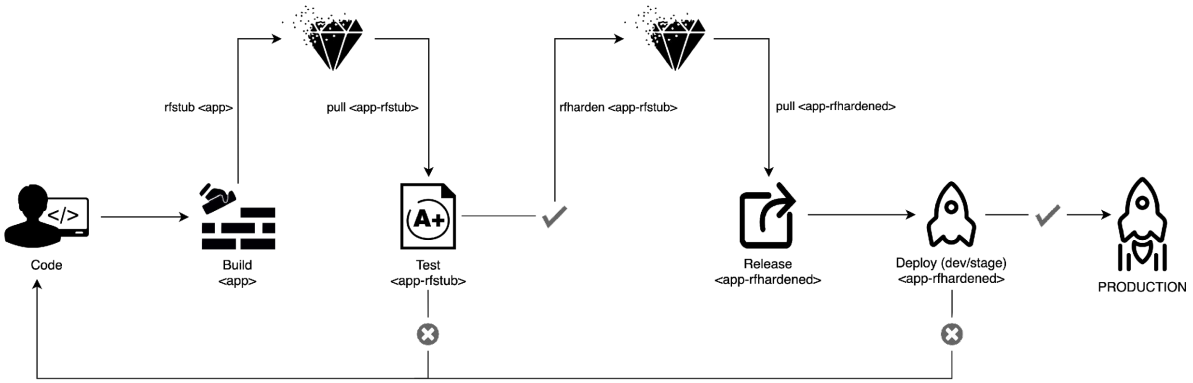


RapidFort finds and secures them **Automatically reducing the software attack surface**

How RapidFort Works: We “learn” what your software is doing by instrumenting it and remove the unused components or put alerts on the unused components

- ✓ First Software Attack Surface Management Platform
- ✓ Revolutionary Instrumentation Technologies
- ✓ Scan
- ✓ Estimate
- ✓ Profile
- ✓ Optimize
- ✓ Monitor

Reduce Your Software Weight By 80% - Automatically

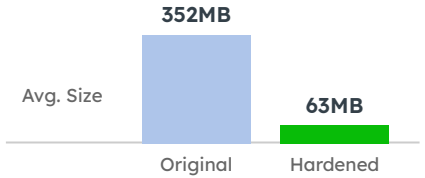


U.S. AIR FORCE

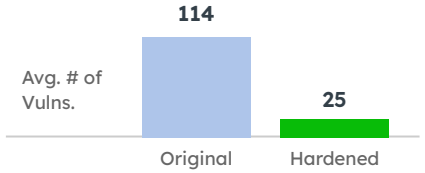
Competitive Advantage: It works!

Department of Defense Case Study

Avg. Workload Size Reduction ▼82%



Avg. Vulnerabilities Reduction ▼78%

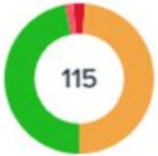


Standard NGINX Container

- Critical 15
- High 28
- Medium 14
- Low 113
- Unknown 0

Total Vulnerabilities

USAF NGINX Container



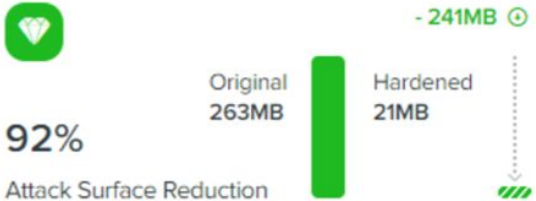
- Critical 3
- High 2
- Medium 56
- Low 54
- Unknown 0

Total Vulnerabilities

RAPIDFORT Hardened Container

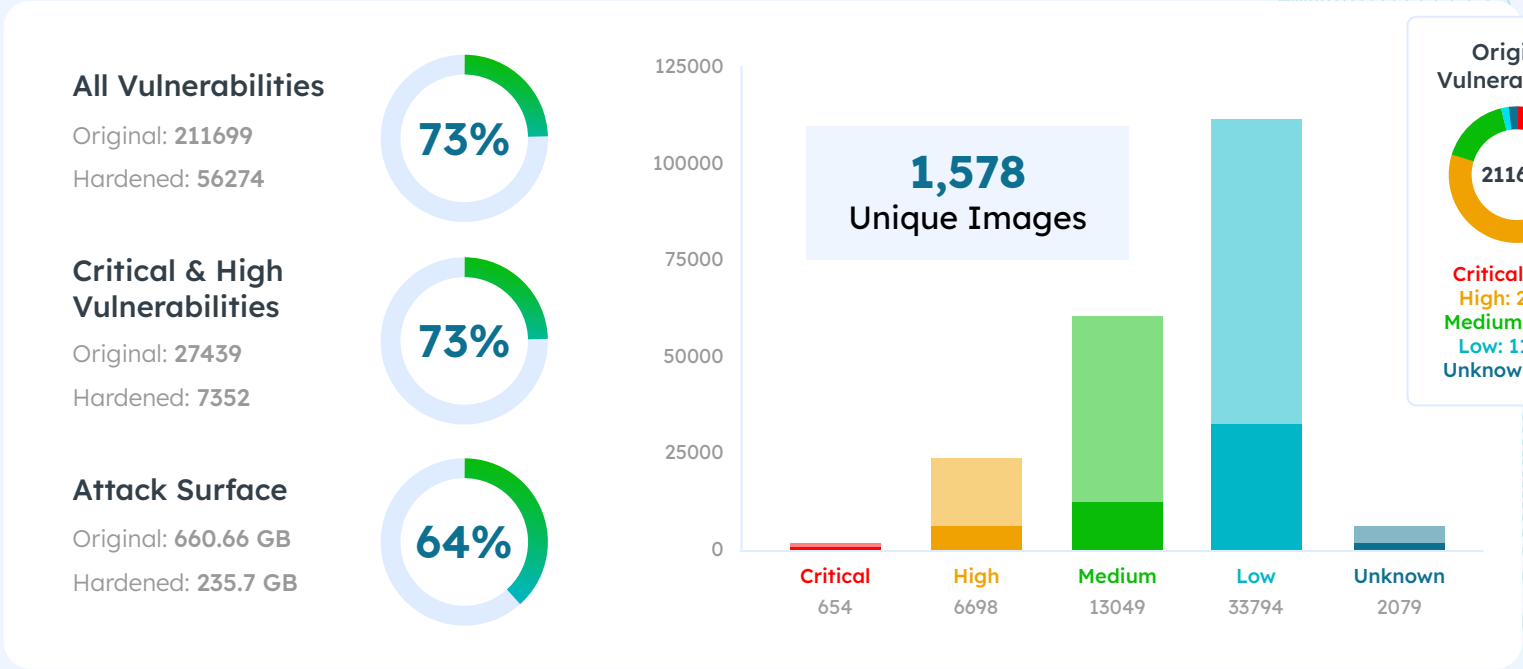
- Critical 1
- High 0
- Medium 7
- Low 9
- Unknown 0

Total Vulnerabilities



Impact Study on a Larger Set of Images

In a study of 1,578 unique images, RapidFort automatically removed 73% of total vulnerabilities, 73% of criticals and highs, and reduced the overall software attack surface by 64%, resulting in automatic hardening of 155,400 vulnerabilities and 425GB of software!



Solution: Software Attack Surface Management

RapidFort has developed a comprehensive Software Attack Surface Management (SASM) platform automating vulnerability detection and remediation. This section summarizes the platform and the interoperability of the toolsets used by security and development teams.

Run-time Toolset (Security)

1 Scan & Observe

Scan your infrastructure (Registries, Kubernetes, VMs)

Generate SBOMs

Create accurate vulnerability reports

Measure risk with Rapid Risk Scores ML model

Opportunity-to-improve metrics with reduction estimates statistical model

2 Profile & Understand

Understand your software attack surface

Generate RBOMs (Real BOMs)

Prioritize vulnerability remediation

Obtain full list of unused packages for discussion with engineering

3 Harden & Secure

Minimize your software attack surface

Reduce your workload size

Improve your security posture

Manage 80% less software: Less risk, vulnerabilities, patches, alerts

Build-time Toolset (Devs)

RapidFort Community Containers: It is working for 3.5M+ downloads

ENTERPRISE:

What containers are supported?

We've optimized and hardened some of the most popular container images on Docker Hub and are making them available to the community.

Repository	View Report	RapidFort Image	Pull Count
MariaDB	Get full report	View on DockerHub	219,347
PostgreSQL Official	Get full report	View on DockerHub	122,961
PostgreSQL	Get full report	View on DockerHub	117,320
Redis™ Cluster	Get full report	View on DockerHub	101,967
MySQL	Get full report	View on DockerHub	90,087
NGINX IronBank	Get full report	View on DockerHub	88,565
Redis™ IronBank	Get full report	View on DockerHub	87,228
PostgreSQL IronBank	Get full report	View on DockerHub	86,995
Redis™	Get full report	View on DockerHub	86,723
MongoDB®	Get full report	View on DockerHub	79,564
Consul IronBank	Get full report	View on DockerHub	76,466
MongoDB® IronBank	Get full report	View on DockerHub	74,447
MySQL IronBank	Get full report	View on DockerHub	70,772
MariaDB IronBank	Get full report	View on DockerHub	70,674
NGINX	Get full report	View on DockerHub	69,186
Grafana Oncall	Get full report	View on DockerHub	68,337
Envoy	Get full report	View on DockerHub	61,445
Zookeeper IronBank	Get full report	View on DockerHub	57,452
Etcd	Get full report	View on DockerHub	54,868
Fluentd	Get full report	View on DockerHub	50,458

DOD:

What IronBank containers are supported?

We've optimized and hardened some of the most popular container images on IronBank and are making them available to the community.

Repository	View Report	RapidFort Image	Pull Count
NGINX IronBank	Get full report	View on DockerHub	88,565
Redis™ IronBank	Get full report	View on DockerHub	87,228
PostgreSQL IronBank	Get full report	View on DockerHub	86,995
Consul IronBank	Get full report	View on DockerHub	76,466
MongoDB® IronBank	Get full report	View on DockerHub	74,447
MySQL IronBank	Get full report	View on DockerHub	70,772
MariaDB IronBank	Get full report	View on DockerHub	70,674
Zookeeper IronBank	Get full report	View on DockerHub	57,452
HAProxy IronBank	Get full report	View on DockerHub	36,128
Memcached IronBank	Get full report	View on DockerHub	35,735
Apache IronBank	Get full report	View on DockerHub	34,078
Fluentd IronBank	Get full report	View on DockerHub	27,978
Couchdb Database Server IronBank	Get full report	View on DockerHub	25,660
Microsoft SQL Server 2019	Get full report	View on DockerHub	20,987

https://github.com/rapidfort/community-images

📝 The Most Comprehensive SBOM Tooling Suite At Your Disposal

- **SBOM Build Time Scanning Suite:** can be run from CLI using API call Supporting 11 Programming Languages and all major Linux Variants (doesn't support windows, binary scans) (needs to be modified to direct output to local machine) Has licensing support.
- **Kubernetes Run-Time SBOM Scanner:** provides SBOMs from a Kubernetes Clusters with a one-line code instal. (need to ensure supports K8s variant supported)
- **SBOM Warehouse "Light:"** A repository to warehouse SBOMs … doesn't contain RBAC but will by the time the SBIR starts it will
- **SBOM Quality Tool:** to ensure that SBOMs are well formed and meets NTIA conformance requirements.
- **SBOM Comparison Tool:** to Compare Different SBOMs and identify drift, use of un-authorized components
- **SBOM Translation Tool:** to ingest, translate, and publish SBOMs to and from common SBOM formats (SPDX to CycloneDX) needs to be expanded to ingest SBOMs into RapidFort platform
- **SBOM Estimation Tool:** that estimates how much bloat can be removed from a container.
- **RBOM (Real Bill of Materials) Tool:** to generate an SBOM that shows which components are actually used, reducing vulnerability backlog by 80%
- **SBOM Optimization Tool:** to remove unused components from SBOMs and automatically rebuilds software containers with only the components required to run.
- **AI Prediction Module** that shows if POC is available and predicts if an SBOM will have a published exploit in the wild within the next 90 days.
- **Patching Module** to identify available patches that have not been applied to an SBOM. Used to enforce patching SLAs/ priorities patching.

Seeing is believing: RapidFort is seeking opportunities to validate its technology

Within a few hours an Ironbank certified version of RapidFort will validate:

- Increased developer velocity by ~8% to ~12%
- Reduced vulnerabilities by as much as ~80%
- Reduced patching backlogs by 90%
- Reduced the sizes of container images by 75%
- Improved load times by 300%
- While using less memory and bandwidth
- And increasing the range of technologies available to expand mission capabilities

Seeing is Believing … allow us to prove it!


A
DEMO
100
50
0
D-C90
2

Q&A
Thank You