RAPIDFORT

DAFITC 2023
Event 185

Developing Automated DevSecOps Vulnerability Remediation Tooling for USAF/USSF Software Factories using USAF PlatformOne Ironbank

29 August 2023

Overview

- The True Source of Software Supply Chain Risk: Complexity
- RapidFort's Approach to Reducing SSCR by Removing the Source: Too much software
- Collaboration with the DoD:
    - Pre-Hardened Ironbank Containers
    - Build-Time Tools Available at Ironbank
    - Run-Time Tools Available at Ironbank potentially
- Meaningful Collaboration Discussions
- Brief Solution Demo

"How do we meaningfully engage and measure our success by # of production vulnerabilities removed?"

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.

The Source of Software Supply Chain Risk: Complexity!

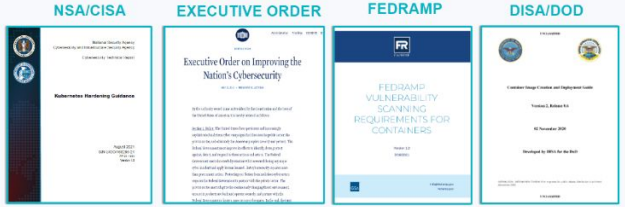
- Compounded Risks: 20 components 2% of breach in next year, 98% "safe" BUT! = 33% chance of breach this year. (1-0.98^20)
- Only as strong as the weakest link: 20 component system: 19 100% safe, 1 30% = 30% (Think of Uber and # of employees, only takes one failure to result in a breach)
- Component 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 Open-Source we don't own the doors
- Our approach is to reduce the number of vulnerability doors by removing them completely.

"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"

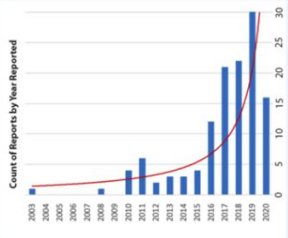
Our Need for Improved SSCR

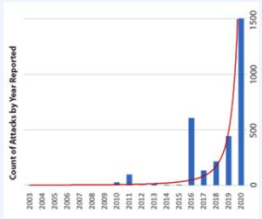
- Software Supply Chain Risk is gaining attention because of compliance and security concerns:
  - COMPLIANCE regulation is growing meaning DoD developers must ensure this software meets new cybersecurity policy and requirements so it can be ATO'd
  - SECURITY risks are increasing because the volume, frequency and intensity of attacks is exploding
- DoD must secure all their next gen software so that:
  - We can support our new mission capabilities
  - We are compliant with new regulation & policy
  - We can get ATOs for the systems rapidly
  - We are secure from foreign threat-actors

SBOM Drivers: Compliance and Risk

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

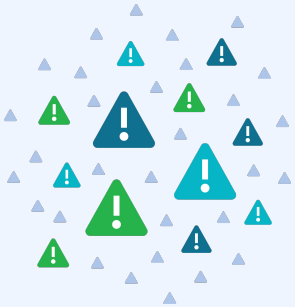
NIST, NSA, CISA, NTIA …
- Security Need: Software supply chain attacks growing bu ~650% YoY





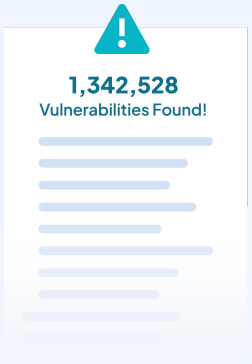
Geer et al, "Counting Broken Links," *USENIX ;login:*, 2020

Current solutions make a small dent in the problem



Millions of vulnerabilities

Vulnerabilities are scanned

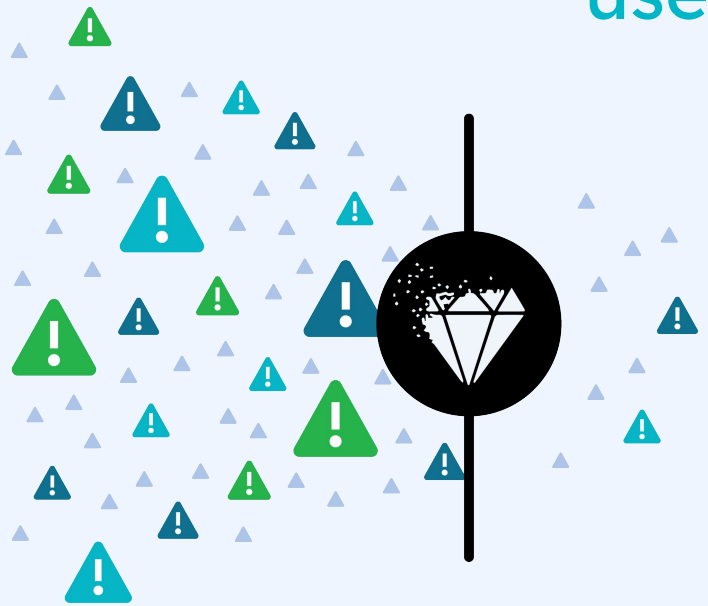


Left with extensive lists and alerts

Game of whack-a-mole

Key Insight

50-90% of software in modern workloads is not used in production

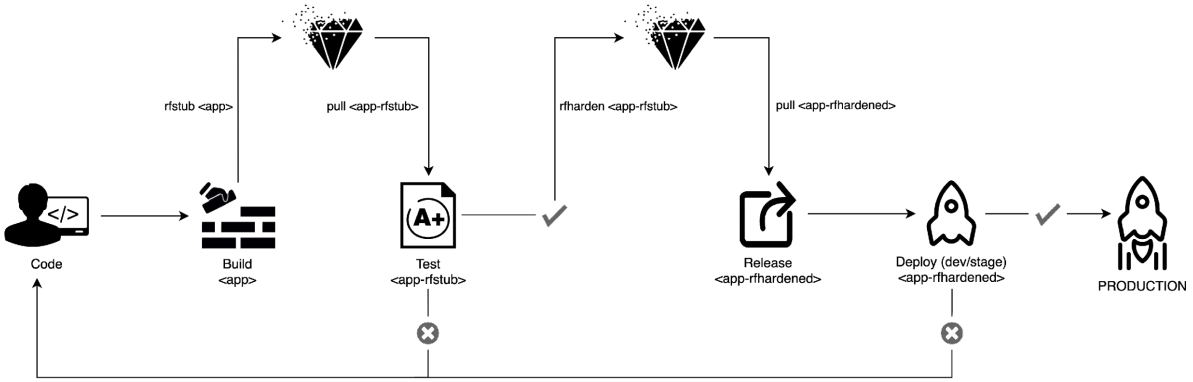


RapidFort finds and secures them **Automatically, reducing the Software Attack Surface**

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



Software Attack Surface Management Platform

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

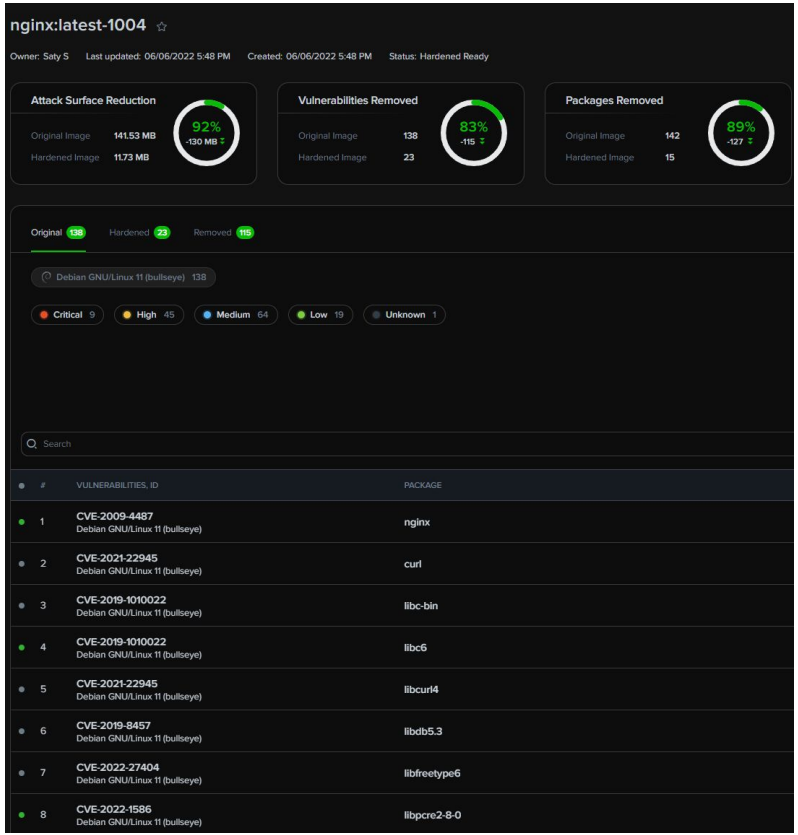
Improve your security posture

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

Build-time Toolset (Devs)

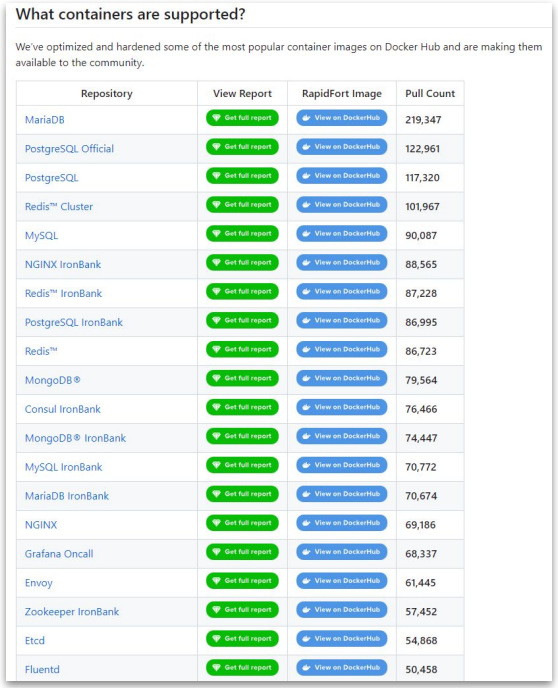
A Comprehensive Software Supply Chain Platform for the DoD

- **OPEN SOURCE COMMUNITY REPOSITORY:**
  - 70 commercial images / 20 DoD images
- **COMPLIANCE TOOLSET: FINDING VULNERABILITIES**
  - Build Time CLI SCA Scanner
  - Registry SCA Scanner
  - Run-time SCA Scanner
  - SBOM Warehouse* FA864923P0564
  - STIG Scanner* FA864923P0565
- **SECURITY TOOLSET: REMOVING VULNERABILITIES**
  - Run-time profiling for security teams
  - Build-time profiling for engineering teams
  - Run-time vulnerability prioritization
  - Run-time Build Manifests
  - Automated Hardening: “Animal hardening”



Technical Validation from Community Containers: 2.5M+ downloads

ENTERPRISE: 2M+ downloads

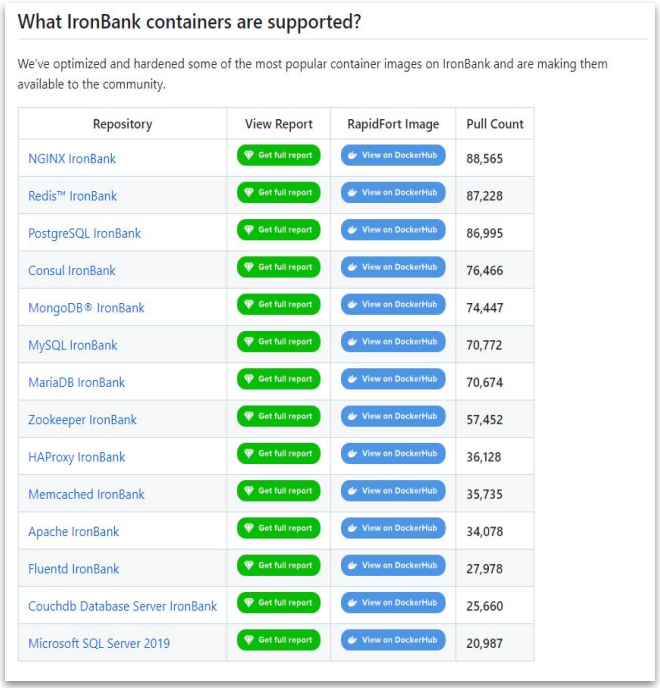


What containers are supported?

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: 500K downloads



What IronBank containers are supported?

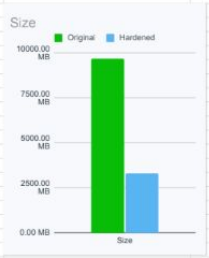
We've optimized and hardened some of the most popular container images on IronBank and are making them available to the community.

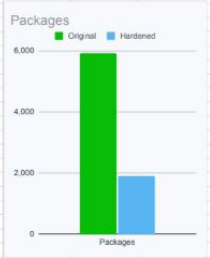
Repository	View Report	RapidFort Image	Pull Count
NGINX IronBank	Get full report	View on DockerHub	88,565
Redis™ IronBank	Get full report	View on DockerHub	87,228
PostgreSQL IronBank	Get full report	View on DockerHub	86,995
Consul IronBank	Get full report	View on DockerHub	76,466
MongoDB® IronBank	Get 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

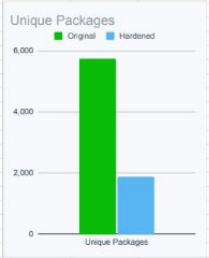
https://github.com/rapidfort/community-images

Results from Ironbank Container Study: Encouraging Results

Total # of Containers	20			
General Totals	**Original**	**Hardened**	**Delta**	**Average**
Size	9688.95 MB	3301.47 MB	-65.93%	-73.36%
Packages	5,921	1,903	-67.86%	-71.24%
Unique Packages	5,736	1,887	-67.10%	-70.73%





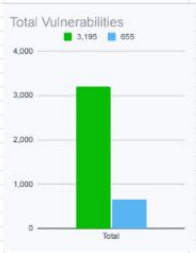


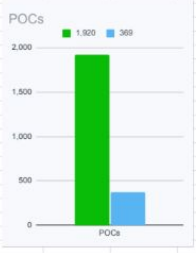
	Size			Packages			Unique Packages		
Image	**Original**	**Hardened**	**Delta**	**Original**	**Hardened**	**Delta**	**Original**	**Hardened**	**Delta**
NGINX IronBank	261.10 MB	20.35 MB	-92.21%	219	27	-87.67%	214	27	-87.38%
Redis™ IronBank	294.18 MB	42.48 MB	-85.56%	221	21	-90.50%	217	21	-90.32%
PostgreSQL IronBank	370.70 MB	88.68 MB	-76.08%	273	50	-81.68%	268	35	-86.94%
MariaDB IronBank	797.25 MB	92.36 MB	-88.42%	298	49	-83.56%	292	49	-83.22%
MySQL IronBank	724.40 MB	144.31 MB	-80.08%	277	34	-87.73%	271	34	-87.45%
Consul IronBank	374.14 MB	139.52 MB	-62.71%	380	193	-49.21%	376	193	-48.67%
Zookeeper IronBank	521.58 MB	218.00 MB	-58.20%	278	59	-78.78%	274	58	-78.83%
MongoDB® IronBank	860.75 MB	557.75 MB	-35.20%	382	185	-51.57%	257	66	-74.32%
HAProxy IronBank	259.63 MB	33.52 MB	-87.09%	221	21	-90.50%	217	21	-90.32%
Memcached IronBank	257.71 MB	15.66 MB	-93.92%	224	23	-89.73%	220	23	-89.55%
Apache IronBank	225.12 MB	26.09 MB	-88.41%	171	43	-74.85%	170	42	-75.29%
CouchDB IronBank	222.52 MB	29.09 MB	-86.93%	178	62	-65.17%	478	62	-87.03%
Fluentd IronBank	403.89 MB	51.56 MB	-87.23%	321	74	-76.95%	312	73	-76.60%
Microsoft SQL Server 2019	1649.20 MB	1169.86 MB	-29.07%	261	43	-83.52%	167	29	-82.63%
NATS-server Ironbank	29.42 MB	14.36 MB	-51.19%	26	13	-50.00%	26	13	-50.00%
Traefik Ironbank	378.78 MB	146.67 MB	-61.28%	511	306	-40.12%	507	302	-40.43%
Prometheus Ironbank	472.85 MB	131.24 MB	-72.25%	538	186	-65.43%	384	332	-13.54%
Wordpress Ironbank	651.51 MB	181.08 MB	-72.21%	284	61	-78.52%	280	60	-78.57%
Etcd IronBank	279.56 MB	50.86 MB	-81.81%	333	132	-60.36%	286	131	-54.20%
Grafana Ironbank	654.63 MB	148.03 MB	-77.39%	525	321	-38.86%	520	316	-39.23%

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

Results from Ironbank Container Study: Reducing Criticals and Highs

Vulnerability Severities	Original	Hardened	Delta	Average
Critical	76	11	-85.53%	-84.54%
High	281	71	-74.73%	-75.30%
Medium	1,868	339	-81.85%	-83.61%
Low	859	200	-76.72%	-72.72%
Unkown	111	34	-69.37%	-70.98%
POCs	1,920	369	-80.78%	-76.77%
Critical and High	357	82	-77.03%	-79.04%
Total	3,195	655	-79.50%	-76.28%
Density	159.75	32.75	-79.50%	

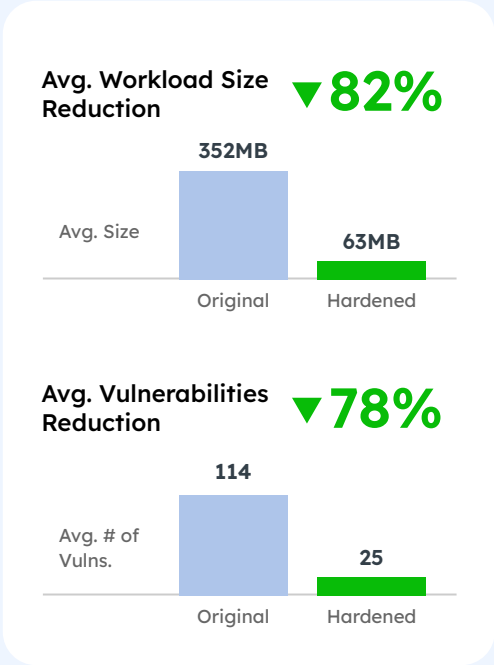


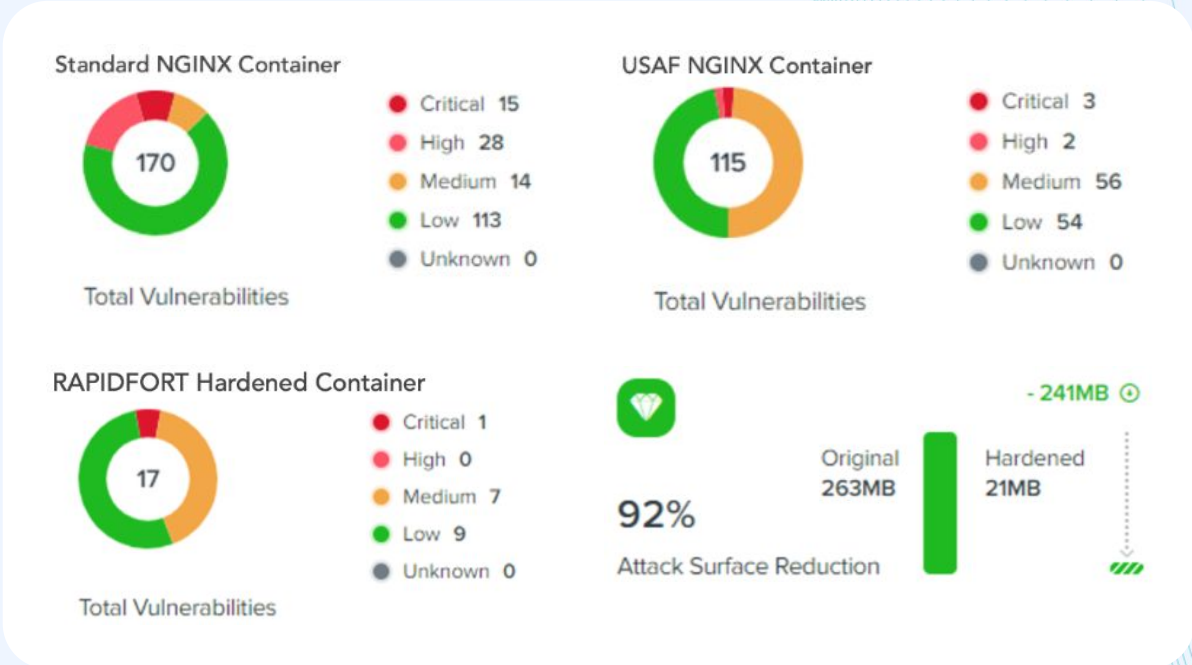


	Critical			High			Medium			Low		
Image	Original	Hardened	Delta	Original	Hardened	Delta	Original	Hardened	Delta	Original	Hardened	Delta
NGINX IronBank	0	0		6	3	-50.00%	68	8	-88.24%	29	6	-79.31%
Redis™ IronBank	4	0	-100.00%	8	0	-100.00%	85	10	-88.24%	33	7	-78.79%
PostgreSQL IronBank	4	1	-75.00%	8	1	-87.50%	96	24	-75.00%	39	15	-61.54%
MariaDB IronBank	8	2	-75.00%	46	10	-78.26%	235	47	-80.00%	99	19	-80.81%
MySQL IronBank	4	0	-100.00%	8	0	-100.00%	95	15	-84.21%	38	15	-60.53%
Consul IronBank	4	0	-100.00%	21	13	-38.10%	96	25	-73.96%	41	13	-68.29%
Zookeeper IronBank	4	0	-100.00%	8	0	-100.00%	89	9	-89.89%	38	4	-89.47%
MongoDB® IronBank	4	1	-75.00%	19	9	-52.63%	91	19	-79.12%	41	12	-70.73%
HAProxy IronBank	4	0	-100.00%	8	0	-100.00%	85	8	-90.59%	33	9	-72.73%
Memcached IronBank	4	0	-100.00%	8	0	-100.00%	86	8	-90.70%	36	6	-83.33%
Apache IronBank	0	0		6	1	-83.33%	56	10	-82.14%	26	7	-73.08%
CouchDB IronBank	3	0	-100.00%	27	3	-88.89%	9	0	-100.00%	90	20	-77.78%
Fluentd IronBank	4	0	-100.00%	9	1	-88.89%	85	10	-88.24%	33	7	-78.79%
Microsoft SQL Server 2019	6	2	-66.67%	35	6	-82.86%	178	25	-85.96%	94	13	-86.17%
NATS-server Ironbank	2	2	0.00%	5	5	0.00%	0	0		2	2	0.00%
Traefik Ironbank	4	0	-100.00%	14	6	-57.14%	93	14	-84.95%	34	4	-88.24%
Prometheus Ironbank	4	0	-100.00%	10	1	-90.00%	87	10	-88.51%	33	4	-87.88%
Wordpress Ironbank	4	2	-50.00%	12	7	-41.67%	132	48	-63.64%	50	26	-48.00%
Etcd IronBank	4	0	-100.00%	8	0	-100.00%	85	9	-89.41%	33	4	-87.88%
Grafana Ironbank	5	1	-80.00%	15	5	-66.67%	117	40	-65.81%	37	7	-81.08%

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

Build Time Profiling: SpaceCamp Case Study





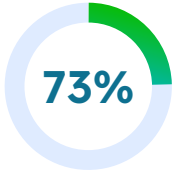
Impact Study: Large Set of Enterprise Images

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!

All Vulnerabilities

Original: **211699**

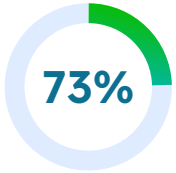
Hardened: **56274**



Critical & High Vulnerabilities

Original: **27439**

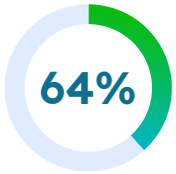
Hardened: **7352**

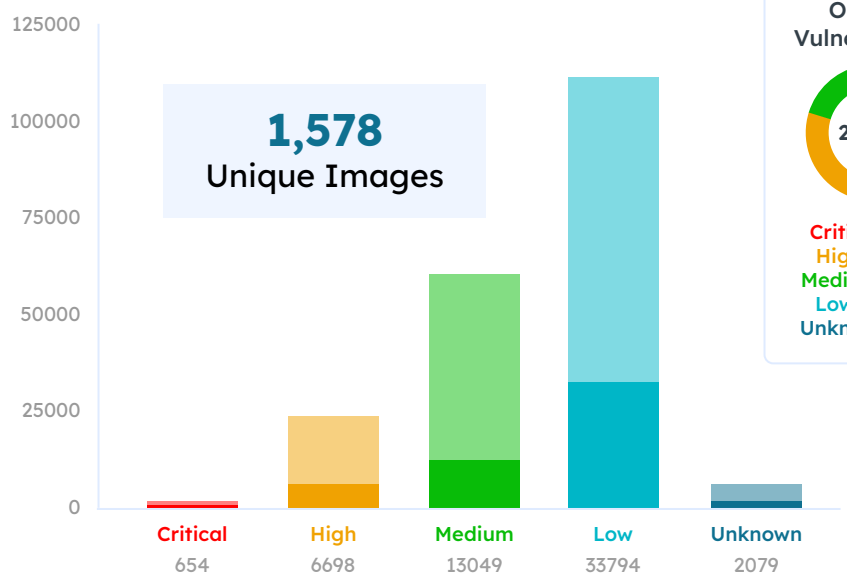


Attack Surface

Original: **660.66 GB**

Hardened: **235.7 GB**





Original Vulnerabilities

Critical: 2430
High: 25009
Medium: 62294
Low: 115425
Unknown: 6541

Seeing is believing: RapidFort is seeking opportunities to genuinely collaborate with DoD Users

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

There is potentially a matching funds opportunity.

Please schedule a presentation by emailing Russ@rapidfort.com to confirm that the technology works as advertised.


A
DEMO
100
50
0
D-C90
2

Harden & Secure Your Cloud

Thank you!