Vulnerability Comparison Report

A comprehensive analysis comparing vulnerabilities in your container images versus Chainguard's hardened alternatives.

Executive Summary

Security Vulnerability Assessment for Sample-Customer

This comprehensive vulnerability assessment demonstrates the challenges that Sample-Customer face in managing CVE's at scale. Sample-Customer is not alone in this challenge as many in the industry are grappling with CVE spawl & controls around OSS. This report shows the significant security advantages of migrating from standard container images to **Chainguard's hardened alternatives**. Analysis of 3 container image pairs reveals a **99.7% overall CVE reduction**, eliminating 1058 vulnerabilities across your infrastructure.

Key Findings

- **Significant Vulnerability Reduction**: 3 of 3 images show measurable improvement with Chainguard alternatives
- **Average Per-Image Improvement**: 98.4% average CVE reduction per improved image
- **Total Impact**: 1061 vulnerabilities in current images reduced to 3 with Chainguard
- **Reduced Attack Surface**: Distroless and minimal base images eliminate unnecessary components
- **Faster Remediation**: Streamlined images enable quicker security updates and patches

Business Impact

Overall Business Value A direct cost savings can be calculated as follows. 1-4hrs to resolve a CVE when you consider the research, business process/approvals and actual engineering effort. The equates to a cost of over **$2.7m** based on average wage/engineering effort metrics.

- **Enhanced Security Posture**: 99.7% reduction translates to significantly lower risk of a breach
- **Compliance Readiness**: Fewer vulnerabilities mean easier security compliance achievement
- **Operational Efficiency**: 1058 fewer CVEs to track, patch, and manage
- **Developer Productivity**: Less time addressing security issues, more time on shipping value to the business

Recommendation

With demonstrated **99.7% CVE reduction** across 3 analyzed images, we strongly recommend transitioning to Chainguard images as part of your DevSecOps strategy to mature security practices and reduce operational toil across platform, security, and development teams.

CVE Reduction Analysis

99.7%

CVE REDUCTION

1058 fewer vulnerabilities with Chainguard images

Your Images

1061

TOTAL VULNERABILITIES

SEVERITY	COUNT
🟪 Critical	**15**
🟥 High	**96**
🟧 Medium	**159**
🟨 Low	**93**
⬜ Negligible	**698**
□ Unknown	**0**

Chainguard Images

3

TOTAL VULNERABILITIES

SEVERITY	COUNT
🟪 Critical	**0**
🟥 High	**1**
🟧 Medium	**0**
🟨 Low	**2**
⬜ Negligible	**0**
□ Unknown	**0**

Images Scanned

Vulnerability Severity Legend

C Critical H High M Medium L Low N Negligible U Unknown CLEAN No Vulnerabilities

YOUR IMAGE	TOTAL VULNERABILITIES	CHAINGUARD IMAGE (CGR.DEV)	TOTAL VULNERABILITIES
nginx:latest	3 17 28 9 90	nginx:latest	CLEAN
alpine/java:21	2 12 20 9	jdk:openjdk-21	2
python:latest	10 67 111 75 608	python:latest	1

* Images marked with an asterisk were retried with the :latest tag after initial scan failure.

Appendix

Sample-Customer Specific Logic/Assumptions

- Sample-Customer provided 3 images
- If the upstream software was EOL we mapped to :latest in Chainguard image
- Grype is leveraged as the scanner tool to scan both the Sample-Customer provided image as well as the Chainguard image
- If a scan with grype failed on any image, it attempted a tag for re-scanning which is represented with a *
- If the above logic fails, the entire row will fail and is not included in the report. This is to ensure 1:1 comparison. Eg: some Customer images are behind a paywall or simply not available in the public registry
- CVE cost figure based on: Average 1hr to resolve a single CVE (including business process). An engineer wage of $75 per hour multiplied by # of CVE's

Methodology

This report was generated using the following methodology:

- **Scanning Tool:** Grype vulnerability scanner
- **Data Sources:** National Vulnerability Database (NVD) and other security databases
- **Image Analysis:** Container images were scanned for known vulnerabilities
- **Comparison:** Customer images compared against Chainguard hardened alternatives

Appendix (continued)

Severity Levels

Vulnerabilities are classified using the following severity levels:

- **Critical:** Vulnerabilities with CVSS scores of 9.0-10.0
- **High:** Vulnerabilities with CVSS scores of 7.0-8.9
- **Medium:** Vulnerabilities with CVSS scores of 4.0-6.9
- **Low:** Vulnerabilities with CVSS scores of 0.1-3.9
- **Negligible:** Vulnerabilities with minimal impact
- **Unknown:** Vulnerabilities without assigned severity scores

About Chainguard Images

Chainguard Images are container images built with security-first principles:

- **Minimal Base:** Built on minimal base images to reduce attack surface
- **Distroless:** Contains only application dependencies, no package managers
- **Regular Updates:** Continuously updated with latest security patches
- **Zero CVEs:** Many images maintain zero known vulnerabilities
- **SBOM Included:** Software Bill of Materials for transparency
- **Provenance Tracking:** Complete software supply chain transparency with cryptographic attestations and verifiable build processes

This report is Sample-Customer & Chainguard Confidential | Generated on 2025-08-04 08:51:05