

SECURE YOUR SOFTWARE SUPPLY CHAIN

ACHIEVE LOW TO ZERO CVEs WITH BELLSOFT HARDENED IMAGES

Two-thirds of organizations experienced a container security incident in the past year. **The average container carries 600+ known vulnerabilities.** BellSoft Hardened Images provide a clean, secure foundation — secure by design and backed by real engineering expertise.

ALMOST ZERO CVEs. SLA FOR CVE REMEDIATION. TECHNICAL SUPPORT.

OPENJDK IMAGE VS. BELLSOFT HARDENED LIBERICA RUNTIME

Metrics	OpenJDK Image	BellSoft Hardened Image
Total Vulnerabilities	44	0
Critical/High CVEs	1	0
Image Size	196.59 MB	77.59 MB
CVE Remediation	–	SLA-backed
Support	NO	Yes

Scans performed on Oct 27, 2025. eclipse-temurin:17 (Grype) vs bellsoft/hardened-liberica-runtime-container:jdk-17-glibc (OSV Scanner).

BASED ON A SECURITY-FIRST FOUNDATION

BellSoft Hardened Images are based on **Alpaquita Linux**, a lightweight, open-source distribution optimized for containers. You get enterprise-grade hardening, minimal attack surface, and **end-to-end support** — all from one vendor.



Mimimized and Secure by Design

- Images with no package managers and immutable component set
- Non-essential components removed to shrink attack surface
- Continuous CVE monitoring and proactive patching
- SBOM and OSV schema reporting for easy audits



Flexible and Compatible

- **glibc** and **musl** variants for any environment
- Support for x86_64 and ARM64 (AArch64)
- Prebuilt for **OpenJDK, Python, Go, C/C++, GraalVM**
- Up to **30% lower RAM and disk use** for Java workloads

MORE THAN HARDENING. TRUE ENTERPRISE PROTECTION.

Most hardened images stop at CVE management. BellSoft delivers **security + expertise + accountability**:

ONE VENDOR, ONE SLA

- BellSoft covers everything — OS, runtime, and container security:
- Guaranteed CVE remediation SLA (7 days for critical, 14 days for others)
 - Technical support for production issues
 - One contact point, no vendor hand-offs

DEEP EXPERTISE — NOT JUST PATCHING

While others wait for upstream fixes, BellSoft engineers — members of the OpenJDK Vulnerability Group — can develop and deliver patches in-house, keeping your workloads secure and running.

FLEXIBLE PRICING — FROM COMMUNITY TO ENTERPRISE

COMMUNITY	STANDARD	PREMIUM
Free	Ask for a price	Ask for a price
Free access to selected hardened images, SBOMs, and full architecture support	7-day SLA for critical CVEs, FIPS-ready compliance, business-hours support	Technical support, runtime & OS issue resolution, dedicated engineer

WHY CHOOSE BELLSOFT

<h3>Security-First Open Source</h3> <p>Built on Alpaquita Linux for a transparent, auditable foundation — no vendor lock-in.</p>	<h3>Sustainable Operations</h3> <p>Single SLA, continuous remediation, and simplified compliance to keep you production-ready.</p>
<h3>Expert Engineering Support</h3> <p>Direct help from the team behind OpenJDK and Linux experts — not just ticket routing.</p>	<h3>Optimization for Java Workloads</h3> <p>From OS to JVM, every layer is tuned for performance and resource efficiency.</p>

WANT TO FIND OUT MORE? | CONTACT US!

📍 111 North Market Street, Suite 300, San Jose, CA 95113

📞 +1 (702) 2135959

✉ info@bell-sw.com

Linux is a registered trademark of Linus Torvalds. Java, JavaFX, Java Swing are the registered trademarks of Oracle Corporation. Spring is a registered trademark of VMware. Windows, macOS, JetBrains, VMware, and other marks are the property of their respective owners.

bell-sw.com

