Chainguard

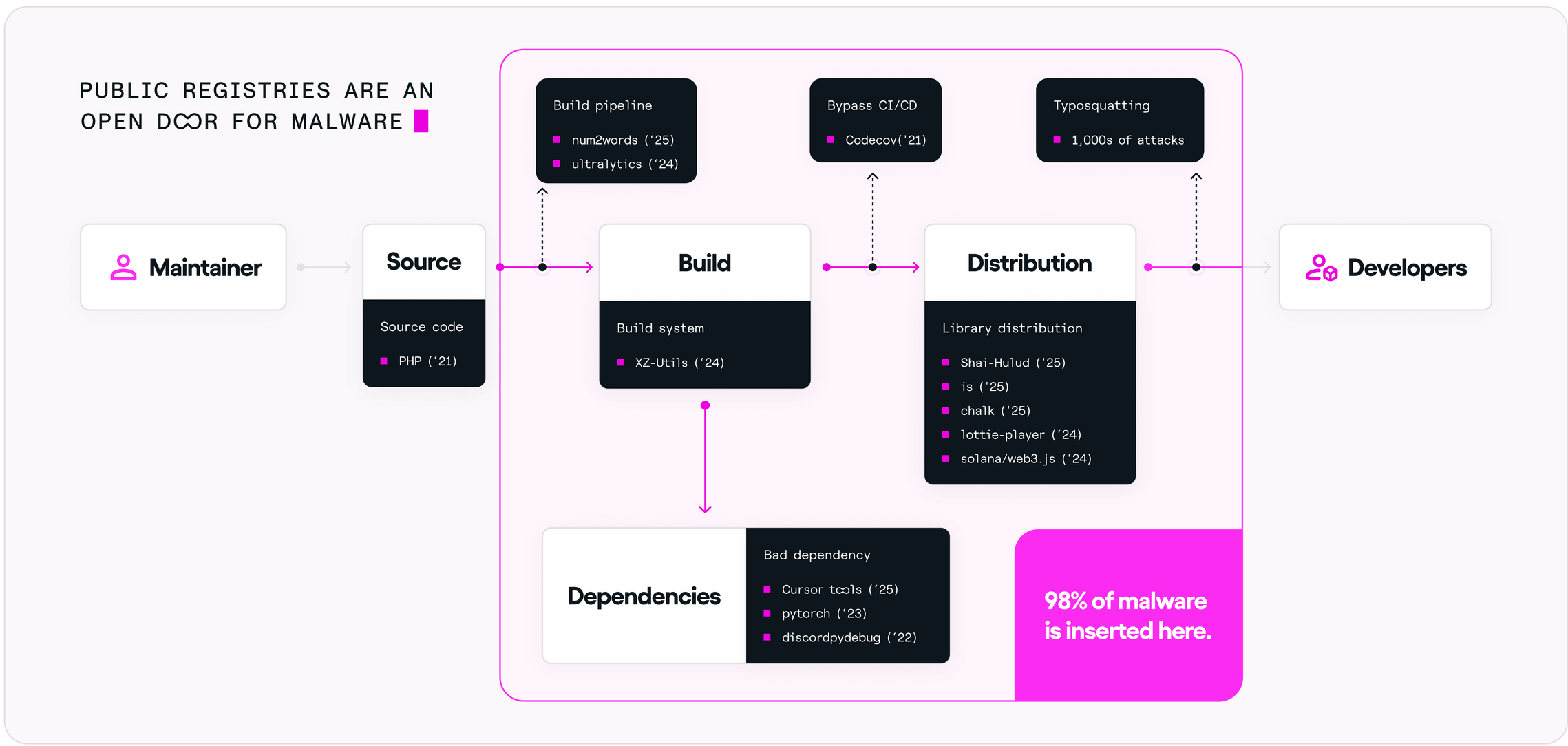
# Chainguard Libraries

The Python, Java, and JavaScript libraries you love—built from verified source to prevent catastrophic malware risk.

## The hidden cost of untrustworthy libraries

The world runs on open source, but the threat landscape has changed dramatically. Software supply chain attacks have evolved from rare anomalies to an industrialized crisis targeting open source. Breaches now cost millions while they erode customer trust.

Real-world malware incidents like the Shai-Hulud worms, `ultralytics`, and `chalk` demonstrate how easily attackers exploit opaque binaries to steal secrets and money. This escalating risk leads to an average supply chain breach cost of $5.1 million and forces your engineers to spend up to 20% of their time on incident response and security triage work, stalling your team's innovation and momentum. Chainguard Libraries solve this problem at the root: unlike scanners or policy engines layered on top of public registries, we proactively prevent 98%+ of malware from ever entering your environment because only packages with verified, buildable source are included.




## The libraries you know, with the security you demand

### Prevent entire classes of supply chain attacks

Access 100K+ libraries built in an isolated, tamper-proof environment that neutralizes build-time and distribution-based malware injections by default.

### Eliminate "are we impacted?" fire drills

When the next headline-grabbing library attack hits, don't stall development to prove a negative. Insulate your team against the panic and disruption of upstream compromises.

### Streamline compliance evidence

Prove that your libraries are protected from third-party manipulation by providing auditors with automated provenance and signed SBOMs that verify component integrity.

# Ecosystems

1M+ versions of libraries that have been built from source code to keep your business safe from malicious attacks without slowing development velocity.

| | |
|---|---|
| **Python** | Trusted, verified libraries from PyPI, including backported CVE fixes for popular libraries like `Django` and `flask`. |
| **Java** | Trusted, built-from-source libraries from Maven Central, providing verifiably secure dependencies for your core applications. |
| **JavaScript** | Currently available in closed beta — trusted, built-from-source libraries from the npm registry. |

## Built with provenance, protection, and assurance

Chainguard Libraries provides continuous security across your core language ecosystems, minimizing your risk without any added developer toil.

- **Proactive Malware Prevention:** Protected from malicious packages and supply chain attacks such as Shai-Hulud, XZ-Utils, `ultralytics`, and `num2words`.
- **Verified by Default:** Every library is built in a tamper-proof, SLSA L2-certified environment with full provenance and signed SBOMs, ensuring you have what you need to provide compliance evidence.
- **Ecosystem Coverage:** Access to 100,000+ libraries across Java, Python, and JavaScript, with more being added every month.

> **“Chainguard's new Python library with CVE remediations has quickly become a key part of our security model at Abridge. By extending their approach to include active CVE remediation, they are helping us streamline how we secure our software supply chain without increasing overhead on our developers.”**
>
> TREY CALIVA, STAFF PLATFORM ENGINEER AT ABRIDGE AI

## Seamlessly integrates with your tech stack

Chainguard Libraries integrates easily into your existing security and development tools, maximizing your return on existing investments.

| | | | |
|---|---|---|---|
| **Artifact Managers** | JFrog Artifactory | Cloudsmith | Sonatype Nexus |
| **Scanners** | Grype | Trivy | AWS Inspector | Anchore Enterprise |
| **Chainguard Products** | Chainguard Containers | Chainguard VMs | |

READY TO IMPROVE YOUR SECURITY POSTURE? LEARN MORE AT CHAINGUARD.DEV/LIBRARIES.