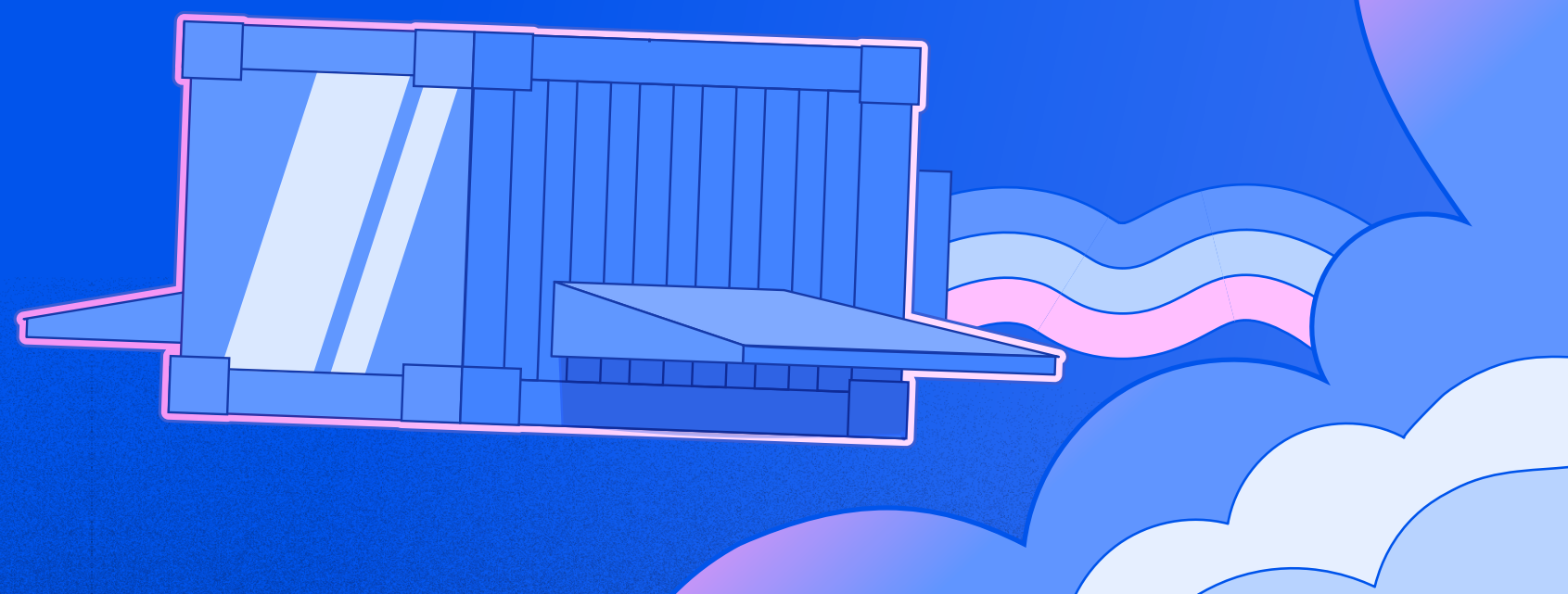




Start and stay secure with WizOS near-zero CVE container images

Container images are the foundation of modern applications, but too often, teams inherit bloated base images packed with unnecessary packages and known vulnerabilities. Even minimal images can introduce CVEs, require constant maintenance, and create a gap between development velocity and security posture. Devs are forced to chase vulnerabilities they didn't introduce, and those CVEs often break builds, causing delays and frustration. Meanwhile, security teams get overwhelmed by vulnerability noise.

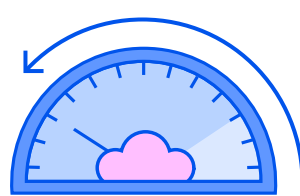
WizOS images give teams a secure, production-ready foundation for containerized applications, backed by a platform to drive migration and scale adoption. Every image is built from source and maintained by Wiz at near-zero CVEs, removing the remediation burden from developers. WizOS reduces vulnerability noise for security teams, helps organizations meet internal SLAs, and fast-tracks compliance.

Secure images are just the start. WizOS is part of a comprehensive platform that helps you drive adoption of secure images and migrate your existing applications. With full visibility into your existing containers, WizOS identifies image migration opportunities, prioritizes based on risk, and makes it easy to drive developer adoption through image swap opportunities directly in pull requests. The result is a clear path to transforming container security with secure foundations.



Eliminate container image CVEs

Wiz maintains strict SLAs around CVE remediation in WizOS images: 7 days for criticals and 14 days for high and medium. This quiets vulnerability scanners and reduces triage time for security teams, enabling them to focus on higher priority CVEs.



Reduce image maintenance

WizOS removes the burden of constantly patching container images, so development teams can spend less time on upkeep and more time building. Security stays tight, innovation keeps moving.



Accelerate compliance

WizOS provides FIPS versions of images, built using FIPS-validated cryptographic modules. All WizOS image builds include SBOMs and provenance metadata, helping teams meet internal security requirements and accelerate compliance efforts.

Wiz is trusted by the world's best brands

ASOS

MARS



Morgan Stanley

LVMH



priceline

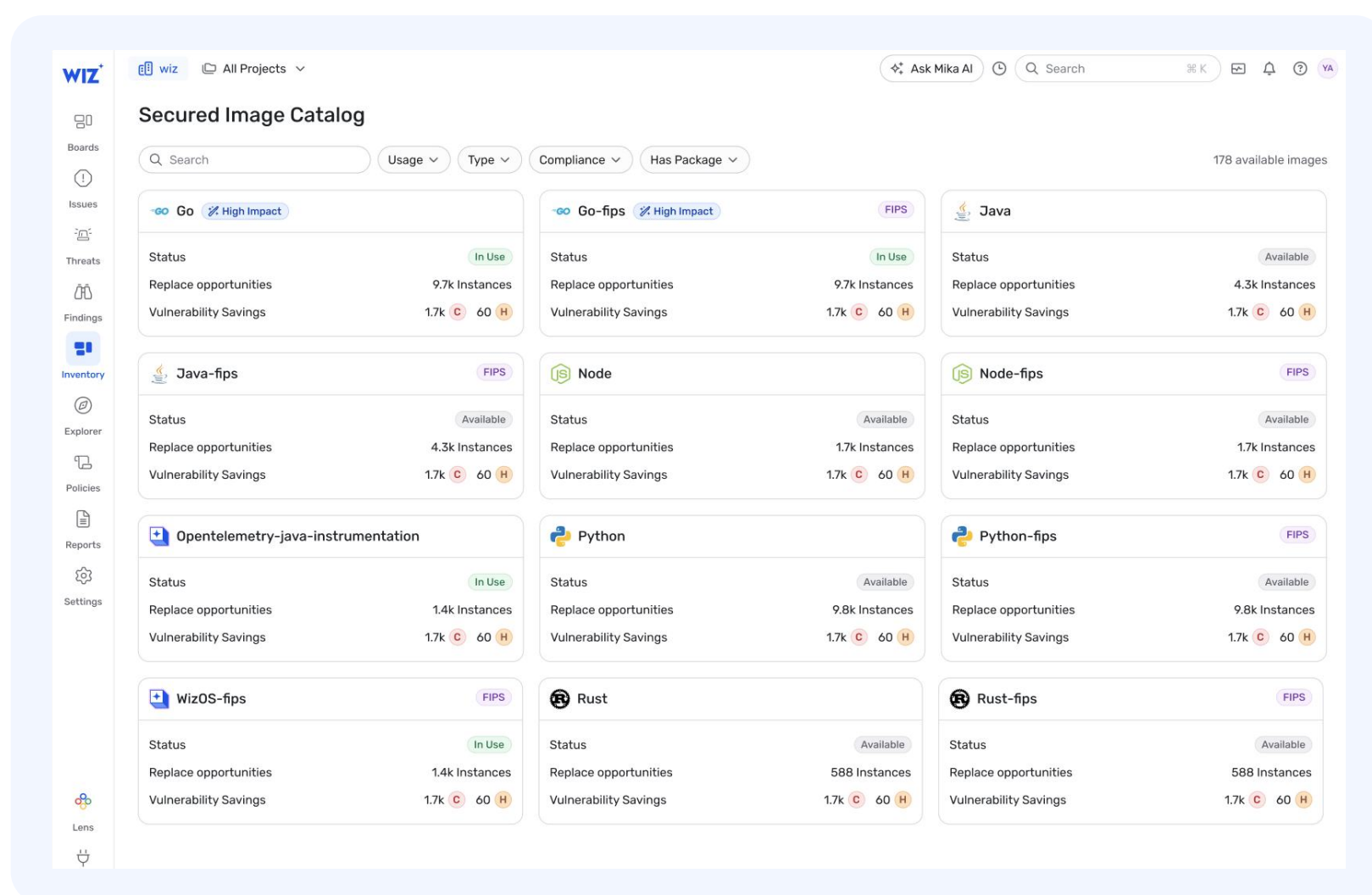


experian.

WizOS transforms container security from the image up with a full platform approach

WizOS images are trusted by security teams and loved by developers

- **Built from Source:** WizOS images are built from source in a custom-hardened build pipeline created specifically for WizOS. Images are rebuilt daily with SBOMs and provenance in every build, so you can trust what's entering your software supply chain.
- **Customizable:** Each image type comes with a package repository that includes secured packages tested and vetted by Wiz, so you can customize images without sacrificing security.
- **Developer Ready:** WizOS images were engineered with compatibility in mind. They use glibc for broad compatibility, and come with a package manager installed so developers can easily customize with additional packages from the Wiz repository.
- **High Availability:** WizOS is scalable and highly available, with a rate limit of 10,000 image pulls per minute and geo-replication for low latency.



Wiz makes adopting and migrating to secured images seamless

- **Complete container image visibility and risk assessment:** Wiz scans images across every stage of the container lifecycle, giving you visibility into your existing container image landscape along with vulnerability findings for each image, so you can identify top images by risk.
- **Risk-Prioritized image migration opportunities:** Wiz automatically identifies images in your environment that are eligible for migration to a secured WizOS image, and prioritizes the top migration opportunities based on vulnerability impact.
- **Image swaps in developer workflows:** Empowers developers by providing vulnerability context and one-click image swaps in the IDE and pull requests, making the secure choice the easy choice.
- **Guardrails:** Enforce guardrails in the CI/CD and with the Wiz Admissions controller to ensure that only secured, trusted images are deployed to production.

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from \$1M to \$100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 50% of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé. Visit <https://www.wiz.io/> for more information.



The combination of WizOS and the Wiz platform changes the way we approach container images vulnerability management. Instead of addressing CVEs one by one, Wiz highlights high-impact image replacement opportunities – so by fixing the base image, we reduce hundreds of vulnerabilities at once. That visibility and replicability is what makes adopting secured images both practical and valuable.

Tuomas Vähänen
Staff Security Engineer, Wolt

Wolt

"Adopting WizOS images was seamless – our developers didn't need to change their workflows. One simple migration gave us secure, up-to-date images with ongoing automated patching. We've gone from reactive fixes to proactive security in a fraction of the time.

Emil Vaagland
Head of Product Security, Vend

Vend

WIZ