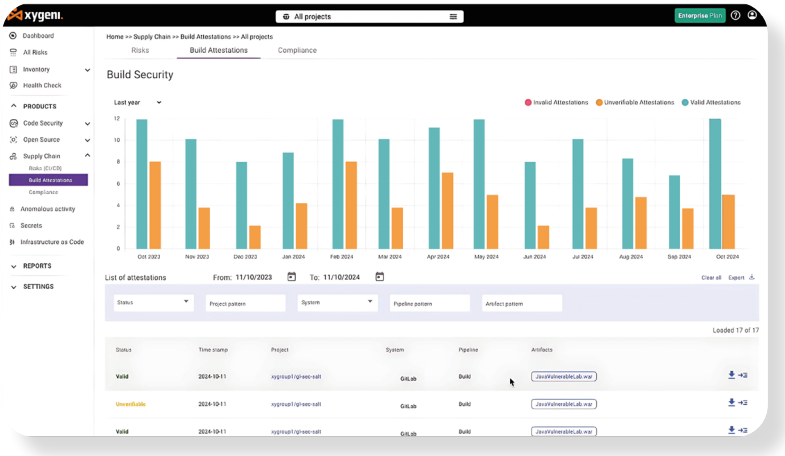
Build Security

Solution Brief

Secure Your Build Process from Code to Deployment

Xygeni's Build Security locks down your CI/CD pipeline with attestation-based verification, cryptographic signatures, and provenance tracking. Ensure every artifact is authentic, tamper-proof, and compliant—without slowing down development



About Company

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Recent reports show that over 60% of software supply chain attacks exploit unverified build artifacts, while tampering and dependency hijacking are at an all-time high. Without strong validation, malicious code, misconfigurations, and compromised dependencies can slip into production, leading to security breaches and compliance failures.

Third-party integrations and outsourced development further increase risks, exposing core systems to untrusted code and unauthorized modifications. Without build integrity verification, organizations face costly downtime, security incidents, and regulatory penalties.

Xygeni's Build Security stops these threats by securing every stage of your CI/CD pipeline. Our attestation-based verification, cryptographic signatures, and artifact provenance tracking ensure every build is authentic, untampered, and fully traceable.

With real-time validation and automated enforcement, Xygeni helps DevOps teams prevent unverified code from reaching production—without slowing down development.

$46B
estimated global losses due to software supply chain attacks.
Cybersecurity Ventures

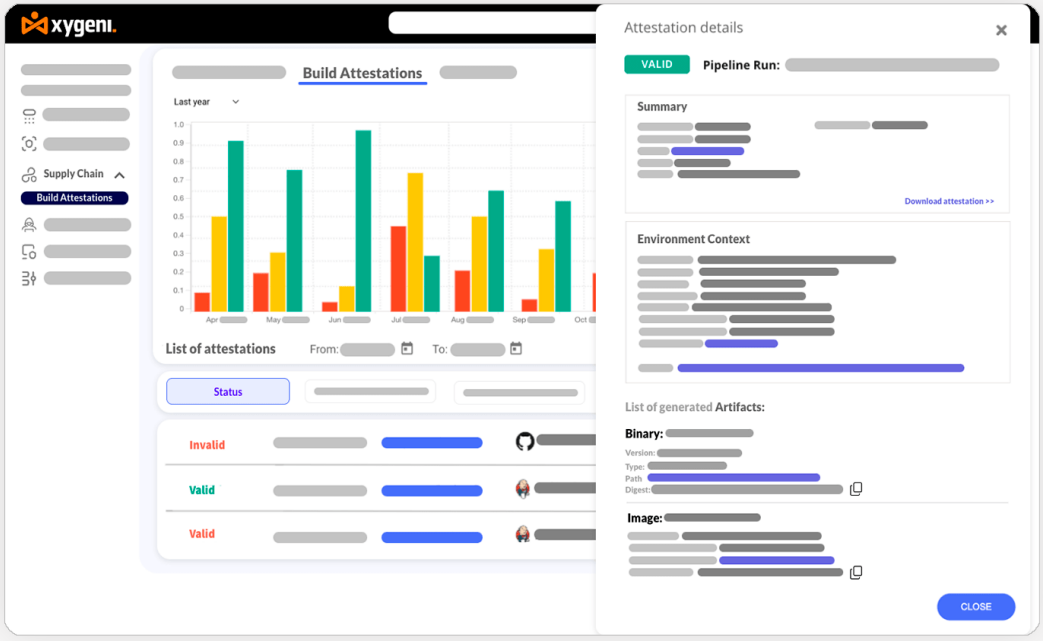
Build Security

Solution Brief

Build Provenance with SLSA Compliance

Protecting your software supply chain requires full transparency into how software is built. **Xygeni enhances Build Provenance** by automating **SLSA-compliant attestation generation**, ensuring every artifact is traceable to a secure source.

- **Automated SLSA Provenance:** Automatically capture and store metadata about builds, including source code, dependencies, and build steps. This guarantees full visibility and prevents unauthorized modifications.
- **Secure and Verifiable Builds:** Ensure that every software artifact—such as container images and compiled binaries—remains authentic and tamper-proof.



Secure Build Attestation with In-Toto

In-Toto attestations enhance build security by creating **verifiable, tamper-proof records** of all software artifacts. **Xygeni automates attestation generation**, protecting against supply chain attacks and ensuring trust across the development lifecycle.

- **Attestation Generation:** Automatically generate and sign in-toto attestations during the build process to certify artifact integrity and origin.
- **Verification and Centralized Management:** Validate attestations against their respective software artifacts using the Xygeni platform. Centrally manage all attestations to maintain security and compliance.
- **CLI and CI/CD Integration:** SALT's command-line interface (CLI) enables security teams to generate and verify attestations efficiently. Fully compatible with CI/CD pipelines for seamless, continuous security enforcement.
- **End-to-End Software Trust:** With in-toto attestations, every step of the software development lifecycle is secure, auditable, and tamper-proof—ensuring trust at every level.

Build Security

Solution Brief

Detect and Block Malicious Code Attacks

Securing the build process is the first step to protecting the software supply chain. Without proper validation, compromised dependencies, unauthorized modifications, and unverified code can infiltrate production, leading to security breaches and compliance risks.

Xygeni's Build Security solution integrates automated attestation-based verification into CI/CD pipelines, preventing supply chain attacks and ensuring that only trusted artifacts are deployed. By generating cryptographic attestations, tracking software provenance, and enforcing verification policies, Xygeni delivers a secure, transparent, and tamper-proof software delivery process.

Seamless CI/CD Integration

Xygeni integrates with GitHub Actions, GitLab CI, Jenkins, Azure DevOps, and more, enabling automated attestation verification at every build stage. With a one-line setup, teams can enforce security policies, validate artifacts, and block unverified software without slowing development.

Tamper-Proof Artifact Verification

Xygeni ensures that source code, dependencies, binaries, and container images are authenticated and cryptographically signed before deployment. By tracking integrity and provenance, organizations can detect unauthorized changes early and block compromised builds before production.

Flexible Attestation Storage & Accessibility

Xygeni allows teams to store, manage, and verify attestations in real time from any OCI-compliant registry like ORAS, AWS ECR, GCP Artifact Registry, and Docker Hub. Co-locate attestations with artifacts for seamless compliance or deploy private attestation registries for full control.

Advanced Security with Keyless Signing

Xygeni eliminates key management complexity with keyless signing, using ephemeral signing keys and OpenID Connect (OIDC) authentication. By integrating with GitHub, GitLab, and Azure, Xygeni ensures only trusted identities sign artifacts, preventing unauthorized modifications.

Comprehensive Visibility with Attestations

Xygeni enhances supply chain transparency by embedding Software Bill of Materials (SBOMs), security reports, and vulnerability scans into attestations. With SPDX and CycloneDX support, teams gain real-time insights into dependencies and prioritize security fixes efficiently.

Real-Time Attestation Access & Monitoring

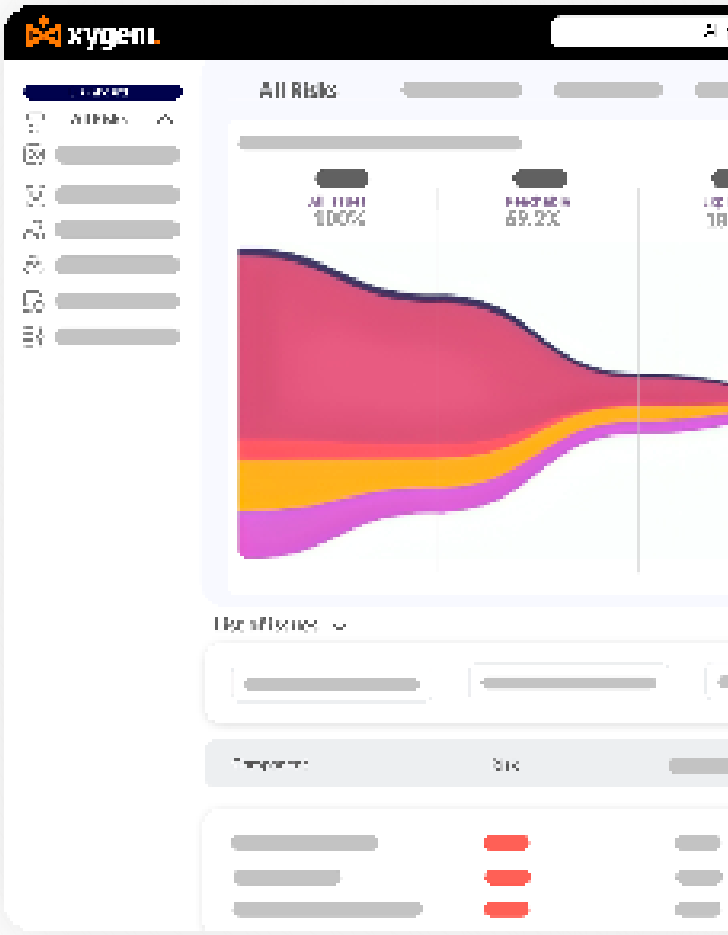
Xygeni provides instant access to attestations for compliance, audits, and security enforcement. With a full audit trail, organizations can track software lineage, enforce policies, and prevent unverified artifacts from deployment.

Secure Your Builds with Xygeni Build Security

Verify builds, prevent tampering, and secure your CI/CD pipeline—all in one powerful solution.

- **No credit card needed**
- **Quick setup, instant results**

Start your free trial



Get in touch today!

www.xygeni.io
https://www.linkedin.com/company/xygeni
https://twitter.com/xygeni