DATA SHEET

Securing CI/CD Pipelines and Software IP with Terniion™

The Problem: Open Pipelines, Growing Attack Surface

CI/CD pipelines have become the backbone of modern software delivery — and one of its most exposed attack surfaces. From code repositories and build runners to artifact stores and deployment targets, every stage of the pipeline is a potential entry point for credential theft, supply chain attacks, and IP exfiltration. The SolarWinds breach proved how catastrophic a compromised pipeline can be.

The constraints are real:

- CI/CD servers, runners, and repositories sit on networks reachable from the public internet.
- API keys, tokens, and credentials live in environment variables — one misconfiguration away from exposure.
- Source control systems like GitLab carry critical vulnerabilities that go unpatched for weeks or months.

Traditional perimeter security was never designed for the software supply chain, but Xiid's Terniion is.

Terniion eliminates the attack surface for CI/CD infrastructure without disrupting development velocity or requiring pipeline redesigns.

Business Outcomes

Eliminates Credential Exposure

SealedTunnel takes CI/CD architecture offline by rejecting all inbound traffic. API keys, tokens, and environment variables stay safe — even those committed to repositories by accident.

Exceeds Zero Trust Access Standards

SealedTunnel goes beyond authentication and authorization by segmenting resources at the process level, eliminating the risk of lateral movement through the pipeline.

Mitigates Data-in-Transit Threats

Quantum-resistant, triple-encrypted communication channels protect sensitive data exchanged between CI/CD components against eavesdropping, interception, and man-in-the-middle attacks.

Seamless Integration, No Pipeline Rework

SealedTunnel integrates with Jenkins, GitLab CI/CD, GitHub Actions, and CircleCI with few or no modifications. Security hardens without slowing development cycles.

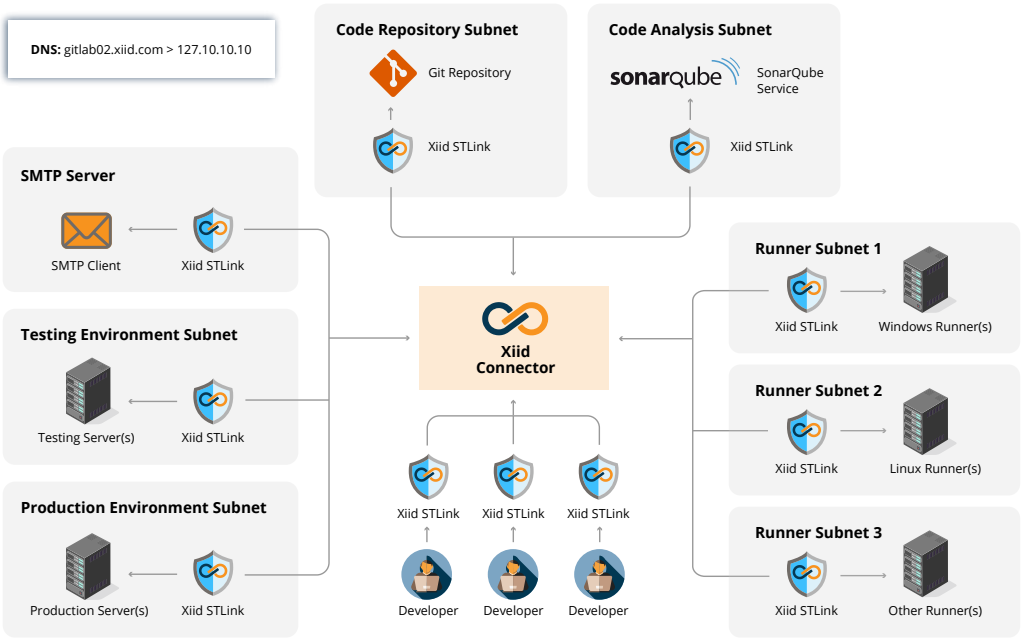
5 Best Practices for CI/CD Pipeline Security

Best Practice	Key Actions	Xiid Terniion Solution
Lock Down Code Repositories	Prevent unauthorized access to source code, branches, and merge requests. Keep repositories unreachable from the public internet.	SealedTunnel eliminates inbound network access to centralized code repositories. Repositories become impossible for outside attackers to reach, but remain easy to access for authorized, authenticated staff.
Secure Build Runners and Artifacts	Restrict runner access to authorized DevOps team members. Prevent tampering with build artifacts and pipeline configurations.	SealedTunnel secures runners by rejecting all inbound access and enforcing quantum-secure, process-level connections. Unauthorized users cannot reach runners or tamper with artifacts.
Protect Credentials and API Keys	Remove direct exposure of API keys, tokens, and secrets used for deployments and integrations.	By taking CI/CD infrastructure offline from inbound traffic, SealedTunnel keeps credentials inaccessible to external threats — even if accidentally committed to a repository.
Prevent Lateral Movement in the Pipeline	A compromised component in one stage of the pipeline should not become a pivot point into other systems, databases, or production environments.	Terniion enforces process-level microsegmentation. A breach in one component is contained — it cannot reach other pipeline stages, production servers, or databases over the network.
Quantum-Secure the Software Supply Chain	Assume adversaries are capturing pipeline traffic today to decrypt later with quantum capabilities.	Triple-layer, post-quantum encryption protects source code, build artifacts, and deployment credentials against “harvest-now, decrypt-later” strategies across the full software delivery lifecycle.

How Terniion Secures CI/CD Pipelines

Terniion is a secure network access control platform designed as an overlay. It does not require you to rip and replace networks, firewalls, or existing CI/CD toolchains.

Xiid's SealedTunnel uses Zero Knowledge Networking (ZKN) technology to eliminate attack surface by closing all inbound ports. Triple-encrypted, quantum-secure, process-to-process tunnels make CI/CD systems accessible to authorized users while blocking unauthorized entry, tampering, and man-in-the-middle attacks.



No subnets or servers need any open inbound ports or public IP addresses.

Key Components

- **SealedTunnel**
  Executed via STLink — a lightweight software agent on either end, these are outbound-only, triple-encrypted, process-to-process tunnels that perform reliably even over unstable networks, ideal for distributed development teams.
- **Commander**
  The control brain coordinating secure connections across cloud, on-prem, and hybrid environments. It centralizes policy so "who can talk to what" becomes maintainable rules instead of 10,000 firewall exceptions.
- **Connector**
  Joins two outbound-only communication halves without ever decrypting traffic. It serves as a secure rendezvous where quantum-encrypted messages are dropped off and picked up by authorized STLinks, keeping critical infrastructure undiscoverable.
- **Aclave™**
  Credential-less authentication that lets staff and partners access systems without usernames, passwords or long-lived credentials.

What This Looks Like in the SDLC Environment

Source Control and Code Repositories

- GitLab, Gitea, and other self-hosted repositories run with all inbound ports closed.
- Authorized developers and automated processes connect through outbound-only tunnels, scoped to specific resources, not entire networks.
- Malicious actors or compromised workstations cannot address the repository from outside.

Build, Test, and Artifact Pipelines

- CI/CD runners, artifact stores, and testing environments are unreachable from the public internet.
- Pipeline communications are triple-encrypted and quantum-secure, even over shared or untrusted networks.
- Code injection attacks and configuration tampering are blocked at the network level.

Deployment and Production Access

- Connections to production servers, databases, and cloud services remain isolated and sealed.
- API keys and deployment credentials never traverse exposed networks.
- Vulnerability exploitation windows shrink dramatically — even unpatched systems are unreachable to outside attackers.

FAQS

Will this disrupt our development workflow or require pipeline changes?

No. Terniion is designed as an overlay. It wraps existing CI/CD infrastructure without requiring pipeline redesigns or tool replacements. Rollout can be phased starting with the highest-risk components — source control and production deployment paths.

Do we need to replace our existing firewalls, VPNs, or identity systems?

No. Terniion reduces your reliance on VPNs for developer access, but it works alongside your current firewalls and identity providers, immediately shrinking exposed attack surface to nearly zero.

How does this help with compliance and auditors?

Auditors and compliance frameworks increasingly focus on supply chain security, access controls, and lateral movement prevention. Terniion closes inbound ports, hardens remote access, and provides strong cryptographic controls, making it straightforward to demonstrate reduced attack surface and alignment with frameworks like NIST SSDF and SOC 2.

The Bottom Line

Your CI/CD pipelines and source code are among your most valuable—and most targeted—assets. Your security model needs to match the stakes.

Terniion gives you a way to:

- Eliminate credential exposure without changing developer workflows.
- Lock down repositories, runners, and artifact stores from external attackers.
- Prevent lateral movement across pipeline stages and into production.
- Protect the entire software supply chain with quantum-secure, future-ready encryption.

Secure the pipeline that builds and delivers your software against today's and tomorrow's attackers.

Ready to harden your CI/CD pipeline without disrupting development velocity?
Request a briefing | See a live demo