

Securing SDLC and GitHub with Zero Trust Cloud

SOLUTION BRIEF

©2026 Zscaler, Inc. All rights reserved.

The Software Development Lifecycle (SDLC) is a collaborative framework where code is constructed, evaluated, and verified — with GitHub serving as a vital component — making it a critical part of the software development supply chain.

GitHub interacts with various public and private applications like Slack, Jira, or Artifactory that are hosted in a multicloud environment. These interactions are powered by GitHub Runners and AI coding agents.

Attackers compromise SDLC infrastructure and embed malware through multiple attack vectors, including GitHub:

- **Supply Chain Attacks:** Attackers register malicious public packages matching the names of internal private ones, tricking GitHub build runners into downloading them.

- **Pipeline Poisoning:** Attackers exploit misconfigured GitHub Actions or malicious pull requests to force runners to execute unauthorized code.

- **Secret Harvesting:** Attackers scan for hardcoded credentials inadvertently committed to GitHub repositories.

While GitHub offers built-in security, organizations remain responsible for securing their repository content and configurations. Firewall-based conventional security models falls short for three reasons:

- **Expanded attack surface:** Firewalls around self-hosted AI agents and GitHub Runners expose them to the internet.

- **Lateral threat movement:** A breach can let attackers reach secret managers and runners, spreading backdoors or malware.

- **Operational complexity:** Managing firewalls across multicloud environments creates policy sprawl, higher costs, and more administrative overhead.

The Zero Trust Approach

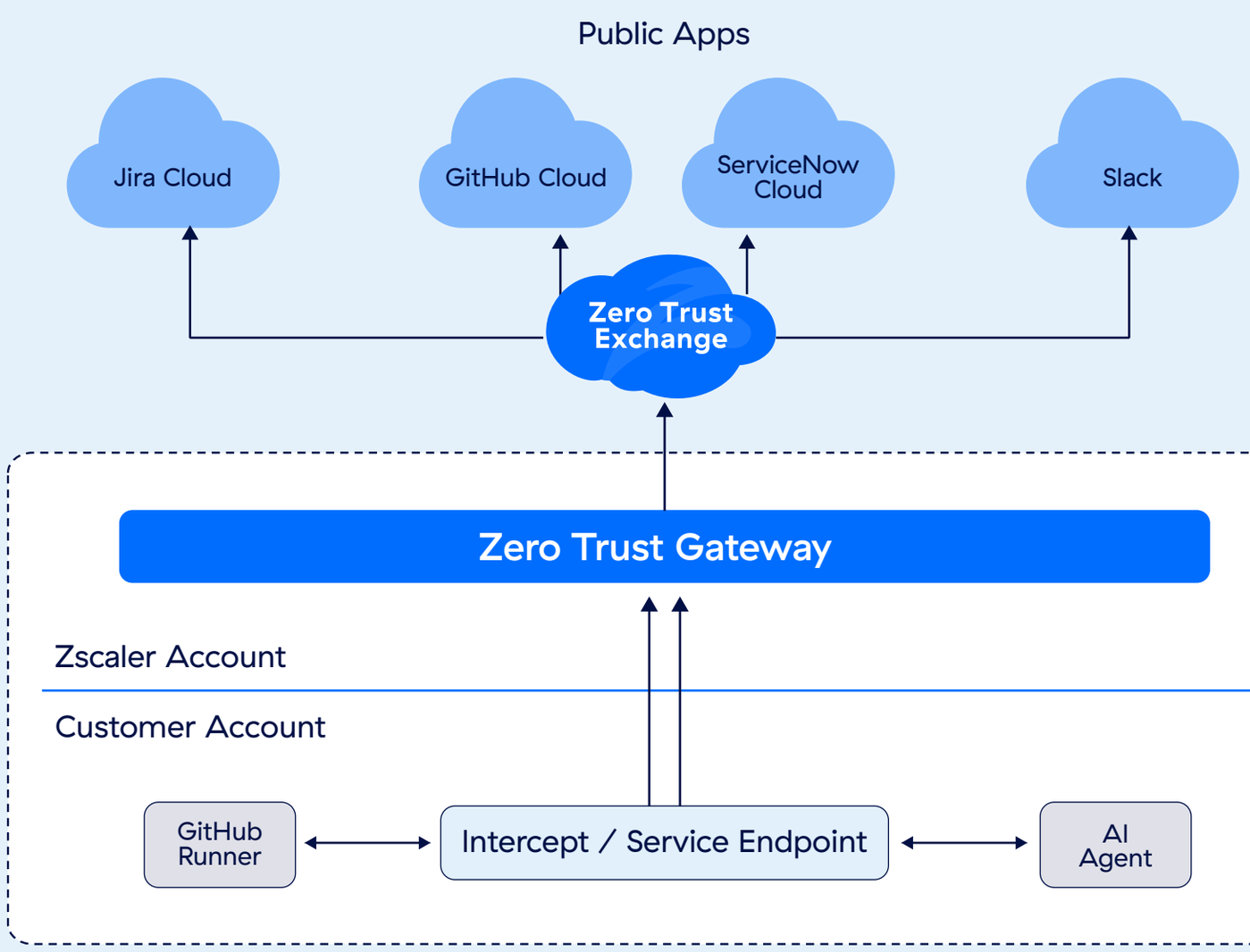
Zscaler Zero Trust Cloud (ZTC) is a cloud-native platform based on zero trust principles to revolutionize security across the software development life cycle. It hides GitHub Runners and AI coding agents on the network, effectively shielding them from discovery and preventing targeted exploits. It provides cloud-scale TLS decryption and inline data protection for all outbound GitHub traffic directed to public apps like Jira, ServiceNow, or Slack.

Instead of placing the GitHub workloads on a shared network, ZTC establishes secure, 1-to-1 connections based on workload identity and policy. This effectively blocks the lateral movement of threats from compromised private apps. Consolidating security into one unified platform, it provides visibility and control over GitHub workload traffic.

©2026 Zscaler, Inc. All rights reserved.

Core Capabilities

1. Secure connectivity to public apps like Jira, Slack & ServiceNow: ZTC continuously monitors all outbound traffic whenever GitHub Runners and AI agents interact with public applications. The traffic is routed from a service endpoint to Zero Trust Exchange via Zero Trust Gateway. ZTC provides cloud-scale TLS inspection and inline data protection. It ensures that the GitHub workloads remain entirely hidden from the public internet.



2. Secure connectivity to private apps: GitHub Runners and AI agents interact with various private applications, such as Artifactory for storing production-ready packages and Confluence for storing documentation. ZTC enforces least-privilege access allowing only 1-to-1 interactions based on workload identity and security policies. There are 2 scenarios:

- **2.1. When the private apps are hosted in the same region:** Under this scenario, the private application VPC is located within the same cloud region as the AI Agent VPC or GitHub Runner VPC. Traffic originating from the AI agent or GitHub Runner is directed to the Zero Trust Gateway via service endpoint, where local inspection is conducted before granting access to the private application.

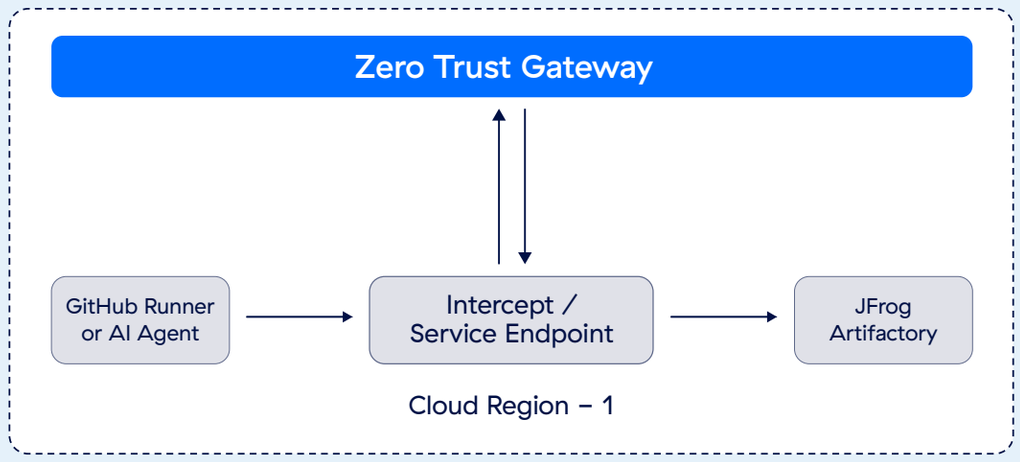


Figure: *Secure connectivity to private apps (JFrog Artifactory) when they are hosted in the same region*

©2026 Zscaler, Inc. All rights reserved.

- **2.2. When the private apps are hosted in different regions, availability zones (AZ), or cloud:** In scenarios where the private application VPC and the GitHub Runner or AI Agent VPC are distributed across distinct cloud providers, regions, or AZs, traffic travels from a service endpoint through the Zero Trust Gateway to the Zero Trust Exchange prior to private application access being authorized.

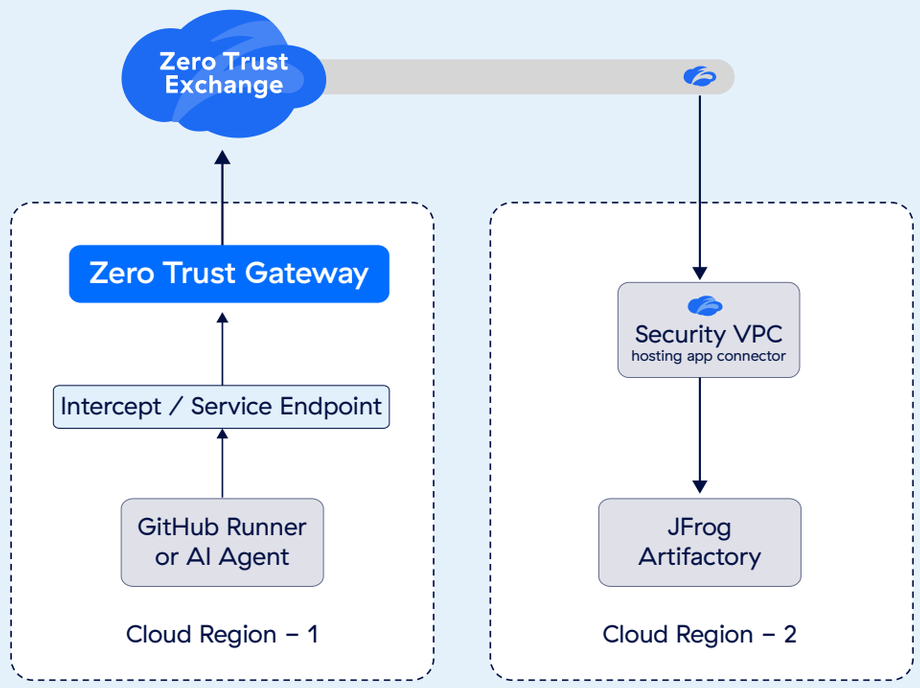


Figure: *Secure connectivity to private applications (Artifactory) when it is hosted in a different region*

Business Outcomes and Benefits

1. Protect software development from discovery and attacks

ZTC shields your critical development environments from discovery, preventing targeted exploits and pre-empting costly cyberattacks before they can begin. The self-hosted AI agents and GitHub Runners are concealed from the open internet at every communication point.

2. Prevent and contain supply chain attacks by malicious code

Attackers upload malicious packages with identical names to internal ones but higher version numbers, tricking build runners into automatically installing the compromised versions. ZTC prevents GitHub runners from pulling such malicious packages. Should a GitHub runner become compromised, ZTC automatically intervenes to block any unauthorized attempts to connect to private applications.

3. Protect secrets, tokens & private keys

ZTC prevents unauthorized data extraction, ensuring that sensitive organizational information, API keys, and cloud credentials cannot be silently siphoned out, while simultaneously blocking unauthorized or unsanctioned external connections.

4. Empower developer velocity

ZTC eliminates operational bottlenecks associated with firewall configuration updates. It provides faster, secure connectivity between GitHub Runners and public or private applications, removing friction from software development pipelines.

Next Steps

Zero Trust Cloud secures multicloud workloads, reducing attack surface and lateral movement.
One platform ensures consistent policy for all traffic flows, cutting complexity and cost.
To learn more about Zero Trust Cloud, contact us today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

Act Fast.
Stay Secure.