DATASHEET

aperon

Secure Your Source Code Ecosystem



Identity-Centric SSE Protection for GitHub

In today's decentralized development environment, your source code is your most valuable intellectual property. Yet, GitHub environments face growing risks:

1. Unauthorized access due to **credential compromise**
2. Developers accessing repositories from **unmanaged personal devices**
3. Code downloads on **insecure endpoints**
4. **Code exfiltration** to external repositories
5. Insider threats and accidental **data leakage**

Standard GitHub security often stops at basic authentication, leaving a critical gap for credential theft, shadow IT, and data exfiltration. Zaperon closes this gap by wrapping GitHub in an **Identity-Centric Security Service Edge (SSE)** layer, ensuring that only trusted identities on secure devices can interact with your repositories.



The Zaperon Approach



Zaperon extends Zero Trust principles directly to GitHub access by continuously verifying:

1 **WHO IS ACCESSING THE REPOSITORY?**



2 **WHAT DEVICE THEY ARE USING?**



3 **WHETHER THE DEVICE IS SECURE?**



4 **WHERE THE CODE IS BEING TRANSFERRED?**



Access is not just authenticated — it is continuously validated and governed.

Core GitHub Protection Features



PHISHING-RESISTANT MFA ENFORCEMENT

Stop account takeovers before they start. Zaperon eliminates the risk of compromised credentials by enforcing phishing-resistant Multi-Factor Authentication (MFA) for every GitHub login.

- **How it works:** Access is granted only after a secure verification via the **Zaperon Verify** authenticator app, replacing vulnerable SMS or push-based codes with asymmetric cryptography.



TRUSTED DEVICE BINDING

Ensure corporate code stays on corporate hardware. Zaperon enforces a strict **Hardware-to-Identity binding** policy.

- **GitHub Login:** Users are blocked from logging into corporate GitHub accounts on personal devices.
- **Data Guard:** Prevents the download of sensitive code repositories onto any device that has not been explicitly authorized and registered by the enterprise.



CONTINUOUS DEVICE POSTURE MONITORING

Security isn't a one-time check at login; it's a constant requirement. Zaperon ensures that the device remains secure throughout the entire session.

- **Real-time Health Checks:** Continuously checks for active antivirus, up-to-date operating system, disk encryption, IP and geo-location. If a device becomes non-compliant, GitHub access is instantly revoked.



UNAUTHORIZED REPOSITORY GUARD

Prevent "accidental" or malicious leaks where proprietary code is pushed to external or personal repositories.

- **Control:** Zaperon's **Cloud Access Security Broker (CASB)** monitors destination traffic, enforcing policies that restrict code uploads exclusively to sanctioned enterprise repositories not to personal repositories.



UNIFIED WEB PORTAL & CLI ENFORCEMENT

Whether your developers prefer the browser or the terminal, Zaperon provides total coverage.

- **CLI Interception:** Unlike basic browser extensions, Zaperon's endpoint-aware agent intercepts and secures traffic from the GitHub Command Line Interface (CLI).
- **Total Lockdown:** Prevents unauthorized code uploads from both the GitHub web portal and the CLI, closing the most common loop-holes used for data exfiltration.

Business Impact

IP PROTECTION

Eliminates the risk of source code leaks to personal accounts or public repositories.

COMPLIANCE READY

Helps meet SOC2, ISO 27001, and DPDP requirements for access and data control.

FRICTIONLESS EXPERIENCE

Provides a seamless, passwordless login experience that developers love.



Zaperon

Zaperon is an Identity-centric Security Service Edge (SSE) platform designed to secure access to applications, data, and cloud infrastructure from any user or device, regardless of location or network. It continuously enforces access policies based on user behavior, device posture, and contextual parameters, ensuring least-privilege access while preventing lateral movement. By minimizing attack surface, proactively detecting anomalies, and providing real-time visibility, Zaperon fortifies hybrid IT environment. Organizations can proactively manage access, reduce risks from credential based threats, and safeguard sensitive information, making security adaptive, scalable, and resilient against evolving cyber threats.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com

© 2026 Zaperon, Inc.
All Rights Reserved.

