VARINDIA

eScan enterprise DLP closes critical GitHub access control gap for organizations

by VARINDIA 2026-02-11

eScan announces the successful deployment of GitHub Tenant Control within its Enterprise DLP solution, addressing a critical security gap affecting thousands of organisations that use GitHub Team or Organisation accounts without Enterprise-level access controls.

The common thread? Organisations struggle to control how employees access GitHub, particularly when they haven't invested in expensive Enterprise accounts with built-in authentication controls.

When a Mercedes-Benz employee accidentally leaked a GitHub token in June 2024, it granted unrestricted access to the company's entire GitHub Enterprise server source code. When The New York Times had credentials to their GitHub repositories inadvertently exposed in January 2024, their complete codebase appeared on 4chan months later. And in March 2025, the tj-actions/changed-files GitHub Action compromise exposed CI/CD secrets - including AWS keys, GitHub tokens, and private RSA keys - across 23,000 repositories.

The GitHub Access Control Problem

GitHub's pricing structure creates a significant security dilemma. While GitHub Enterprise ($21/user/month) includes SAML single sign-on and centralized authentication controls, many organizations use GitHub Team accounts ($4/user/month) to manage costs - particularly when purchasing seats for dozens or hundreds of developers. Team accounts lack GitHub's native tenant control features, leaving organizations vulnerable to employees accessing repositories through personal credentials, third-party SSO providers like Google or Microsoft, or Apple ID authentication.

"Organizations face an impossible choice," said **Govind Rammurthy, CEO & Managing Director, eScan**. "Either spend 5x more for GitHub Enterprise just to get access controls or accept the risk that employees might access your source code repositories through personal accounts that you can't monitor or audit. eScan's GitHub Tenant Control eliminates that dilemma."

How eScan solves It

eScan Enterprise DLP's new GitHub Tenant Control capability works regardless of GitHub account type - Team, Organization, or Enterprise. When an employee attempts to access GitHub using personal credentials or third-party authentication providers (Google, Apple, Microsoft), eScan's DLP intercepts the authentication attempt and blocks it. Access succeeds only when

employees authenticate using their corporate domain credentials, maintaining workflow continuity while ensuring complete visibility and control.

"This isn't about replacing GitHub's security features for Enterprise customers," **Shweta Thakare, VP of Global Sales,** explained. "It's about extending enterprise-grade access control to organizations using Team or Organization accounts, and providing an additional layer of authentication enforcement even for Enterprise customers who want defense-in-depth."

Why This Matters Now

GitHub reported that 39 million secrets were leaked across its platform in 2024 alone. The recent tj-actions compromise in March 2025 affected over 23,000 repositories, exposing credentials that could enable lateral movement into production environments. With India's DPDP Act driving unprecedented focus on data sovereignty and access control, source code repositories have become a critical compliance concern.

eScan's GitHub Tenant Control integrates with the company's broader Workspace Tenant Control feature set, which already manages authentication for Google Workspace, Microsoft 365, Dropbox, Atlassian, Slack, Webex, ChatGPT, and dozens of other platforms. The unified approach enables organizations to enforce consistent authentication policies across their entire cloud application ecosystem from a single DLP platform.

eScan enterprise DLP closes critical GitHub access control gap for organizations