eScan Enterprise DLP Closes Critical GitHub Access Control Gap for Organizations

GitHub Team accounts leave enterprises exposed. eScan enforces corporate-only authentication across all GitHub tiers — no Enterprise plan required.

eScan Enterprise DLP closes the GitHub authentication gap — enforcing corporate-only access across Team, Organization, and Enterprise accounts without requiring a GitHub Enterprise plan.

MI, UNITED STATES, April 29, 2026 /EINPresswire.com/ -- New capability delivers enterprise-grade GitHub authentication enforcement without requiring GitHub Enterprise — protecting source code, CI/CD pipelines, and secrets across North American organizations

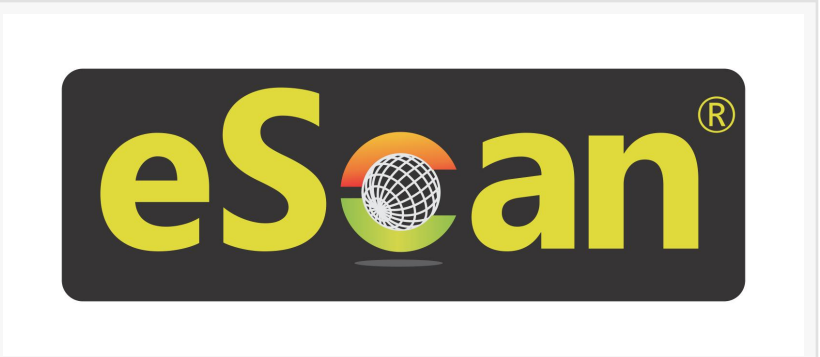
MICHIGAN, USA — eScan (MicroWorld Technologies Inc.) today announced the successful deployment of GitHub Tenant Control within its Enterprise DLP solution, addressing a critical security gap that affects thousands of organizations using GitHub Team or Organization accounts without enterprise-level access controls.

> Organizations face an impossible choice. Spend 5x more for GitHub Enterprise just to get access controls, or accept the risk of unmonitored repository access."
>
> *Govind Rammurthy, CEO & Managing Director, MicroWorld Technologies Inc.*

A Pattern of High-Profile Source Code Exposures
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 common thread: organizations struggle to control how employees access GitHub,

particularly when they have not invested in expensive GitHub Enterprise accounts with built-in authentication controls.



eScan — Enterprise Cybersecurity Solutions trusted by organizations across 90+ countries

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. 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." — Govind Rammurthy, CEO & Managing Director, eScan

How eScan Solves It
eScan Enterprise DLP's 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 is not about replacing GitHub's security features for Enterprise customers. It is 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 affected over 23,000 repositories, exposing credentials that could enable lateral movement into production environments. With North American organizations facing increasing regulatory scrutiny over data sovereignty and access governance, source code repositories have become a critical compliance concern for security and legal teams alike.

Broader Workspace Tenant Control

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.

About eScan (MicroWorld Technologies Inc.)
eScan is a globally established cybersecurity company providing comprehensive security solutions including Enterprise EDR, Vision Core XDR, Enterprise DLP, and Business DLP. With over 300 R&D professionals, eScan serves enterprises, government agencies, and small to medium businesses across 90+ countries, delivering protection against evolving cyber threats. For more information, visit www.escanav.com.

Media Contact
eScan Communications
Email: rohini@escanav.com
Website: www.escanav.com

eScan Communications
MicroWorld Technologies Inc.
rohini@escanav.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
Other
