Enterprise IT WORLD
FOR THE CIOs. BY THE CIOs.

News Security

eScan Enterprise DLP Closes Critical GitHub Access Control Gap for Organizations

by enterpriseitworld February 11, 2026 185

New capability brings enterprise-grade repository authentication enforcement to GitHub Team and Organization customers

eScan (MicroWorld Technologies Inc.) has rolled out GitHub Tenant Control within its Enterprise DLP solution, directly addressing a longstanding access control gap that affects thousands of organizations using GitHub Team or Organization accounts without Enterprise-level authentication features.

The security challenge is well documented. Organizations on GitHub Team plans often lack the native controls required to restrict how employees authenticate leaving the door open to personal accounts, unmanaged credentials, and third-party logins. In high-profile breaches involving Mercedes-Benz (2024), The New York Times (2024), and the tj-actions compromise (2025), leaked credentials provided attackers with expansive repository access, ultimately exposing source code, CI/CD secrets, and cloud keys.

The root issue lies in GitHub's pricing model. GitHub Enterprise includes SAML SSO and centralized authentication, but at more than five times the cost of Team accounts. As a result, many organizations especially those supporting large developer teamsopt for the lower tier and inherit the access-control blind spot.

"Organizations shouldn't have to choose between affordability and security when protecting their source code," said Govind Rammurthy, CEO & Managing Director, eScan, as the company announced a major enhancement to its Enterprise DLP platform: GitHub Tenant Control.

"Organizations shouldn't have to choose between affordability and security when protecting their source

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

"Either companies pay 5x more for GitHub Enterprise just to get authentication control, or they accept the risk of developers accessing repositories with private credentials," Rammurthy noted. "eScan's GitHub Tenant Control eliminates that trade-off."

How eScan Fixes the Gap

The new capability enforces corporate-domain authentication across GitHub regardless of account tier. When a user attempts to access GitHub using personal or third-party credentials (Google, Microsoft, Apple), eScan intercepts and blocks the attempt. Only corporate-approved authentication is allowed, ensuring auditability and preventing unauthorized access without disrupting developer workflows.

"This isn't about replacing GitHub Enterprise security," said Shweta Thakare, VP of Global Sales. "It's about extending enterprise-grade control to every GitHub customer and offering an additional enforcement layer even for those who already use Enterprise."

Why It Matters in 2026

With 39 million leaked secrets detected on GitHub in 2024, and 23,000 repositories impacted by the 2025 tj-actions breach, source-code security is under intense regulatory and compliance scrutiny. In India, the DPDP Act has further accelerated the need for strict access governance.

GitHub Tenant Control integrates with eScan's broader Workspace Tenant Control framework, which already enforces authentication policies across Google Workspace, Microsoft 365, Slack, Dropbox, Atlassian, Webex, ChatGPT, and dozens more.

By unifying authentication governance across cloud applications, eScan is closing one of the most critical and overlooked entry points for modern cyber risk.