BlueFlag Security delivered by Knovation Solutions

SOLUTION BRIEF

As your GitHub Enterprise Cloud and Azure DevOps environments scale, identity governance becomes critical. While Azure Entra ID governs corporate identities, it cannot see the identities operating inside your development environments. Neither can Microsoft Defender for DevOps or GitHub Advanced Security. This is where **BlueFlag Security** steps in.

BlueFlag extends identity governance into your SDLC, discovering and governing all identities operating across your development environments: from service principals to deployment identities to hardcoded secrets.

BlueFlag ingests GitHub Advanced Security findings, GitHub Actions workflows, Azure Pipelines execution, and Entra ID access logs to correlate identity governance with code risk, enforcing policies where your existing tools cannot reach.

Identity and Activity Visibility Across Your Microsoft SDLC

BlueFlag ingests identity and activity data from the platforms where SDLC identities actually operate:

Azure Entra ID: Service principals, managed identities, app registrations, conditional access policies, access logs, authentication events, application permissions.

Azure DevOps:

- **Source Control:** Repositories, branches, permissions, pull requests, code history, branch protection policies, team memberships.
- **Azure Pipelines:** CI/CD workflows, pipeline definitions, build agents, deployment jobs, service connections, release approvals, run history, agent pools.

GitHub Enterprise Cloud:

- **Source Code Management:** Repositories, branches, permissions, collaborators, deploy keys, SSH keys, team memberships, member access levels.
- **GitHub Advanced Security:** Secrets scanning (hardcoded credentials, API keys, tokens), supply chain analysis (SCA findings, vulnerable dependencies), SAST findings.
- **GitHub Actions:** Workflow automation, CI/CD pipelines, runner agents, job logs, deployment history, action usage patterns.

What this data reveals: A continuous graph of identity actions across your entire SDLC. **Which** service principal accessed which repository. **Which** deployment identity executed which pipeline. **Which** GitHub Action committed code and from which environment. **Which** credentials are hardcoded in repositories. **Which** Advanced Security findings correlate with identity access patterns. **Which** identities are orphaned, dormant, or behaving unusually.

The 45:1 Reality: Where Your Blind Spot Lives

In a 50-developer organisation in transition: new teams building on GitHub Enterprise, legacy teams still on Azure DevOps:

50	2,250	98%
HUMAN IDENTITIES (ENTRA)	NON-HUMAN IDENTITIES (UNGOVERNED)	UNMANAGED IDENTITY ESTATE
Developer accounts visible to Entra	Service accounts, PATs, tokens, secrets invisible to Entra	Credential sprawl across repos and dev tools

Breakdown of 2,250 NHIs (GitHub and Azure DevOps focus):

- **Service Accounts & Bots (650):** GitHub/Azure DevOps service accounts, bot tokens, automation identities, release approval accounts.
- **Personal Access Tokens (500):** GitHub PATs, Azure DevOps PATs, OAuth tokens, webhook credentials.
- **Deploy Keys & SSH Keys (200):** GitHub deploy keys, machine-to-machine automation credentials.
- **Hardcoded Secrets (300):** Credentials exposed in repositories (surfaced by GitHub Advanced Security).
- **Pipeline & Webhook Bots (400):** GitHub Actions runners, Azure Pipelines agents, webhooks, ChatOps bots.
- **AI Agent Identities (200):** Cursor and other AI agents accessing repos and pipelines.

Every unmanaged identity is an attack vector. GitHub Advanced Security finds secrets; BlueFlag governs who created them and who has access.

Six Key Capabilities

BlueFlag translates identity and activity data into governance across your GitHub and Azure DevOps estate:

Identity and Access Visibility

Discover every service principal, PAT, and deployment identity. Map permissions. Detect excessive privileges and toxic role combinations.

Secrets and Credential Management

Inventory hardcoded secrets, API keys, and credentials. Track access, usage, and rotation status. Enforce policies.

Pipeline and Deployment Identity Governance

Govern service connections and deployment identities. Enforce least privilege for pipeline execution. Control environment access.

Behavioural Risk Detection

Baseline every identity. Detect anomalous commits, access patterns, and unusual executions. Correlate data into one risk view.

Configuration and Posture Enforcement

Identify misconfigurations across GitHub and Azure DevOps. Enforce secure development standards and branch protection.

Continuous Compliance and Audit

Generate compliance evidence (NIST SSDF, ISO 27001, DORA, SOC 2) automatically. Maintain audit trails.

GitHub Copilot Governance: Beyond Code Quality

GitHub Copilot commits code directly to your repositories. Each Copilot instance represents a non-human identity with uncontrolled permissions and no audit trail. As Copilot adoption scales across your organisation, so does the risk: Copilot-generated code entering production with unvetted AI logic, Copilot accessing your secrets and credentials, Copilot altering sensitive infrastructure.

BlueFlag's Four Layers of Copilot Control:

- **Copilot Identity and Activity Mapping:** Auto-discovers every Copilot instance across your organisation. Maps each instance as a non-human identity. Tracks which developers use Copilot, how often, and which repositories are receiving Copilot-generated commits.
- **Code Provenance and Audit Trail:** Tracks the origin of every commit: human-written or Copilot-generated. Generates a tamper-evident audit trail for IP protection, regulatory reporting, and M&A due diligence.
- **Behavioural Risk Detection:** Correlates Copilot activity with developer behaviour and pipeline execution to detect anomalies. Flags abnormal patterns (unusual commit spikes, risky code acceptance behaviour, Copilot accessing production credentials) in real time.
- **Policy Enforcement and Compliance:** PolicyGPT authors natural-language Copilot governance policies. Block unapproved Copilot instances, enforce approval workflows, and govern Copilot access to secrets and production environments. Generate compliance evidence automatically for DORA, EU AI Act, SOC 2, NIST SSDF.

GitHub Advanced Security does not provide Copilot identity governance, Copilot activity audit trails, or policy enforcement at the identity layer. That is the critical gap **BlueFlag** closes.

Defender detects threats.
GitHub Advanced Security finds code vulnerabilities.
BlueFlag governs the identities that created them, preventing the conditions that make breaches possible.