BlueFlag Security

DEVELOPER RISK & GOVERNANCE · SOLUTION BRIEF · JULI 2026

Schwachstellen stoppen, bevor sie entstehen

Von der Erkennung zur Prävention an der Quelle.

Organisationen geben Millionen aus, um Schwachstellen präzise zu lokalisieren — und lassen das Verhalten unangetastet, das sie immer wieder erzeugt. In der BlueFlag-Telemetrie verursachen 10–15 % der Entwicklungsteams 85–90 % der neuen Schwachstellen — über Open-Source-Entscheidungen, KI-generierten Code und riskante Workflows.

HIGH-RISK-TEAMS

10–15 %

der Entwicklungsteams verursachen die meisten neuen Security-Findings in Kundenumgebungen

DER NEUEN SCHWACHSTELLEN

85–90 %

des verwundbaren Codes gehen auf diese Kohorte zurück — über OSS-Entscheidungen, KI-Code und riskante Workflows

KI-CODE UNSICHER

45 %

des KI-generierten Codes fällt durch Security-Tests (Veracode 2025, 100+ LLMs getestet)

OSS-DOWNLOADS '25

9,8 Bio.

Open-Source-Downloads in 2025 — jeder einzelne eine ungoverned Supply-Chain-Entscheidung

Quelle: BlueFlag-Plattform-Telemetrie & veröffentlichte Branchenforschung, 2025–26. BlueFlag Security ist als IDC Innovator für Software-Development-Lifecycle-Identität und -Zugriff benannt.

EXECUTIVE SUMMARY

Exzellent im Finden von Schwachstellen. Selten in deren Prävention.

SAST, DAST, SCA, SBOM, CNAPP und ASPM beschreiben, **was falsch ist — nachdem der Code bereits existiert.** Sie finden Defekte im Code, inventarisieren bekannt-verwundbare Komponenten und aggregieren die Findings. Keines dieser Tools governt die Identitäten, KI-Agenten und Workflows, die das Risiko überhaupt erst erzeugen.

Dieses Risiko ist **konzentriert, nicht gleichverteilt** — und es beginnt, bevor der Code existiert: in den gewählten Abhängigkeiten, dem akzeptierten KI-generierten Code und der Art, wie menschliche und maschinelle Identitäten tatsächlich arbeiten. BlueFlag ergänzt Detection-Tools auf der **Präventionsebene** und governt die kleine Kohorte und die vorgelagerten Verhaltensweisen, die den meisten verwundbaren Code produzieren. Es ersetzt sie nicht.

BESTEHENDER STACK — FINDET DIE SCHWACHSTELLEN

- SAST · DAST · SCA · SBOM
- ASPM · CNAPP · Vulnerability Management

Exzellent im Lokalisieren von Schwachstellen in Code, Komponenten und Workloads — den Artefakten, die das Risiko bereits erreicht hat.

→

BLUEFLAG — GOVERNT, WAS DEN CODE ERZEUGT

- **Die Identitäten hinter jedem Commit** — Mensch, Non-Human oder KI-Agent
- **Dependency-Entscheidungen und riskante Workflows** — erkannt zur Commit-Zeit
- **KI-Discovery, Provenienz und Policy-Durchsetzung**
- **Die Hochrisiko-Kohorte von 10–15 %** — governed, bevor Code shippt

WO RISIKO ENTSTEHT

Fünf vorgelagerte Quellen, die Ihre Scanner nie sehen

Open Source

Verwundbare, verwaiste oder bösartige Pakete — gewählt unter Zeitdruck.

KI-Coding-Agenten

Unsichere Muster, halluzinierte APIs und Shadow AI — akzeptiert in den Code.

Entwicklerverhalten

Umgangene Reviews, wiederverwendete Secrets, Direct Commits in Produktion.

Identitätsrisiko

Gestohlene Credentials, schlafende Konten, exzessive Berechtigungen.

Non-Human Identities

Service-Accounts, Tokens und CI/CD-Bots mit mehr Privilegien als Menschen.

PRÄVENTION, GEMAPPT

Jede Risikoquelle — einem Präventions-Control zugeordnet

RISIKOQUELLE	DAS VERHALTEN DAHINTER	BLUEFLAG-PRÄVENTION
Open-Source-Dependencies	Verwundbare, verwaiste oder bösartige Pakete, gewählt unter Zeitdruck.	Policy-Durchsetzung auf Dependency-Entscheidungen; Erkennung riskanten Verhaltens zur Commit-Zeit.
KI-Coding-Agenten	Unsichere Muster, halluzinierte APIs und Shadow AI, akzeptiert in den Code.	KI-Agenten-Inventar; Modell- & Repository-Zugriffs-Governance; KI-Code-Attribution.
Entwicklerverhalten	Umgangene Reviews, wiederverwendete Secrets, Direct Commits in Produktion.	Developer-Risk-Scoring; Durchsetzung von Branch-Protection- und Code-Review-Policies.
Identitätsrisiko	Gestohlene Credentials, schlafende Konten, exzessive Berechtigungen.	Least-Privilege-Durchsetzung, Anomalie-Erkennung, kontinuierliche Access Reviews.
Non-Human Identities	Service-Accounts, Tokens und CI/CD-Bots mit mehr Privilegien als Menschen.	NHI-Inventar und Governance als vollwertige Identitäten über die gesamte Pipeline.

WAS SECURITY-LEADER SAGEN

„Entwickler sind durch die Fortschritte der KI das größte Risiko. Eine Risk-and-Governance-Plattform für menschliche und übermenschliche Identitäten ist ein Must-have in der neuen Welt der Entwicklung.“

David Levin · Chief Information Security Officer, American Express Global Business Travel

DIE PLATTFORM

Eine Plattform. Fünf Governance-Ebenen.

I Identity-Centric Risk

Die einzige Plattform mit identity-first Risiko für Menschen, Non-Human Identities und KI-Agenten — jeweils mit Verhaltens-Baseline.

OUTCOME

Jeder Commit, jedes Review und jedes Deployment einer governeten Identität zuzuordnen.

II Multi-Layered Defense

Eine Plattform über jeden SDLC-Angriffsvektor — Identitäten, Tools, Code und Pipelines — vereinheitlicht statt zusammengeschraubt.

OUTCOME

Die Konsolidierungsebene für Developer-Risiko — nicht noch ein Point-Tool.

III Proactive Risk

Überprivilegierung, IP-Leckage, Insider-Bedrohungen und Tool-Fehlkonfigurationen früh sichtbar machen — bevor verwundbarer Code shippt.

OUTCOME

Die Hochrisiko-Kohorte von 10–15 % sichtbar und governed — nicht erst im Breach entdeckt.

IV Continuous Compliance

Evidenz automatisieren und Policies über disparate Dev-Tools standardisieren — gemappt auf CRA, EU AI Act, NIST SSDF und ISO 27001.

OUTCOME

Audit-ready by default — Evidenz wird erzeugt, nicht rekonstruiert.

V Developer-Friendly

Nahtlose Integration in bestehende Dev-Tools — KI-Coding und riskante Workflows governen, ohne das Team auszubremsen.

OUTCOME

Prävention ohne Entwickler-Friktion — kein Agent, keine Code-Änderungen.

STACK-NATIVE · API-ONLY · POWERED BY THE ACTIVITY INTELLIGENCE GRAPH

Entwickler · NHIs · KI › **Code- & Pipeline-Aktivität** › **BlueFlag Governance** › **SCM & CI/CD** › **SIEM / SOC**

WIE BLUEFLAG FUNKTIONIERT

Connect, Discover, Detect, Remediate — in vier Schritten

1 Connect

Vorgefertigte API-Integrationen mit 60+ SCM-, CI/CD-, IAM-, Registry- und SIEM-Tools — kein Agent, keine Code-Änderungen.

GitHub · GitLab · Jenkins · Okta · Splunk · JFrog

2 Discover

Jeder Mensch, jede NHI und jeder KI-Agent inventarisiert — in einem Identity Graph mit Verhaltens-Baselines.

Menschen · NHIs · KI-Agenten · Tools · Pipelines

3 Detect

Riskantes Verhalten, Überprivilegierung, toxische Kombinationen, KI-Anomalien und Provenienz-Lücken — mit vollem Identitätskontext.

Anomalien · Überprivilegierung · Insider-Risiko · KI-Risiko

4 Remediate

Policy-Durchsetzung in Echtzeit, richtig dimensionierte Zugriffe, SDLC-Posture-Management und kontinuierliche, audit-fertige Evidenz.

Block · Auto-Fix · Alert · Audit

DER RETURN ON PREVENTION

§

80 % weniger manuelle Arbeit

über SDLC-Governance-Aufgaben hinweg — Audit-Vorbereitung und Access Reviews automatisiert.

»

40 % schnellere Remediation

von Identitätsrisiken und Fehlkonfigurationen — behoben an der Quelle, nicht am Symptom.

✓

45 % Tool-Kosteneinsparung

durch Rückgewinnung untergenutzter SDLC-Lizenzen und inaktiver Identitäten.

◉

Wochen → 0 Audit-Vorbereitung

Evidenz automatisch kompiliert, auf Abruf — nicht von Hand zusammengestellt.

WAS SICH DOWNSTREAM ÄNDERT

Continuous Compliance	Evidenz wird kontinuierlich erzeugt — nicht vor Audits zusammengestellt. Secure-by-Design über Cyber Resilience Act, EU AI Act, NIST SSDF und ISO 27001 souverän nachweisen.
Identity- & KI-Governance	Jede menschliche, maschinelle und KI-Coding-Identität governed über den SDLC. Jeder Commit, jedes Review und jedes Deployment voll attribuierbar — schützt IP und ermöglicht vertrauenswürdige KI-Adoption.
Developer-Produktivität	Weniger Rework, weniger Untersuchungen, weniger unnötige Kontrollen. Risikobasierte Guardrails fokussieren Coaching auf die Hochrisiko-Kohorte — und halten leistungsstarke Teams schnell.
Security Operations & MTTR	Weniger, dafür hochwertigere Findings mit vollem Kontext — Entwickler, Repository, KI-Agent und Deployment. Schnellere Attribution bedeutet schnellere Remediation und geringere operative Kosten.

Evidenzbasis: *Veracode 2025 GenAI Report (45 % des KI-generierten Codes fällt durch Security-Tests; 100+ LLMs, 80 Aufgaben); Apiiro 2025 (KI-unterstützte Teams shippen ~4× mehr Code mit ~10× mehr Findings); Sonatype (454K neue bösartige OSS-Pakete in einem Jahr; ~95 % der verwundbaren Pulls hatten zum Download-Zeitpunkt einen verfügbaren Fix); GitGuardian (~2× Secret-Leakage in Copilot-aktiven Repos); Pearce et al. (40 % der Copilot-Vorschläge verwundbar über 89 CWE-gemappte Szenarien).*

EXECUTIVE MESSAGE

„Detection-Tools sagen Ihnen, wo Schwachstellen sind. Sie zu verhindern heißt, die Identitäten, KI-Agenten, Repositories und Workflows zu governen, die Software erzeugen — genau die Ebene, für die BlueFlag Security gebaut wurde.“

BlueFlag Security · Prevent first. Detect second.

Schwachstellen an der Quelle verhindern — in Tagen.

Deployment in <30 Minuten · vollständiges SDLC-Posture-Assessment · priorisierter Report in 48 Stunden

blueflagsecurity.com