



GOVERN WHO — AND WHAT — SHIPS YOUR CODE

The Developer Risk & *Governance Platform* for the AI-driven SDLC.

Every identity operating in your SDLC — human, non-human, and AI — discovered, governed, and audit-ready.

CISO

CSO

APPSEC

blueflagsecurity.com

FIRST MEETING • EXECUTIVE
EDITION



BLUEFLAG SECURITY

BlueFlag Security at a glance

Founded by security veterans. Trusted by global enterprises. Recognized by Gartner and IDC.

LEADERSHIP



Raj Mallempati

Founder & CEO

Microsoft · CloudKnox · MobileIron · VMware



Ken Schneider

Founder

Symantec Enterprise Security · Brightmail



Maya Neelakandhan

VP of Engineering

CloudKnox · Oracle

INVESTORS

Maverick Ventures

KEY CUSTOMERS



ANALYST TRACTION



JAN 2025 · IDC Innovator: SDLC Identity & Access



JAN 2025 · Innovation Insight: AppSec Posture Management



APR 2025 · Market Guide for Software Supply Chain Security



JUN 2025 · Hype Cycle for Platform Engineering



JUL 2025 · Hype Cycle for Agile and DevOps



JUL 2025 · Hype Cycle for Application Security



FEB 2026 · Journey Guide to choosing Software Engineering Security Tools

Four forces are hitting the SDLC — all at once

AI-driven development, an exploding non-human workforce, regulator pressure, and breach economics are reshaping what security leaders are accountable for.



9 in 10

AI is writing your code

Developers use AI tools, often without security approval. AI agents now commit, review and merge.



10×

NHIs outnumber humans

Service accounts, bots, agents and tokens dwarf your human dev population.



5+

Regulators have arrived

NIS2 · NIST SSDF · SOC 2 — supply chain is now a board-level reporting duty.



\$4.9M

Breach economics shifted

Average breach cost. 90% of SDLC attacks now originate at identity, not code.

Source: BlueFlag customer research & published industry benchmarks, 2025–26

Developer breaches are accelerating — and they all look alike

The pattern in every major incident: the way in was an identity, a token or a developer machine — not the code.

MAY 2026

NEW

Poisoned VS Code extension

~3,800 internal GitHub repos exfiltrated from one infected developer device.

MAY 2026

NEW

Megalodon malware

5,500+ GitHub repos backdoored via automated CI/CD injection — in six hours.

2024

PyPI admin token leak

A single leaked GitHub token put 2.6 billion package downloads at risk.

2024

XZ Utils backdoor

Two years spent earning developer trust before planting a supply-chain backdoor.

2023

CircleCI breach

One engineer's laptop compromised — every customer secret exposed.

2022

LastPass vault breach

A DevOps engineer's home computer opened the path to the corporate vault.

KEY TAKEAWAY Not one began with a code vulnerability. Every one began with a developer identity or credential.

90% of SDLC attacks start at identity — not in code

Application Security tools were built for code. The identity layer — human developers, non-human identities, and AI agents — is the overlooked attack surface BlueFlag uniquely governs.



90% · IDENTITY

10% · CODE



Human developers

Insider risk · IP leakage · manual access reviews · malicious behaviour · offshore exposure



Non-human identities

Service accounts · apps · stale tokens · NHI account abuse · excessive permissions



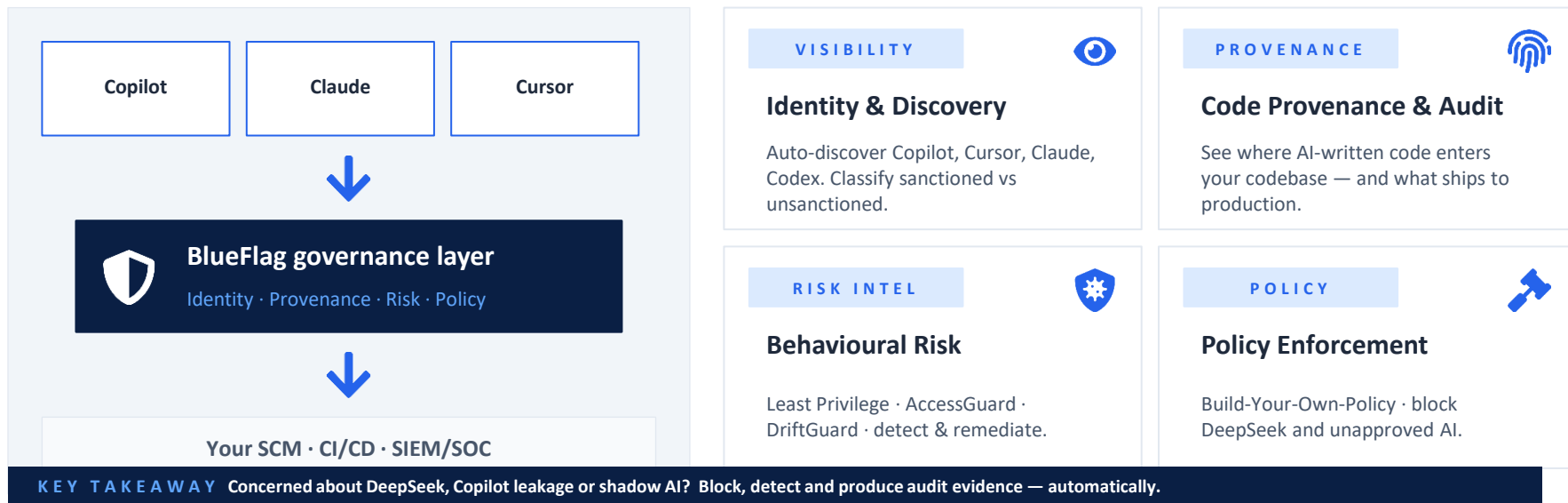
AI agents — newest vector

Unsanctioned usage · autonomous activity · no identity record · no behavioural baseline

KEY TAKEAWAY You AppSec budget funds code security. Attackers use identity. That gap is your exposure.

Every AI agent is an identity. Govern it like one

Discovered, identified, attributed, and policy-enforced — every AI coding tool and agent treated as a non-human identity.



Agentic AI Economics: from token burn to business value.

Give agentic AI an identity, a governance model and a P&L

01 THE BLIND SPOT

Agents already commit, review and merge — with no identity in the IdP, no cost center, no access review.

02 SDLC AGENT ACTIVITY

Agents ranked by real 90-day activity; every commit attributed agent-primary vs. human-primary.

03 SHADOW-AI DISCOVERY

The AI estate you licensed vs. the one you run — unregistered agents become a governed inventory.

04 AI CODING ECONOMICS

Seats, spend, tokens and lines accepted in one dataset — \$ per accepted line, per tool and team.

05 AGENTIC APPLICATIONS · AI-BOM

Where your own repos embed LLMs — the machine-readable inventory EU AI Act & CRA assume exists.

06 AGENT IDENTITY GOVERNANCE

Every agent a first-class identity with an OverPrivilege Score — reviewable like any employee.

Agentic AI is the fastest-growing workforce in your software factory — and the only one with no badge, no manager and no cost center. BlueFlag gives it all three

AGENTIC AI ECONOMICS — THE VALUE CHAIN, EVERY LINK INSTRUMENTED

Spend



Token consumption



Accepted code



Features delivered



Business value

KEY TAKEAWAY What did that feature actually cost in AI spend — and was it worth it? One module answers the CISO, the CFO and the CTO.

Developer Risk & Governance — built for the AI-driven SDLC

Five governance layers. One identity-centric platform. Identity, behaviour, tools, code and compliance — unified, not bolted together.

01**Identity-centric**

Only platform with identity-first risk for humans, NHIs and AI agents — with behavioural baselines.

02**Multi-layered defense**

One platform across every SDLC attack vector — identities, tools, code, pipelines.

03**Proactive risk**

Surface over-privilege, IP leakage, insider threats and tool misconfigurations early.

04**Continuous compliance**

Automate evidence. Standardise policies across disparate dev tools and environments.

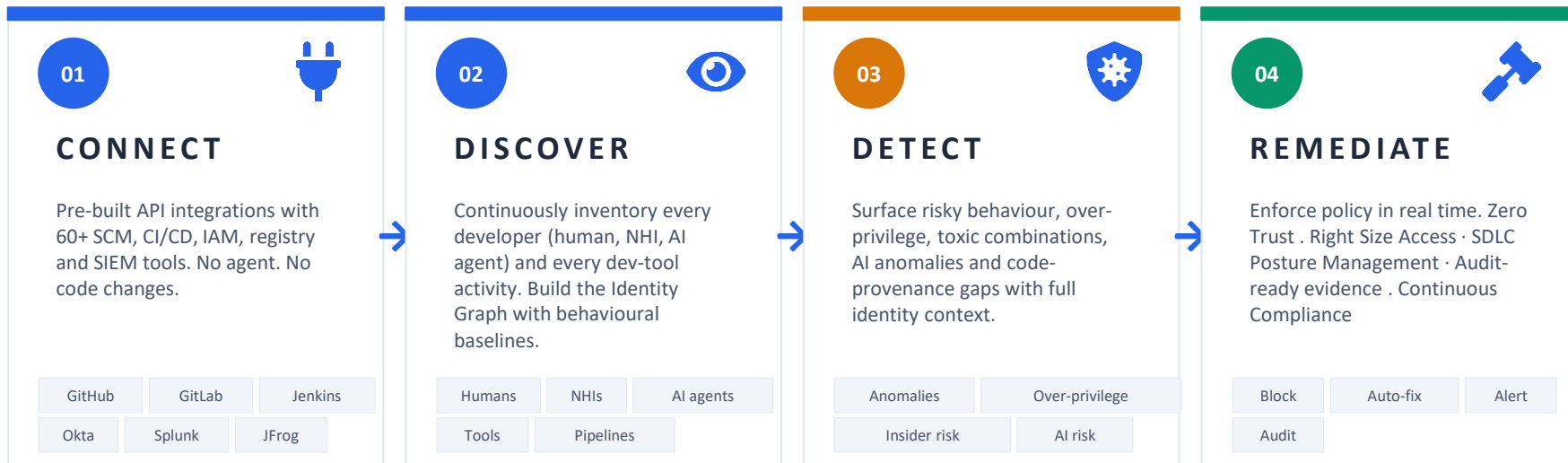
05**Developer-friendly**

Seamless integration with dev tools. Govern AI coding without slowing the team down.

KEY TAKEAWAY Purpose-built for the AI-driven SDLC — code to deployment.

From connect to remediate — in four steps

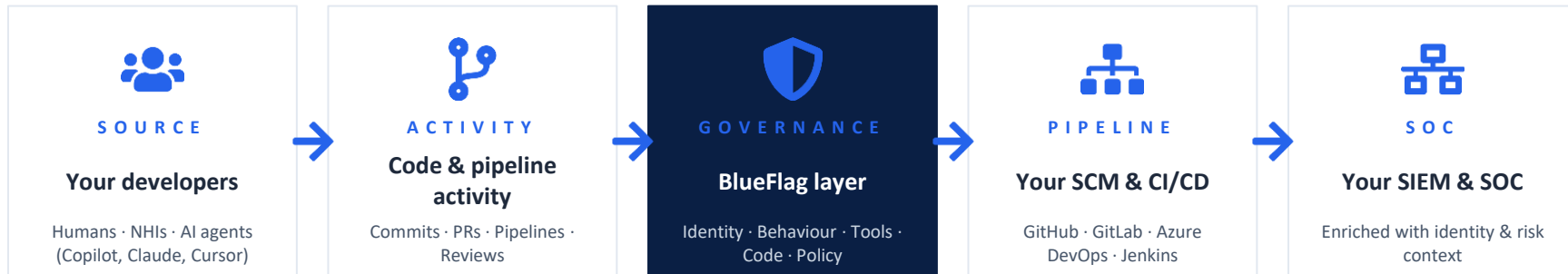
BlueFlag deploys non-intrusively, builds a behavioural baseline across every identity, surfaces correlated risk, and enforces policy in real time.



KEY TAKEAWAY Powered by the activity Intelligence Graph: ML-driven baselining and risk correlation across your SDLC.

Stack-native. API-only. Deployed in minutes

BlueFlag sits as a control plane and governance layer between your developers (human + AI) and your existing SCM, CI/CD and SOC. No agent. No code changes. No developer disruption.



No agent required

API-only connection to existing SCM & CI/CD.



Tool-agnostic

60+ dev tools, every AI coding assistant.



Feeds your SIEM/SOC

Identity-context risk signals enrich detections.



Deployed in minutes

Pre-built integrations across major SCM & CI/CD.

KEY TAKEAWAY Alongside your stack, not inside it — no agents, no code changes, nothing to adopt.

The only identity-centric SDLC security platform

We solve the 75% of SDLC risk everyone else misses — by knowing WHO is doing WHAT across your entire SDLC.

WHAT WE DO DIFFERENTLY



Identity-centric risk

Behavioural baselines for every human, service account, bot and AI agent — one risk view across 60+ dev tools.



Threats caught early

Insider risk, credential abuse and toxic combinations traced to the specific identity — before damage.



Compliance on autopilot

Weeks of audit prep become automated, on-demand reports.

CUSTOMER IMPACT

80%

LESS MANUAL WORK

45%

TOOL COST SAVINGS

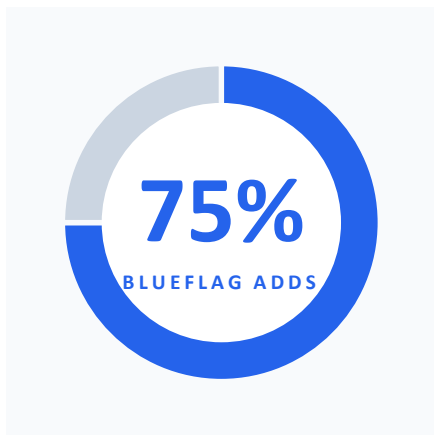
40%

FASTER REMEDIATION

KEY TAKEAWAY The control plane to secure and govern your AI-driven development environment

Your stack covers 25% of SDLC risk. We govern the other 75%

SAST, SCA and ASPM tools scan and detect vulnerabilities in code. Only BlueFlag governs identity, behaviour and AI activity in your developer toolchain.



75% · BLUEFLAG

25% · EXISTING

of SDLC risk that no other tool addresses

LAYER	EXISTING STACK	WITH BLUEFLAG
APPLICATION CODE	SAST · SCA · ASPM scans	Govern WHO writes code
TOOLS & PIPELINES	Partial CI/CD scan	Complete SCM, CI/CD posture
HUMAN DEVELOPERS	—	Discovery, risk (access, permissions, behavior), governance
NON-HUMAN IDENTITIES	—	
AI AGENTS	—	
COMPLIANCE	Manual reports	Continuous, audit-ready evidence

KEY TAKEAWAY SAST, SCA and ASPM scan code. The other 75% of risk is identity — that is BlueFlag.

What changes when you deploy BlueFlag

Every blind spot in your SDLC becomes a tracked, attributable, audit-ready signal.

	✗ WITHOUT BLUEFLAG	✓ WITH BLUEFLAG
Developer identity	No inventory of who — human, NHI or AI — touches your code	Full identity inventory, continuously updated
AI coding	Shadow AI writes, reviews and merges code, ungoverned	Every AI agent discovered, attributed and policy-enforced
Code provenance & IP	AI-generated code with no defensible provenance or ownership	Board-ready provenance for IP ownership, audit and M&A diligence
Behavioural risk	Insider risk and credential abuse surface after the damage	Anomalies caught in real time, with full identity context
Compliance	Audit prep takes weeks of manual evidence-gathering	Continuous, audit-ready evidence generated on demand

KEY TAKEAWAY Every SDLC blind spot becomes a tracked, attributable, board-defensible signal.

Six use cases. One identity-centric platform

From AI governance to M&A — where security leaders realise value with BlueFlag.

01 Govern AI in your SDLC

Discover every AI tool and agent — sanctioned or not. Block unapproved AI; see where AI-written code reaches production.

→ *AI's footprint — visible, governed, enforced.*

02 Stop insider threats & IP loss

Behavioural baselines catch anomalous clones, exfiltration and credential abuse — traced to the identity.

→ *Threats caught before damage, not after.*

03 Govern the non-human workforce

Service accounts, bots and tokens under IAM discipline — discovery, least privilege, lifecycle.

→ *Every NHI accounted for and right-sized.*

04 Harden SDLC posture

Detect and auto-remediate misconfigurations, branch-protection gaps and drift across SCM and CI/CD.

→ *Toolchain posture that stays fixed.*

05 Automate compliance

Continuous, audit-ready evidence mapped to NIST SSDF, ISO 27001 and SOC 2.

→ *Audit prep becomes on-demand reports.*

06 Secure the software in every deal

Assess SDLC risk before the deal, protect IP while it closes, standardise governance across the portfolio after.

→ *Diligence tells the price — we protect the value.*

KEY TAKEAWAY One platform, six ways to prove value — from AI governance to M&A diligence.

Outcomes you can defend to your board and your auditors

Five outcomes you can take to your board within a quarter of deploying BlueFlag.

01	 Board-defensible visibility	Every developer, AI tool and identity in one attributable inventory.
02	 Non-human workforce covered	Service accounts, bots and AI agents as first-class identities.
03	 Audit evidence regulators accept	Mapped to NIST SSDF, ISO 27001 and SOC 2.
04	 Risk signal in your existing SOC	Developer-behaviour anomalies with identity context, in your SIEM.
05	 Policy that's enforced	Real-time blocking of unapproved AI · automated remediation.

KEY TAKEAWAY Five board-defensible outcomes — within one quarter of deployment.

See your SDLC risk in 48 hours. No cost

30 minutes to deploy. 48 hours to board-ready evidence.

01

DEPLOY

<30 minutes · No agent · Zero developer friction



02

DISCOVER

Full assessment of your SDLC security posture — every identity, tool and pipeline



03

REPORT & ACT

Detailed report in 48 hours with prioritised, board-ready remediation

NEXT STEP Deploy this week via API — no agent, no code changes, zero developer friction.



Thank you

Developer Risk & Governance Platform — purpose-built for the security leaders accountable for what every developer (human, non-human, AI agent) ships into production

CISO

CSO

APPSEC



Run Mythos at enterprise scale — governed from day one

Mythos operates across your SDLC as a non-human identity. BlueFlag provides the visibility, provenance and controls to run it safely.

01	Complete visibility	Auto-discover, classify every agent — who has it, where it runs, what it accesses
02	IP & compliance protection	Provenance, attribution for Mythos-authored code — board-ready evidence
03	Real Time Behavioral risk intelligence	Out-of-scope actions — unexpected commits, privilege escalation — signalled to your SOC.
04	Continuous Compliance	Block high-risk actions, require human-in-the-loop review, generate audit evidence automatically

KEY TAKEAWAY Mythos at enterprise scale — with complete governance and board-defensible audit evidence.

The window is open. First movers set the standard

Developer-driven risk is outrunning regulation and traditional AppSec. The category is being defined right now — and security organisations that act first will set the standard.

01**Adoption outpacing controls**

AI coding, non-human identities and developer velocity are accelerating faster than your governance frameworks can keep up.

02**Regulation is now in force**

NIS2, NIST SSDF and SOC 2 expectations are tightening across the software supply chain — and boards are asking for evidence.

03**No integrated tool exists**

No platform unifies developer identity, behaviour, tools and code governance — until BlueFlag.

04**First movers set the standard**

Security orgs governing the SDLC now avoid the next wave of breaches and become the reference for their industry.

KEY TAKEAWAY Govern the SDLC now — or inherit someone else's standard.

Developer identities are the SDLC's biggest blind spot.

AI agents are exploding across SDLC environments — as superhuman identities that must be governed.



Developers are the biggest risk because of advancements in AI. A Risk and Governance Platform for human and superhuman identities is a must-have in the new world of development.

DAVID LEVIN

Chief Information Security Officer · American Express Global Business Travel

The governance layer for AI development at scale

Mythos operates across your SDLC as a non-human identity. Without governance you have no visibility into what it does, no provenance on what it writes, and no way to enforce policy.

01	Complete Mythos visibility	Auto-discover and classify every Mythos agent — who has it, where it runs, what it accesses. Continuous, no agent required.
02	IP & compliance protection	Full provenance and attribution for Mythos-authored code — board-ready evidence for regulatory inquiry, M&A diligence and IP claims.
03	Real-time behavioural risk intelligence	Detect out-of-scope actions — unexpected commits, privilege escalation, policy drift — signalled to your SOC.
04	Policy enforcement & continuous compliance	Block high-risk actions, require human-in-the-loop review, generate audit-ready evidence automatically.

KEY TAKEAWAY Mythos at scale — governed and audit-ready from day one.

BlueFlag Security Customers at a Glance

KEY TAKEAWAY In production across FinServ, healthcare, media and manufacturing — not pilots.

A global FinTech standardises SDLC across in-house, M&A and contractors

Vast international developer org. Land-and-expand from 2,000 to 4,000+ licences over 5 quarters as new use cases come online.

2,500+

DEVELOPER IDENTITIES

Industry · Global FinTech

Scale · Multi-region, M&A active



CHALLENGES

- Over-privileged identities across a sprawling, multi-region SDLC
- Inherited tech stacks from forthcoming M&A activity to normalise
- Legacy code-scanning infrastructure ripe for displacement



SOLUTION

- Auto-curtail over-privileged identities & remediate risky behaviour
- Normalise WU policies across inherited tools and external environments
- Track over-entitled human + non-human identities; right-size access



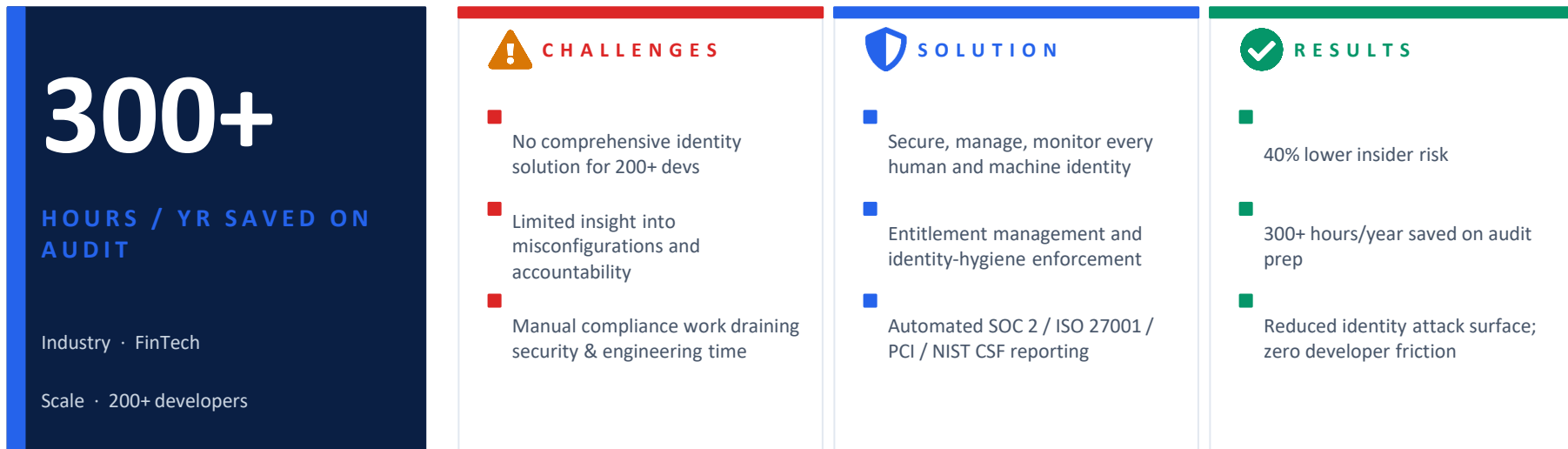
RESULTS

- Land at 2,000 licences → forecast 4,000+ within 5 quarters
- Expansion into offshore dev risk, CI/CD observability, M&A diligence
- 3-year forecast renewal & expansion at \$750K

KEY TAKEAWAY 2,500+ developer identities governed across in-house, offshore and M&A environments.

A FinTech automates developer governance and audit

200+ developers, SOC 2 / ISO 27001 / PCI / NIST CSF — but limited visibility into developer identities and tool configurations.



KEY TAKEAWAY 300+ audit hours saved per year — developer governance and compliance on autopilot.

A global CX leader hardens its SDLC identity surface

Manual permissions and tool misconfigurations were creating SDLC risk across a distributed engineering org.

40%+

CI TOOL LICENCE
SAVINGS

Industry · CX / SaaS

Scale · Global engineering org



CHALLENGES

- Permission drift — manual processes opened unauthorised access
- High licence costs — significant spend on unused CI tool licences
- Team-membership drift — frequent team changes creating hidden risk



SOLUTION

- Proactive identity security — automated monitoring & remediation
- Comprehensive risk mitigation — fixed excessive permissions
- Cost-efficient licensing — identified every inactive identity



RESULTS

- 40%+ savings on CI tool licences
- Reduced unauthorised access via automated permissions
- Enhanced security posture — continuous team monitoring

KEY TAKEAWAY 40%+ CI tool licence savings while hardening the SDLC identity surface.

Secure the software in every deal

For software companies, value lives in the SDLC — exactly the part traditional M&A diligence overlooks.

BEFORE THE DEAL

01

Pre-acquisition due diligence

SDLC Maturity & Risk Assessment across developer identities, repositories, CI/CD, AI usage and software supply chain — scored to support valuation.

DURING THE DEAL

02

Transaction protection

Monitor developer and contractor access, detect anomalous repository activity, govern time-bound advisor access, protect IP with least privilege.

AFTER THE DEAL

03

Portfolio governance

Standardise identity and repository policies across portfolio companies, measure engineering risk, report with portfolio-wide executive dashboards.

KEY TAKEAWAY Diligence tells you the price — BlueFlag protects the value, before, during and after the transaction.