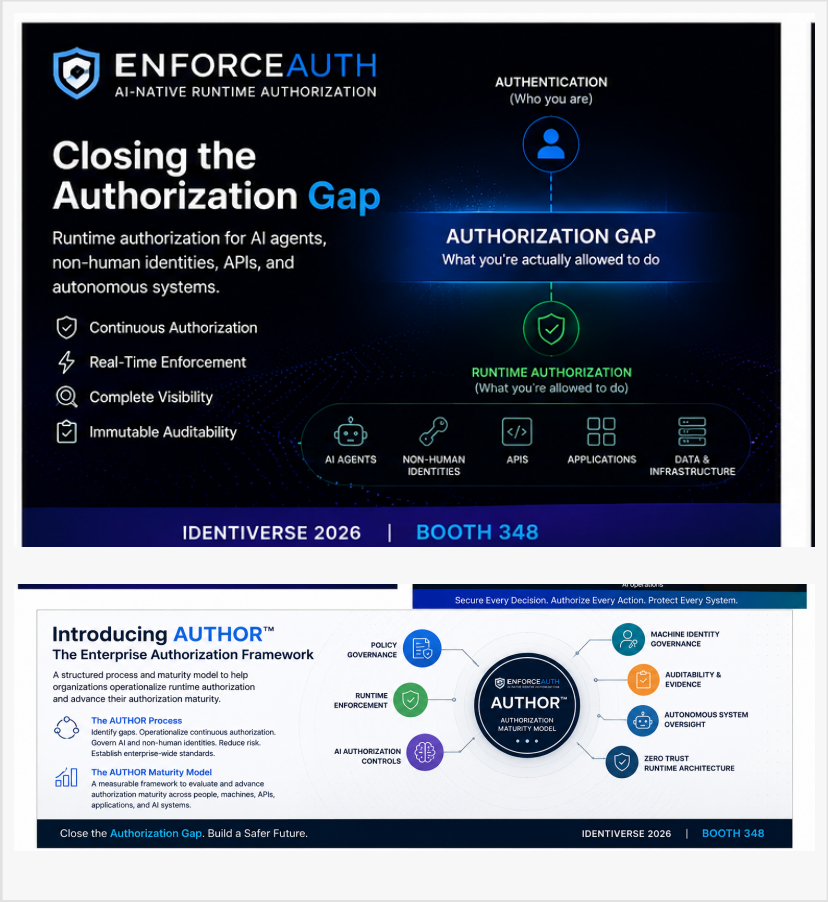
EnforceAuth to Unveil New AI Runtime Authorization Platform Innovations at Identiverse 2026 — Booth 348

Company to Introduce AUTHOR™ Authorization Framework, AUTHOR Maturity Model™, and Four New Runtime Enforcement Components



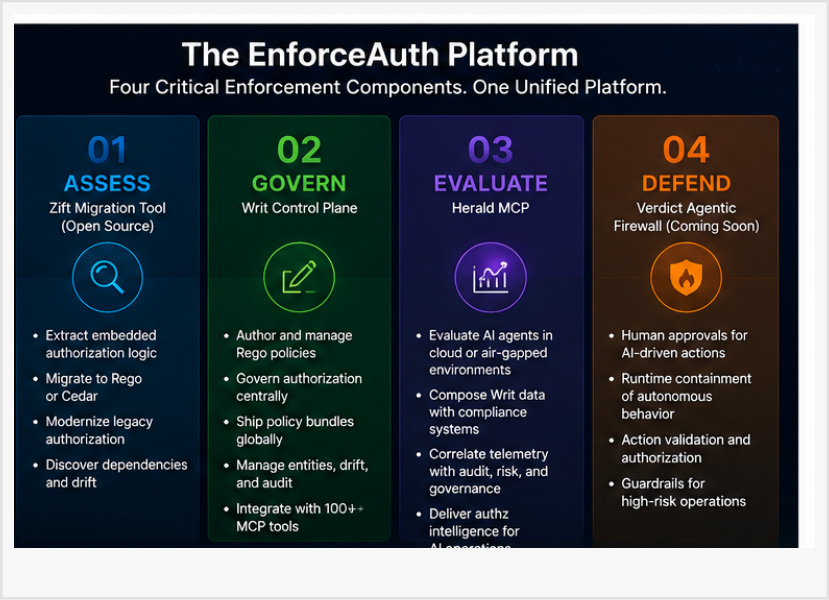
SAN DIEGO, CA, UNITED STATES, May 20, 2026 /EINPresswire.com/ -- EnforceAuth, the AI-native runtime authorization company pioneering the enterprise “Authorization Gap” category, today announced it will exhibit at Identiverse 2026 at Booth 348, where the company will unveil major new platform innovations focused on runtime enforcement for AI agents, non-human identities, APIs, and autonomous systems.

During the event, EnforceAuth will conduct hands-on demonstrations, technical architecture walkthroughs, and executive briefings showcasing its next-generation runtime authorization platform alongside a new enterprise authorization methodology called AUTHOR™ and the newly introduced AUTHOR Maturity Model™.

The announcements come as enterprises increasingly confront a growing security problem created by autonomous AI systems operating with insufficient runtime governance, excessive privileges, and limited policy enforcement after authentication. EnforceAuth defines this industry-wide problem as the Authorization Gap.

“Identity answers who logged in. Authorization determines whether the AI should have been allowed to act at all,” said Mark O. Rogge. “AI agents, APIs, and machine identities are now making autonomous decisions inside critical systems at machine speed. Runtime authorization

is becoming the control plane for enterprise AI security.”



New Platform Announcements at Booth 348

At Identiverse 2026, EnforceAuth will formally introduce four critical enforcement components within the EnforceAuth platform architecture:

01 — Assess
Zift Migration Tool (Open Source)

Designed to help enterprises extract embedded authorization logic into policy-as-code, migrate hardcoded authorization into Rego or Cedar, modernize legacy authorization architectures, and identify fragmented authorization dependencies across applications, APIs, middleware, and AI orchestration systems.

02 — Govern
Writ Control Plane

A centralized runtime authorization governance layer that enables organizations to author Rego policies, ship policy bundles globally, govern entity relationships, monitor policy drift, manage audit operations, and integrate with more than 100 MCP tools and enterprise workflows.

03 — Evaluate
Herald MCP

Built to evaluate AI agents in cloud or air-gapped environments while composing authorization telemetry with enterprise compliance, audit, risk, and governance systems to operationalize runtime authorization intelligence across regulated environments.

04 — Defend
Verdict Agentic Firewall (Coming Soon)

A new runtime enforcement model designed to govern autonomous AI systems through human approvals for AI-driven actions, runtime containment, action validation, and enforcement guardrails for high-risk AI operations.

Introducing AUTHOR™ and the AUTHOR Maturity Model™

EnforceAuth will also introduce AUTHOR™, a structured enterprise authorization framework

designed to help organizations operationalize continuous runtime authorization across AI systems, machine identities, APIs, applications, and distributed infrastructure.

AUTHOR™ is designed to help enterprises:

identify runtime authorization gaps
reduce excessive privileges
govern AI-driven systems
operationalize continuous authorization
improve auditability and compliance evidence
establish runtime enforcement standards

The company will additionally unveil the AUTHOR Maturity Model™, a framework for evaluating authorization maturity across:

runtime enforcement
policy governance
AI authorization controls
machine identity governance
auditability
autonomous system oversight
Zero Trust runtime architecture
Live Demonstrations at Identiverse

EnforceAuth demonstrations at Booth 348 will include:

runtime authorization for AI agents and autonomous systems
fine-grained authorization using policy-as-code
dynamic ABAC and contextual authorization
real-time API and microservice authorization enforcement
non-human identity governance
runtime AI guardrails for agentic systems
sub-millisecond authorization decisioning
immutable authorization telemetry and audit evidence generation
continuous authorization across multi-agent orchestration workflows

“AI agents no longer need to break into systems,” added Rogge. “They authenticate legitimately and exceed their authority autonomously. Detection tools may tell you what happened afterward. Runtime authorization determines whether the action should have been allowed in the first place.”

Security leaders, IAM architects, enterprise architects, AI platform teams, analysts, and CISOs are encouraged to stop by Booth 348 for live demonstrations and deep technical discussions.

Private executive briefings and technical meetings may be requested at:

www.EnforceAuth.com/contact

Mark Rogge
EnforceAuth
+1 612-868-7193
email us here
Visit us on social media:
LinkedIn
