

EnforceAuth Announces Integration NVIDIA OpenShell to Deliver Continuous Authorization Governance AI Agent Deployments

Somewhere in your enterprise, An AI agent is running right now that shouldn't be...

SAN DIEGO, CA, UNITED STATES, March 31, 2026 /EINPresswire.com/ --

EnforceAuth, Inc. today announced support for NVIDIA OpenShell, combining kernel-level execution isolation with continuous identity and authorization governance for enterprise AI agent environments. The integration — arriving in the coming weeks — addresses a structural gap that has remained unresolved in enterprise security architecture as AI agent adoption accelerates.

The announcement coincides with remarks from NVIDIA CEO Jensen Huang at GTC 2026, where he described the current period as the beginning of an inflection point.

Industry analyst research has identified authorization governance across non-human and AI identities as an emerging priority for enterprise security teams.

Market Context

Enterprise AI adoption has created a class of non-human identities operating at machine speed, with permissions granted at provisioning and rarely revisited. Research indicates that 82 non-human AI identities exist for every human user in enterprise environments today, and the average cost of an AI-related data breach reached \$4.9 million in 2025 (IBM) — with

The Complete AI Agent Security Stack: Closing the Authorization Gap

Joint Architecture of **EnforceAuth** (Authorization Fabric) & **NVIDIA OpenShell** (Execution Isolation) for Autonomous Enterprise AI Agents.

THE AI AUTHORIZATION CRISIS

82:1
Ratio of Non-Human Identities (lacking continuous governance)

\$4.9M
Average AI Data Breach Cost (stemming from authorization failures).
According to IBM (2025)

The "Politeness Trap"
Mistaking AI safety (content filters) for security.

Enterprise: AI Agent Runtime
Executes tasks & maintains context (e.g., Claude Code, LangGraph)

Layer 5: AI Agent Runtime

Layer 4: NVIDIA OpenShell
NVIDIA OpenShell: Sandboxes, Name-space control, and thread-level

Layer 3: EnforceAuth Connector
Joint (EA-NV): Transition Layer Synchronizes EnforceAuth policies to Sandboxed configurations

Layer 2: Authorization Fabric
EnforceAuth: Identity & Policy Plane Continuous enforcement. Context & device info - session ID revealed

Layer 1: Compliance & Audit
High-velocity Automated evidence reported to SOC, SCC, etc

BUSINESS OUTCOMES & COMPLIANCE

Regulatory Ready: DORA & EU AI Act Meets Article 16 (DIT risk management) and Article 9 (governance controls) with per-agent audit trails.

Operational Efficiency via Policy-as-Code Uses OPA/Rego, eliminating manual spreadsheets.

Board-Ready Reporting Real-time view, converting execution logs into business compliance reports.

Closing the AI Agent Authorization Gap: The EnforceAuth + NVIDIA OpenShell Security Stack

THE PROBLEM: THE AUTHORIZATION GAP

82:1 Non-Human Identity Ratio

The "Politeness Trap"

\$4.9M Average Cost of AI Data Breaches

Polite AI is not secure AI.

THE MID-SESSION REVOCATION RISK

WITHOUT CONTINUOUS AUTHORIZATION: Agent continues executing dozens of unauthorized API calls even after credentials are revoked.

WITH ENFORCEAUTH & OPENSHELL: Request is **DETECTED & DENIED** immediately at the moment of execution.

THE SOLUTION: A FIVE-LAYER SECURITY STACK

LAYER 1: IDENTITY ASSERTION (Enterprise IDP)
Validates identity provider tokens.

LAYER 2: ENFORCEAUTH AUTHORIZATION FABRIC
Provides continuous identity assertion and group-agent scope enforcement using an OPA/Rego policy engine.

LAYER 3: FC CONNECTOR & TRANSLATION BRIDGE
Synchronizes EnforceAuth policies directly into OpenShell sandbox configurations, ensuring a single source of truth for security.

LAYER 4: NVIDIA OPENSHELL EXECUTION ISOLATION
Uses Linux Security Modules (LSM) and Process Isolation (PI) to create kernel-level sandboxes that control operations, memory, and process flow.

LAYER 5: HARDWARE & OS SECURITY (TPM) (Secure Boot)
Provides fundamental hardware root of trust.

COMPARING CAPABILITIES

Capability	EnforceAuth (Identity Fabric)	NVIDIA OpenShell (Execution Isolation)
Core Operation	Policy Enforcement	Kernel-level Execution
Enforcement Layer	Authorization Fabric	OS Kernel Sandboxing
Identity Assertion	Continuous SaaS Types	None
Mid-session Revocation	Detective & Denial	Not Visible
Policy Language	OPA / Rego	YAML, Declarative
Compliance Output	Audit Decision Records	Execution Event Logs

BUSINESS VALUE & COMPLIANCE

CONTINUOUS COMPLIANCE FOR DORA & EU AI ACT
The joint stack provides the high-velocity, structured authorization decision records required by Article 16 of DORA and Article 9 of the EU AI Act.

PREVENTION OF SCOPE ESCALATION
EnforceAuth enforces that when an agent operates a sub-agent, the child authorization scope only narrows and never expands beyond the parent's permission.

POLICY-AS-CODE EFFICIENCY
Uses OPA/Rego, automating updates to be reviewed, tested, and deployed like software, eliminating manual spreadsheet-based management.

"The Joint Architecture is Obvious Once You See It"
OpenShell enforces what agents can execute, while EnforceAuth enforces who is authorized to execute it.

authorization failure cited as the underlying cause rather than model behavior.

The security industry has historically addressed AI risk through endpoint protection and behavioral controls. Endpoint and network security platforms provide threat detection and execution monitoring. They are not designed to govern whether an AI agent remains authorized to act after it has been provisioned — a distinct and unaddressed problem. Behavioral guardrails and content filters address model outputs. They do not revoke credentials mid-session or enforce scope boundaries across agent-to-agent interactions. The result is an Authorization Gap: no existing security category continuously governs AI agent identity at the moment of action.

The Integration: OpenShell and EnforceAuth

NVIDIA OpenShell — an open source runtime that enforces policy-based security, network and privacy guardrails that make autonomous agents safer to deploy. — NVIDIA Official Press Release, March 16, 2026, GTC 2026, San Jose

NVIDIA OpenShell enforces what agents can execute — providing kernel-level sandboxing, filesystem and network control, and process isolation via Landlock LSM and Seccomp BPF. It answers the question: can this agent perform this operation?

EnforceAuth addresses the prior question: is this agent authorized to operate at all? The two systems answer different questions. Both are required for a complete security posture. Neither is sufficient on its own.

Five-Layer Architecture

The joint architecture operates across five layers:

- Layer 5 — Agent Runtime: Claude Code, LangGraph, OpenClaw, and other agent frameworks execute within a governed perimeter.
- Layer 4 — OpenShell: Kernel isolation via Landlock LSM and Seccomp BPF governs execution.
- Layer 3 — Connector: OPA/Rego policies are translated directly into OpenShell sandbox configurations.
- Layer 2 — Authorization Fabric: Continuous identity verification, cross-agent scope enforcement, and real-time mid-session revocation are applied to all human and non-human identities.
- Layer 1 — Compliance Record: Hash-chained audit logs are generated automatically, mapped to DORA, SOC 2, and EU AI Act Articles 9 and 16.

A key capability of the joint stack is scope escalation prevention. When a parent agent spawns a sub-agent, that child agent's authorization scope can only narrow, never expand. Execution-layer tools do not have visibility into what the parent agent was authorized to do. EnforceAuth enforces this constraint at every hop — closing a vulnerability class that runtime sandboxing alone cannot address.

QUESTION NVIDIA OPENSHELL ENFORCEAUTH

Core Question Can this agent execute this? Is this agent authorized to act at all?

- Identity Awareness -None -Continuous — all identity types
- Mid-Session Revocation -Not visible -Detected & denied in real time
- Sub-Agent Scope -Not enforced -Child scope cannot exceed parent
- Policy Language -YAML declarative -OPA / Rego — policy-as-code
- Compliance Output -Execution event logs -Hash-chained auth decision records

The two systems answer different questions. Both are necessary. The joint stack is the complete answer.

Statement from EnforceAuth

"Jensen Huang identified policy engines as a required component of enterprise AI at GTC — not firewalls, not content filters. Policy engines. That is the category EnforceAuth was built for. NVIDIA built the most powerful AI execution infrastructure in the world. EnforceAuth provides the authorization layer that makes it safe to run inside an enterprise. OpenShell governs what agents can execute. EnforceAuth governs who is authorized to execute it. Any enterprise running one without the other has a gap. That gap carries a \$4.9 million average cost." — Mark Rogge, CEO and Founder, EnforceAuth, Inc., San Diego, CA, March 2026

Deployment and Availability

Any enterprise currently running NIM microservices, DGX Cloud, OpenClaw, LangGraph, or Claude Code is operating inside the Authorization Gap. EnforceAuth is in active deployment conversations with organizations across financial services, healthcare, and critical infrastructure — sectors where authorization failure carries regulatory penalties.

The NVIDIA OpenShell integration arrives in the coming weeks. A live technical briefing is scheduled for enterprise security leaders and AI infrastructure architects.

Key Statistics

- 82:1 Non-human AI identities to every human user in enterprise environments today
- \$4.9M Average cost of an AI data breach in 2025 (IBM); root cause: authorization failure, not model behavior
- 0 Existing security vendors providing continuous authorization governance across the AI agent identity plane prior to this announcement

Mark Rogge

EnforceAuth

+1 612-868-7193

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/902133285>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.