Vendor Profile

FIOR Vendor Profile: Enforcing Agentic Identity and Governance for the AI Era

Duncan Brown Emanuel Figueroa

IDC OPINION

FIOR is addressing emerging changes in AI agent security and governance through its patented identity infrastructure and enforcement-centric approach. Unlike traditional identity and access management (IAM) or AI security platforms that focus on detection or compliance reporting, FIOR enforces cryptographic identity and policy at the network boundary and agent level. Its Gateway and Auth products deliver cryptographically anchored authentication and real-time policy enforcement for AI agents, machines, and IoT, addressing the emerging risks of agentic automation in critical sectors. FIOR's focus on trust enforcement, rapid revocation, and audit-grade governance positions it as a differentiated player in the rapidly evolving AI security landscape.

This reflects a broader shift in AI security toward deterministic control of autonomous systems, rather than retrospective visibility into their behavior.

IN THIS VENDOR PROFILE

This vendor profile examines FIOR's enforcement-centric approach to AI agent security and governance, with a particular focus on its Gateway and Auth products. It highlights how FIOR differentiates itself by providing cryptographically anchored identity and real-time policy enforcement for AI agents and machines, addressing critical risks in sectors such as telecom, space, and banking. The profile also assesses FIOR's commercial prospects, noting its rapid early traction, competitive pricing, and strong positioning in the emerging market for agentic identity infrastructure.

SITUATION OVERVIEW

Company overview

Founded in the U.K. in 2024, FIOR.Group Limited (FIOR) launched its general availability products in 2026. The firm targets the identity and governance gap created by the proliferation of autonomous AI agents. A team leads the company with deep experience in

telecom, security, and cryptography, and has secured venture funding from founders and institutional investors. FIOR's founders bring extensive experience in telecommunications, security, and cryptography, including 56 granted patents spanning immutable audit trails, sub-second revocation, and hardware-rooted agent identity, and have previously received industry recognition, including the GSMA GLOMO CTO Choice Award and IDC Innovator status in post-quantum cryptography.

Company strategy

FIOR's company strategy is built around positioning itself as foundational infrastructure for AI agent identity, governance, and enforcement. Rather than focusing on compliance documentation or post hoc detection, FIOR's approach is to enforce governance at the infrastructure level, ensuring that AI agents are cryptographically identified, governed by policy, and can be rapidly revoked if a breach occurs. This enforcement-centric model creates audit-grade evidence by default, supporting both operational assurance and regulatory compliance.

FIOR's go-to-market (GTM) strategy targets enterprise buyers in high-risk sectors (such as telecom, space, and banking) who require deterministic control over autonomous agents. The company differentiates itself by selling trust, control, and accountability, not just dashboards or compliance reports. Its API-first integration model and rapid deployment (no software development kit [SDK] or infrastructure changes required for Gateway) are designed to lower adoption barriers. FIOR's marketing emphasizes its ability to provide real-time, policy-driven enforcement and auditability, positioning itself as infrastructure that enables enterprises to move beyond traditional security and compliance tools toward proactive, agentic risk management.

Key facts snapshot

- Core offerings:
  - FIOR.Gateway — network boundary enforcement for AI agents
  - FIOR.Auth — autonomous agent/machine authentication and governance
  - FIOR.MobileShield — endpoint protection for mobile devices
  - FIOR.Voice — cryptographically-bound voice authentication
  - GTM — SaaS and enterprise license, direct and channel sales
  - Target verticals — space and aerospace, telecom, banking, supply chain, sovereign cloud, government/defense
  - Early traction — deployments in space/aerospace, telecoms, and banking; partnerships with standards bodies (e.g., GSMA CAMARA API Gateway)

Product focus

FIOR.Gateway

FIOR.Gateway is a software-based enforcement plane deployed at the network boundary to verify, govern, and, if necessary, rapidly revoke AI agents entering the environment. It authenticates agents with FIOR.Auth identities in millisecond-scale time, assigns temporary identities to unknown agents, and enforces policy through more than 60 configurable controls across five engines (AI threat detection, runtime policy, zero trust, exploit prevention, and policy templates). Revocation of compromised agents is propagated globally, with millisecond-scale propagation across all FIOR.Gateway instances, supporting rapid containment and auditability. No SDK or infrastructure changes are required for deployment, supporting frictionless adoption.

FIOR.Auth

FIOR.Auth provides the identity and governance layer for AI agents and machines, integrating via SDK and API into closed networks or applications. Each agent receives a unique, cryptographic identity at creation or arrival, is linked to a responsible operator, and is governed by granular, policy-driven permissions. The platform supports over 60 APIs across 11 categories, enabling full auditability, rapid revocation, and the generation of compliance evidence. Built on National Institute of Standards and Technology (NIST)-standardized post-quantum cryptography (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA), with authentication assurance aligned to NIST SP 800-63 AAL3, FIOR.Auth operates autonomously at scale and is compatible with existing infrastructure.

Differentiators

FIOR's key differentiator is its three-party trust model. This establishes a chain of accountability and enforcement for AI agent authentication and governance. In this model:

- Provider (such as OpenAI, Anthropic, or an internal certification authority [CA]) acts as the certificate authority, vetting operators, issuing cryptographically signed certificates, maintaining revocation lists, and publishing public keys.
- Operator (enterprise, developer, or start-up) applies for certificates, deploys AI agents, operates within defined constraints, and is responsible for renewing certificates and reporting compromises.
- Gateway (enterprise security boundary) validates agent certificates, checks trusted certificate authorities, enforces access policies, blocks unauthorized agents, and logs every event for audit and compliance.

This architecture guarantees that every agent action is authenticated, authorized, non-repudiable, and instantly revocable. Unlike traditional public key infrastructure (PKI), FIOR's

trust chain is designed for continuous, per-action validation and real-time revocation, tailored specifically for AI agents and their operational constraints.

Other key features include:

- **Enforcement, not documentation**. Governance is enforced at the network boundary in real time, not reported after the fact.
- **Quantum-safe, hardware-rooted identity**. Agent identities anchored to a Trusted Platform Module (TPM) and Secure Enclave with NIST FIPS 203/204/205 algorithms; supports continuous attestation and offline verification.
- **Millisecond-scale global revocation**. Policy breaches trigger near-instant revocation across every FIOR.Gateway instance worldwide.
- **Audit-grade evidence by default.** Every agent action is signed, hash-chained, and exportable for regulator review.
- **On-premise or cloud deployable**. Self-hostable on K3S and Kubernetes with no external dependencies — supports EU, U.K., and government deployments.
- **API-first, Zero-SDK adoption**. Gateway requires no agent-side code changes; Auth integrates via API or SDK.

Commercial prospects

FIOR is positioned for growth in sectors where identity or security failure is catastrophic (space, telecom, banking, supply chain, sovereign cloud, etc.). The company estimates a total addressable market (TAM) of tens of billions of dollars for agentic identity and authentication, with pricing positioned competitively relative to alternative approaches. Early commercial proposals feature aggressive policy bundling, low entry price points, and flexible licensing. Financial projections indicate a strong potential revenue ramp from FY26 to FY30, with Auth and MobileShield as primary drivers.

FIOR's infrastructure-centric approach and focus on trust enforcement, rather than post-hoc detection, differentiate it from competitors such as Protect AI and Koi (both acquired by Palo Alto Networks) and Credo AI. It is an increasingly crowded space, with Microsoft launching Entra Agent ID and Cisco acquiring Astrix Security.

In terms of more direct competition, think of Teleport's Beams. This comparison reflects a broader shift in how infrastructure access and authorization are being reconceptualized in the age of AI.

In contrast, FIOR's architecture is more narrowly optimized around the deterministic control of AI agents and machines. Its emphasis on runtime policy enforcement, rapid revocation, and audit-grade governance reflects a focus on constraining autonomous behavior where risk concentration is highest, particularly in regulated and high-impact environments.

IDC views these approaches as largely complementary. Teleport addresses identity modernization at the infrastructure layer, while FIOR targets enforcement and governance challenges specific to autonomous agents. As agentic AI adoption accelerates, some organizations may adopt FIOR tactically to govern high-risk agent workloads, while others may pursue broader identity replatforming initiatives aligned with Teleport's infrastructure-centric model. Over time, overlap between infrastructure identity and agent governance is likely as market boundaries continue to evolve.

FUTURE OUTLOOK

Broader adoption of enforcement-centric agentic identity platforms will depend on the ability to scale deployments, maintain technical differentiation, and educate the market on the necessity of agentic identity infrastructure. As AI agent adoption accelerates and regulatory scrutiny increases, FIOR's enforcement-first model and cryptographic architecture are well-positioned to address enterprise and regulated sector demand. The next phase will require building out reference customers, expanding integration partnerships, and demonstrating operational resilience at scale. Time is a key factor as companies build their agentic infrastructures: gaining critical scale by 2028 is essential.

ESSENTIAL GUIDANCE

Advice for FIOR

Visualize continuous agent discovery and governance

Provide customers with dashboards and tools for agent registration, ownership assignment, risk classification, and lifecycle management. This aligns with IDC's five-pillar governance framework and addresses the growing risk of agent sprawl and shadow AI.

Deliver unified, telemetry-native identity and policy enforcement

Advance FIOR's Gateway and Auth products to unify identity issuance, attestation, authorization, and runtime controls into a single evidence and decision plane. Ensure every agent action is observable, attributable, bounded, and reversible, with regulator-grade audit trails. Integrate identity telemetry with security operations (SecOps) for real-time detection, session kill, and rapid containment, as recommended by IDC's Agent Governance Fabric model.

Prioritize interoperability and orchestration standards

Support emerging standards for agent communication (e.g., Model Context Protocol [MCP], Agent2Agent [A2A] messaging) and orchestration patterns (sequential, hierarchical, collaborative). Enable customers to coordinate multiagent workflows securely and efficiently,

preventing agent silos and redundant development. This will position FIOR as a platform for scalable, composable agentic architectures.

Embed sovereignty, compliance, and economic controls by design

Build compliance mapping (EU AI Act, NIST AI RMF, ISO 42001, sectoral regulations) and explainability mechanisms into the core of FIOR's offerings. Provide tools for policy-as-code, automated compliance checks, and audit-ready evidence. Additionally, help customers monitor and optimize agent economic impact (token/call usage, cost per transaction) to prevent budget overruns and support ROI justification.

AI sovereignty is a dimension of an AI strategy that describes the ability to have free choice and control over the design, development, deployment, accessibility, operation, maintenance, and governance of AI systems and applications, and the technologies that those systems and applications depend on. AI Sovereignty is a key consideration for many organizations, and FIOR should emphasize its technologies that promote aspects of sovereignty, such as privacy, governance, and AI access control.

Invest in customer education, cross-functional engagement, and reference architectures

Develop programs and collateral to educate customers on agentic AI risks, governance best practices, and the operational value of enforcement-centric identity. Engage with CAIOs, CISOs, and AI centers of excellence to co-create use cases and reference architectures. Support cross-functional governance teams and provide guidance for phased adoption, pilot selection, and continuous improvement, as emphasized in IDC's 90-day agent governance launch plan.

LEARN MORE

Related research

- *RSAC 2026: Data Security Is a Top Priority for Agentic AI* (IDC #IcUS54471026, April 2026)
- *Cisco Talks Agentic Identity at RSAC* (IDC #IcUS54467826, April 2026)
- *Identity for Agentic AI: Teleport Launches Beams* (IDC #IcUS54449226, March 2026)
- *Identity for AI Agents: From Gatekeeper to Command Center* (IDC #US54357626, March 2026)
- *From Technology Provider to Orchestrator of Autonomy: The CIO's Framework for Industrializing Agent Vetting* (IDC #US54307326, February 2026)
- *Palo Alto's Ignite: "What's Next" Is the Agentic Era* (IDC #IcUS53899025, October 2025)

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com