SOLUTION BRIEF

Fortinet and Backflipt Security Solution

Fortinet and Backflipt Lumen Bring Every Enterprise AI Agent Under Discovery, Policy, and Ephemeral-Credential Control

Executive Summary

Enterprises are putting AI agents into production faster than they can govern them, resulting in shadow agents reaching production systems unseen, shifting each agent's effective scope as it evolves, and leaving permanent tokens in circulation with no safe path to scale. Fortinet and Backflipt deliver a joint solution that discovers every agent, binds it to a verifiable identity, contains it to the resources it is entitled to, monitors the intent of every call, and replaces permanent tokens with ephemeral, task-scoped credentials. All of these actions are enforced on the Fortinet Security Fabric the customer already operates, without re-architecting the applications behind it. Fortinet FortiAIGate secures the agent-to-model interaction itself, inspecting prompts and responses for prompt injection and data leakage, while the Lumen control plane governs the agent-to-tool and agent-to-agent traffic that surrounds it.

The Challenge

Agentic AI is reaching production systems before the controls to govern it exist. Three gaps determine whether an enterprise can contain what its agents touch, monitor what they intend, and still let them scale.

1. **Shadow agents reaching production systems:** Agents reach production systems before anyone registers them. Unregistered shadow agents cannot be identified, contained, or brought under policy, so their traffic flows to enterprise resources unseen and the attack surface expands invisibly.
2. **Scope that shifts as agents evolve:** An agent's effective reach is not fixed. As models gain capabilities and agents chain new tools, the scope of what a single agent can attempt changes faster than any static grant can anticipate. Two controls follow: Access to each target system must be contained to the resources the agent is entitled to, and the intent of every call must be monitored as the agent evolves. Intent, not the credential, reveals whether the agent is still acting within bounds.
3. **Permanent tokens:** Target resources issue permanent, long-lived tokens, and most applications cannot accept short-term ones. Every governed agent then multiplies the number of standing credentials in circulation, so growth in the agent fleet means growth in risk. A short-lived, task-scoped token model, brokered at the target, resolves this without re-architecting the applications behind it.

Joint Solution

Backflipt and Fortinet have partnered to bring enterprise AI agents under discovery, policy, and ephemeral-credential control without re-architecting the applications behind them. Backflipt Lumen provides the runtime control plane that decides and brokers; the Fortinet Security Fabric provides the enforcement points that the enterprise already operates.

Solution Components

- Lumen A2A Gateway
- Lumen POET Credential Broker
- Fortinet FortiGate Next-Generation Firewall
- Fortinet FortiSASE
- Fortinet FortiWeb
- Fortinet FortiAnalyzer
- Fortinet FortiPAM
- Fortinet FortiAIGate

Solution Benefits

- Full visibility into every AI agent, including unregistered shadow agents
- Verifiable mTLS and SPIFFE identity bound to every agent before any access
- Zero standing access: permanent tokens replaced with ephemeral, scoped credentials
- Inline, default-deny enforcement on Fortinet controls already deployed
- Continuous, audit-ready records mapped to the frameworks the enterprise answers to
- Unparalleled security protection using the Fortinet Security Fabric

FORTINET FABRIC-READY

The integration of the Backflipt Lumen A2A Gateway and Lumen POET Credential Broker with Fortinet FortiGate Next-Generation Firewall (NGFW), FortiSASE, FortiWeb, FortiAnalyzer, FortiPAM, and FortiAIGate delivers inline governance for agent-to-agent and agent-to-MCP traffic and a safe path to scale agent fleets on infrastructure customers run today. The roles stay distinct and complementary: FortiAIGate inspects the content of each agent-to-large language model (LLM) interaction, while the Lumen A2A Gateway and POET Credential Broker govern the identity, policy, and credentials on the agent-to-MCP and agent-to-agent paths.

Solution Components

Backflipt Lumen is a runtime control plane for AI agent traffic. The Lumen A2A Gateway is an inline policy decision and enforcement point (PDP/PEP) that authenticates agents with mTLS and SPIFFE, segments resources into PeerGroups, and decides every agent-to-agent and agent-to-MCP call based on user, role, agent, and intent. The Lumen POET Credential Broker exchanges standing tokens for ephemeral, reduced-scope credentials at the target, with no application re-architecture.

Fortinet FortiGate NGFWs protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help you prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats.

Fortinet FortiAIGate combines application delivery with AI runtime security capabilities. FortiAIGate is designed to protect LLMs from security risks. Deployed between the app and the model, it manages traffic flows and applies guardrails on the model input and output, preventing model manipulations, prompt injections, excessive consumption, and data leakage.

Fortinet FortiSASE delivers secure access to applications and resources from anywhere, ensuring consistent security for remote and hybrid workforces. By integrating advanced threat protection, data loss prevention, and secure web gateway capabilities, FortiSASE provides seamless, cloud-delivered security aligned with zero-trust principles.

Fortinet FortiWeb is a robust web application firewall that protects web applications and APIs from known and unknown threats. Leveraging AI-driven threat detection and advanced bot mitigation, FortiWeb ensures application security while maintaining optimal performance and compliance with industry standards.

Fortinet FortiAnalyzer provides centralized visibility and analytics for your entire security infrastructure. With real-time threat intelligence, automated incident response, and compliance reporting, FortiAnalyzer empowers organizations to make data-driven decisions and strengthen their security posture.

Fortinet FortiPAM secures and manages privileged accounts, reducing the risk of insider threats and unauthorized access. By providing granular access controls, session monitoring, and automated credential management, FortiPAM ensures secure and compliant access to critical systems and data.

Solution Integration

The joint solution runs as one continuous loop, with the Lumen control plane deciding and the Fortinet Security Fabric performing enforcement.

Discover: Fortinet FortiAnalyzer logs surface AI, A2A, and MCP traffic crossing the SASE environment, so agent activity appears even when no one has declared it. Lumen reconciles this against AI agent registries (AWS AgentCore, Azure Entra Agent ID) and flags unlisted callers as shadow agents, routing them into governance rather than leaving them invisible.

Register and identify: Each agent presents and receives a certificate at enrollment, so the Lumen A2A Gateway authenticates both ends with mTLS before any traffic flows. Where agents already carry SPIFFE workload identity, the gateway consumes the SPIFFE ID. No anonymous caller reaches a resource.

Segment and set policy, PDP for agentic traffic: A PeerGroup pairs one enterprise target resource with the specific agents permitted to access it, ensuring each agent has access only to the resources to which it is entitled. Within the PeerGroup, smart rules decide every call across four dimensions: The user the agent acts on behalf of, the role granted to that identity, the agent itself, as defined by its bound identity, and the intent of the call. Intent is evaluated on each request, so an agent whose behavior drifts as it evolves is measured against what it is trying to do, not only the credential it carries.

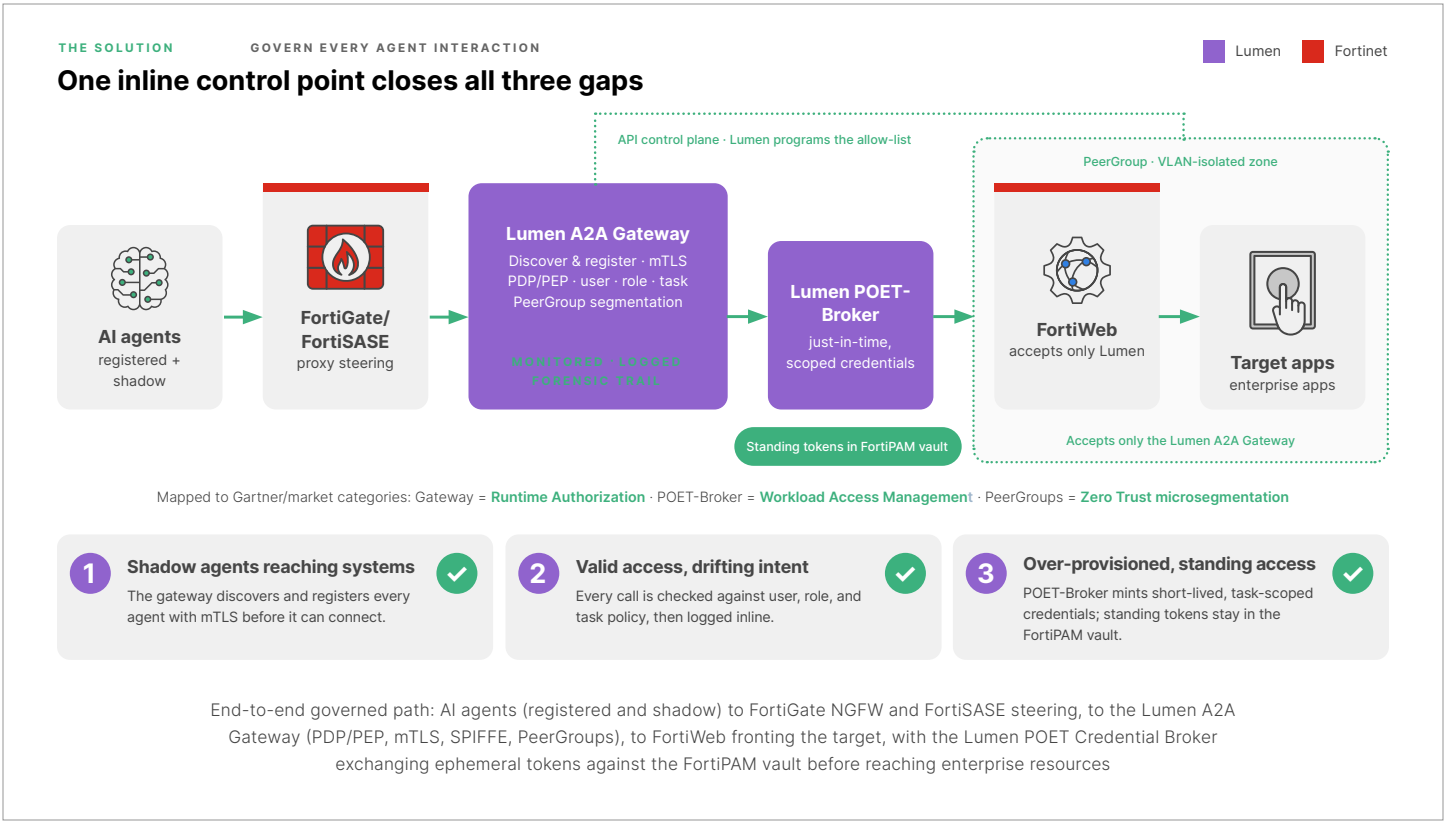
Enforce inline, PEP for agentic traffic: For the PeerGroup assignment, Lumen programs the fronting Fortinet FortiWeb allow-list through its API, so the target accepts and returns AI traffic only via the Lumen A2A Gateway. At that single choke point, the gateway checks three things on every call: the identity of the AI agent, the PeerGroup it is allowed to reach, and the intent of the interaction. For shadow resources, FortiGate NGFW and FortiSASE proxy settings steer traffic through Lumen, which applies network PDP and PEP in real time.

Secure the model interaction: FortiAIGate sits between the agent and the LLM, serving as a runtime AI firewall. It inspects every prompt and response, blocks prompt injection and jailbreak attempts, and applies DLP to stop sensitive data and PII from reaching the model. This is complementary to the Lumen control plane: FortiAIGate secures what the agent says to the model, while the Lumen A2A Gateway governs which resources and agents it may reach on the agent-to-MCP and agent-to-agent paths, and the POET Credential Broker controls the credentials it uses to get there.

Workload access management and runtime authorization: Scaling with ephemeral credentials. IAM issues a reduced-scope ephemeral token (per Entra and Okta RFCs); where IAM cannot, the Lumen A2A Gateway issues it as a federated entity on behalf of the agent. The Lumen POET Credential Broker decodes and validates the token and its scope at the target, then uses PAM and vault services (FortiPAM) to apply the permanent token it holds and retrieve the service. The application admin sets per-delegation scope, mapping each user, group, or agent to what it may access.

Every step lands on a Fortinet control that the enterprise already runs.

Methodology Step	Fortinet Control	What It Does in the Joint Solution
Discover AI activity	FortiAnalyzer	Logs surface AI, A2A, and MCP traffic so Lumen can read it for discovery.
Steer the traffic	FortiGate NGFW, FortiSASE	Proxy settings route shadow traffic through the Lumen A2A Gateway.
Front the target	FortiWeb	The app firewall accepts traffic only from the Lumen A2A Gateway.
Secure the model interaction	FortiAIGate	Inspects agent-to-LLM prompts and responses for prompt injection, jailbreaks, and data leakage.
Hold standing tokens	FortiPAM	The vault holds permanent tokens out of agent reach; the POET Credential Broker brokers access.



End-to-end governed path: AI agents (registered and shadow) to FortiGate NGFW and FortiSASE steering, to the Lumen A2A Gateway (PDP/PEP, mTLS, SPIFFE, PeerGroups), to FortiWeb fronting the target, with the Lumen POET Credential Broker exchanging ephemeral tokens against the FortiPAM vault before reaching enterprise resources

Joint Use Cases

Use case #1: Shadow agent discovery and inline governance

Fortinet FortiAnalyzer surfaces undeclared and potentially risky AI, A2A, and MCP traffic. Lumen reconciles it against registries, flags shadow agents, binds each to an mTLS and SPIFFE identity, and enforces PeerGroup policy inline through FortiGate NGFW and FortiSASE steering and a FortiWeb allowlist, turning invisible callers into governed, default-deny access.

Use case #2: Zero standing access at scale

The Lumen POET Credential Broker replaces broad, permanent tokens with ephemeral, reduced-scope credentials. FortiPAM vaults standing tokens out of agents' reach while the broker validates scope and exchanges access at the target, allowing enterprises to scale agent fleets without re-architecting applications or multiplying credentials in circulation.

Use case #3: Continuous, audit-ready compliance

Every agent call is logged with the agent identity, the user it acts on behalf of, the policy applied, the scope granted, and its lifetime. Fed by the Lumen forensic trail, FortiAnalyzer logs, and POET Broker scope decisions, activity maps continuously align with the EU AI Act, ISO 42001, NIST, SOC 2, HIPAA, and PCI DSS.

Use case #4: Prompt-injection-safe agent interactions

FortiAIGate inspects every agent-to-LLM prompt and response, blocking prompt injection and jailbreak attempts and redacting sensitive data before it reaches the model. The Lumen A2A Gateway governs the same agent's access to MCP tools and to other agents, so each leg of the agent's activity is secured by the control built for it.

About Backflipt

Backflipt, a product line of Xenovus, Inc., is an enterprise software company headquartered in Santa Clara, California. Backflipt builds the Lumen product line for securing and governing AI agents in regulated enterprises: the Lumen A2A Gateway, an inline policy decision-and-enforcement point for agent-to-agent and MCP traffic, and Lumen POET, a no-code platform for transforming APIs into governed agents and brokering ephemeral credentials. Founder-funded since 2013, Backflipt has production deployments in regulated Fortune 500 environments. For more information, visit backflipt.com.

About Fortinet

Founded in the San Francisco Bay Area in 2000, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 900,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry. For more information, visit fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 26, 2026 12:49 AM / MKTG-3705-0-0-EN