Enkrypt AI and Citrix NetScaler Enable Secure Enterprise Deployment of Generative AI Applications

Integrated solution delivers real-time protection against prompt injection, data leakage, and unsafe outputs while accelerating AI adoption

Enkrypt AI and Citrix NetScaler

BOSTON, MA, UNITED STATES, April 29, 2026 /EINPresswire.com/ -- Enkrypt AI, a leading provider of security and governance solutions for generative AI systems, today announced a reference architecture integrating its AI-native protection platform with Citrix NetScaler®, the application delivery and security solution from Citrix. The combined deployment enables organizations to scale generative AI applications securely while maintaining compliance, reliability, and user trust.

Generative AI has rapidly transitioned from experimental pilots to core enterprise infrastructure. Industry projections suggest that by 2026, the majority of organizations will run large language models (LLMs) in production environments. At the same time, security threats targeting AI systems are increasing and evolving, including prompt injection attacks, sensitive data exposure, and policy-violating outputs.

"Enterprises are racing to adopt AI, but without the right controls in place, every model interaction is a potential liability. Citrix NetScaler AI Gateway delivers layered protection across the entire AI traffic flow — and our collaboration with Enkrypt AI adds a critical layer of model-level security intelligence that enterprises need to deploy AI with confidence," said Steve Shah, senior vice president and general manager of Citrix NetScaler. "Together, we're giving IT and security teams the visibility and control to say yes to AI without compromising on governance."

Protecting AI Systems from Emerging Threats

Traditional cybersecurity tools were not designed for natural-language interfaces. Unlike conventional applications, LLM-based systems can be manipulated through carefully crafted

> Enterprises want to move fast with AI, but security concerns slow deployments. Our Citrix NetScaler integration provides layered defense — protecting AI infrastructure, agents and applications,”” *Enkrypt AI, Chief Product Officer, Nathan Trueblood.*

prompts that attempt to override safeguards, extract confidential information, or trigger unintended actions.

Common AI Risks Include:

- Data Exposure — Sensitive or proprietary information may be inadvertently accessed or leaked
- Compliance Violations — Models may generate outputs that violate regulatory or internal policies
- Brand Impact — Unsafe or toxic content could be published under your company's name
- Operational Disruption — Excessive or malicious use of AI can increase costs or reduce service availability

Without AI-specific safeguards, organizations may delay innovation due to security concerns or deploy systems that expose them to legal, regulatory, and reputational risk.

Infrastructure Security Meets AI-Native Guardrails

In the integrated architecture, NetScaler® operates as an application delivery controller in front of AI inference services, providing enterprise-grade capabilities such as SSL/TLS offload, authentication, access control, and load balancing.

Enkrypt AI adds a specialized protection layer designed specifically for generative AI interactions. The platform analyzes prompts, responses, and conversational context in real time, enabling organizations to block unsafe inputs before they reach the model and prevent harmful outputs from reaching users.

Key Enkrypt AI capabilities include:

- Semantic Threat Detection — Identifies adversarial intent, prompt injection, and manipulation attempts in milliseconds
- Dynamic Context Tracking — Monitors multi-turn conversations to detect hidden instructions or intent shifts
- Policy-Based Governance — Enforces organizational rules aligned with frameworks such as NIST AI RMF, OWASP Top 10 for LLM Applications, and emerging global regulations
- Enterprise Integrations — Connects with API gateways, SIEM platforms, analytics tools, and AI development frameworks

This integration provides layered security, combining enterprise-grade infrastructure controls with AI-native protections, while maintaining performance and operational simplicity.

Enabling Compliance-Ready AI Deployments

As regulatory scrutiny of AI intensifies worldwide, enterprises must demonstrate governance over how AI systems are used. The integrated solution provides monitoring, enforcement, and audit-ready evidence to support compliance initiatives and internal risk management programs.

The architecture delivers bidirectional protection across the AI interaction lifecycle:

1. Incoming user prompts are validated for risk and policy violations
2. Approved requests are forwarded to the model
3. Generated responses are inspected before delivery
4. Unsafe outputs are blocked or sanitized

This approach allows organizations to deploy AI applications confidently without degrading user experience or operational performance.

Supporting Enterprise Stakeholders

Secure GenAI deployment delivers value for multiple roles across the organization:

- Security leaders gain assurance that AI systems meet regulatory requirements
- IT leaders can scale AI initiatives while maintaining reliability and governance
- Engineering teams can develop AI features faster with automated safeguards

By combining proven infrastructure security with AI-specific protections, the NetScaler and Enkrypt AI integration enables enterprises to move from experimentation to production AI safely and efficiently.

About Enkrypt AI:

Enkrypt AI is an enterprise AI security, compliance, and governance platform purpose-built to secure AI, agents, multimodal systems, and MCP. The company delivers ultra-low latency, policy-based guardrails that enforce security, safety, and compliance in real time—helping prevent risks such as prompt injection, sensitive data exposure, unsafe outputs, and non-compliant agent behavior across models and toolchains. Enkrypt AI's red teaming engine provides comprehensive, policy-driven, multimodal attack simulation across models and agents, while its MCP Scan Hub and Secure MCP Gateway help protect MCP servers, tools, and agent toolchains end-to-end. Serving enterprises in regulated industries including finance, healthcare, insurance, and government, Enkrypt AI helps organizations ship fast, ship safe, and stay ahead. For more information, visit enkryptai.com

affiliates in the United States and/or other countries. All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification.

###

Sheetal Janala
Enkrypt AI
email us here
Visit us on social media:
LinkedIn
YouTube
X
