Enkrypt AI and NetApp Collaborate to Bring AI Risk Enforcement to the Data Layer

Strategic Collaboration Connects Real-Time AI Governance Intelligence with Storage-Layer Access Control for Enterprise Hybrid Environments

Enkrypt AI and NetApp

BOSTON, MA, UNITED STATES, May 12, 2026 /EINPresswire.com/ -- Enkrypt AI, the AI security platform purpose-built for enterprise AI governance, today announced a strategic collaboration with NetApp, a global leader in intelligent data infrastructure, designed to connect AI risk intelligence with data-layer access control. The collaboration establishes an architectural framework in which AI workload risk signals from Enkrypt AI are correlated with NetApp's data-centric security graph — designed to enforce governance at the point of data access — with a particular focus on the autonomous agents now operating at the center of enterprise AI architecture.

> AI governance must be enforced where data lives — in real time, at machine scale. Our NetApp collaboration gives security leaders control without slowing AI innovation."
> *Sahil Agarwal, CEO, Enkrypt AI*

As enterprise AI adoption accelerates, autonomous agents and training pipelines increasingly read directly from enterprise file systems and object stores at machine scale — often under broad service identities that bypass the application control layers security teams have historically relied upon. Unlike bounded AI workloads, agents act continuously and without human intervention, generating access patterns that static permissions and periodic offline scans were never designed to handle. When sensitive data is ingested into a model or reached by an agent, the exposure is immediate and irreversible.

The Enkrypt AI and NetApp strategic collaboration addresses this challenge through a unified security architectural framework. Enkrypt AI contributes deep visibility into agent and AI system

risk — designed to evaluate agent behavior, unsafe prompts, policy violations, and compliance posture — while NetApp provides a data-centric security graph that integrates data sensitivity classifications, regulatory attributes, identity context, lineage, and observed access behavior. Together, these capabilities are designed to enable real-time, context-aware access decisions at the storage I/O layer, before data is consumed by AI agents or workloads.

The forward-looking architectural framework is designed to enable organizations to: identify precisely which agents and AI systems are interacting with regulated or high-value datasets across hybrid environments; dynamically adapt access enforcement as agent behavior and data characteristics evolve; and apply governance intent continuously — not just at policy-writing time — without dependence on manual recalibration or periodic review cycles.

The collaboration reflects a growing recognition across the enterprise security industry that AI governance must be embedded at the infrastructure layer rather than applied as an overlay. As agents proliferate and non-human identities become the dominant mode of enterprise AI interaction, enforcing policy at the data access point — using live, correlated risk context — represents the next maturity stage for enterprise AI security programs.

The full technical perspective is available on the Enkrypt AI and the NetApp blog. Additional information about Enkrypt AI's Agent Red Teaming, Agent Guardrails, AI Data Risk Audit, and Agent Policy Engine products is available at enkryptai.com.

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 www.enkryptai.com

About NetApp

NetApp is a global leader in intelligent data infrastructure, helping organizations manage and secure their data across on-premises, hybrid, and multi-cloud environments. With over 30 years of storage and data management expertise, NetApp delivers unified infrastructure that enables enterprises to unlock the value of their data while maintaining control, compliance, and resilience. NetApp's data-centric security architecture integrates data sensitivity, identity, lineage, and access behavior into a unified security graph — purpose-built to govern AI workloads at

machine scale. For more information, visit www.netapp.com.

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