EINPRESSWIRE

ClearML Rolls Out New IT Governance and Security Controls for AI Models and Agents

Enabling Extensive IT Control with Built-in Networking and Security and Making It Easy for AI Builders to Create AI Agents and Apps and Launch with One Click

SAN FRANCISCO, CA, UNITED STATES, March 19, 2025 /EINPresswire.com/ -- ClearML, the leading open-source AI infrastructure platform, today announced robust new IT governance and cybersecurity controls over live AI agents and AI model endpoints, complete with monitoring, management, and pre-configured security features.

These new capabilities enable enterprise IT teams to provide their company's AI builders with a platform for building, testing, and launching AI agents and Generative AI applications with just a single click. ClearML's pre-integrated orchestration, networking, Role-based Access Control (RBAC), and authentication features reduce risk and mitigate concerns over AI security, as well as dramatically decrease the overhead and resources required to support rapid GenAI adoption.

Unlike traditional AI platforms that require separate security tools and external infrastructure for serving AI models and agents, ClearML offers a unified, platform-wide approach to RBAC and permissions, so that they extend beyond just the AI development environment to include endpoints. With this consolidated approach, IT admins can now have confidence in the security of their AI models without the need to manually configure each API – saving both time and the cost of additional security tools. This "set-it-and-forget-it" flexibility allows developers to effortlessly deploy any application, whether a model, process, or full-fledged AI agent, within ClearML's secure framework.

"The adoption of Generative AI within an organization requires more testing and customization than traditional machine learning models due to the wide variety of available LLMs, how well they perform for particular use cases, and the resources required to run them," said Moses Guttmann, Co-founder and CEO of ClearML. "Our latest advancements enable IT teams to support their organization's AI ambitions with frictionless, secure scalability and minimal overhead. With ClearML, customers can build, test, and deploy agents and LLMs at scale with completely secure endpoints and permission-based access to data, models, and compute, preventing unauthorized access to AI assets. As organizations increasingly look for secure and efficient ways to deploy AI-driven solutions, ClearML's innovations provide a future-ready alternative to other serving platforms."

Key New Governance and Security Controls:

1) ClearML has introduced a new Containerized Application Launcher with integrated networking and persistence so that users can take advantage of the security of the ClearML platform to run custom or third-party applications like AI agents and models.

2) The company also released a new Application Gateway to provide a secure and effortless way for organizations to deploy secure AI/ML models and AI agents, allowing external users to interact with AI models while maintaining strict security protocols. The Application Gateway also simplifies networking, enabling AI agents and applications to run without complex security or networking configurations.

3) Integrated Access to Compute: Once administrators have set up resource policies, permissions, and credentials, ClearML now automatically enables one-click secure compute access without additional provisioning or manual intervention.

4) Built-in Networking, Authentication, and RBAC: AI builders can now deploy LLMs, agents, apps, and custom containers with pre-configured infrastructure, networking, and security.

5) Enterprise-Grade Authentication: ClearML's infrastructure supports RBAC and authentication mechanisms platform-wide, ensuring that AI agents and apps operate securely in any environment.

6) Custom AI Agent Creation, so that customers can now write their own code and create custom AI agents that execute tasks using a proprietary model or LLM. With a single click, AI builders can launch agents without needing to configure the underlying network or infrastructure.

7) ClearML has also introduced an Integrated Vector Database for RAG so that customers can leverage ClearML's new vector fields and vector database apps to implement Retrieval-Augmented Generation (RAG) in their AI agents and GenAI apps, ensuring more relevant and context-aware outputs. ClearML simplifies the RAG-building process, reducing the setup time as well as providing controlled access to the database with ClearML's platform-wide security measures. Learn more about that here: https://www.einpresswire.com/article/794570645/clearml-integrates-vector-image-search-and-vector-databases-for-ai-builders-supercharging-rag-development

These improvements come as ClearML's Infrastructure Control Plane continues to gain rapid market traction. That's because ClearML bridges the gap between IT teams and AI builders by eliminating the friction between software and hardware and maximizing the utilization of every resource. Companies derive more value from their existing infrastructure and accelerate AI adoption without additional investment. For example, ClearML customers can increase throughput by 10X, with dependable performance, greater operational efficiency, and streamlined AI workflows. To see how ClearML is redefining AI infrastructure, visit https://clear.ml or request a demo at https://clear.ml/demo.

About ClearML
As the leading infrastructure platform for unleashing AI in organizations worldwide, ClearML is used by more than 1,600 customers to manage GPU clusters and optimize utilization, streamline AI/ML workflows, and deploy GenAI models effortlessly. ClearML is an NVIDIA partner and is trusted by more than 250,000 forward-thinking AI builders and IT teams at leading Fortune 500 companies, enterprises, academia, public sector agencies, and innovative start-ups worldwide. To learn more, visit the company’s website at https://clear.ml.

Noam Harel
ClearML
email us here
Visit us on social media:
X
LinkedIn
YouTube