News Release

November 11, 2026
ExaWizards Inc.
(TSE Code No.4259)

exaBase Studio Strengthens Security with a Multi-Layered Approach Providing a Closed Environment Equipped with a Local LLM to Enhance the Security and Maintainability of AI Agent Development & Operations

— The SaaS Edition Visualizes Vulnerability Management on a Dashboard, and Emergency Shutdown Rules Will Be Developed Jointly with Customers —

ExaWizards Inc. (Minato-ku, Tokyo; Representative Director, President & CEO: Makoto Haruta; hereinafter "ExaWizards") today announced multi-layered security enhancements to exaBase Studio, its platform for developing and operating AI agents.

Centered on the private cloud edition, the new solution brings together an AI agent execution and governance platform, an AI-driven development environment, and a local LLM in an isolated network environment dedicated to each customer and disconnected from the internet. AI-driven development refers to an approach in which coding agents assist with building, testing, and maintaining software. The solution enables customers to develop and validate AI agents without sending highly confidential production data outside their environment, and also streamlines root-cause investigation and maintenance after deployment. It is delivered jointly by the four companies of the ExaWizards Group.

For the SaaS edition, ExaWizards has adopted the cloud security platform Wiz[*1] to monitor the security of its own infrastructure, strengthening continuous vulnerability monitoring that also covers the container environments customers develop and run. The company also plans to provide a security dashboard feature in exaBase Studio that will let customers check the security status of their own environments, and will work with customers to clarify operating rules for emergency shutdown conditions and response policies when critical vulnerabilities are discovered.

Through these initiatives, ExaWizards supports enterprises in using AI in line with their security requirements, from secure AI-driven development and operations in isolated network environments to continuous vulnerability management.



☑Background: As Cyberattacks Grow More Sophisticated, AI Services Also Need Comprehensive Security Measures

In recent years, there has been a string of incidents involving intrusions that exploit software vulnerabilities, supply chain attacks, and ransomware. Furthermore, generative AI is now being used for reconnaissance of targets, phishing, malware development, and more, making cyberattacks increasingly sophisticated and efficient. Enterprises are being called on to implement more advanced and continuous security measures that keep pace with these changing threats.

At the same time, as the business use of AI expands, multi-layered security measures covering not only applications but also networks, authentication and authorization, data, LLMs, and development environments have become essential.

Enterprises advancing their use of AI agents have also raised another challenge. Because AI agent behavior changes depending on actual business data and usage conditions, validation using production data is essential to ensure quality. However, these companies cannot send highly confidential data to external LLM services or development services, which prevents them from moving forward with development and validation using production data.

To respond both to this changing threat landscape and to the practical constraints enterprises face, the ExaWizards Group is strengthening the security of exaBase Studio with a multi-layered approach.

☑Isolated AI Platform: Integrating the Private Cloud Edition of exaBase Studio with a Local LLM and an AI-Driven Development Environment

The defining feature of this solution is that it allows not only the platform that runs AI agents, but also the coding agents that develop and maintain them, and the local LLM used by both, to be deployed together within an isolated network environment dedicated to the customer.

Specifically, exaBase Studio, equipped with MCP Gateway, MCP Registry, and authentication and authorization services, along with an AI-driven development environment and a local LLM running on dedicated GPUs, is built in a private cloud environment dedicated to the customer, such as on Microsoft Azure or AWS, and connected within an isolated network. No entry points directly accessible from the internet are provided, and the environment is tailored to each customer's security requirements.

This makes it possible to use AI-driven development to streamline everything from the development and validation of AI agents to post-deployment root-cause investigation, fixes, and regression evaluation, without sending highly confidential production data or execution logs to external LLM or development services, with the aim of reducing the burden of development and maintenance.

This configuration consists of the following three platforms.

(1) AI Agent Execution and Governance Platform: Integrating MCP Gateway with Authentication and Authorization for Secure Connections to Business Systems

The AI agent development and execution environment of exaBase Studio is combined with MCP Gateway, MCP Registry, AI Gateway, and authentication and authorization services. The AI agent execution environment is isolated, and access to LLMs and business systems is governed through a common mechanism.

The platform is also designed to support NHI (Non-Human Identity), which assigns a unique ID to each AI agent, as well as authorization methods that access external SaaS and business systems based on users' permissions.

This provides a secure and highly extensible AI agent execution environment designed for integration with existing identity platforms and business services such as email, chat, and document management.

(2) AI-Driven Development Environment: Streamlining Everything from Development and Validation Using Production Data to Post-Deployment Monitoring and Maintenance

An AI-driven development environment where coding agents can be used is built within the customer's private cloud.

Scenarios envisioned during the development phase alone are not enough to fully ensure the quality of AI agents. With this configuration, under appropriate access controls, operational testing, prompt and configuration tuning, program fixes, regression evaluation, and more can be carried out through AI-driven development using production data kept within the isolated network.

Even after production deployment, coding agents refer to execution logs and related programs and configurations under appropriate permissions to support anomaly analysis, investigation of causes and impact, drafting of fixes, and test generation and execution.

(3) Local LLM Platform: Supporting Both AI Agent Execution and AI-Driven Development with an LLM Inside the Isolated Network

An open-weight LLM is deployed in a GPU environment dedicated to the customer and used not only for AI agent inference but also for AI-driven development by coding agents.

This gives companies that cannot send production data to external LLM services a way to carry out AI-driven development using that data. In addition to easing the data management constraints that come with using external LLMs, the company will also work to optimize the LLM usage costs required for AI-driven development.

☑SaaS Edition: Visualizing Vulnerabilities and Strengthening Security Operations in Collaboration with Customers

Alongside providing an isolated AI platform through the private cloud edition, ExaWizards is also enhancing vulnerability management and security operations for the SaaS edition.

(1) Visualizing Security Status

In the SaaS edition of exaBase Studio, continuous vulnerability detection and infrastructure monitoring are performed using the cloud security platform Wiz, including the containers of applications developed by customers.

As part of exaBase Studio's functionality, the company plans to provide a feature that will let customers view, on a dedicated dashboard, the security status of the applications they have developed and their running containers, including health and vulnerabilities. This will enable rapid sharing of risk information with customers and highly transparent service operations.

(2) Clarifying Vulnerability Response and Emergency Shutdown Rules in Collaboration with Customers

When a critical vulnerability is discovered, it is important to make response decisions based not only on the severity of the vulnerability but also on factors such as external reachability, the actual scope of impact, and existing defenses.

Through discussions with customers, the ExaWizards Group will begin an initiative to clarify in advance matters such as risk assessment when vulnerabilities are discovered, response priorities, criteria for deciding on emergency shutdowns or feature restrictions, and policies for information sharing and recovery.

By sharing response policies with customers in advance, the company will promote service operations that balance security with business continuity.

☑Strengths of the ExaWizards Group: End-to-End Delivery from AI Agent Development to Operations and Maintenance

With exaBase Studio at its core, the four companies of the ExaWizards Group combine their specialized expertise in AI-driven development, local LLMs, security, and other areas to provide comprehensive support for enterprises' use of AI.

Figure: AI Adoption Support by the ExaWizards Group, Centered on exaBase Studio

Area of Responsibility	Company / Product
Business design, AI agent platform provision, overall coordination	ExaWizards (exaBase Studio, "Issho ni Sekkei")
Building AI-driven development environments, development and testing support	Exa Frontier Edge
Building and operating local LLM platforms	Exa Interaction Design Lab
AI security assessments and red teaming	ExaSecurity

The Group provides unified support from the design and development of AI agents to post-deployment monitoring, security measures, maintenance, and continuous improvement. Customers do not need to combine multiple vendors and technologies on their own and coordinate with each of them.

In addition, when responding to vulnerabilities or investigating issues after production deployment, experts in each area, including the AI agent platform, development environment, and local LLM, work together to support secure and efficient service operations.

☑Future Plans

The ExaWizards Group will focus on the following three areas.

1. Expanding Target Industries

The Group will roll out solutions that combine the private cloud edition of exaBase Studio with a local LLM platform and an AI-driven development environment in an isolated network, targeting enterprises in industries such as finance, manufacturing, construction, and the public sector that handle highly confidential data or require strict security controls.

2. Applying AI Across the Entire Response Process

Going beyond detecting vulnerabilities and identifying abnormal AI agent behavior, the Group will build mechanisms that use AI to streamline the entire process, including investigating the scope of impact, considering countermeasures, fixing programs, and validation. While keeping human judgment and approval in place, it aims both to improve the accuracy of security measures and to reduce the workload of development, operations, and maintenance.

3. Building a Common Platform to Support Large Numbers of AI Agents
Anticipating growth in the number of AI agents running within enterprises and the advance of automation spanning multiple business systems, the Group will develop authentication and authorization, execution management, auditing, and security measures as a common platform.

By bringing together the specialized expertise of each Group company, the ExaWizards Group will promote an environment in which enterprises can develop and operate large numbers of AI agents securely and efficiently, and continuously improve them.

*1 A cloud security platform provided by Wiz, Inc. ExaWizards has introduced and uses it for the safety management and security operations of the service delivery infrastructure and operating environment of exaBase Studio.
*2 Company names and product/service names mentioned herein are registered trademarks or trademarks of their respective companies.

ExaWizards Company Profile
Company name: ExaWizards Inc.
Location: 4-2-8 Shibaura, Minato-ku, Tokyo, 5F
Established: February 2016
Representative: Makoto Haruta, Representative Director, President & CEO
Business: Industrial innovation and resolution of social issues via AI service development
URL: https://exawizards.com/en/

<Media Contact>
ExaWizards Inc. Public Relations: publicrelations@exwzd.com