

GA technologies Strengthens Insider Threat Defenses and Accelerates Incident Response with Exabeam

GA technologies Co., Ltd. is a Japan-based technology company driving business transformation across a wide range of industries, including the real estate industry with their AI real estate investment service "RENOSY". As their business has expanded, establishing a user-friendly IT environment for employees while strengthening measures against insider threats and data exfiltration has become a pressing challenge. To address this, the company adopted Exabeam, which leverages user and entity behavior analytics (UEBA) and enables efficient operations even with a small team. With the power of AI-driven behavior intelligence and automation capabilities from Exabeam, threat detection, investigation, and response times have been dramatically streamlined, delivering immediate, tangible benefits.

The Challenge: Balancing Security Needs with a Seamless Employee Experience

In addition to developing and operating real estate services like RENOSY, GA technologies has expanded its portfolio into M&A and the financial sector. As it extended its footprint not only domestically but also to North America and Asia through its group companies, its cybersecurity requirements became increasingly complex.

With a mission to "Continuously create excitement and inspiration by fusing technology with innovation," the company places immense value on fostering a user-friendly IT environment for its employees. On the other hand, with a real estate business serving over 600,000 customers, along with new ventures in sectors with high confidentiality requirements, the need to fortify insider threat countermeasures to protect critical data became an urgent priority.

This approach is deeply rooted in the company's culture. Takuto Yamada, Chief of the IT Strategy/Security Team, emphasizes this balance: "Our goal is not to create a 100-point perfect security system. GA technologies is filled with

Key Highlights

→ Enhanced Security Governance:

The introduction of the Exabeam New-Scale Security Operations Platform has strengthened security governance across group companies by unifying security standards and enforcing strict risk management.

→ Enhanced Security Governance:

UEBA capabilities within the Exabeam Platform have significantly bolstered insider threat defenses. AI-powered analytics enable the early detection of unknown threats and signs of malicious activity.

→ Security Risk Visualization:

Exabeam dashboards provide clear visibility into security risks. This risk-based approach has accelerated and streamlined incident response.

passionate people who want to change the analog world and drive it forward. IT should not get in the way of that passion; in fact, we want to accelerate it."

The Solution: Streamlining Security Operations with a Small Team Using UEBA

GA technologies chose Exabeam for three primary reasons: the ability to proactively track and analyze employee behavior; to operate efficiently even with a small team; and to maintain convenience for employees.

Insider threat risks are diversifying and becoming more complex every year. Satoshi Tsubaki, General Manager of the IT Strategy/Corporate IT Department, explains: "We believed that we needed a foundation that could not merely store SaaS and endpoint logs, but continuously track and analyze what kind of actions internal users were taking."

Ensuring the system could be managed without expanding headcount was critical. "As we strengthened our insider threat program, one key requirement was ensuring that it could be operated effectively by a small security team," notes Yamada. "With a traditional SIEM, where dedicated analysts constantly need to write and run search queries, it was obvious that operations would eventually become unsustainable."

With Exabeam, UEBA can automatically score deviations from normal behavioral patterns without the need to manually create detection rules. This led to the realization of the company's goal: a system that can be operated without being dependent on individual manual skills, even with a small security team. Additionally, the mechanism to centrally aggregate multiple logs and analyze them automatically proved to be a major advantage in advancing business expansion.

"This level of automation and operational simplicity was exactly what we were looking for," adds Yamada.

Furthermore, without excessively tightening existing information leakage countermeasures like DLP, the ability for Exabeam to detect "gray" actions that might slip through the cracks convinced the team that security could

be fortified without sacrificing employee convenience, ultimately leading them to choose Exabeam.

Securing Executive Support for Exabeam

The company began comparing and evaluating SIEM products in January 2025. A PoV was conducted in July, and the contract was finalized in December. Following a build period of approximately two months, full-scale operations commenced in March 2026.

To meet the organization's budget and security needs, the management team clearly laid out a division of roles: large volumes of logs for external threats would be handled by their existing endpoint detection and response (EDR) solution, while Exabeam would specialize in analyzing user behavior related to insider threats. By optimizing costs, they were able to easily gain executive support to move forward with the Exabeam solution.

The Results: Improved Efficiency in TDIR

In terms of cross-departmental collaboration, the GA technologies team prioritized advancing the implementation in phases, starting from areas that the IT Strategy Department could complete on its own. To avoid impacting the work of other departments, they limited the scope to company-wide common platforms like Google Workspace and Slack, transitioning to production operations in a short period while minimizing the coordination load.

Before this streamlined approach, the reality of tracking threats was a tedious, manual effort. Yamada illustrates the contrast: "Previously, whenever an alert was triggered, we had to log into multiple SaaS administration consoles, manually export logs, and correlate them ourselves."

Previously scattered logs — such as mass downloads from Google Drive or uploads to cloud storage — are now visualized chronologically as the behavioral history of a single user. This visibility has had a major impact on the small team's ability to quickly respond to threats.

"As a result, our initial response time has improved dramatically, and anyone on the team can quickly understand what happened," Yamada highlights.

A Winning Strategy

The ideal cybersecurity approach is often to integrate all logs into a single SIEM. However, doing so without a clear strategy can create cost and operational fatigue. GA technologies succeeded by taking an alternative approach: dividing responsibilities between EDR and SIEM based on their organizational priorities. By deploying Exabeam specifically where it delivers the highest value for their team — behavioral analytics and insider threat detection — GA technologies has been able to scale their security program efficiently while maximizing return on investment.

Summarizing their journey and offering advice to peers, Mr. Tsubaki and Mr. Yamada share a unified message: "If your organization wants to strengthen security, maintain a great employee experience, while also optimizing operational costs... if those are the challenges you're facing, Exabeam may be the right solution for your organization."

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity leader, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).



Learn more at
www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.
2025 Exabeam, LLC. All rights reserved.