SUCCESS STORY

NETHERLANDS | SOFTWARE & TECHNOLOGY | ELASTIC SECURITY

Intermax protects IT infrastructure with AI-driven security analytics from Elastic Security

Cutting-edge threat detection, enhanced observability, and AI-driven search empower Intermax to protect clients and streamline operations.

Watch video

Enhances threat detection

With Elastic Security, Intermax can detect threats earlier and respond faster, streamlining investigations.

Reduces storage costs

Intermax can retain recent logs in high-performance storage and older data in frozen storage, significantly reducing costs while maintaining searchability.

Increases search relevance for security and observability

Employees save time using Elastic AI Assistant, which surfaces relevant organizational information using retrieval augmented generation (RAG).

From healthcare to utilities and other public industries, IT services play a critical role. Established in 1994, Intermax provides clients with secure, compliant, and resilient IT infrastructures based on a mix of cloud technology, managed applications, platform services, and security and compliance solutions.

Protecting sensitive data is at the core of Intermax's mission. A single data breach could compromise healthcare records, expose intellectual property, and damage client trust. "In security, we're in an arms race. Attackers are becoming more advanced, and traditional methods like vulnerability management and endpoint protection are no longer enough," says René Kalff, technical lead of the Intermax Cyber Defense Center.

Staying ahead in a fast-moving security landscape

Intermax initially used an open source software framework for security monitoring, but the platform's slow development and uncertain future raised concerns. The team needed a long-term solution that offered real-time threat detection and advanced attack pattern identification that traditional security tools might miss.

"When we looked at Elastic, it was the obvious choice, especially because of the rapid and regular release of AI features that keep us ahead of malicious actors," says Kalff. He gives the example of machine learning capabilities in Elastic Security that enhance threat detection by identifying patterns across multiple events rather than flagging isolated anomalies. This makes it possible to detect sophisticated attack sequences, even when adversaries mimic normal user behavior.

Kalff was also reassured by features such as real-time threat detection with customizable detection rules.

> Many security tools operate as black boxes: Data goes in, and alerts appear, but the reasoning behind them isn't always clear. With Elastic, we're in full control. We can create our own detection rules and customize alerts to fit our business needs.
>
> **René Kalff**
> Technical Lead, Intermax Cyber Defense Center

A powerful platform for security, observability, and Search AI

Elastic Security exemplifies how large data volumes and AI-driven security analytics combine to deliver real-time insights that save time and deliver value. "The beauty of Elastic is that you can apply this model to other activities, including observability and search," says Kalff.

Intermax's operations teams have taken full advantage of powerful inbuilt search and monitoring capabilities to track system health and IT infrastructure, ensuring that potential issues are detected before they impact customers.

A good example is backup monitoring. Every night, Intermax backs up thousands of machines. If backups run slower than expected, Elastic generates real-time alerts so the team can resolve performance issues before the start of the business day.

"Backup performance may seem simple, but delays can impact customers the next morning. Elastic alerts us immediately, so we can fix issues before they become a problem," says Kalff.

Elastic has also enabled Intermax to take advantage of powerful AI capabilities. With Elastic AI Assistant, Intermax can ask questions in natural language and receive actionable guidance, as well as automatically contextualize prompts with organization-specific knowledge to tailor insights to the situation at hand. The company implemented retrieval augmented generation (RAG), enabling employees to ask their large language model (LLM) questions and receive direct answers sourced from company knowledge bases. Instead of searching through multiple file systems, employees can now retrieve precise, AI-generated responses with clear references to source data.

Unlocking team potential with Elastic training and certification

Kalff highlights how validating team skills through the Elastic Certification Program accelerated the successful adoption of relevant use cases within Intermax.

He says, “Over the years, the Elastic Stack has evolved to include a wide range of new features. While these are user-friendly and well-documented, their original intent and design philosophy may not always be immediately apparent.”

Importantly, investing in skills and certification enables Intermax engineers to successfully design, deploy, and manage Elasticsearch solutions and to improve performance and efficiency.

Kalff also adds, “Continued training and certifying the team’s skills in Elastic has increased confidence and technical abilities, allowing us to move beyond general use cases and fully leverage the platform’s capabilities.”

Discovering unseen attack patterns with Attack Discovery

By integrating security, observability, and AI-powered search into a single platform, Intermax has improved efficiency, reduced costs, and empowered multiple teams to make faster data-driven decisions.

Security teams now detect threats earlier with Elastic Security's AI-driven Attack Discovery feature. The system triages alerts, identifies attack sequences, and helps analysts prioritize incidents, streamlining security investigations. "In addition, the AI Assistant for Security helps our analysts quickly understand what's happening. It allows us to respond faster and work more efficiently," says Kalff.

Cost efficiency has improved significantly with tiered storage. Intermax stores recent logs in fast, high-performance storage, while older data is moved to frozen storage, keeping costs low without losing searchability. "With Elastic's approach to hot-warm-cold-frozen data tiers, we can still access five years of archived data, which offers us valuable flexibility concerning value, performance, and retention periods. That's a game changer for our operations," says Kalff.

Answering questions with AI context

Enterprise search has been transformed with RAG. Employees no longer waste time hunting for information across multiple systems. Instead, Elastic delivers precise answers, increasing productivity across departments. "Elastic's RAG finds the relevant information and summarizes it in a clear, AI-generated response. It's a huge time saver," says Kalff.

> Without Elastic, we wouldn't have been able to fill so many data-driven use cases across our company. It's more than just a security tool — it's an essential part of our infrastructure.
>
> **René Kalff**
> Technical Lead, Intermax Cyber Defense Center

Start your free trial

See for yourself how your business can benefit from Elastic in the Cloud, with a free 14 day trial.

Get started