



## SUCCESS STORY

GERMANY

PROFESSIONAL SERVICES

ELASTIC SECURITY

# Hermes Germany secures its critical logistics operations for half the price of its previous on-premise platform

Officially listed as part of Germany's critical national infrastructure, Hermes Germany uses Elastic Security to protect its systems and secure its essential delivery operations.



### Elastic Security in the cloud resulted in 50% reduction in costs

Elastic Security gives Hermes Germany a faster, more powerful security platform at 50% of the price of its previous on-premise solution.



### Gains comprehensive visibility into 40,000 endpoints

With Elastic Security, Hermes Germany has easily integrated the data from the handheld scanners of all 40,000 delivery staff for better visibility across its systems.



### AI and machine learning automate security workflows

Elastic Security's AI and machine learning capabilities help automate processes, allowing Hermes' security team to focus on more complex investigations.

[Hermes Germany](#), part of the Hermes Group, delivers parcels and goods to homes and businesses both in Germany and abroad. As the country's second-largest logistics company, it is officially listed as part of the nation's critical infrastructure ([Kritis](#)).

KRITIS, short for "Kritische Infrastrukturen" (Critical Infrastructures), refers to essential services whose disruption would impact public safety, security, and economic stability. These include sectors like energy, water, healthcare, finance, and telecommunications. The German Federal Office for Information Security (BSI) ensures their protection against cyber threats and other risks by implementing security measures and fostering public-private collaboration to maintain their continuous operation.

As Marco Uhl, SIEM Engineer at Hermes Germany explains, "Effective system security is essential for Hermes Germany. It is not a side issue, but critical for both our company and the country."

With security threats on the increase, Hermes Germany needs a powerful security operations platform to protect itself. At the same time, it needs to be cost-efficient to allow the company to weather the country's current economic environment. However, Hermes Germany experienced both performance and cost challenges with its previous third-party security platform. Running completely on-premise, the platform made it difficult for the company to get its vast amount of security [log data](#) into storage efficiently, and the team faced issues searching the data quickly and accurately once it was there.

"It was a very complex environment, with frequent outages. More than once the whole cluster practically blew up in our faces," recalls Uhl. "It was also very expensive, with high license costs, along with the operational costs, such as infrastructure and energy, that come with running it on-premise."

Driven by these constraints, as well as the company's corporate strategy to migrate all infrastructure to the cloud, Hermes Germany searched for a cloud-based security platform, evaluating a number of large providers.



We chose Elastic Security because we preferred the way it was structured and processes data. It is flexible enough to tailor it to our needs and is easily integrated with other systems and data sources.

**Marco Uhl**

SIEM Engineer,  
Hermes Germany

## Taking delivery of a high-performing, easy-to-use security platform deployed on Google Cloud

Hermes Germany chose Elastic over its current SIEM deployment due to scalability issues with the on-premises solution and misalignment with Hermes' cloud-first strategy. The cost of maintaining the incumbent SIEM and migrating to the cloud was also five times higher than Elastic.

One of the major factors in the decision to move to Elastic involved the company's 40,000 handheld delivery scanners that captured critical data on delivery operations. This data is essential for efficiency and compliance, particularly with KRITIS regulations. However, due to the high costs associated with their previous SIEM, Hermes Germany was unable to ingest and retain this data effectively. With Elastic, the company was able to take advantage of a cost-effective solution that allows them to ingest and analyze this critical data without prohibitive expenses, ensuring they meet regulatory requirements and maintain operational excellence.

Hermes Germany partnered with the [Elastic Support](#) team to migrate to [Elastic Security](#). This collaboration ensured a smooth setup and seamless data integration, allowing the Hermes Germany security team to quickly experience the platform's speed, reliability, and powerful search capabilities.



Our previous solution would have been twice as expensive in terms of licenses alone. With Elastic Security, we get everything in one platform — we can isolate devices, pull files, query processes, we get endpoint protection. It's the complete package.

**Marco Uhl**

SIEM Engineer,  
Hermes Germany

Security analysts were also impressed with the ease of use of Elastic Security, with no need to manually copy and paste information from one part of the system to another while investigating a security alert, unlike their previous system. With [Elastic Common Schema](#) — the platform's consistent approach to

organizing data — Hermes Germany can now unify and normalize data from disparate sources, enabling analysts to quickly and easily visualize and understand network traffic flow to perform effective security investigations.

ECS standardizes the way data is ingested and analyzed, making it easier to understand destination IPs and how connections flow through the network. This standardization is crucial for accurate and efficient threat detection and response, which is an essential functionality for Hermes.

Throughout the migration and subsequent use of Elastic Security, the Hermes Germany team has benefited from the platform's extensive documentation, which allows them to easily understand how to make the most of their solution.

## Eliminating blind spots with comprehensive system visibility

With Elastic Security, Hermes Germany has a comprehensive security platform for improved visibility across its IT infrastructure. The company can now ingest and analyze data from previously overlooked sources, such as the handheld scanners used by its delivery staff, enabling it to protect against threats from this core part of its operations.

When Hermes Germany receives a security alert, their analysts leverage the powerful Elastic Timeline to visualize all related events seamlessly. By simply dragging and dropping filters — without the need for complex query writing — they can swiftly investigate incidents. This intuitive process allows analysts to trace the path of connections and identify any suspicious activities with ease.

Through this streamlined approach, Hermes Germany's analysts can quickly determine whether an incident is a false positive, noise that can be or has already been automatically filtered out, or a genuine security threat. For genuine threats, they either follow a standard playbook or escalate the situation to a collaborative "war room" for more complex scenarios. This rapid and efficient response mechanism ensures that Hermes Germany can maintain the security of its systems and guarantee the smooth operation of its nationally critical logistics services.



Previously, the sheer volume of data from over 40,000 delivery staff using handheld scanners made it impossible to process. Now, we ingest all that data into Elastic Security for analysis. This eliminates a critical blind spot and enables us to meet our requirements as a Kritis organization.

**Marco Uhl**  
SIEM Engineer,  
Hermes Germany

# Increasing operational efficiency with AI and machine learning

Hermes Germany is also using a range of [generative AI and machine learning](#) (ML) capabilities within Elastic Security to streamline and enhance security and elevate its security capabilities further with the roll-out of the [Elastic AI Assistant](#) to all its analysts.

Securely linked to Google Gemini, the [LLM](#) of choice for Hermes Germany, the AI Assistant for Security allows them to safely connect all its private data with the large language model, enabling the company's analysts to resolve problems more quickly with natural language interactions. The AI Assistant can help analysts quickly interpret log messages and errors, optimize code, write reports, and ultimately help secure the company's systems more effectively and efficiently.

With [Attack Discovery](#), Hermes Germany can automatically detect and group suspicious patterns of behavior and potential threats that might otherwise have gone unnoticed. Using machine learning and contextual threat intelligence, Attack Discovery leverages advanced machine learning algorithms enables analysts to triage hundreds of alerts down to the few attacks that matter. This significantly reduces alert fatigue and allows security teams to focus on the most critical threats.. This streamlined process not only accelerates the investigation and response times but also empowers the security team to take immediate and informed follow-up actions, thereby enhancing the overall security posture of Hermes Germany.



With the Elastic AI Assistant for Security, we can help to take the pressure off our analysts by enabling them to do their jobs more easily, allowing them to spend their time focusing on more complex cases.

**Marco Uhl**  
SIEM Engineer,  
Hermes Germany



## 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](#)