

LEITWERK's CYBER FOX cuts digital forensics from weeks to days with Elastic Security

CYBER FOX, LEITWERK AG's cybersecurity team, replaced a single-agent security tool with self-hosted Elastic Security, onboarding 30 managed-SOC customers in nine months and cutting digital forensics from three to four weeks to three to four days.

Weeks → days

Digital forensics, 3–4 weeks to 3–4 days

30

Customers onboarded in nine months

Any source

Firewalls, Microsoft 365, Entra ID, endpoints

Self-hosted

Own data centers, for GDPR and DORA

The challenge

- ✗ The previous tool worked with one agent on one platform, so every customer had to replace their existing antivirus or EDR before onboarding.
- ✗ Firewall and other IT-layer data could not be integrated, blocking full infrastructure visibility.
- ✗ Analysts had little access to raw log detail during investigations.
- ✗ SaaS hosting in a public cloud outside Germany did not fit regulated customers' GDPR and DORA needs.

The solution

- ✓ LEITWERK implemented a self-hosted Elastic Security cluster in its own data centers, sized with Elastic solution architects after testing on Elastic Cloud.
- ✓ SIEM and Elastic Defend are used across customer endpoints, with firewall, Microsoft 365, and Entra ID data alongside.
- ✓ Timeline and Event Analyzer expose connections, processes, and registry changes in full detail.
- ✓ Cases share analysts' triage and risk scoring directly with customers.

How the workflow runs

1. Collect

Elastic Agent on endpoints, plus firewalls and M365

2. Store

Self-hosted cluster in own data centers

3. Detect & protect

SIEM and Elastic Defend (EDR)

4. Investigate

Timeline and Event Analyzer, full raw detail

5. Collaborate

Cases shared with each customer

Before

- Digital forensics took three to four weeks.
- Customers had to swap out their existing EDR before onboarding.
- SaaS operated in a public cloud outside the team's control.

After

- Digital forensics are available in three to four days, with data already in place.
- It deploys alongside existing infrastructure, ingesting any source.
- LEITWERK self-hosts in its own data centers, aligned to GDPR and DORA.

"The forensics that used to take us three to four weeks, we can now do in **three to four days**, because the endpoint data is already sitting in our own Elastic cluster."

— Kevin Zimmermann, Team Lead, CYBER FOX, LEITWERK AG

Why it matters beyond one SOC

Whether protecting a 10-seat business or thousands of endpoints across energy, healthcare, and defense, the principle holds: own your data, see it in full, and put analysts on top of the investigation. CYBER FOX is now testing Attack Discovery to speed Tier 1 triage and evaluating Elastic Agent Builder and Elastic Workflows, and the team plans to onboard at least 30 more customers next year.

[See how Elastic Security keeps years of security data searchable for investigations](#)
or [start a free trial](#) →