RAPID7

CUSTOMER STORY

Industry
Utilities & Energy

Region
EMEA

Size
Enterprise (mid-size)

Products
InsightConnect, Managed Detection & Response, Managed Service VM, Threat Command, Threat Intelligence Other, Threat Intelligence Platform

Package
Managed Threat Complete Advanced)

DOES YOUR BUSINESS REALLY HAVE AN ON-OFF SWITCH? THIS COMPANY CAN'T HAVE ONE.

ESB
ENERGIE SÜDBAYERN

OVERVIEW

Benjamin Nawrath says he's never liked people who break things. Things should work and be on.

He did not like them years ago when he started out at the help desk of German energy giant Energie Suedbayern (ESB). And today, in his role as the company's Deputy CISO, he likes them even less.

The energy sector is critical infrastructure.
ESB is a particular challenge to defend

It's a natural gas and electricity supplier to 120,000 households in the south of Germany, making it the largest operator in the region with a complex, sprawling environment that includes 2,000 IP addresses and highly sensitive industrial control systems.

Like so many energy companies, ESB has been in a transformational process: reacting to climate change, focusing on renewables, solar parks, charging infrastructure for electric vehicles, even trying to use old gas pipelines to transport hydropower.

During this transformation – which has IT and security burdens of its own – Germany passed the IT Security Act. It ordered critical infrastructure like ESB to establish advanced cybersecurity programs, ensure the availability and integrity of IT infrastructure, and start providing regular proof of compliance. Failure to do so could result in a fine of hundreds of thousands Euro.

It was a journey from solo operation to real sophistication.
Rapid7 was right there, every day.

Nawrath used to call himself "a one man cyber army."

ESB IS A NATURAL GAS AND ELECTRICITY SUPPLIER TO

120,000 HOUSEHOLDS

IN THE SOUTH OF GERMANY

The energy sector is critical infrastructure.

ESB IS A PARTICULAR CHALLENGE TO DEFEND.

THE SOLUTION

Using the Rapid7 Command Platform, he says everything was easy to set up and maintain with one agent to rule them all. By unifying SIEM, user behavior analytics (UBA), and extended detection and response (XDR), he was able to ease compliance and clock 60% time savings.

But at some point, even the most committed security guy wants a good night's sleep. Maybe even a vacation. That's when Nawrath started moving the company into Rapid7 managed services, which he considered a natural next step.

Managed Detection and Response (MDR) delivers continuous 24/7 attack detection and regular updates to detection rules, ensuring protection from the latest threats. The service includes a 13-month data retention period, allowing customers to meet compliance requirements and perform long-term analysis.

Rapid7's MDR also offers unlimited Incident Response (IR) and forensic support, giving confidence that any security incidents will be addressed promptly and thoroughly.

THE UPGRADE TO MANAGED THREAT COMPLETE WAS NEXT.

THE OBJECTIVE: A STRATEGIC REBALANCING OF WORK.

Managed Threat Complete combines MDR with industry-leading vulnerability management technology. And it's for customers who agree cybersecurity has over indexed on reactivity, leading to fire drills, burnout, and missed threats. It's time to make environments less likely to be breached in the first place.

Rapid7 continues to take care of monitoring and reacting 24/7, and Nawrath's team leans proactive, shutting down vulnerabilities. But he's also on the platform daily, keeping an eye on anomalies, going through his own task list. He finds the Microsoft Defender for Endpoint interface complicated, so all alerts run through Rapid7's SOC. (It's time to, say "No" to black box technology, and "yes" to third-party event sources, everybody!)

Go on offense and watch what happens.

ESB'S RESPONSE SPEED IS 40% FASTER.

Threat Command by Rapid7 allows Nawrath's team to uncover intelligence that matters to ESB and Germany's energy sector from the clear, deep, and dark web. As always, it was easily, effortlessly integrated into the platform.

When the team wanted to monitor malicious IPs and malware file hashes for quicker threat detection, Rapid7's Threat Intelligence Platform (TIP) gave them expert access to Rapid7's threat database, enabling deep dives into dark web threats. The Threat Library goes even further by including feeds from various other trusted sources, offering a broader threat landscape view.

While there's always something next to do, Nawrath has never had so much confidence in the security program. "It's a managed platform where everything gets together," he says, "and I'm not the only one looking at it. It's an all-in-one solution."

> **"It's a managed platform where everything gets together," he says, "and I'm not the only one looking at it. It's an all-in-one solution."**
>
> Benjamin Nawrath, Head of IT Systems Engineering and CISO at ESB

TEAMWORK: RAPID7 IS THERE FOR THAT.

View more success stories.

CUSTOMER STORIES

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight