MATRIX42

Case Study

Endpoint Security ZAE Bayern

> **"**
>
> **Endpoint Detection Response (powered by enSilo) out of Matrix42 Security Suite came out on top because it performed to a consistently high level across all the elements in our testing process.**
>
> Christian Hilgers, IT Group Leader, ZAE Bayern

Brief Overview ZAE Bayern

ZAE Bayern is a non-university institute for applied energyresearch with about 240 employees, institutionally funded by the Bavarian Ministry of Economic Affairs, Energy and Technology. In its central fields of expertise, renewable energies, energy storage, and energy efficiency, ZAE Bayern combines materials research, development of components, and system optimization in an interdisciplinary approach. ZAE's researchers work, among other things, on thermal and electrochemical energy storages, energy efficiency in processes, energetically optimized buildings, photovoltaics, nanomaterials, smart grids, and cross-sector energy systems (electricity and heat/cold). With its three main locations Erlangen, Garching near Munich, and Würzburg, as well as its branches in Nuremberg and Hof, ZAE Bayern is present statewide and offers complete innovation packages to its customers when it comes to efficient and sustainable energy systems. For further information visit www.zae-bayern.de.

Challenge

In 2017, the IT team at ZAE Bayern decided it was time to modernize its approach to securing its inventory of PCs and laptops from increasingly numerous and sophisticated cyber threats. The organization needed a solution that could protect over 300 devices from a wide range of malware and ransomware. The solution also needed to be fast and easy to deploy, and provide excellent centralized, real-time visibility over device status. And, as a non-profit organization with a small IT team, ZAE Bayern also needed the solution to be easy to use and manage. At a TAP.DE event in Munich, the ZAE team learned about the extended Matrix42 portfolio and the possibilities it offers. Due to the existing relationship of trust between ZAE and TAP.DE, they decided to include Matrix42 Endpoint Detection Response (powered by enSilo) into the running evaluation. Together with Matrix42 TAP.DE Solutions accompanied the complete evaluation phase.

Solution

After testing eight solutions thoroughly, Matrix42 EDR was selected for its high levels of performance across the board. The responsiveness of the pre-sales team and senior executives, and the addition of attractive new features during the selection process were also key factors. The EDR software was deployed quickly and easily across all ZAE Bayern's devices by mid-2018. It will also be running on the organization's twenty servers by the end of the year.

Company
ZAE Bayern

A modern endpoint security solution that can cope with the sophisticated reality of 21st century IT security threats.

As a non-profit research organization, ZAE Bayern has more reason than most to ensure maximum cost-effectiveness in every investment it makes, including IT. At the same time however, the nature of its work in supporting industrial innovation demands that it leverages the latest technology as well. That's why, after using a signature-based antivirus product for many years, IT leaders within the organization decided in early 2017 that it was time to look for a modern, commercial solution. Christian Hilgers, IT Group leader at ZAE Bayern explains: "We determined that the potential threats to our 300 or so PCs and laptops running Windows 7 and Windows 10 were becoming more numerous and sophisticated. We also knew that the solution we had in place to protect those endpoints from viruses and malware was not really suitable for today's world. For example, it provided no exploit protection, and we had no deep visibility over events on our devices."

Establishing selection criteria

Speaking about the process involved in selecting a new solution, Hilgers says, "We started thinking seriously about it in the summer of 2017 and began testing in earnest in October/November. Initially we looked at 14 different products and then narrowed that down to a shortlist of eight." The key selection criteria Hilgers and his colleagues focused on included:

❯ **Broad protection:** Coverage of a wide range of threats, including ransomware

❯ **High recognition rate:** The ability of the solution to recognize malware

❯ **Exploit detection:** The ability to detect threat penetration, tested mainly using the Metasploit penetration testing framework

❯ **Deployment speed:** The ability to roll out the solution across all devices using a single deployment agent

❯ **Ease of use:** Especially in the mobile environment, it should be straightforward for users to stay secure without having to log on to a VPN

❯ **Ease of management:** Because a small organization like ZAE Bayern does not have the resources for complex administration

❯ **High visibility:** The ability to see what is happening on particular end points and respond appropriately

❯ **Event graphs:** To illustrate what is being blocked and why

❯ **High availability:** The solution should continue to function even if the cloud isn't available, for whatever reason

Matrix42 EDR proves its worth

At the end of the evaluation process, there could be only one outcome, as Hilgers confirms: "Matrix42 EDR came out on top because it performed to a consistently high level in all aspects of our tests." However, that wasn't the only reason behind the decision. "We were already long-term customers of Matrix42's enterprise management and service store solutions. So, the fact that enSilo was one of Matrix42's new key technology partners was an important factor. We were also very impressed with enSilo's level of respon-siveness– we had face-to-face contact with the CTO, which is something that would never have happened with the other vendors we talked to, because our company is relatively small. This gave us great confidence in the relationshipand the roadmap. Even though Matrix42 EDR is a young product, we saw a lot of potential. The fact that several features we needed were added to the solution during the presales process made Matrix42 EDR an even more attractive proposition for us."

Smooth rollout, satisfied customer

Matrix42 EDR was deployed to around 50 devices in January 2018 to examine how the solution handled false positives. After some outstand-ing work from the pre-sales team to clarify technical issues, ZAE Bayern switched from a test license to a commercial one in April. The full agent-led deployment was completed quickly and will be extended to cover around twenty servers by the end of the year 2018.

"After three days, around 70% of the computers used for scientific work were protected by the new solution. Deployment to devices that are not always running took around a month in total. Overall, the process was fast, easy and didn't require device restarts, which was important. I am extremely happy with the EDR solution of Matrix42, and I'm looking forward to how its functionality will evolve to provide us with even better endpoint security in the coming years," concludes Hilgers.

> **"**
>
> **We were also very impressed with enSilo's level of responsiveness – we had face-to-face contact with the CTO, which is some-thing that would never have happened with the other vendors we talked to.**
>
> Christian Hilgers, IT Group Leader, ZAE Bayern

MATRIX42

www.matrix42.com

Simplify and Secure
Digital Work

About Matrix42

Matrix42 helps organizations digitize and secure the workspace environment of their employees. The software for digital workspace experience manages devices, applications, processes and services simple, secure and compliant. The innovative software supports the integration of physical, virtual, mobile and cloudbased workspace environments seamlessly into existing infrastructures.

TAP.DE

The TAP.DE group of companies supports medium-sized companies, corporations and public institutions in the development and optimization of business processes and the sustainable operation of IT work environments. The specialists of TAP.DE develop strategic concepts for the areas Workplace Automation, Endpoint Security, IT Service Management and Compliance. The focus is always on practicality, quickwins and the improvement of internal processes and services.

Follow us