



Case Study

Software developer monitors critical infrastructure

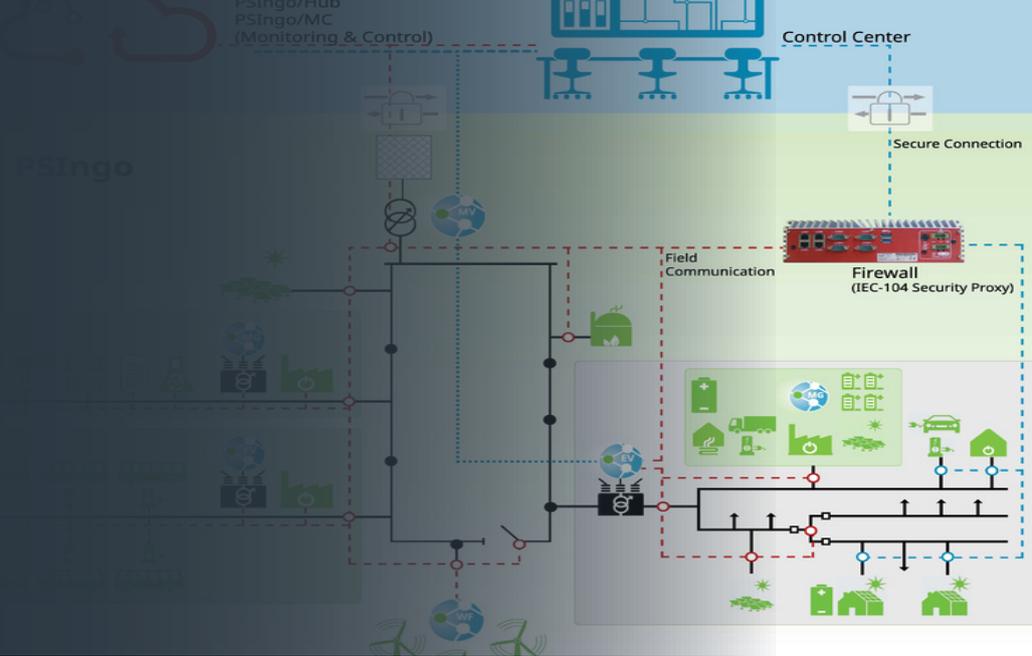
THE CLIENT

Company: PSI Software AG

Size: 2,000 employees

Location: Berlin, Germany

Website: www.psi.de



The PSI Group develops and integrates complete solutions for optimizing the flow of energy and materials at utilities and industrial enterprises on the basis of its own software products. Part of its range includes various managed services in which strict security requirements are observed for all tools used. Depending on the industry and customer specifications, differing compliance guidelines may need to be implemented.

KEY POINTS

-  PSI has relied on Checkmk's Managed Services Edition since 2017 to monitor assets at its customers. These include, for example, Europe's largest electricity producers and providers of critical infrastructure.
-  PSI's IT team chose Checkmk because, among other factors, it is suitable for monitoring assets in sealed-off environments.
-  PSI currently operates 20 Checkmk instances with a total of around 8,000 hosts and 60,000 services. Their IT team has configured the monitoring to regularly transfer all customer monitoring data to the central Checkmk instance exclusively by email.

SOFTWARE PIONEER SEEKS MONITORING TOOL

PSI has been enjoying success as a provider of software solutions for energy utilities since 1976. Since then, the company has grown sustainably by continuously optimizing its technologies and adapting its products to market requirements. Against the backdrop of increasing security requirements on the part of customers, PSI decided to set up a monitoring service and for this purpose was looking for a suitable tool.

Following an intensive review, in 2017 the company decided to adopt the Checkmk Managed Services Edition. This was found to be the only tool suitable for meeting strict security requirements, such as the guidelines under the German IT Security Act or the EU Cybersecurity Act, while at the same time being highly flexible in its transferring of monitoring data. In addition, it can be set up locally at the customer's site in isolated environments and is easy to use.



Figure 1: PSI monitors critical infrastructure

The ability to transfer monitoring data to the central Checkmk instance via email is particularly important. This is necessary because most monitored assets are located in data centres with sealed environments and these data centres can only communicate with the outside world via email. The first step in the implementation is essentially the same as in other scenarios: PSI sets up a Checkmk instance as a virtual appliance in the customer's data centre. IT assets of all kinds, such as servers or network devices, are monitored there. PSI receives the necessary access rights from its customers for the implementation.

THE CHALLENGE

PSI was looking for a solution for providing monitoring services to energy companies. In addition to the general requirements for large companies, such as scalability and easy management of distributed monitoring, this also had to meet strict specifications. These include, for example, the IT security regulations and internal compliance requirements for electricity producers.

The systems and the monitoring mechanisms differ depending on the environment. As a rule, PSI relies on monitoring via Checkmk agents and rolls these out locally via the Ansible automation tool. In addition, PSI monitors devices via SNMP thanks to the numerous official Checkmk plug-ins. PSI also uses some of its own self-written extensions.



The options for the integrations never cease to amaze me. The range of devices that can be integrated is, in my opinion, unique in the monitoring world.

Gerald Amrhein, System Support at PSI Software AG

There are still some active installations where the IT team has set up Checkmk on SLES11. However, using the virtual Checkmk appliance is much more convenient and simplifies security audits. It also makes it easier for the IT team to roll out new Checkmk versions.

MONITORING FOR HIGHLY-SECURE ENVIRONMENTS

Currently, customer instances cannot be connected to the central Checkmk instance in Aschaffenburg via the live status interface. Instead, the IT team made it possible for data to be transferred from the customer instances to the PSI head office via email without the central instance having to make an external request.

For this purpose, the IT team sets up a mirrored site with identical hosts and services for each customer Checkmk instance at PSI's IT centre in Aschaffenburg. The customer instances transfer their monitoring data every two minutes using `cmcdump`. A Cron job ensures that the config files are sent by email to a mail server at PSI central office. A `fetchmail` then extracts the emails from

THE SOLUTION

PSI opted for the Checkmk Managed Services Edition in 2017 and set up a special monitoring system. The Checkmk instances at the customer's site were configured in such a way that they transfer information on hosts and services via email every two minutes to mirrored sites at PSI. The mirror sites, in turn, are remote sites of the central Checkmk instance, which is also set up at PSI's Aschaffenburg site.

the inbox folder for further processing. A bash script recognises the matching mirror site via the customer's name in the subject line and imports the monitoring data on the matching Checkmk instance. This approach works because Checkmk never relies on central data storage and is flexible in processing input.

The mirrored sites are located in a segmented network together with the central instance. As a result, distributed monitoring with live status is now possible here. All information converges in the central Checkmk instance. PSI thus has an overview of all details and can react immediately to incidents. All email communication is encrypted via PGP. The IT team wrote the necessary scripts themselves.

Currently, data from 20 data centres at more than 10 customers in the energy sector converge in the central instance. PSI monitors a total of 8,000 hosts and 60,000 services. The mail server processes 15,000 emails daily.

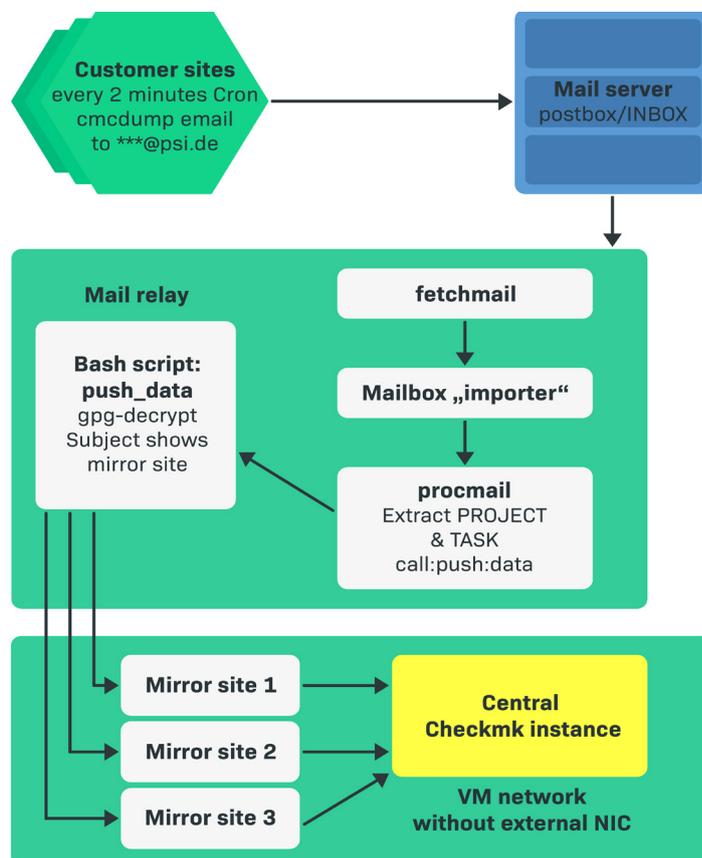


Figure 2: Structure of distributed monitoring via email

The enabling of read rights allows each client to view their assets and thus creates transparency. The Managed Services Edition of Checkmk allows for the secure separation of client data and protects against unwanted access.

THE ADVANTAGES

PSI has created a unique service solution. Despite locking down and observing the highest security requirements for the monitored infrastructure, the IT team has a full overview at all times and can react quickly to even the smallest anomalies. The IT experts have all metrics in their sight and can efficiently initiate measures should the need arise.

INTEGRATION OF FURTHER LOCATIONS IS IN PROGRESS

The transfer by email works very well and provides great added value for the customers. The IT team does not always have to be on site and still has an overview at all times. PSI is working on the integration of ten more customer sites and would like to expand the monitoring to include new systems.



I am pleased that we were so discerning in the selection of the monitoring tool. With Checkmk, we are very well positioned for audits and new challenges.

Gerald Amrhein, System Support at PSI Software AG

For example, PSI plans to monitor its customers' control modules. Checkmk can monitor these via SNMP, but such assets are usually located in other network segments. For this reason, the software company is working on a proxy server that serves as a kind of secure SNMP relay.



Figure 4: Europe's largest energy companies rely on PSI

A further challenge is the implementation of the company's own Information Security Management System (ISMS) process to ensure certification according to ISO/IEC 27001. Here, the IT team is in dialogue with their internal compliance officer. The requirements are high, but thanks to the experience of the PSI staff and the adaptability of Checkmk, the implementation is progressing well.

Press contact:

tribe29 — the Checkmk company
Kellerstrasse 29
81667 Munich
Germany

E: info@tribe29.com
T: +49 89 9982 097 00