THERMANA
Laško

CASE STUDY

The protection of critical system guaranteeing seamless business operations and the safety of guests at Thermana Laško

> When choosing solutions, we always keep in mind that we need to maximise the security of our guests, which is taken care of by both, our employees and the systems.

Jernej Gostečnik
Head of Organisation and IT

Foto: Aleš Rosa

SMART COM

TREND MICRO
Technology partner

Thermana d. d. *is one of the most modern tourist facilities in Slovenia with a long-standing tradition of more than 160 years. With services based on superior knowledge, extensive experience of recognised medical experts, and healing properties of the thermal water, they help guests stay healthy. The company consists of three key centres: The Laško Health Resort, which offers mostly medical services, the tourist complex and the Thermana Park Convention Center, and the Laško Retirement Home.*

The safety of their guests, patients and residents is their primary focus. The operation and control of industrial systems that are critical to business operations, with the most important being the chlorine dosage swimming pool technology system, are also key factors. When integrating the industrial systems into the business environment, they were faced with security risks.

In accordance with the security policy and the business continuity policy, they were looking for a solution to provide the security and seamless operation of the integrated system.

The complementary technological solution by Trend Micro, as well as the Safe Lock and Portable Security 2 products, provided a comprehensive protection of those systems against malicious codes and allowed control over the running applications. This ensures an effective protection of critical systems without an Internet connection (offline).

The Smart Com team participated in the successful project implementation.

The challenge

To ensure the safety of industrial systems that control the swimming pool technology, heating, etc. when connecting to the business environment in light of malicious code risks and in accordance with the business continuity policy.

The solution

The introduction of the complementary Trend Micro Safe Lock and Trend Micro Portable Security 2 products provides protection for the older, closed systems that are not connected to the Internet and therefore do not have the possibility of installing an anti-virus protection and security patches. The key is to ensure control over the installation of unauthorised applications, thus guaranteeing the security of surveillance systems.

The effects

- Insight and control over the implementation of critical industrial systems management.
- A detailed inventory of the system (controllers), and the security and process risks involved.
- A list of programs that are not being allowed into the system, which is very important for the business and the work of external contractors.

Foto: Thermane Laško archives

Thermana d.d. places great emphasis on cybersecurity as well as the management of security and process risks. This is the responsibility of the Organisation and IT Department, which is responsible for business and system informatics as well as process organisation. Together with his colleagues, Head of Department Jernej Gostečnik is responsible for the implementation and maintenance of systems that meet the needs of their processes.

They enforce both the security policy and business continuity policy that identifies critical systems which need to be protected and duplicated by all means for the business to run smoothly. The first security objective is to stop a security incident or make sure it does not occur at all. The second security objective is to make sure that the redundancy system takes care of data security in the event of an incident.

Integration of industrial systems into the business environment introduces new security risks

The entire system is based on the virtualisation of server systems that are installed and managed in a central system space. All three sites that are managed by the Organisation and IT department are connected by optical links. Until 2018, the industrial systems that control the swimming pool technology, heating etc. were always separated from the other IT systems. In 2018, these systems have been unified and deployed in a virtual environment. The centralisation has introduced new security risks associated with the possibility of unauthorised access and uncontrolled deployment of applications. It was therefore necessary to strengthen the security mechanisms.

The challenge, however, was not to connect the systems in technological terms, but also to ensure a connection between the teams – the Organisation and IT department and the Maintenance department, which is responsible for managing and properly controlling the industrial systems, even in the event of a failure due to a security incident.

Even the closed, isolated systems are not safe from malware infections

The protection of industrial systems has been guaranteed by the introduction of the solution proposed by the Trend Micro technology provider. The older systems that are in use on a daily basis work properly, but they cannot benefit from the installation of a modern anti-virus protection or an operating system upgrades conditioning the upgrade of system patches with an Internet connection.

The Trend Micro Portable Security 2 solution provides adequate protection, because it allows the users to scan the systems for malicious software (anti-virus, anti-malware) and remove it without an Internet connection, which means it is suitable for systems where anti-virus protection cannot be installed. This allows the management of upgrades (even the unexpected ones) which would otherwise expose the functioning of critical systems to certain risks in the event of uncontrolled updates.

> There was a possibility that someone could come with a USB and download a new version of the application, update the controller, and compromise the performance of critical systems.
>
> We solved this issue with the Trend Micro solution, which protects the old (legacy) systems without an Internet connection and prevents an uncontrolled installation of unauthorised applications.

Furthermore, the Trend Micro Safe Lock solution prevents the installation and launch of unauthorised applications which can cause malfunctions of controllers that are critical to the operation of systems. The solution also provides protection against the introduction of malicious code from external drives (network folders, USB sticks).

Foto: Aleš Rosa

From this point of view, the protection of the pool's technical system, i.e. controllers for the regulation of disinfection chlorine dosages, is very important for Thermana d.d. While harmless in lower doses, chlorine is a health hazard when used excessively.

The Trend Micro Safe Lock solution enables the user to build a database of allowed applications (executables, various system libraries, drivers and other files required for system operation) to manually or automatically manage the applications, actively monitor processes, and control external disks.

> It is important for us to have control over the events in our systems, and to prevent the implementation of unauthorised programs.
>
> We simply cannot afford for a virus to disable the programs responsible for control, which, in view of our continuous operation policy, can result in major issues in system operation or their failure, which can in turn cause business damage or even threaten the life and health of our guests.

Smart Com solution provider and integrator also provided training for the maintenance team in the form of a workshop where they learned about the practical use of the solution. It is the maintenance department that is responsible for periodically checking the performance of the system, monitoring the status of the systems and updating them. Due to the 'offline' mode of operation and security policy, protocol updates are performed once a month.

Use the Trend Micro solutions to fight security and process risks that may result in business disruption or commercial damage

With the introduction of the Trend Micro solution, Thermana d.d. reduced the risks that arose when connecting together the industrial and business systems.

The solution allows them to easily protect their systems against advanced cyber threats. The solution provides a system verification and allows malware removal and protection against its execution, as well as protection against the installation of unauthorised applications.

A full insight into the system events improves the security and confidence in the work of external providers who access the systems for maintenance. Verification of their systems and the computer they connect to is no longer necessary, as the Trend Micro solution makes sure that unauthorised programs are not allowed to enter the system.

A detailed inventory and list of systems and controllers were prepared when implementing the solution. This helped determine the actual situation, which allowed control over the elements and prevented security risks associated with the unfamiliarity with the network situation.

Experience

- Since the installation of the Trend Micro solution, there have been no system failure complaints.
- The control systems and the process network management work flawlessly.

Foto: Aleš Rosa

The main advantages of the Trend Micro solution

- ✔ Simple to use, requiring minimal resources.
- ✔ Centralized or stand-alone management.
- ✔ Offers wide support for various Windows operating systems.
- ✔ Suitable for industrial ICS control systems (SCADA), HMIs as well as dedicated closed systems and terminals.

Trend Micro Portable Security 2

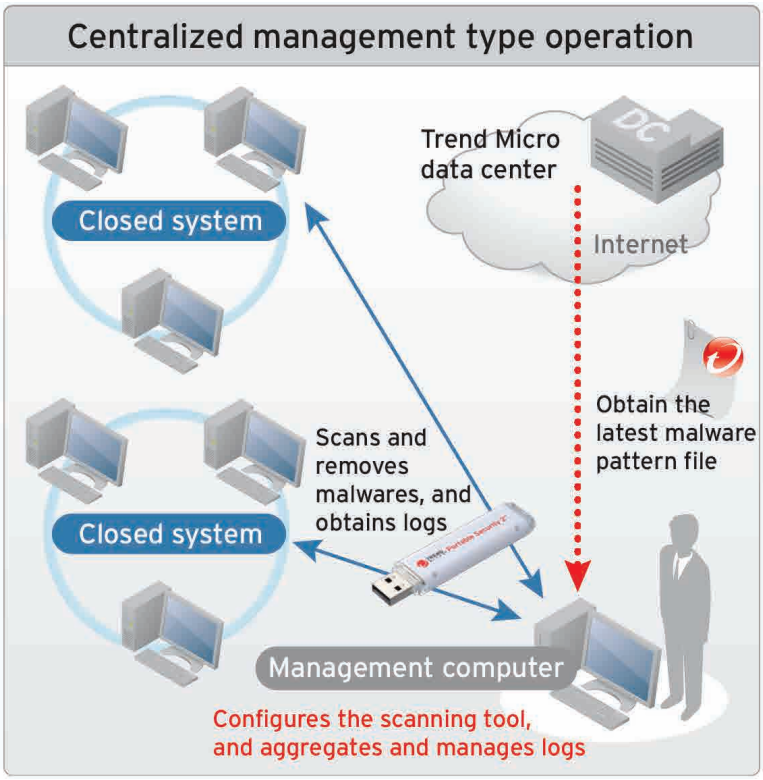
- ✔ Allows system verification and removal of malicious code.
- ✔ Suitable for offline systems that cannot benefit from security fixes and antivirus protection.
- ✔ Requires no additional software installation, since the software protection is started directly from an USB stick.

Trend Micro Safe Lock

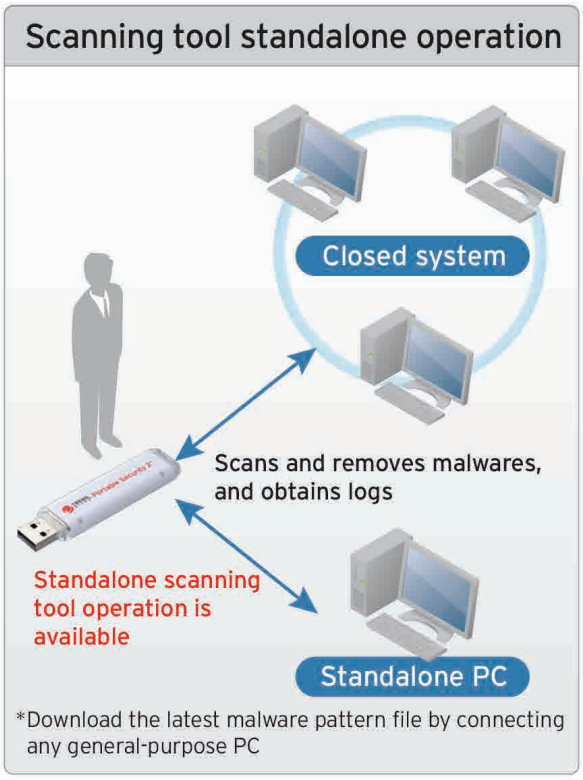
- ✔ Prevents unauthorised applications from running.
- ✔ Protects against the execution of malicious code (viruses, malicious code, advanced threats).
- ✔ Control over external drives (USB, network drives).
- ✔ Allows a centralised agent management:
  - event overview (agent statuses and breaches),
  - automated system status reporting and e-mail notifications.

Overview of the Trend Micro Portable Security 2 solution implementation

Centralized management type operation

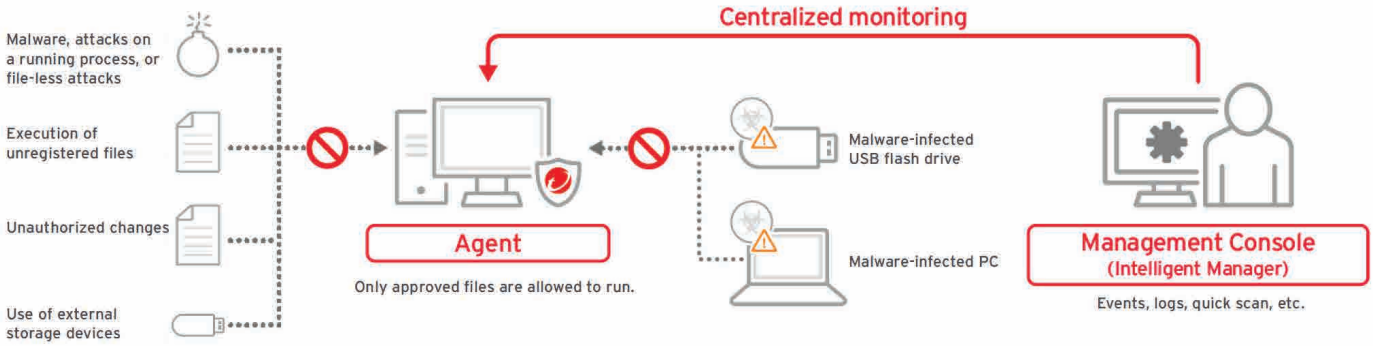


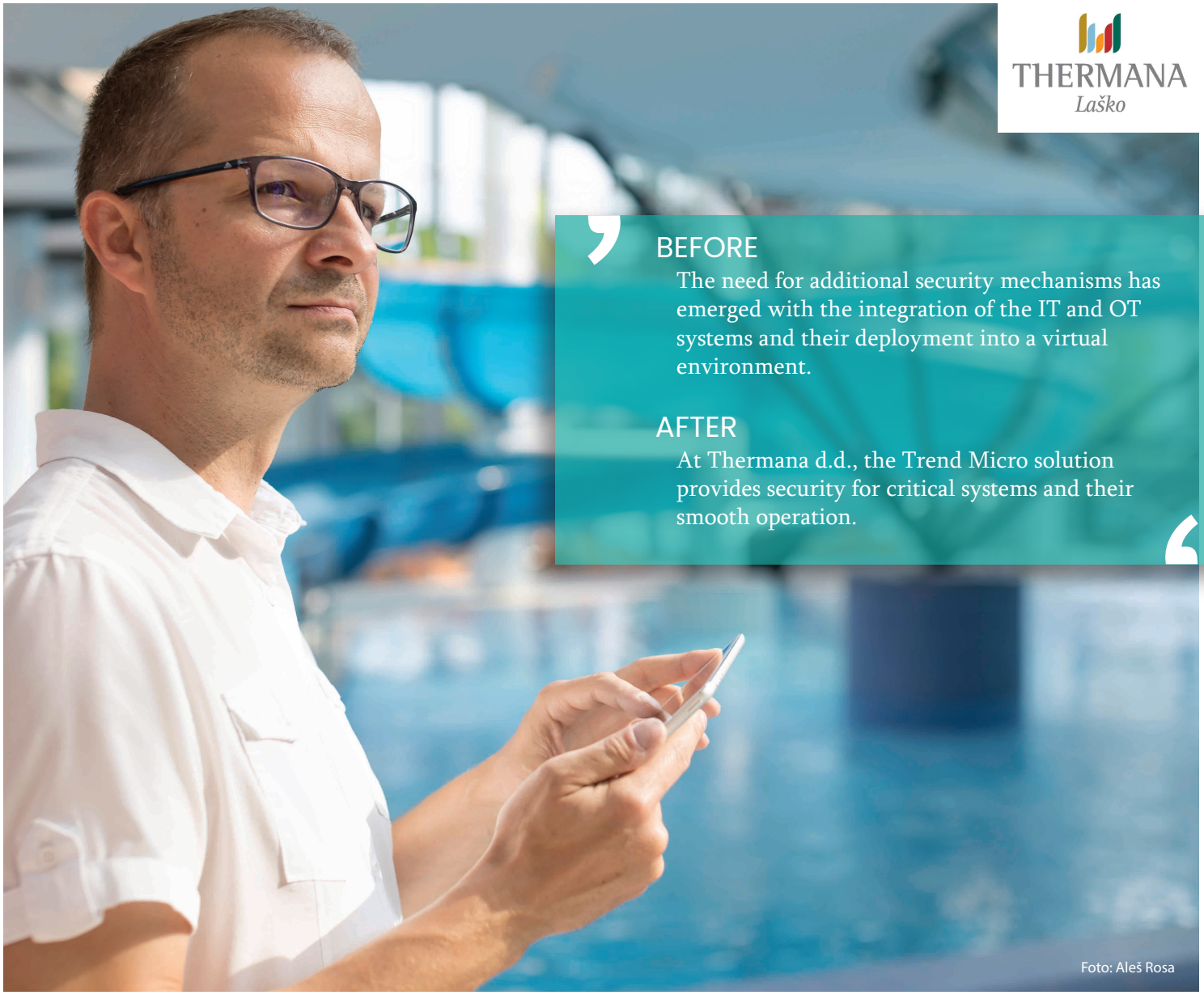
Scanning tool standalone operation



*Download the latest malware pattern file by connecting any general-purpose PC

Overview of the Trend Micro Safe Lock implementation





The inactivity of specific units or the entire industrial environment and, thus, of critical systems, can be a disaster for the company. For this reason, the information and communication security measures must be carefully planned before the integration of industrial and business processes. The Smart Com team of experts can offer assistance in such cases.

If you are facing such challenges, we would be happy to assist you in selecting and implementing a technology solution that is user-friendly, functionally sophisticated, and affordable. In addition to implementing the system and providing consulting services, we can also provide system maintenance and technical support.

info@smart-com.si 01 5611 606 www.smart-com.si

SMART COM

TREND MICRO
Technology partner