IKARUS security software

IKARUS mail.security

Datasheet

Email security with ATP option

Thanks to world-leading security technologies, **IKARUS mail.security** not only detects viruses, malware and harmful attachments in emails: harmful URLs, malicious codes, phishing attempts and zero day attacks are blocked before they reach your network.

The cloud-based high-performance security solution for email gateways secure the main gateway against spam, malware and phishing attempts: With real-time protection, ATP add-on and unlimited recursive archive scans, **IKARUS mail.security** blocks undesired emails, malware, harmful URLs and attachments unnoticed, even before these penetrate your systems and cause damage.

Inbox gateway: growing number of ATP attacks

Ransomware or targeted high-tech attacks (APT - advanced persistent threats) are often personally addressed to the recipient and freely customized to the selected companies. Some use plausible attachments such as invoices for purchases actually made or application letters to current job vacancies. Others do not come with malware but with a tempting URL instead that lurks behind the actual malicious code. Once the attackers gain access to the system, they behave inconspicuously to remain undetected for as long as possible (persistent). They initially identify further weaknesses in the system before reloading suitable damage routines.

Delaying and cover-up tactics

This delayed momentum and exploitation of as current as possible, unpatched weaknesses make it very difficult to identify a successful attack. By means of targeted, multi-level analyses, **IKARUS mail.security** reduces the risk of intruders to an absolute minimum and provides you with clarification as to whether the attackers currently have you in their sights.

With one of the world's best carrier-grade scan engines for enhanced content analysis and the supplementary ATP add-on, **IKARUS mail.security** offers maximum security for your SMTP traffic: In addition to the dynamic and heuristic analytical method of the IKARUS scan.engine, all emails that have been classified as neither harmful nor harmless, even after hundreds of reputation and content-based checks, are checked using the signatureless sandboxing approach of FireEye and other market leaders. The targeted application of these extended possibilities for analysis provides small and medium-sized enterprises (SMEs) with affordable access to highly professional security measures and the highest possible level of protection.

© IKARUS Security Software GmbH

Maximum data security and user friendliness

Additional benefit for your data security: Software development, data processing, analysis and support take place in Austria, adhering meticulously to the European General Data Protection Regulation. No data is passed on to third parties, all analyses are carried out exclusively in the data-processing centre in Vienna. A central dashboard offers flexible access and a quick overview of all security services, equipment and network status as well as statistics and analyses.

Multi sandbox approach and post incident management

For the extended ATP analyses by partner technologies, only data for which the IKARUS scan.engine does not come to any reliable conclusion is analysed again in parallel – these are in the per mile range of the entire data volume. Our technology partners' sandboxes are installed in the IKARUS Scan Center, so that all data – according to the EU GDPR only meta data such as attachments or scripts are sent – remain in Austria. Although the sandboxes themselves constantly receive updates from the manufacturer, they are sealed off so that they cannot telephone home.

Even if an attacker succeeds in placing its code via email, despite multi-level defence barriers, time is against them: **IKARUS mail.security** also reviews emails, attachments and URLs already sent for up to 14 days with every update. In case of a security incident – a delivered email that could yet not be identified as malware at the time of delivery – the post incident management system sounds the alert immediately. IKARUS therefore offers the most efficient protections against malware, spam and targeted attacks currently available. EU GDPR compliant, cost-efficient and with no additional technical expense on your part.

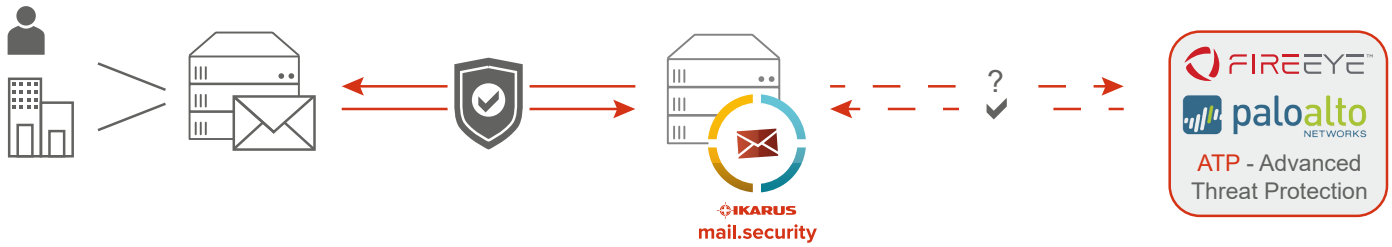

Fig. 1 - **IKARUS mail.security** scans all incoming and outgoing emails before they reach your network.
The sandboxes by FireEye and PaloAlto can optionally be switched on.

Advantages

- Highly-professional scalable solutions, suitable for multiple clients and individually customizable
- Real-time protection with the highest possible detection performance as well as the fastest possible scan and reaction times
- Highly efficient global threat intelligence thanks to international data and partnerships
- Multi-level behaviour-based analyses using your own simulators and integrated sandboxes
- Automated reports & statistics on the threat situation as well as detailed logging of all functions
- Temporary archive solution for incoming and outgoing emails and post incident alerts

Highlights

- Virus and malware scans, reactive and proactive malware detection
- Behaviour-based analyses of executable files, macros, scripts, archives
- Antispam concept with greylisting, Bayesian & lexical analysis, SPF and other protocols
- Adaptive spam evaluation system and client-specific filters and actions
- Flexible configuration options with blacklists and whitelists, including flexible filter options
- TLS encryption
- Multi-client capability with customizable admin and user interface

© IKARUS Security Software GmbH

»The IKARUS software reacts extremely quickly to local threats and has already protected us from numerous attacks – it is a fixed component of our security concept.«

Eng. Janusz Russocki - Head of IT at WITTMANN Group

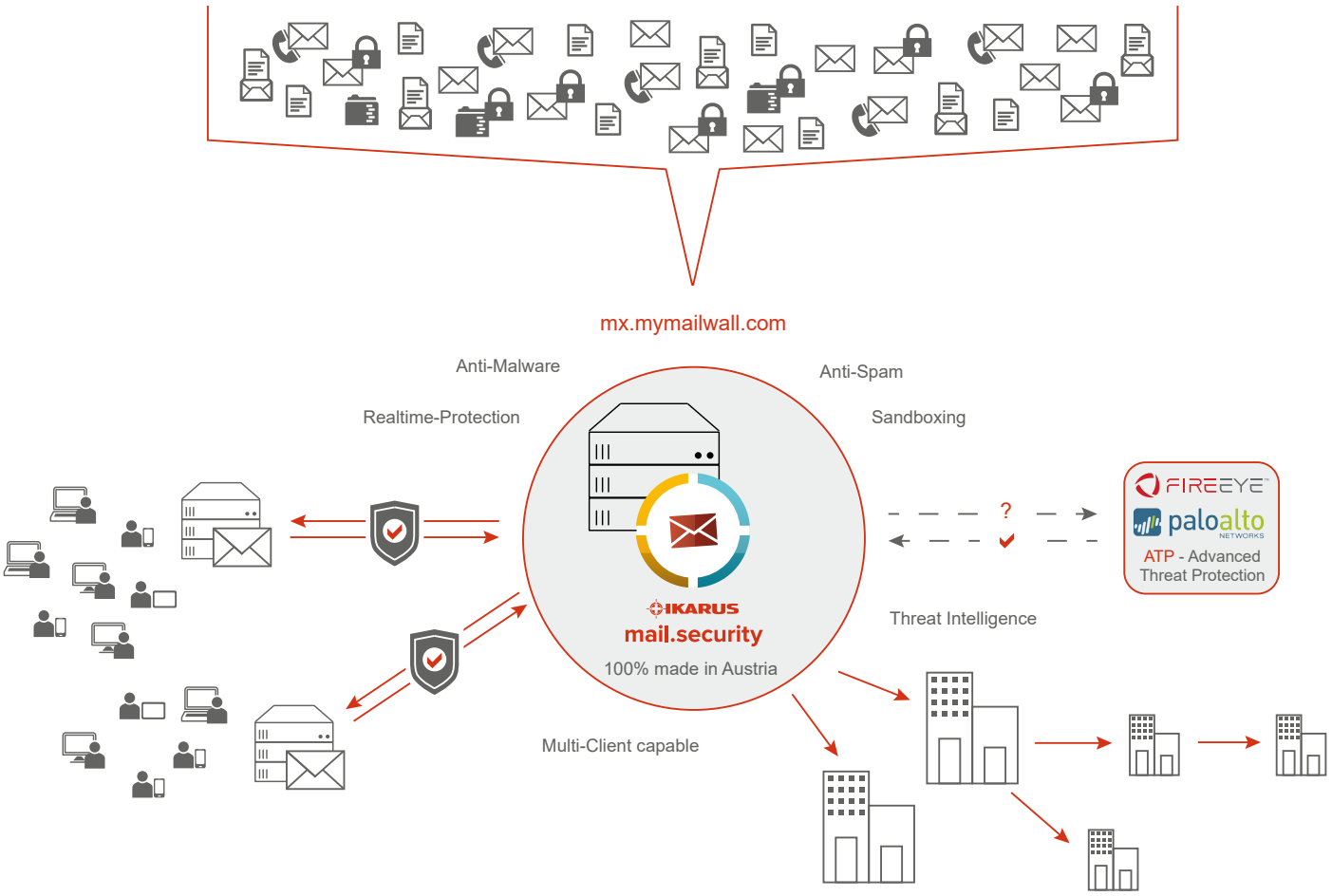

Fig. 2 - **IKARUS mail.security** features: Anti-Malware, Antispam, Attachment-Filter & Sandboxing

System requirements

- Internet connection
- Own email domain

About IKARUS Security Software

As a pioneer of the antivirus industry, IKARUS Security Software has been familiar with the requirements for intelligent IT security systems since 1986. The Austrian antivirus specialist, IKARUS Security Software, has been developing and operating viable security solutions from its own scan engine through managed security services up to SOC/SiEM services for IT / OT / ICS environments.
With its in-house scan engine and local development, data processing, support and virus laboratory, IKARUS is the Austrian contact for your IT and OT security questions.