



IKARUS mail.security

Secure Email Gateway to
protect against phishing,
spam, malware and abuse

Most cyber-attacks start with an email - from phishing, ransomware and malware attachments to social engineering attacks, credential harvesting and data theft. Email security is therefore essential for all organisations.

IKARUS mail.security is a comprehensive cloud solution that is multi-tenant and scalable for organisations of all sizes. Through a targeted combination of analysis techniques, IKARUS mail.security not only detects malicious code and spoofed URLs in real time. It also prevents phishing attempts, zero-day attacks, identity misuse, targeted attacks, and manipulation.

Malware scanning and phishing detection

The IKARUS Malware Scan Engine, developed in Austria, scans, and analyses all emails and attachments for malicious code and malicious behaviour. It stands out for its speed and consistently high detection rates, regardless of the operating system for which the malicious code was written.

In addition to traditional signature-based methods, it uses multi-stage analysis techniques that analyse, execute, monitor, and evaluate content regardless of its format. It also analyses URLs in emails and attachments and evaluates the target pages behind them - a process that is repeated each time the link is clicked to block subsequent infected websites.

Spam detection and spam defence

IKARUS mail.security uses a multi-layered approach of greylisting, Bayesian and lexical analysis and other in-house developed analysis techniques to evaluate emails for spam characteristics. The spam scoring thresholds and actions for suspected spam - deletion, tagging or forwarding to an internal mailbox - can be customised, as can the associated notification texts. All emails are archived for 14 days as a back-up.

Advanced Threat Protection (ATP)

For the highest level of protection against targeted attacks and zero-day exploits, files of unknown status - content that has not yet been definitively classified as malicious or benign - can be subjected to additional sandbox analysis. Attachments are executed and analysed on a wide range of combinations of operating systems, web browsers, applications, and plug-ins. This targeted use enables our customers to benefit from this complex technology in a time- and cost-efficient manner.

The global sandboxes of our technology partner Trellix are installed and isolated in the IKARUS data centre in Vienna to ensure local data processing and strict compliance with the EU GDPR. In addition, only metadata, attachments and scripts are transmitted for the sandbox analyses.

Email encryption and signature with S/MIME certificates

To prevent data theft and social engineering attacks and to protect your business secrets, IKARUS mail.security enables the integration of S/MIME certificates. S/MIME certificates are issued by the recognised certification authority Certum and enable automated, client-independent encryption and signing of your emails. IKARUS handles the transmission of the certificate signing request as well as the verification of the company and the email addresses for you.

Signing and encryption rules - for individual mailboxes or by domain, for all or specific recipients, for incoming and outgoing emails, optional or enforced... - can be varied per mailbox or per recipient and adjusted at any time in the IKARUS Portal. You can also manage the S/MIME certificates yourself, for example to reassign them to other mailboxes: a unique advantage of IKARUS mail.security.

Full transparency and security

In addition to S/MIME certificate authentication, IKARUS mail.security supports Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to prevent not only the forging of emails from your own domain, but also the receiving of forged emails

If an attacker succeeds in planting malicious code via email despite the multi-layered defences, time is against them: With every update, IKARUS mail.security also checks attachments that have already been sent for up to 14 days. In the event of a security incident, the post-incident management system alerts you immediately.

With detailed logging and automated reporting, IKARUS mail.security provides comprehensive visibility into the evolution of your threat posture and defences.

Important features

- ✓ **Behaviour-based analyses** of executable files, macros, scripts, archives.
- ✓ **Local Sandbox integration** for Advanced Threat Protection (ATP).
- ✓ **Anti-spam concept** with adaptive spam rating system and filter options.
- ✓ **Phishing defence and advanced URL defence** for advanced link analysis.
- ✓ **Encryption and digital signing** with S/MIME certificates.
- ✓ **Post Incident Management** with alerting for quick response.
- ✓ **Automated reports and statistics** to assess your threat situation.

Your benefits

- ✓ **High security** through strong detection performance of all types of malwares.
- ✓ **Smooth operation** thanks to high stability and speed.
- ✓ **Comprehensive threat protection** through global and local threat intelligence.
- ✓ **EU-GDPR compliance** through the processing of data in Austria.
- ✓ **Flexibility in scaling and managing** multiple locations or organisations.
- ✓ **Flexible configuration options** for different requirements.
- ✓ **Full visibility** into your current threat posture.

System requirements

- Internet connection
- Own email domain

Further information can be found at:
www.ikarussecurity.com/en/managed-it-ot-security-solutions/ikarus-mail-security



Contact us to get started!

+43 1 58995-500 or sales@ikarus.at

About IKARUS Security

The Austrian cyber security provider IKARUS Security has been making companies, private customers and industrial environments more secure and resilient against digital threats since 1986. IKARUS protects IT, OT and IoT networks against cyber attacks and operational failures with services developed in-house around the renowned IKARUS Malware Scan Engine as well as with complementary solutions from selected technology partners.

Satisfied customers include local and international SMEs, public institutions, industrial companies, ISPs and security manufacturers.

we provide security

www.IKARUSsecurity.com

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400