IKARUS security software

IKARUS mail.security

Datasheet

Email security with Advanced Threat Protection

With leading security technologies, IKARUS mail.security not only detects viruses, malware and harmful attachments in e-mails: manipulated URLs, malicious code, phishing attempts, zero-days and targeted attacks are blocked as well.

Emails are one of the most common attack vectors for cyber attacks. IKARUS mail.security, the cloud-based security solution for email gateways, filters and blocks spam, malware and phishing attempts in real time, even before they can penetrate your systems and cause damage. The ATP add-on also protects against targeted attacks with sandboxing technologies.

Defence against phishing, ransomware, targeted attacks and identity abuse

Advanced persistent threats (APTs), like many ransomware attacks, are customised to the target system. Some attacks start with plausible attachments such as invoices or job applications, others with a seemingly harmless phishing email, and some come only with a tempting URL behind which the actual malicious code is waiting. If the attackers find a way into the system, they behave inconspicuously in order to remain undetected for as long as possible („persistent“). First, further vulnerabilities are identified in the system, then suitable damage routines are reloaded. By the time the attackers are finally discovered, the damage has usually already been done.

The delayed dynamics and the exploitation of as new, unpatched vulnerabilities as possible make the detection of this attack tactic very difficult. With one of the world‘s best malware scan engines for advanced content analysis, the Advanced URL Defense feature for real-time analysis of embedded links and the ATP add-on, IKARUS mail.security offers the utmost security for your SMTP traffic. You reduce the risk of intrusion and misuse to the absolute minimum and get clarity on whether you are currently targeted by attackers.

ATP-Add-on: Multi-sandbox-integration hosted in Austria

E-mails that were classified as neither clearly harmful nor harmless after the analyses of the IKARUS Malware Scan Engine can additionally be checked again with the signatureless sandboxing approach of Trellix and other market leaders. This targeted use - the additional analyses are mostly in the per mille range of the total data volume - also allow small and medium-sized enterprises affordable access to sandbox technologies and thus an optimal level of protection.

The sandboxes of our international technology partners are installed in the IKARUS Scan Center: All data - only metadata such as attachments or scripts are sent in compliance with DSGVO - therefore remain in Austria and are not passed on to third parties. The sandboxes themselves receive continuous updates but cannot send any data.

Post Incident Management and Advanced URL Defense

Should an attacker succeed in placing his code via e-mail despite multi-level defence barriers, time is running against him: with each update, IKARUS mail.security also checks attachments already delivered for malware for up to 14 days. In the event of a security incident - i.e. a delivered e-mail that has not yet been identified as malicious at the time of receipt - the Post-Incident Management System alerts immediately.

In addition, when the Advanced URL Defense feature is activated, IKARUS mail.security scans all links not only when an email is received, but again each time the URL is clicked. This way, even delayed attack tactics are detected and defended against in real time.

Add-on: S/MIME certificates to prevent identity fraud

To protect against misuse and identity theft, unbound S/MIME certificates can optionally be used via IKARUS mail.security. Outgoing e-mails sent via IKARUS mail.security are then signed without further effort and thus authenticated.

The IKARUS-S/MIME certificates come from the recognised certification authority Certum. IKARUS transmits the Certificate Signing Request, takes care of the verification of your company and the e-mail addresses, and enables you to use them flexibly without being bound to specific e-mail addresses. You can assign the desired e-mail addresses yourself in the IKARUS portal and adjust them as required at no extra cost.

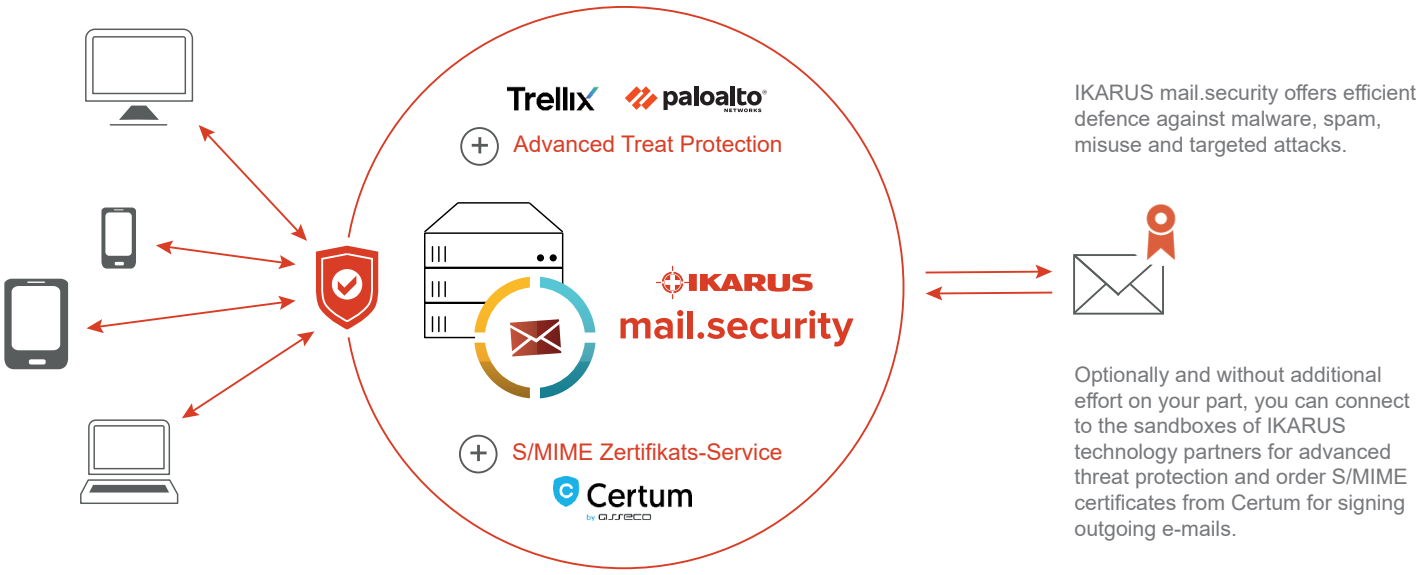
The term of the IKARUS S/MIME certificates is synchronised and charged with the IKARUS mail.security licence. The number of certificates is freely adjustable and independent of the number of mailboxes you manage via IKARUS mail.security. Also already existing S/MIME certificates can be imported into the IKARUS portal for administration.

DSGVO-compliant email security and management

The IKARUS portal allows you a quick overview of your security services, S/MIME certificates, device and network status as well as statistics and analyses. With customisable reports and statistics, you are always up to date.

Software development, data processing, analysis and support for IKARUS mail.security are carried out in Austria in strict compliance with European and local data protection laws. In addition, IKARUS mail.security enables the use of sandbox technologies of international market leaders while complying with local data processing in Austria.

IKARUS mail.security is scalable and multi-client capable, so that large companies can manage several sites at once or as separate instances. ISPs can integrate IKARUS mail.security as an additional feature in their products or pass the service on to their customers in their own branding.



Highlights

- Multi-Sandbox Integration for Advanced Threat Protection (ATP)
- Behavioural analyses of executable files, macros, scripts, archives
- Anti-spam concept with greylisting, Bayesian & lexical analysis, SPF etc.
- Advanced link analysis for every click on embedded links (Advanced URL Defense)
- Post Incident Management with alerting function
- Optional integration of S/MIME signatures, unbound and freely manageable
- Adaptive spam rating system and customised filters and actions
- Automated reports and statistics on the threat situation as well as detailed logging of all the functions

Advantages

- Highest detection performance, optimised for fastest scan and response times
- Global threat intelligence thanks to international data and partnerships
- European GDPR-compliant solution with local data processing in Austria
- Flexible configuration options with blacklists, whitelists and various filter options
- Multi-client capability with customisable admin and user interface, scalable as required
- Temporary archive solution for incoming and outgoing e-mails
- Flexible and powerful overall concept for holistic email security
- Continuously updated insights into the threat situation

System requirements

- Internet connection
- Own email domain

PARTNER BBG BUNDESBESCHAFFUNG

CYBER TRUST AUSTRIA

About IKARUS Security Software

Since 1986, the Austrian cyber security provider IKARUS Security Software has been making companies, private customers and industrial environments more secure and resilient against digital threats. Both with services developed in-house around the renowned IKARUS Malware Scan Engine and with complementary solutions from selected technology partners, IKARUS protects IT, OT and IoT networks against cyber attacks and service outages. Satisfied customers include local and international SMEs, public institutions, industrial companies, ISPs and security manufacturers.