Datasheet

Web and data filters for secure internet traffic

The content security solution IKARUS web.security not only protects against threats on websites or in downloads. The different filter options such as viruses, URLs, file types, countries or browser filters also allow you to consistently implement your company policies. Thanks to its multi-client capability, the service benefits smaller companies as well as large enterprises and internet service providers.

The internet is large and unpredictable: Codes and content are changed constantly, domains acquired and new websites created. The threats hiding behind pages that appear legitimate and download options as are unclear and unpredictable at the net itself. Drive-by infections are therefore one of the greatest sources of danger for your security.

Manage and control web access with individual filtering rules

Our cloud service for secure web gateways facilitates secure and anonymous surfing, regardless of location: Your entire internet traffic is passed through the local IKARUS data processing center in Vienna, scanned for malware and forwarded to your server according to your settings or blocked. Constant updates and quick scans also offer real-time protection against new threats.

Many additional filters and customization options support you in implementing your in-house policies: Which websites may be visited during working hours or using your office equipment, which files types are accepted and which browsers are authorized in the company network? You can, for example, limit access to social media pages, block individual URLs or filter specific content according to predefined categories. All web queries will be reviewed and scanned in the IKARUS data-processing centre in Vienna, according to your settings. You define access profiles as well as access and download rules via a clearly structured web interface. You constantly receive statistics and automated reports about all processes – from clear queries through malware to content blockers.

Manage and control web access with individual filtering rules

Configure IKARUS web.security completely according to your needs. Create black- and whitelists and use our category lists to facilitate the work: All filters are treated hierarchically to allow you to, for example, block certain categories and allow the targeted use of individual URLs of this category. Different access profiles allow you to quickly and easily adapt the filtering rules for individual groups or users: Take your in-house structures and requirements in account without having to incur security risks! Set up different network areas for your company or branches and define different authorization levels for certain groups or users. Individual policies can also be retrieved via PIN or TAN.

Thanks to its multi-client capability and manageable user management, IKARUS web.security is not only ideal for classic application in companies. Large enterprises as well as internet service providers benefit from the option of offering the service under their own brand and using their own design. Use landing- and block response pages for your messages and purposes – for example for registration in your network, to communicate terms of use or for targeted advertising messages. All other instances can be configured independently and offer your clients just as much scope.

Fig. 1 - Central security proxy with reliable malware detection, flexible filter options and global URL category lists.

Advantages:

- Implementing security policies with different authorization levels

- Extremely flexible configuration (all kinds of filter options and user policies)

- Local security proxy in Vienna with data processing according to EU GDPR

- Multiple-client capability with many branding options

Features:

- Antispam and antivirus functions and for HTTP, FTP over http, FTP

- Configuration with different filters: Virus, URL, file type and browser filters

- Individual URL white/blacklist

- Simple creation of access profiles for filtering rules per user/group

- Individually customizable policies per user e.g. through PIN/TAN

- User management with different administrative authorization levels

- Access control with the help of IP address groups or authentication

- Multiple-client capability with many branding options

- Detailed reports/statistics about your network traffic

»Our web security service gives you full control over all internet access. With more than 100 web categories and individual black- and white lists, you define what content may be shown in your network and which websites should be blocked.«

Benny Paar - Technical Presales at IKARUS Security Software

Flexible user management

Virus, URL, file type and browser filters

Individual URL white-/blacklist

Different access profiles and authorization levels

IKARUS URL Report

IKARUS web.security 100% hosted in Austria

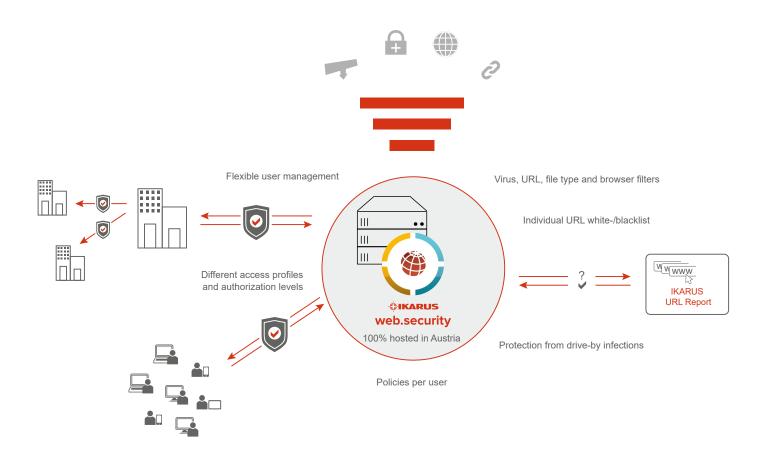Protection from drive-by infections

Policies per user

Fig. 2 - IKARUS web.security scans your internet traffic for malware, blocks unwanted contents and downloads according to your filter settings.

About IKARUS Security Software

The Austrian antivirus specialist company, IKARUS Security Software, has been familiar with the requirements for intelligent IT security systems since 1986. Its software experts have been developing and operating viable security solutions ranging from an original scan engine through managed security services up to SOC/SiEM services for IT, IoT and OT environments. With its in-house scan engine and local development, data processing, support and virus laboratory, IKARUS is your main contact in Austria for IT, IoT and OT security questions.

providing better security

www.**IKARUS**security.com

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

IKARUS web.security