Kaspersky® Web Traffic Security

Strategic defense for your entire network

The proxy server is a natural bottleneck for web traffic passing between the corporate infrastructure and the outside world. This strategic positioning offers excellent opportunities to contain threats early and with relatively little effort.

Kaspersky Web Traffic Security is an application that integrates with proxy servers to protect the corporate IT network from the dangers of the World Wide Web, and increase productivity by governing internet use. It processes passing web traffic and blocks anything dangerous – consistent with corporate security policies. While the approach itself is standard for perimeter security, the breadth of features and unsurpassed quality of threat protection make Kaspersky Web Traffic Security stand out from other offerings on the market.

Highlights

- Real-time, on-demand next-gen anti-malware and anti-phishing protection
- Content filtering to block risky file types and prevent data leaks
- Scalable to suit high-loaded networks
- Available under monthly subscription license for end-users and MSPs
- Zero-hour threat protection
- Backed by global threat intelligence from Kaspersky Security Network
- Microsoft Active Directory support
- Role-based access to administration and web usage
- Web Control to govern web resource use
- Blocks ransomware before it enters the network
- Multitenancy for MSPs and diversified businesses

Benefits

Substantially reduces the risk of infection, preventing business disruption.

By stopping the majority of incoming threats at gateway level, and preventing them from ever reaching endpoints, Kaspersky Web Traffic Security significantly reduces their potential impact on end-users and their workstations.

Boost effectiveness of corporate gateway protection

Featuring one of the most powerful stacks of protective technologies in the industry, with a superior detection rate and near-zero false positive rate, Kaspersky Web Traffic Security application makes a perfect companion to your existing web gateway countermeasures, offering a perceptible boost in protection. This quality is especially important for companies and institutions operating with highly sensitive data and/or with low tolerance for security incidents.

Cuts overheads for IT and IT security staff

Even if endpoint protection is adequate, fewer alarms at endpoint level mean fewer panicked users – and less time spent on incident investigation.

Increases productivity

By governing the use of internet resources, Kaspersky Web Traffic Security not only reduces the risk of cyberattacks, but also prevents distractions – while leaving less opportunity for shadow IT, especially where non-Windows endpoints are concerned.

Fits the size of your business

Depending on the particular system's load, the solution can be scaled, allowing for multiple node management and hierarchical deployment.

Hardware requirements for servers used for installing Kaspersky Web Traffic Security

Worker server:

- CPU: Intel Xeon E5606 (4 cores) 1.86 GHz or more;
- 8 GB RAM;
- swap partition at least 4 GB;
- 100 GB of hard drive space, including:
- 25 GB for temporary file storage;
- 25 GB for log file storage.

Master server:

- CPU: Intel Xeon E5606 (4 cores) 1.86 GHz or more;
- 8 GB RAM;
- swap partition at least 4 GB;
- 100 GB of hard drive space.

If you install the Master server and a Worker server on the same physical server:

- CPU: 2 x Intel Xeon E5606 (8 cores) 1.86 GHz or more;
- 16 GB RAM;
- swap partition at least 4 GB;
- 200 GB of hard drive space, including:
- 25 GB for temporary file storage;
- 25 GB for log file storage.

Software requirements for servers used for installing Kaspersky Web Traffic Security

- Red Hat Enterprise Linux version 7.5 x64.
- Ubuntu 18.04.1 LTS.
- Debian 9.5.
- SUSE Linux Enterprise Server 12 SP3.
- CentOS version 7.5 x64.

Additional requirements

- Ngnix versions 1.10.3, 1.12.2 and 1.14.0.
- Load Balancing HAProxy version 1.5.
- Squid 3.5.20 if you install the Squid service on the Worker server.

For Kaspersky Web Traffic Security to process the traffic of your network, you must install and configure a HTTP(S) proxy server that supports ICAP and Request Modification (REQMOD) and Response Modification (RESPMOD) services. You can use a separate proxy server or, for example, install the Squid service on a Worker server of Kaspersky Web Traffic Security.

Software requirements for managing Kaspersky Web Traffic Security via the web interface

To run the web interface, one of the following browsers must be installed on the computer:

- Mozilla Firefox version 39.
- Internet Explorer version 11.
- Google Chrome version 43.
- Microsoft Edge version 40.

Reduces risks associated with the transmission of certain file types – in both directions

Kaspersky Web Traffic Security helps boost security by restricting the transmission of certain file types. This prevents infections using embedded malicious content inside documents and also reduces the risk of a data leak. Ruling out access to media files for those users who don't need them to do their work also boosts productivity.

Offers convenience for Managed Service Providers (MSPs)

As more MSPs add cybersecurity to their value proposition, Kaspersky Web Traffic Security supports multi-tenant management capabilities and flexible licensing, and allows an appropriate degree of control to be delegated to the tenants' administrators.

Features

HuMachine™-powered, multi-layered threat protection

Kaspersky's next-generation malware protection incorporates multiple proactive security layers, including those based on machine-learning algorithms and assisted by powerful cloud-based mechanisms. It filters out malware, ransomware and potentially unwanted programs in inbound and outbound traffic.

Global threat intelligence: Kaspersky Web Traffic Security uses globally acquired data for the latest view of the threat landscape, even as it evolves.

Machine learning: The big data of global threat intelligence is processed by the combined power of machine learning algorithms and human expertise, delivering proven high detection levels with minimal false positives.

Emulative sandboxing

To protect against even the most sophisticated, heavily obfuscated malware, attachments are executed in a safe emulated environment where they are analyzed to ensure dangerous samples aren't let into the corporate system.

Script detection

According to cybersecurity analysts, scripts are increasingly being used for both web-based attacks and embedding malware into seemingly harmless office files. Kaspersky Web Traffic Security deals with both of these, preventing drive-by attacks and the execution of deadly malware even before they reach the requested endpoint.

Cyberattack-related hosts database

To help avoid even the slightest risk of interaction with dangerous resources, this cloud-based service checks the requested resource against an extensive database of active cyber-attackers' command and control servers, objects with zero-day exploits, toxic web sites and malware distribution points identified as having breach intent. This database continuously updates in real time with intelligence from Kaspersky Lab's renowned GREaT team, blocking even the newest, emerging dangerous resources before the request can execute.

Reputation-based filtering

Kaspersky Web Traffic Security can request file and address reputations from the constantly renewed cloud databases of Kaspersky Security Network. This enables suspicious or unwanted files and internet resources to be blocked instantly, without the need for deeper analysis.

Kaspersky HuMachine™ Approach

Powered by Big Data threat intelligence, robotic machine learning capabilities and the experience of human experts, Kaspersky HuMachine™ provides multiple benefits and delivers more efficient protection. By combining each element, individual components are enhanced into an even more efficient, effective whole.

Advanced anti-phising

Kaspersky's advanced anti-phishing system is based on Neural Networks analysis for effective detection models. With over 1000 criteria used – including pictures, language checks, specific scripting – this cloud-assisted approach is supported by globally acquired data about malicious and phishing URLs to provide protection from both known and unknown/zero-hour phishing URLs contained in downloaded files.

Content filtering

Some file types can be prohibited from transmitting - filtering is based on a number of parameters, such as name, extension/type (format recognizer is used for files with spoofed extensions), size, MIME type and hash. This serves a number of purposes, including reducing the risk of a cyberattack, preventing data leaks, reducing traffic and enhancing productivity

Web control with Kaspersky Lab categories

Not all web resources are necessary for all employees' work activities, and many can pose a considerable danger to corporate security and reputation if they host malware or offer pirated products. Web Control restricts certain categories of web resources to reduce risk, and ensures uninterrupted work without unwanted distractions. If necessary, a Default Deny scenario can be implemented, restricting the use of any web resources with the exception of those absolutely necessary for a particular user's or group's work.

Secure SSL-encrypted traffic monitoring

The solution's architecture allows for easy implementation of corporate traffic monitoring (also known as 'SSL bumping'). With SSL-encrypted web traffic becoming the de-facto standard for internet communications, this is a must-have feature.

Security for ICAP-enabled systems

In addition to proxy servers, Kaspersky Lab's solution can secure traffic on any other device supporting the ICAP protocol. This may include, for example, Network-Attached Storages (NAS) or other systems that can't be protected with an internal security solution.

SIEM integration

If your company utilizes a Security Information and Event Management (SIEM) System to keep track of activities across the corporate network, Kaspersky Web Traffic Security will enrich your security context through exporting information in Common Event Format (CEF), together with widely used syslog.

Convenient management

Kaspersky Web Traffic Security offers a flexible yet easy-to-use management system.

Centralized console: control all your ICAP-capable systems' security, including proxies and storages, via a single-point web interface providing excellent visibility and manageability for your security administrators.

Convenient dashboard: everything necessary to gauge the current state of corporate security at gateway level is collected into a single dashboard. This gives an instant and complete overview of the situation, including urgent events.

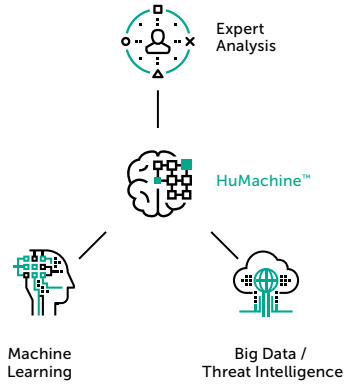
Event management: Threat analysis results are presented using an event-centric approach and show real-time activity. Users' internet behavior can also be analyzed.

Flexible rules configuration system: In addition to the power of the solution's security layers, finely tuned security policies are a cornerstone of the solution's effectiveness, configured to be consistent with existing business processes. Kaspersky Web Traffic Security offers a flexible yet easy-to-use rules configuration system, which allows for the granular management of your gateway security while ensuring your administrators don't have to spend too much time learning it.

Role-based access system: Administrators can define a role to restrict administration rights for different administrator categories. This is useful for internal task delegation or for providing the necessary degree of control for serviced clients in the case of an MSP.

Active Directory integration: Kaspersky Web Traffic Security can obtain information on corporate domain entities (users, user groups, computers, etc.) to configure its role-based access rules and security policies around known objects operating in a company's IT network. The data describing the objects is constantly synchronized between the Active Directory and the application itself to ensure consistency with the most recent changes in corporate infrastructure.

Multi-tenancy: A special mode for MSPs and diversified companies lets you assign dedicated areas ('workspaces') for different units or managed companies and manage them separately, combining 'global' and 'local' policies as appropriate.



How to buy

Kaspersky Web Traffic Security is an application activated in several different Kaspersky Lab products, depending on the license you have purchased.

- Kaspersky Security for Internet Gateways
- Kaspersky Security for Storages
- Kaspersky Security for xSP
- Kaspersky Total Security for Business

www.kaspersky.com