kaspersky

How to integrate Kaspersky Threat Data Feeds with AlienVault USM / OSSIM

kaspersky

Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that this document will help you to use our product.

Document revision date: 04.10.2019

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

kaspersky

Contents

kaspersky

About this document

This document contains instructions for integrating Kaspersky Threat Data Feeds with AlienVault USM (or AlienVault OSSIM).

We recommend that you integrate Kaspersky Threat Data Feeds with AlienVault USM / OSSIM by using Kaspersky CyberTrace. Kaspersky CyberTrace offers the following features:

- Automatic high-performance matching of incoming logs and events with Kaspersky Threat Data Feeds, OSINT feeds, and any other custom feeds in the most popular formats (JSON, STIX™, XML, CSV). Demo feeds from Kaspersky and OSINT are available immediately upon installation of Kaspersky CyberTrace.
- Internalized process of parsing and matching incoming data reduces SIEM solution load significantly. Kaspersky CyberTrace parses incoming logs and events, matches the resulting data to feeds, and generates its own alerts when threats are detected. Consequently, a SIEM solution processes less data.
- Generates feed usage statistics for measuring the effectiveness of feeds.
- In-depth threat investigation through on-demand lookup of indicators (hashes, IP addresses, domains, URLs). Bulk scanning of logs and files is also supported.
- Universal approach to integration of threat matching capabilities with SIEM solutions and other security controls. SIEM connectors for a wide range of SIEM solutions can be used to visualize and manage data about threat detections.
- IoC and related context are efficiently stored in RAM for rapid access and filtering.
- Kaspersky CyberTrace Web, a web user interface for Kaspersky CyberTrace, provides data visualization, on-demand IoC lookup functionality, and access to Kaspersky CyberTrace configuration. Kaspersky CyberTrace Web also supports the management of feeds, log parsing rules, black lists and white lists, and event sources.
- Command-line interface for Windows® and Linux® platforms.
- Advanced filtering for feeds and log events. Feeds can be converted and filtered based on a broad set of criteria such as time, popularity, geographical location, and threat type. Log events can be filtered based on custom conditions.
- DMZ integration support. The computer on which event data is matched against feeds can be located in the DMZ and isolated from the Internet.
- In standalone mode, where Kaspersky CyberTrace is not integrated with a SIEM solution, Kaspersky CyberTrace receives logs from various sources such as networking devices and parses these logs according to defined regular expressions.
- Export lookup results that match feeds to CSV format for integration with other systems (firewalls, network and host IDS, or custom tools).

kaspersky

How to integrate Kaspersky Threat Data Feeds with AlienVault USM / OSSIM using Kaspersky CyberTrace

Integration of Kaspersky Threat Data Feeds with AlienVault USM / OSSIM involves the following steps:

1. Configuration of Kaspersky CyberTrace for integration with AlienVault USM / OSSIM (see section "Configuring Kaspersky CyberTrace for integration with AlienVault USM / OSSIM" on page 5).
2. Configuration of AlienVault USM / OSSIM for forwarding events to Kaspersky CyberTrace (see section "Forwarding events from AlienVault USM / OSSIM to Kaspersky CyberTrace" on page 6).
3. Adding a Kaspersky CyberTrace event source to AlienVault USM / OSSIM (see section "Importing configuration files in AlienVault USM / OSSIM" on page 7).

After integration, you can browse events from Kaspersky CyberTrace in AlienVault USM / OSSIM (see section "Browsing events from Kaspersky CyberTrace in AlienVault USM / OSSIM" on page 10).

In this chapter

Configuring Kaspersky CyberTrace for integration with AlienVault USM / OSSIM

This section describes how to configure Kaspersky CyberTrace for integration with AlienVault USM / OSSIM. You can use any version of Kaspersky CyberTrace available at https://support.kaspersky.com/13858.

Kaspersky CyberTrace and the device (proxy server, or firewall, or IDS, or AV, etc.) whose events will be forwarded to Kaspersky CyberTrace must work on different computers. Forwarding rules are based on IP addresses. Therefore, the IP address of the computer where Kaspersky CyberTrace is installed must be different from the IP addresses of the devices whose events have to be forwarded to Kaspersky CyberTrace.

► *To configure Kaspersky CyberTrace for integration with AlienVault USM / OSSIM:*

1. Install Kaspersky CyberTrace as described at https://click.kaspersky.com/?hl=en-US&link=online_help&pid=CyberTrace&version=1.0&helpid=162489.
   - In Linux, the installation directory is `/opt/kaspersky/ktfs`.
   - In Windows, the installation directory is `%CyberTrace_installDir%`.

2. Configure Kaspersky CyberTrace by using Kaspersky CyberTrace Web (recommended) or by editing the kl_feed_service.conf configuration file (see information at https://click.kaspersky.com/?hl=en-US&link=online_help&pid=CyberTrace&version=1.0&helpid=171625).

   Specify the following Kaspersky CyberTrace settings:

   - IP address of the computer on which AlienVault USM / OSSIM runs, and port `514`.

     These are the IP address and port on which Kaspersky CyberTrace sends detection events.

   - IP address of the computer on which Kaspersky CyberTrace works, and any available port (for example, `9999`)

     These are the IP address and port to which AlienVault USM / OSSIM sends events for checking. This is the port that Kaspersky CyberTrace listens on for incoming events.

   - Service event format as follows:

     ```
     alert=%Alert% context=%RecordContext%
     ```

   - Detection event format as follows:

     ```
     category=%Category% detected=%MatchedIndicator% url=%RE_URL%
     src=%SRC_IP% ip=%RE_IP% hash=%RE_MD5% context=%RecordContext%
     ```

3. In the kl_feed_service.conf file, set the `enabled` attribute of the `OutputSettings > FinishedEventFormat` element to `false`.
4. Save the kl_feed_service.conf file.
5. Restart Kaspersky CyberTrace by using Kaspersky CyberTrace Web or the kl_feed_service script.

Forwarding events from AlienVault USM / OSSIM to Kaspersky CyberTrace

This section describes how to configure AlienVault USM / OSSIM for forwarding events to Kaspersky CyberTrace.

► *To configure AlienVault USM / OSSIM for forwarding events to Kaspersky CyberTrace:*

1. For every device from which you want to forward events to Kaspersky CyberTrace, add the following rule to the `/etc/rsyslog.conf` file:

   ```
   if ($fromhost-ip == '%DEVICE_IP%') then {action (type="omfwd"
   Target="%CyberTrace_IP_IN%" Port="%CyberTrace_PORT_IN%" Protocol="tcp"
   Device="%INTERFACE%") action (type="omfile" File="%PATH%")}
   ```

   Here:

   - `%CyberTrace_IP_IN%`—IP address of the computer on which Kaspersky CyberTrace runs.
   - `%CyberTrace_PORT_IN%`—Port that Kaspersky CyberTrace listens on for incoming events.
   - `%INTERFACE%`—Name of the network interface of the computer on which AlienVault USM / OSSIM runs, which will be used for forwarding events to Kaspersky CyberTrace.

     For example, `eth0`.

   - `%DEVICE_IP%`—IP address of the device from which events arrive at AlienVault USM/OSSIM and must

be forwarded to Kaspersky CyberTrace.

- `action (type="omfile" File="%PATH%")`—Instructions for the rsyslog service to store those events in AlienVault USM / OSSIM that are forwarded to Kaspersky CyberTrace.

  `%PATH%`— Path to the file in which the events will be stored. `%PATH%` can be any file where you want to store the forwarded events.

  `action (type="omfile" File="%PATH%")`—Optional. You can specify this command during the integration process in order to check the following:

  - The fact that events are forwarding to Kaspersky CyberTrace
  - List of the events that are being forwarded to Kaspersky CyberTrace

  When the integration process is finished, it is recommended to remove this line from the configuration file.

This rule must be added after the text `# rsyslog zasec.conf`. If this text is not present in the configuration file, add the rule before the following lines:

```
if not ($fromhost-ip == '127.0.0.1') then -/var/log/ossim/asec_unk.log
if not ($fromhost-ip == '127.0.0.1') then ~
```

2. Restart the rsyslog service by running the following command:

   ```
   /etc/init.d/rsyslog restart
   ```

Importing configuration files in AlienVault USM / OSSIM

This section describes how to configure AlienVault USM / OSSIM for treating Kaspersky CyberTrace as an event source. To configure AlienVault USM / OSSIM for this purpose, make sure to perform the following procedure on the computer on which AlienVault USM / OSSIM runs.

► *To configure AlienVault USM / OSSIM for receiving events from Kaspersky CyberTrace:*

1. Copy the following configuration files to their target directories:
   - Copy kaspersky_cyberTrace.cfg to the `/etc/ossim/agent/plugins/` directory.
   - Copy kaspersky_cyberTrace.sql to the `/usr/share/doc/ossim-mysql/contrib/plugins/` directory.

   The kaspersky_cyberTrace.cfg and kaspersky_cyberTrace.sql files are shipped together with this Help documentation or are received from your technical account manager (TAM).
2. Add the following rule to the `/etc/rsyslog.conf` file:

   ```
   if ($fromhost-ip == '%CyberTrace_IP_OUT%') then
   -/var/log/kaspersky_cyberTrace.log
   ```

   Here `%CyberTrace_IP_OUT%` is the IP address of the computer from which Kaspersky CyberTrace sends events.
3. Run the following command:

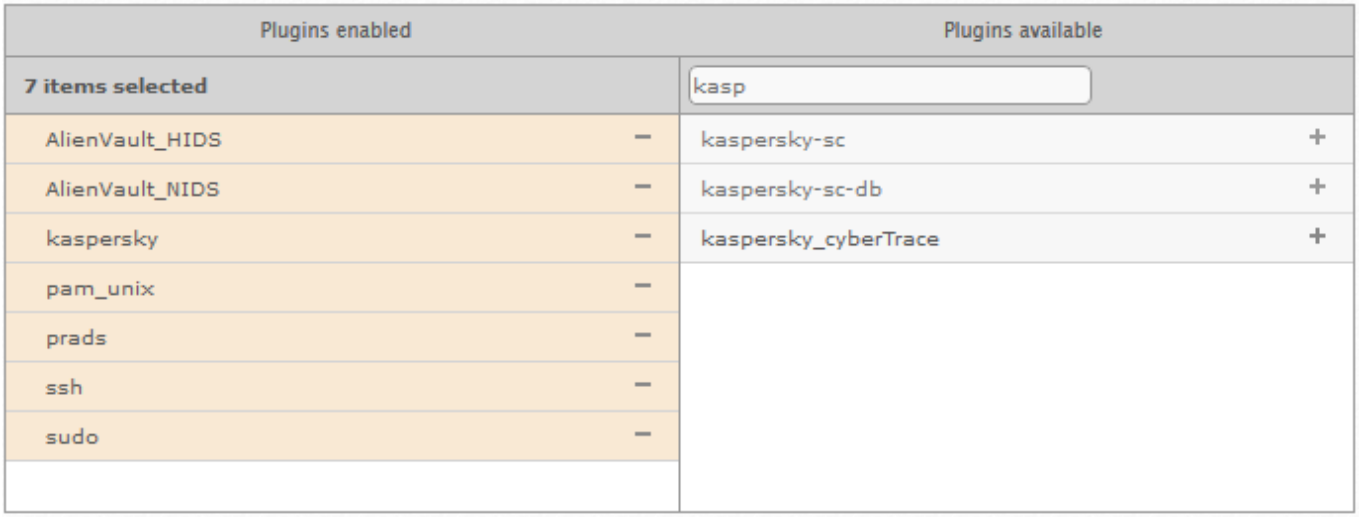
   ```
   cat /usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql
   | ossim-db
   ```

This command adds information about Kaspersky CyberTrace to the AlienVault database.

4. Restart the rsyslog service by running the following command:

   ```
   /etc/init.d/rsyslog restart
   ```

5. In the AlienVault USM / OSSIM web interface, select **Configuration > Deployment > Components > AlienVault Center**.
6. In the **AlienVault Components Information** section, select a USM Appliance Sensor that will receive events from CyberTrace.
7. Select **Sensor Configuration > Collection**.
8. Find the `kaspersky_cyberTrace` plugin in the **Plugins available** list and click the **+** button.



Picture 1: Choosing the Kaspersky_cyberTrace plugin

9. Click **Apply Changes**.
10. Configure the `logrotate` utility to archive Kaspersky CyberTrace events on the computer on which AlienVault USM / OSSIM runs:
    1. Create the `kaspersky_cybertrace` file in the `/etc/logrotate.d` directory.
    2. In the `kaspersky_cybertrace` file, specify the following lines:

       ```
       /var/log/kaspersky_cyberTrace.log
       {
       # save 3 months of logs
       rotate 3
       monthly
       missingok
       notifempty
       compress
       delaycompress
       ```

```
sharedscripts
# run a script after log rotation
postrotate
invoke-rc.d rsyslog rotate > /dev/null
endscript
}
```

3. Save and close the `kaspersky_cybertrace` file.

> If you want to save logs for another period, see the logrotate documentation to configure the `kaspersky_cybertrace` file.

After you perform this procedure, Kaspersky CyberTrace device will be added to AlienVault USM / OSSIM. For example, on the **Configuration > Threat_Intelligence > Data Source** page of the AlienVault USM / OSSIM web interface, you will find Kaspersky CyberTrace in the list of data sources.

The rsyslog service will store events from Kaspersky CyberTrace in the `/var/log/kaspersky_cyberTrace.log` file.

After you configure Kaspersky CyberTrace and AlienVault USM / OSSIM, perform the verification test as described at https://click.kaspersky.com/?hl=en-US&link=online_help&pid=CyberTrace&version=1.0&helpid=171415. For this, send the verification test events to Kaspersky CyberTrace by using the Log Scanner utility (which is part of Kaspersky CyberTrace). The verification test events are contained in the `verification/kl_verification_test.txt` file. Check the verification test result in the AlienVault USM / OSSIM web interface (see section "Browsing events from Kaspersky CyberTrace in AlienVault USM / OSSIM" on page 10).

By default, every detection event, for each Kaspersky Threat Data Feed, has its own type in AlienVault. Detection events for other feeds, for example, OSINT feeds, have the `Kaspersky CyberTrace - Detection event` value in the `event name` field.

You can rename the detection events of the imported feeds in order to classify the detection events according to their categories.

► *To rename the detection events of the imported feed:*

1. Add the following line to the `translation` section of the `/etc/ossim/agent/plugins/kaspersky_cyberTrace.cfg` configuration file:

   `%CATEGORY_ATTRIBUTE_VALUE_OF_THE_IMPORTED_FEED%=%ANY_FREE_NUMERIC_VALUE%`

   where `%CATEGORY_ATTRIBUTE_VALUE_OF_THE_IMPORTED_FEED%` is the value of the category attribute of the imported feed from `kl_feed_service.conf`. For example: `Custom_Feed=50`.

2. Save and close the file.

3. Add the following line before the last line of the `/usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql` file:

   ```
   (23021992, %NUMERIC_VALUE_SPECIFIED_AT_THE_kaspersky_cyberTrace.cfg%,
   15, 71, NULL, 'Kaspersky CyberTrace - %NAME_TO_REPLACE%', 5, 8),
   ```

4. Save and close the file.
5. Run the following commands:

```
cat /usr/share/doc/ossim-mysql/contrib/plugins/kaspersky_cyberTrace.sql | ossim-db
/etc/init.d/ossim-agent restart
/etc/init.d/ossim-server restart
```

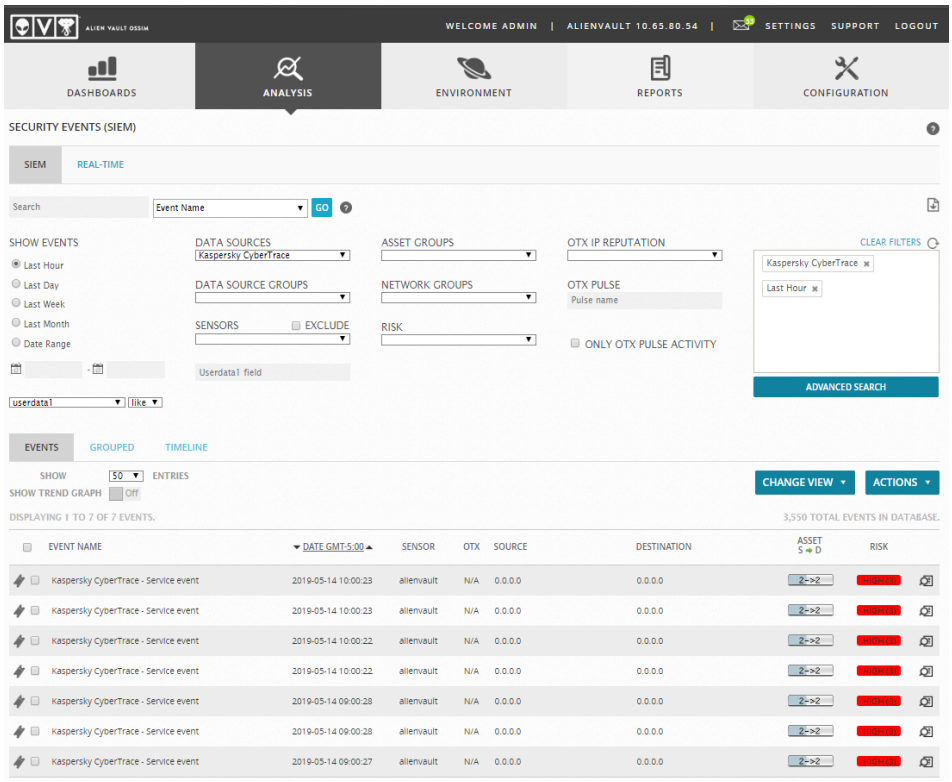
Browsing events from Kaspersky CyberTrace in AlienVault USM / OSSIM

This section describes how to browse events from Kaspersky CyberTrace in AlienVault USM / OSSIM.

► *To browse events from Kaspersky CyberTrace in the AlienVault USM / OSSIM web interface:*

1. In a browser, open the AlienVault USM / OSSIM web interface.
2. Select **Analysis** > **Security events (SIEM)**.
3. In the **Data Sources** drop-down list, select **Kaspersky CyberTrace**.

   AlienVault USM / OSSIM displays events received from Kaspersky CyberTrace.



Picture 2: Events received from Kaspersky CyberTrace

AlienVault USM / OSSIM displays Kaspersky CyberTrace events of two types, which are designated in the **Event Name** column of the event list:

- Service events

  Click the button in the last column of the table ( ). For service events, the following data is displayed (as shown in the figure below).

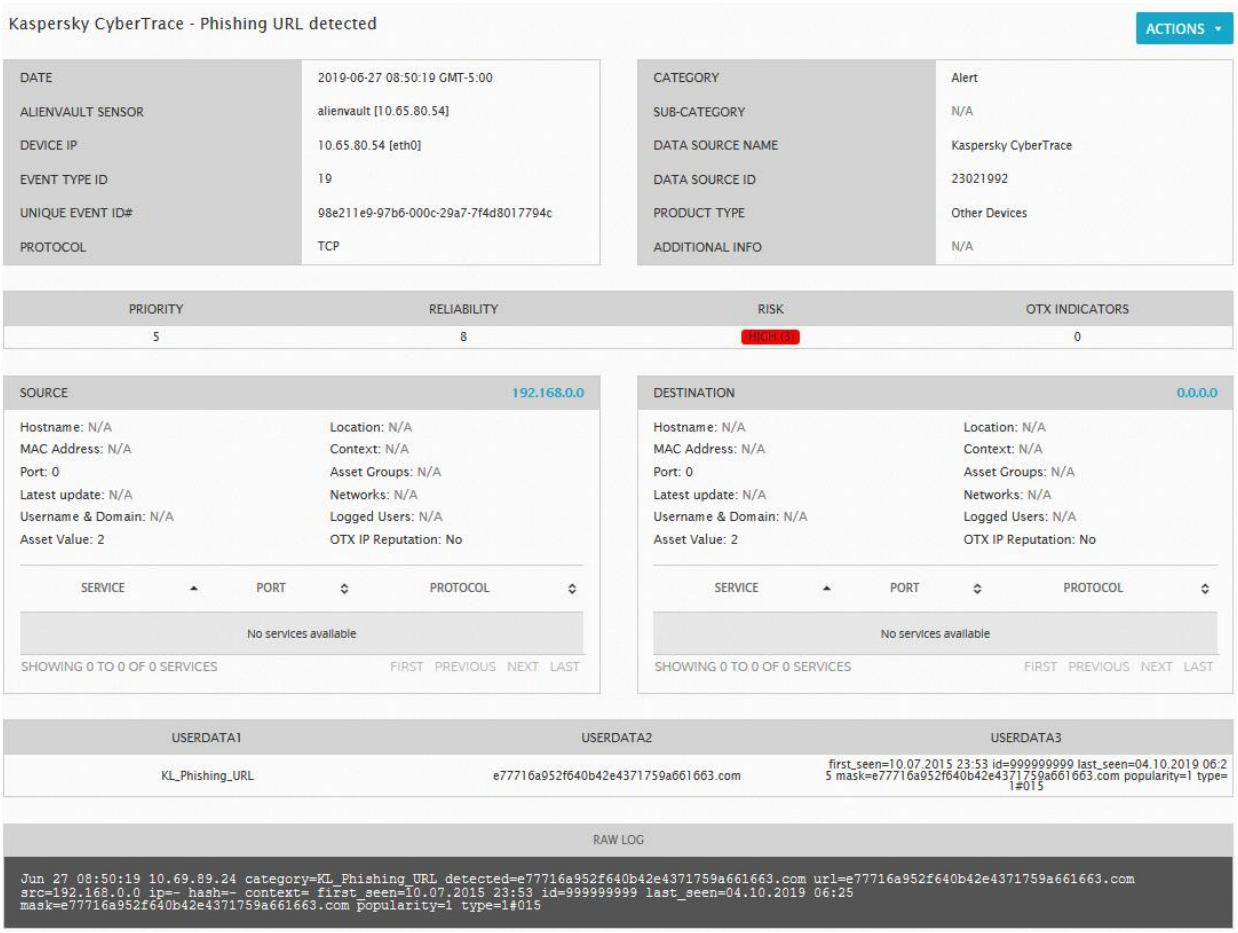
  - The **Userdata1** field contains the service event itself.
  - The **Userdata2** field contains the context of the event, if any.

- Detection events

  Click the button in the last column of the table ( ). For detection events, the following data is displayed (as shown in the figure below).

  - The **Userdata1** field contains the feed that is involved in the detection process.
  - The **Userdata2** field contains the detected indicator.
  - The **Userdata3** field contains the context of the feed record that is involved in the detection process.

    The **Userdata3** field contains up to 1024 symbols, so it may not contain the whole context. The whole event (including the context) is contained in the **RAW LOG** field.



Picture 3: Detection event data

kaspersky

AO Kaspersky Lab

Kaspersky is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky. It is no coincidence that many other developers use the Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Community:	https://community.kaspersky.com