

Kaspersky[®]
Open
Space
Security

Flexible security
for networks and
remote users

All Systems Go!

Kaspersky® Open Space Security

Kaspersky Open Space Security offers new flexibility to network security by extending beyond the traditional workplace to protect an increasingly mobile and distributed workforce.

Today's information technologies present businesses with countless ways to communicate and collaborate, creating a new global work environment that does not follow traditional physical limitations of borders and boundaries.

We can have online access from practically any location on earth to colleagues, clients and partners, online shops, banking services, and an abundance of information. The dark underside from this growing freedom is the myriad of new opportunities it provides cybercriminals, who are continually evolving their methods and technologies to steal confidential data from individuals and organizations.

The contemporary corporate network is a very different environment from just a few years ago, and this is transforming how we approach network security. In the past, networks had clearly defined perimeters on which a protective barrier could be built. Today, a typical network may host multiple sub networks – with laptops and smart devices – forming intersecting and constantly shifting perimeters. The corporate network is now a dynamic open space without rigid structures, which leads to a whole new set of security challenges. To address this new dynamic nature of today's network environments, Kaspersky Lab has developed Kaspersky® Open Space Security.

Kaspersky Open Space Security is our approach to network security that extends protection beyond the workplace to reach remote users and an increasingly mobile workforce. At Kaspersky Lab we believe that flexibility in corporate communications is fully compatible with protection from contemporary security threats, such as viruses and other malicious programs, hacker attacks, spyware and spam.

For truly comprehensive malware protection of corporate networks, an integrated solution must meet the following core requirements:

Defend Each Node and Platform on the Network. In today's dynamic corporate networks, it is becoming difficult to pin down where the network perimeter lies. Contemporary threats can penetrate the network without going through the server (for instance, when a user checks their Yahoo! or Hotmail account or updates their Outlook address book using an infected smart device). A truly comprehensive approach to fully securing the network is to install protection on each network node and device.

Kaspersky Open Space Security is a suite of products that combine to deliver protection for every type of network node – from mobile phones, smart devices, laptops and workstations to file servers, mail servers and Internet gateways – operating under the most popular platforms. Each organization can choose the solution that best fits the scale and complexity of their network.

Protect Against All Types of Threats.

Internet threats are not only numerous at the present time, they also tend to be blended (combining several malware elements in a single attack). What's more, social engineering techniques are often brought into play. A security solution must pull together many different components to deal with all types of cyber-threats, including viruses, spyware, rootkits, hacker attacks, phishing and spam.

Deliver Rapid Response.

With the global nature of today's threats, real-time responses have become a requirement. As the number and variety of malicious attacks increase, the proper defense requires rapid discovery, analysis and distribution of countermeasures. Increasingly sophisticated malicious code, combined with high speed global IP networks, means that any lag time could result in hundreds of thousands of infected systems across the globe in a matter of minutes.

Kaspersky Open Space Security sets a new standard for precision and responsiveness to these increasing levels of attacks. Backed by the unique processes and technologies inside the Kaspersky Internet Security Lab, Kaspersky delivers the industry's highest virus and spyware detection rates, the fastest outbreak response times, and standard hourly anti-malware updates.

Combine Comprehensive Technologies.

For comprehensive protection from Internet threats, it is important to include the right mix of technologies, so they work collaboratively. While anti-malware protection has traditionally been heavily signature-based, in the present climate where threats can spread in a matter of minutes, proactive technologies and heuristic algorithms have become the norm. Proactive technologies can recognize malicious programs strictly from their behavior; their detection is immediate, foregoing the need to wait for signature updates.

Kaspersky Open Space Security combines the highest quality signature-based protection with the most advanced proactive technologies available today, recognizing the warning signs of malicious activity in record time, alerting users to their presence and rolling back any harmful changes made by malicious programs.



Kaspersky
Open Space Security
offers new flexibility
to network security
by extending beyond the
traditional workplace
to protect an
increasingly mobile
and distributed workforce.



All Systems Go!

A security solution should not only take into account the latest mobile technologies, but also leverage them for the benefit of the user and the security of the network as a whole.

Travel Safely.

In today's business environment, staying connected and accessible wherever they are – on the road, or in another part of the country or the world – is a priority for many business professionals. Protection from Internet threats is even more pressing for those working outside the corporate network than for those within it. The security solution must be able to choose the operating mode that best suits the conditions in which the laptop or smart device is working.

Kaspersky Open Space Security uses a specially created policy for laptop users, which initiates as soon as the laptop is disconnected from the administrative server. The policy rules are carefully adapted to ensure the fullest protection for laptops disconnected from their home network, prescribing the source and frequency of updates, scanning schedules, firewall configuration, etc. When the user connects to the corporate network, the data on the laptop and the administrative server is synchronized, providing the administrator with reports of anti-malware activity, while automatically updating the laptop with the most current corporate security policies.

Protected by Kaspersky Open Space Security, users can work securely from any type of network, including WiFi, and remain invisible to hackers. As soon as the laptop or mobile device connects to a new network, it asks the user whether the connection is to the Internet, Intranet or a trusted network, and chooses the firewall's operating mode accordingly. The application saves a list of all networks accessed and offers the option of enabling or disabling invisible mode for each individual connected device.

When a connection to an administrative server is unavailable, Kaspersky Open Space Security ensures that protection is always up-to-date by automatically switching to alternative update sources (via the Internet). Meanwhile, proactive technologies are always in the background to detect new threats, which is extremely important for users who have not had the opportunity to update their anti-malware databases.



Screen Returning and Guest Computers.

When an employee reconnects to the network after being away, the security solution conducts a precautionary scan to safeguard other users on the network. The same scanning policy is applied to guest computers on the network.

Cisco® NAC (Network Admission Control) is supported by Kaspersky Open Space Security, enabling the solution to check computers that have reconnected to the network after an absence. Furthermore, when the program detects an infected computer, it blocks any connections to it, enabling the administrator to track down the potential source of the infection.

Kaspersky Open Space Security has been built to accelerate system performance. For starters, Kaspersky requires the absolute minimal amount of space on any node to run full robust protection. And the system's ISwift™ and IChecker™ technologies significantly optimize scanning for increased performance.

In the game of move and countermove between the anti-virus industry and cybercriminals, malware writers are forced to constantly devise methods of bypassing anti-virus protection to penetrate networks. Thus, being able to perceive new malware techniques is another requirement for a modern security solution.

Protect Against Rootkits.

Rootkits aim to conceal files, folders, register keys, running programs, services, drivers and network connections or activity from the user. Highly-specialized technologies must be used for effective detection of this type of malware.

Kaspersky Open Space Security uses anti-rootkit technology that detects any hidden processes in the system by: 1) Scanning critical system areas. This task launches a scan of all areas of the operating system that are the most vulnerable to infection. Conducting a scan of startup objects, for instance, can help prevent viruses from being launched when the system is booted and can detect rootkits. 2) Analyzing all processes in the system, sending alerts to users when any dangerous, suspicious or hidden processes, such as rootkits, are launched.

All Systems Go!



..... ***Guard Against Identity Theft.***

The majority of malicious programs have the ability to covertly transmit confidential information from the user's computer, such as logins and passwords to bank accounts.

Kaspersky Open Space Security uses heuristic algorithms that are specially designed to detect activity consistent with an attempt to steal passwords and dispatch data from the computer. Together with a personal firewall, Kaspersky's intrusion detection systems (IDS) and intrusion prevention systems (IPS) closely monitor all network activity and prevent any intrusion into the system or data leakage from it.

Backup and Restoration of Data.

A recent trend in the development of malware has been the use of ransomware to damage or encrypt data on a user's computer with the aim of demanding a ransom for its restoration.

A technology unique to Kaspersky Open Space Security is capable of preventing such attacks. The program tracks all suspicious activities in the system to identify malicious processes, removing the malicious program responsible. Not only does the program remove any malicious programs it detects, but also rolls back any harmful changes they have made (this may involve restoring encrypted data).

Self-Defense.

There is little point in deploying highly sophisticated security solutions if a malicious program can disable them during system startup or another process.

Kaspersky Open Space Security has a number of effective self-defense mechanisms at its disposal for all levels of its operation: the program monitors its own processes, files and key registers, and blocks any attacks against itself.

All Systems Go!

Work in Unison with Technologies from Third-party Vendors.

For maximum effectiveness, a modern security solution must take into account the technological features of products from other hardware and software products installed on the system.

Because Kaspersky Open Space Security supports Intel® Active Management (Intel® vPro™), it can conduct remote treatment of workstations. Support for Cisco® NAC (Network Admission Control) makes it possible to isolate and scan computers when they reconnect to the network. Finally, support for Intel® Centrino® Duo technology enables the solution to economize its energy usage on laptops and mobile devices.

Efficient Use of Network Resources.

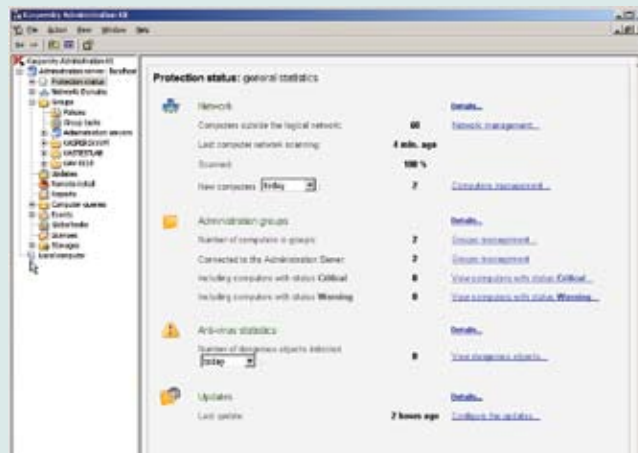
A key consideration for businesses when choosing a security solution is how significantly it will impact network resources and operating speeds.

Kaspersky Open Space Security uses iSwift technology, which ensures against unnecessary repeat scans of files that are received from a workstation or file server already under the protection of Kaspersky Security. This safeguard significantly reduces both time spent on scanning and the time taken to deliver files to the end user.

Centralized administration.

Finally, in developing a complex and finely balanced security solution, we must not lose sight of the need for simple, transparent administration and efficient performance.

New applications and technologies are increasing the complexity and sophistication of contemporary corporate networks. While everyday business users benefit from these new tools, they may lack the expertise in information security to manage them adequately. Professional centralized administration tools are essential for IT departments if they are to successfully protect their users from viruses and malicious programs. To keep anti-virus databases and program modules up-to-date and respond effectively to network incidents, it is essential to have complete, continuous information on the system's status. Moreover, to be fully effective, anti-virus solutions must be backed up by sophisticated centralized administration.



Kaspersky Open Space Security includes a powerful set of administration tools – the Kaspersky Administration Kit – which is designed to meet the needs of networks of any size or complexity. This toolset enables central administration of dynamic networks, extending to remote access and laptop and mobile users.

All Systems Go!



About Kaspersky Lab

With more than a decade of experience in the computer security industry, the experts at Kaspersky Lab have created one of the most highly regarded security labs in the world. Today, more than 150 developers and engineers - operating from five research and development and virus labs worldwide - disarm more than 200 viruses every day. From these same labs come the sophisticated security solutions and regular updates that now protect 200 million users in more than 50 countries around the world.

Headquartered in Moscow, Russian Federation, with North American headquarters in Boston, Massachusetts, Kaspersky Lab has more than 600 employees throughout the world. Kaspersky provides best-of-breed malware protection to more than 100 highly-respected IT, networking, security and messaging vendors who integrate the Kaspersky technology for the most effective and imminent protection.

When it comes to protecting our customers, time to respond is what matters. Kaspersky Lab creates technology that has become an industry standard for combating even the most sophisticated computer threats at a remarkable rate of speed. For the best-of-breed solution to protect your IT infrastructure, choose quality protection from Kaspersky Lab.



Kaspersky Lab, Inc • 300 Unicorn Park • Woburn, MA 01801
phone: (781) 503-1800 • fax: (781) 503-1818
www.kaspersky.com

©2007 Kaspersky® Open Space Security is a registered trademark of Kaspersky Lab.
All other names and trademarks are the copyrighted work of their respective owners.