Kaspersky Secure Remote Workspace

Cyber Immune, manageable and functional thin client infrastructure

The VDI concept entails employees receiving their work tools – virtual PCs – as a set of programs and data on a remote server. Virtual desktop infrastructure, or VDI, has many advantages:

- enables automation of the desktop creation process;
- eliminates need to store and process data on employee devices;
- recovers data quickly after an incident;
- manages remote desktops from one location;
- reduces the risk of attacks from remote desktops.

Special terminals – thin clients (TCs) – are used to connect and work with VDI. Although conventional PCs and laptops can be used with virtual desktops, TCs offer a number of advantages:

- the absence of moving parts has a positive effect on the service life (7-10 years);
- small size and weight, ergonomic, simple maintenance and operation;
- low power consumption and power dissipation;
- favorable price and cost of ownership compared to classic desktops and laptops.

However, the full benefits of thin clients are unlocked by a centralized management system that simplifies setup, administration and support. It should be noted that for all its convenience, VDI cannot fully ensure the security of a virtual infrastructure. If the endpoints are not sufficiently secure, VDI can become a target for a variety of attacks, such as keystroke logging, infections from unmonitored removable media, or the exploitation of vulnerabilities in software that is outdated or not updated in time.

Kaspersky Secure Remote Workspace helps counter potential threats. It incorporates Cyber Immune thin clients based on the secure KasperskyOS operating system. This approach eliminates the need to use antivirus protection. The solution also includes a centralized management tool, which simplifies administration of the thin client infrastructure.

KasperskyOS

Kaspersky Secure Remote Workspace is a solution for building a managed and functional infrastructure of thin clients based on the Cyber Immune operating system KasperskyOS for secure VDI connection and terminal access.

Solution components

Kaspersky Secure Remote Workspace

Kaspersky Thin Client

Operating system and thin client application software installed on the hardware platform

Perpetual license for main version

Kaspersky Security Center

Single console for centralized thin client management

Free installation (if there is no console in the infrastructure)

Kaspersky Security Management Suite

Special add-on module for fleet administration

License to connect to KSC. Subscription model by number of devices for 1, 2 or 3 years

Benefits of Kaspersky Secure Remote Workspace

OS level protection

Thin clients based on KasperskyOS have Cyber Immunity – 'innate' security at the OS architecture level. This means that most types of cyberattacks on a device will have no effect on the security of remote desktop infrastructure.

Reduced costs

Deployment and maintenance costs for Kaspersky Thin Client infrastructure are likely to be lower than those for other solutions. Working with the already familiar Kaspersky Security Center product does not require training or reinstallation.

Support for popular key storage media and external drives

RUTOKEN, SafeNet and JaCarta tokens and USB passthrough.

Centralized management

Centralized monitoring and management of all thin client infrastructure events is performed via the Kaspersky Security Center console. Supports management of up to 100,000 nodes. Thin clients are registered and configured automatically when new devices are connected to the infrastructure.

Easy migration and updating

Security is monitored via the familiar Kaspersky Security Center management console, making it easier to switch from traditional workstations to thin clients. If the software configuration is updated within the Kaspersky Thin Client corporate image, the solution performs a centralized automated update on all thin clients.

Kaspersky Security Center: centralized management and monitoring

Management from a single point

Remote centralized management of all Kaspersky Thin Client settings gives control and visibility over the entire infrastructure

Flexible reports and notifications

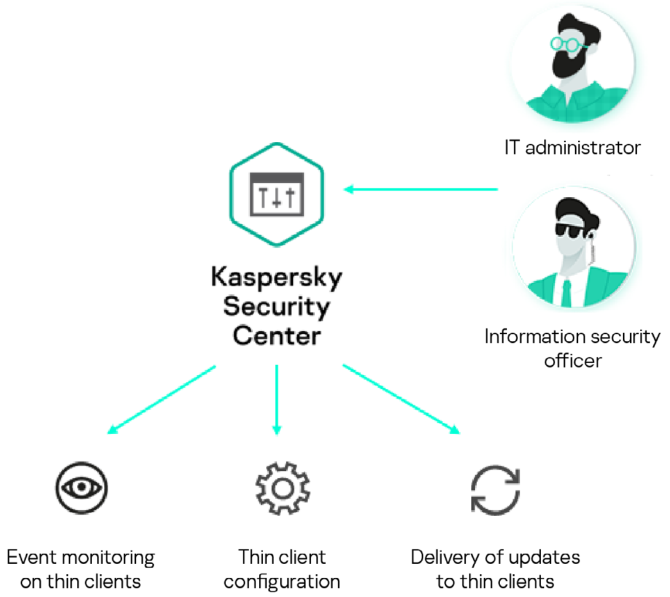
Customizable reports with filtering and sorting by any field. Incident notifications through the administrator's prefered channels: SMS, email, push notifications, etc.

Easy migration

No need to become proficient in a new product — migration to thin clients is straightforward when using KSC

Kaspersky Thin Client controlled by information security experts

Thin clients remain firmly in the focus of information security specialists

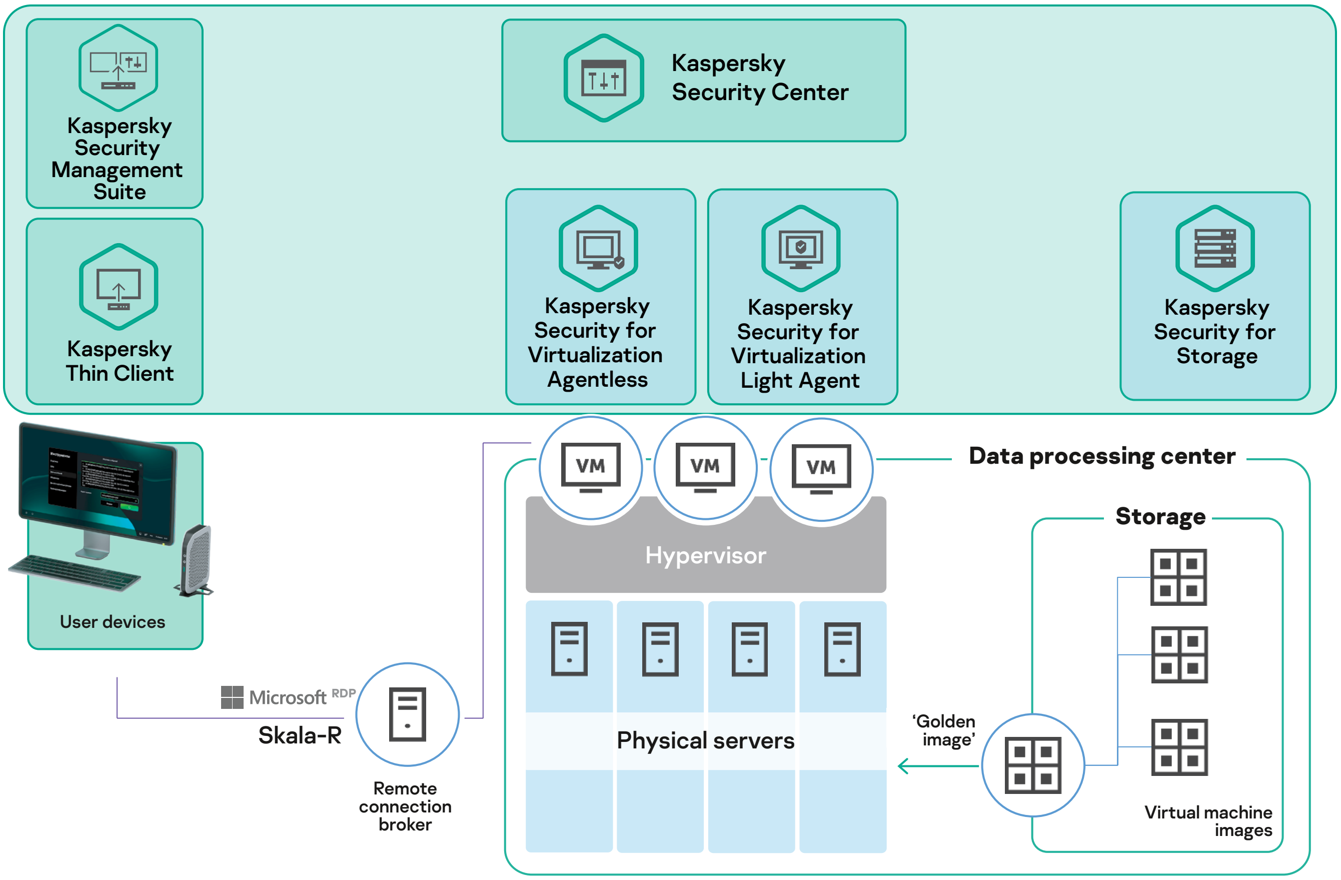

IT administrator
Kaspersky Security Center
Information security officer
Event monitoring on thin clients
Thin client configuration
Delivery of updates to thin clients

Kaspersky Thin Client: Specifications

Hardware platform	TONK TN 1200
Operating system	KasperskyOS
Processor	Intel® Celeron® 4125 Gemini Lake Refresh Quad-Core 2.0GHz (4M L2 cache, up to 2.7GHz)
RAM	4GB DDR4 (maximum 8GB, DDR4/LPDDR4)
Flash drive	64GB, M.2 (2242) SSD
Video	Intel® UHD Graphics 600, up to 1920 x 1080
Network	1 x LAN port (RJ-45) 10/100/1000 for LAN connection
Peripheral interfaces	· 1 x DP · 1 x HDMI · 4 x USB 2.0 · 2 x USB 3.0
Dimensions and weight	· Device: 131mm x 31.5mm x 167mm · Weight: 0.55kg · Packaging: 488mm x 256mm x 108mm
Features	· DC input voltage: from a universal (110-230V) 12V 3A AC adapter · Power consumption: maximum 30W · VESA mount, horizontal or vertical setup · Kensington Lock · Fanless cooling by means of natural air convection

The role of Kaspersky Secure Remote Workspace in integrated VDI protection by Kaspersky products

Kaspersky Secure Remote Workspace is part of a comprehensive VDI project. The solution works in conjunction with conventional antivirus tools for virtual and cloud environments, as well as storage systems. All of these products are also managed using Kaspersky Security Center.



Kaspersky Security Management Suite

Kaspersky Security Center

Kaspersky Thin Client

Kaspersky Security for Virtualization Agentless

Kaspersky Security for Virtualization Light Agent

Kaspersky Security for Storage

User devices

Microsoft RDP

Skala-R

Remote connection broker

VM

VM

VM

Data processing center

Hypervisor

Physical servers

'Golden image'

Storage

Virtual machine images

KasperskyOS: fundamentally new approach to the cybersecurity of IT products

KasperskyOS is Kaspersky's very own operating system a platform for developing Cyber Immune IT products. The inherent security of KasperskyOS is built in to its architecture and philosophy: only what is allowed by the system administrators and application developers can run and work. For IT products based on KasperskyOS, the security policies that specify each permissible action are already defined at the design stage. Any action not explicitly permitted by the security policy will be blocked before it is performed. Products based on KasperskyOS are in demand in sectors where IT systems are subject to higher cybersecurity, reliability and predictability requirements from the industrial internet of things to transport, smart cities and manufacturing.

KasperskyOS

Kaspersky Secure Remote Workspace

Learn more on os.kaspersky.com

www.kaspersky.com