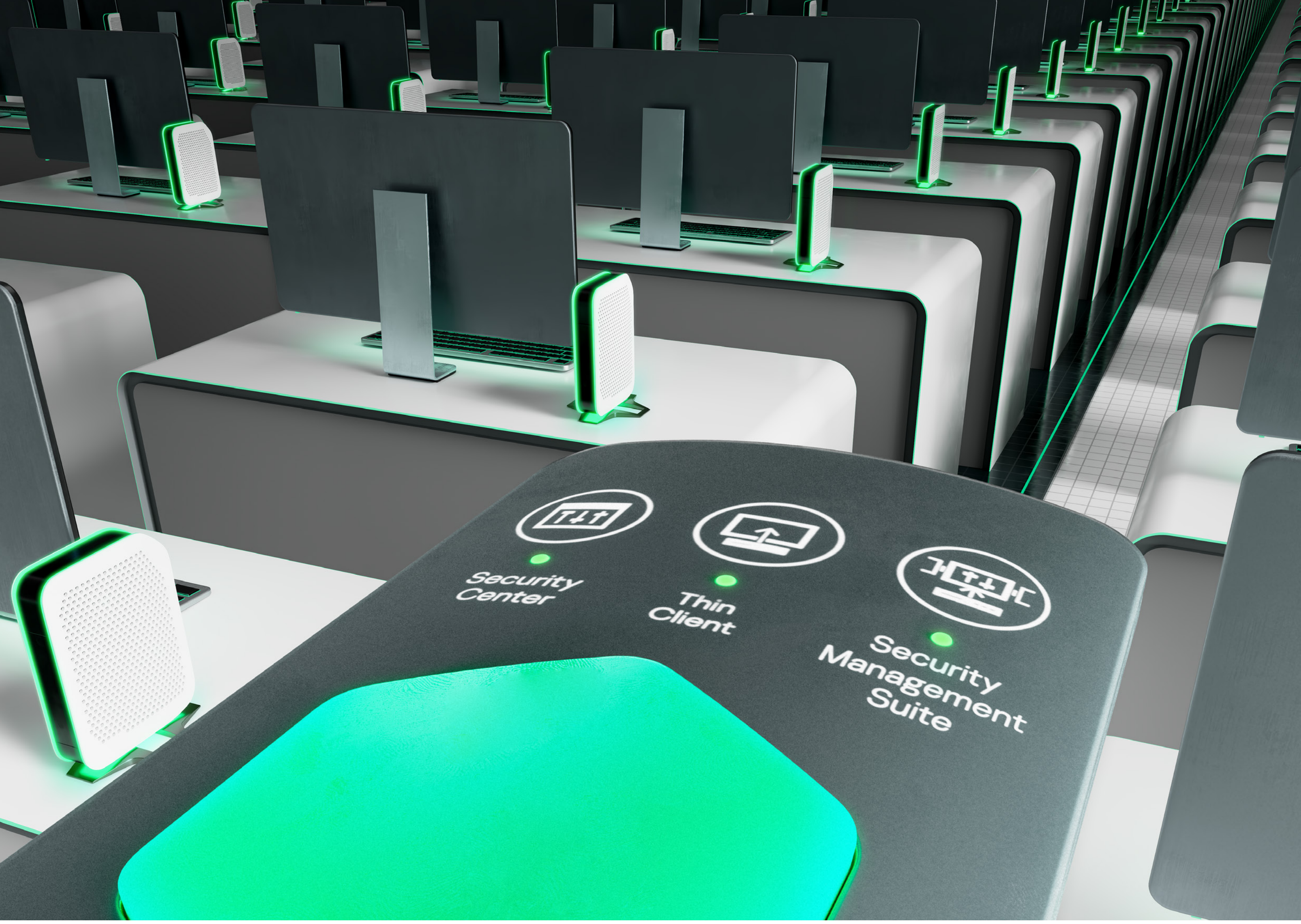


Cyber Immune, manageable and functional thin client infrastructure

Kaspersky Secure Remote Workspace

KasperskyOS

VDI – the modern technology for remote workspaces

Virtual Desktop Infrastructure, or VDI, involves employees getting their work tools – virtual PCs – as a set of programs and data on a remote server. Connection to the server is established via special terminals – thin clients (TCs). This concept has many advantages over traditional workstations:

- 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.

Thin clients offer a number of advantages over PCs and laptops:

- 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 conventional desktops and laptops.

Why protect VDI?

For all its convenience, VDI cannot fully ensure the security of a virtual infrastructure. VDI may be targeted by different types of attacks if the endpoints are not sufficiently secured.

Potential threats to thin clients

Malware and network attacks

A thin client can become a target for malware attacks if it is not properly secured. This will block operation of the device and endanger the data on the remote machine or even the entire VDI

Dangerous pluggable devices

Unmonitored removable media present a potential avenue for malware proliferation and data theft

Interception of keystrokes

Although information processing takes place on the virtual machine side, the user still uses the keyboard to enter account passwords on the thin client, meaning an intruder can use a keylogger

New vulnerabilities in system software

Superimposed security features cannot guarantee security without regular installation of system software updates

Prerequisite: infrastructure manageability

Without a convenient centralized management system for thin clients, configuring, updating or auditing them is a time-consuming and risky process. The full benefits of thin clients are unlocked by a centralized management system that simplifies setup, administration and support.

Kaspersky's approach to VDI protection and thin client infrastructure manageability

Potential threats can be prevented and a fleet of thin clients protected thanks to the Cyber Immune approach used in **Kaspersky Secure Remote Workspace** (KSRW). Thin clients in the solution are based on the KasperskyOS operating system. The secure-by-design operating system eliminates the need for additional antivirus protection. Another component of the solution – the unified management console – solves the problem of managing and monitoring thin client infrastructure.

Solution components

Kaspersky Secure Remote Workspace

Kaspersky Thin Client	Kaspersky Security Center	Kaspersky Security Management Suite
KasperskyOS-based software product installed on a hardware platform	Unified console for managing thin clients and other Kaspersky products	Special add-on module for fleet administration
Perpetual license for main version	Free installation (if there is no console in the infrastructure)	License to connect to KSC. Subscription model by number of devices for 1, 2 or 3 years

Where Kaspersky Secure Remote Workspace is used

Kaspersky Secure Remote Workspace is suitable for many areas where a large number of workstations with similar tasks and a standard set of applications are used. For example:

- public sector;
- educational institutions;
- industry;
- fuel and energy sector;
- healthcare;
- financial organizations;
- retail.

Cyber Immunity is the "inherent" protection of an IT system – its ability to withstand cyberattacks without any additional (superimposed) security tools. The overwhelming majority of types of attacks on a Cyber Immune system are ineffective and unable to impact its critical functions.

Cyber Immune products are virtually impossible to compromise under ordinary conditions. They minimize the number of potential vulnerabilities.

KasperskyOS is an operating system used in areas with high security requirements: smart cities, transportation, manufacturing, the electric power industry, the public sector and other areas. It ensures the confidentiality and integrity of data and secures it against spoofing.

Cyber Immune thin clients an important component of VDI security

The inherent security of the KSRW solution ensures the following requirements are met:

- the integrity of data received from the user, the **Kaspersky Security Center** centralized management server, and connection broker servers
- secure **Kaspersky Thin Client** updates;
- the confidentiality and integrity of data transferred between **Kaspersky Thin Client**, remote desktops, the KSC server, the logging server and connection broker.

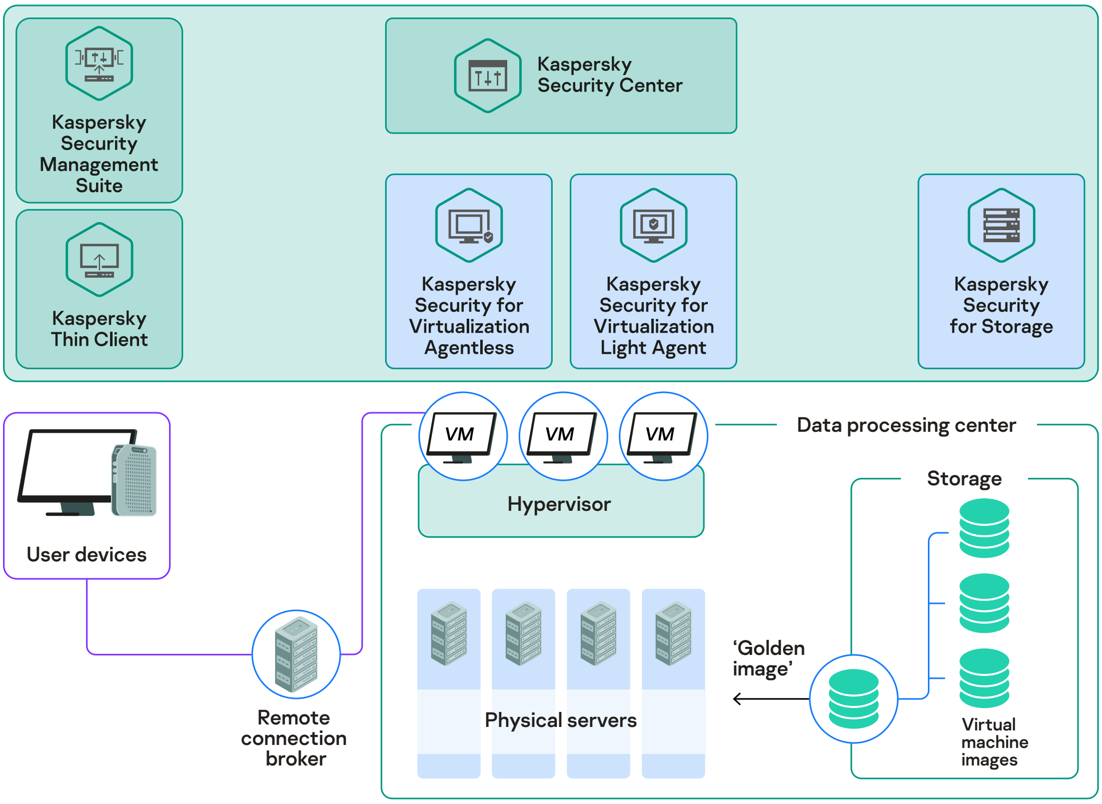
Cyber Immune thin clients are the secure "last mile" in building a reliable IT infrastructure for working with virtual desktops.

Centralized management of thin client infrastructure

The **Kaspersky Security Center** console, which is included in the solution, allows you to manage, configure and administer thin clients from a single center, as well as deliver updates and collect system events. KSC is actively used in other Kaspersky products, which makes integrating KSRW into the existing corporate IT protection ecosystem as seamless as possible without the need to hire extra staff.

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

Kaspersky Secure Remote Workspace is part of a comprehensive VDI protection 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**.

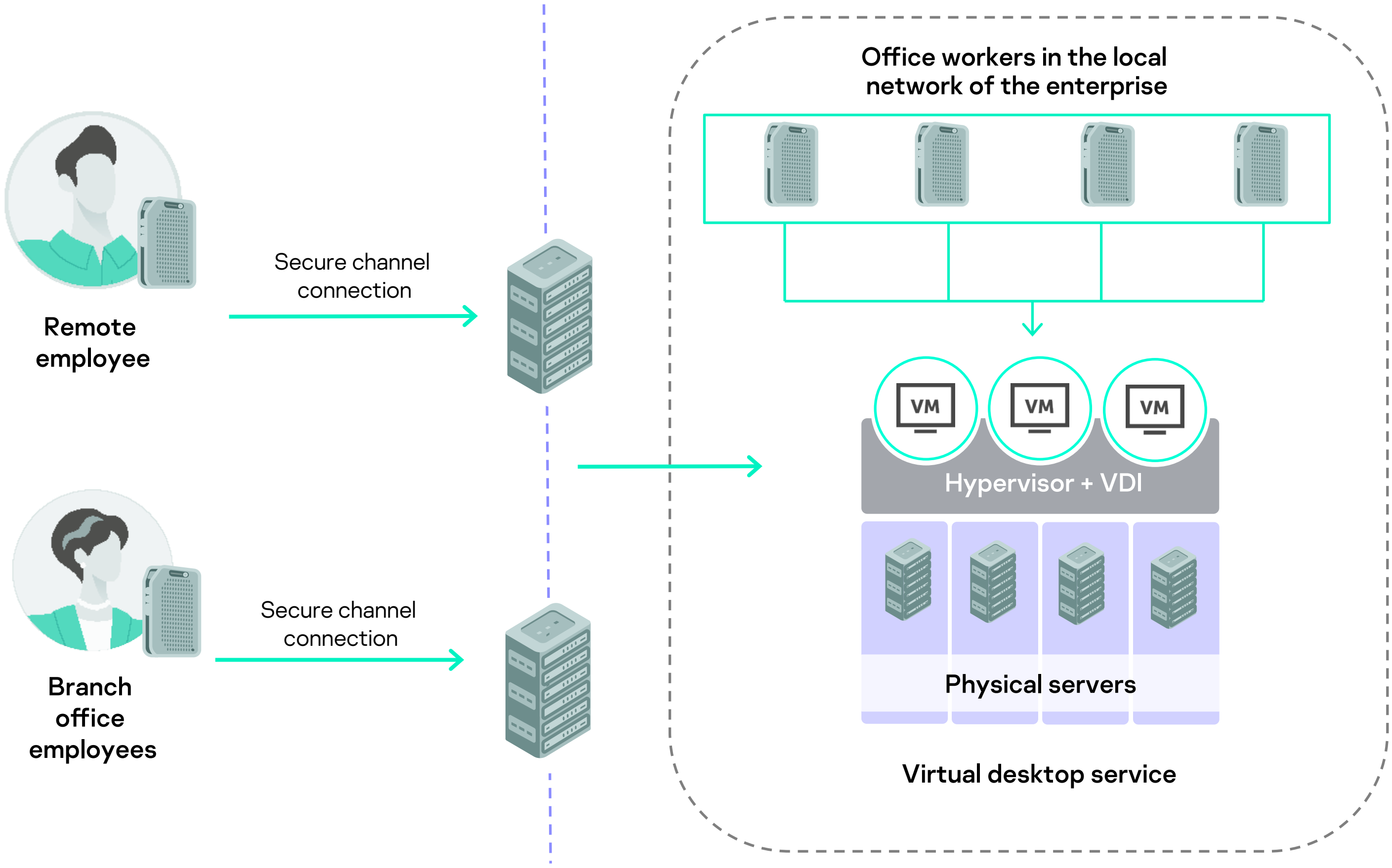


Kaspersky Security Management Suite
Kaspersky Security Center
Kaspersky Thin Client
Kaspersky Security for Virtualization Agentless
Kaspersky Security for Virtualization Light Agent
Kaspersky Security for Storage
User devices
VM
VM
VM
Data processing center
Hypervisor
Storage
Physical servers
'Golden image'
Virtual machine images
Remote connection broker

Use cases

1. Head office and branch offices

Kaspersky Secure Remote Workspace is an effective solution for companies with an extensive network of branch offices. Preconfigured thin clients are installed in remote branch offices. They connect securely to virtual desktops and are centrally managed via the KSC console. Compared to conventional desktops and laptops, the solution has a more favorable price and cost of ownership. It also reduces administration and support costs.

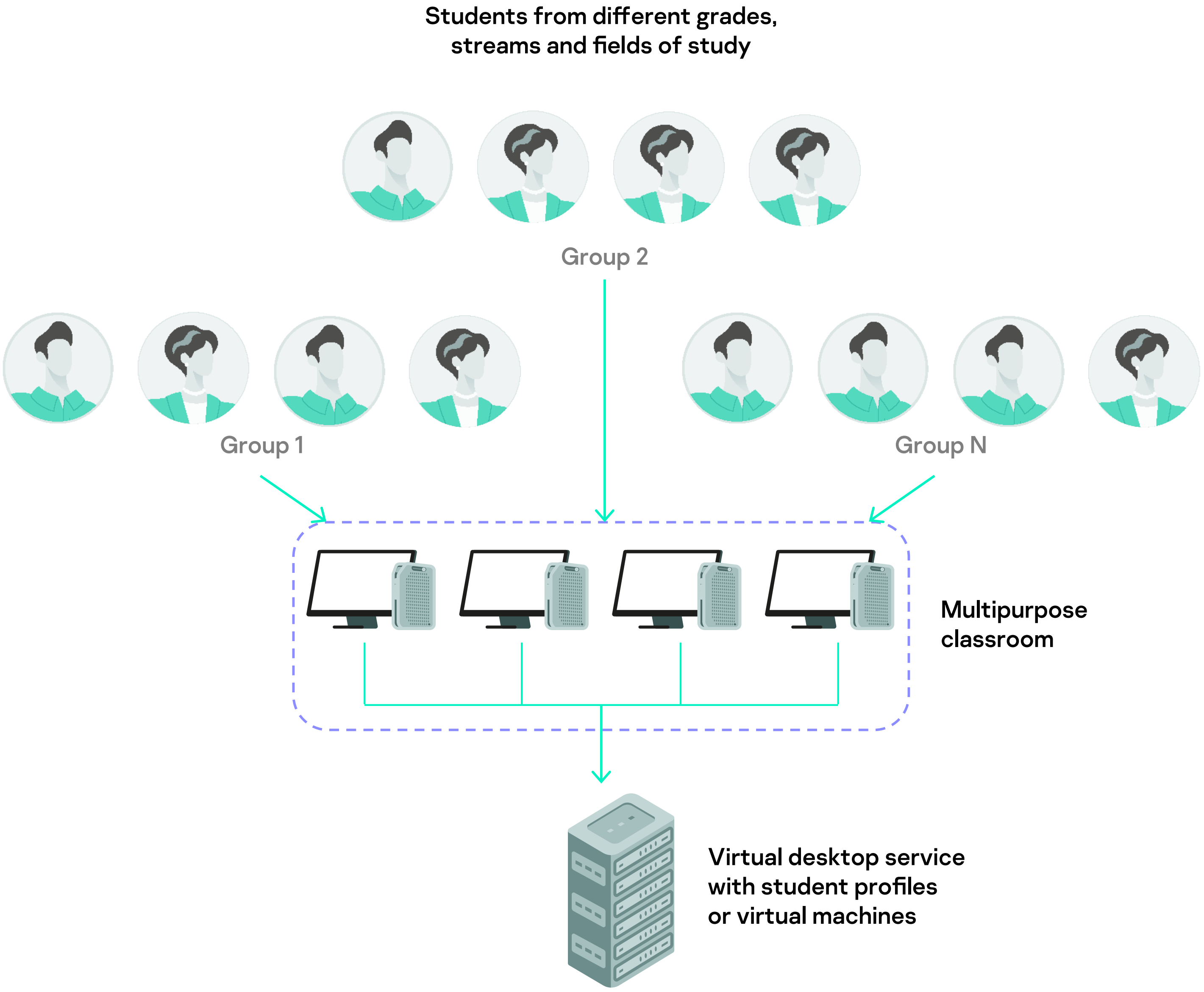

Remote employee
Secure channel connection
Branch office employees
Secure channel connection
Office workers in the local network of the enterprise
VM
VM
VM
Hypervisor + VDI
Physical servers
Virtual desktop service

2. Classrooms in educational institutions

The problem of standard desktops or laptops not being used for their intended purpose often arises in classroom environments. There is a significant risk of network compromise or malware infection when removable media are connected.

There are several advantages to using thin clients in a classroom setting:

- students can only connect to the required services;
- the ability to quickly deploy a learning environment for laboratory practice;
- it is possible to limit the use of removable media and other peripheral devices;
- there is no need to replace the fleet of thin clients – they have a relatively long service life, and the likelihood of them breaking down is much less than that of desktops and laptops.

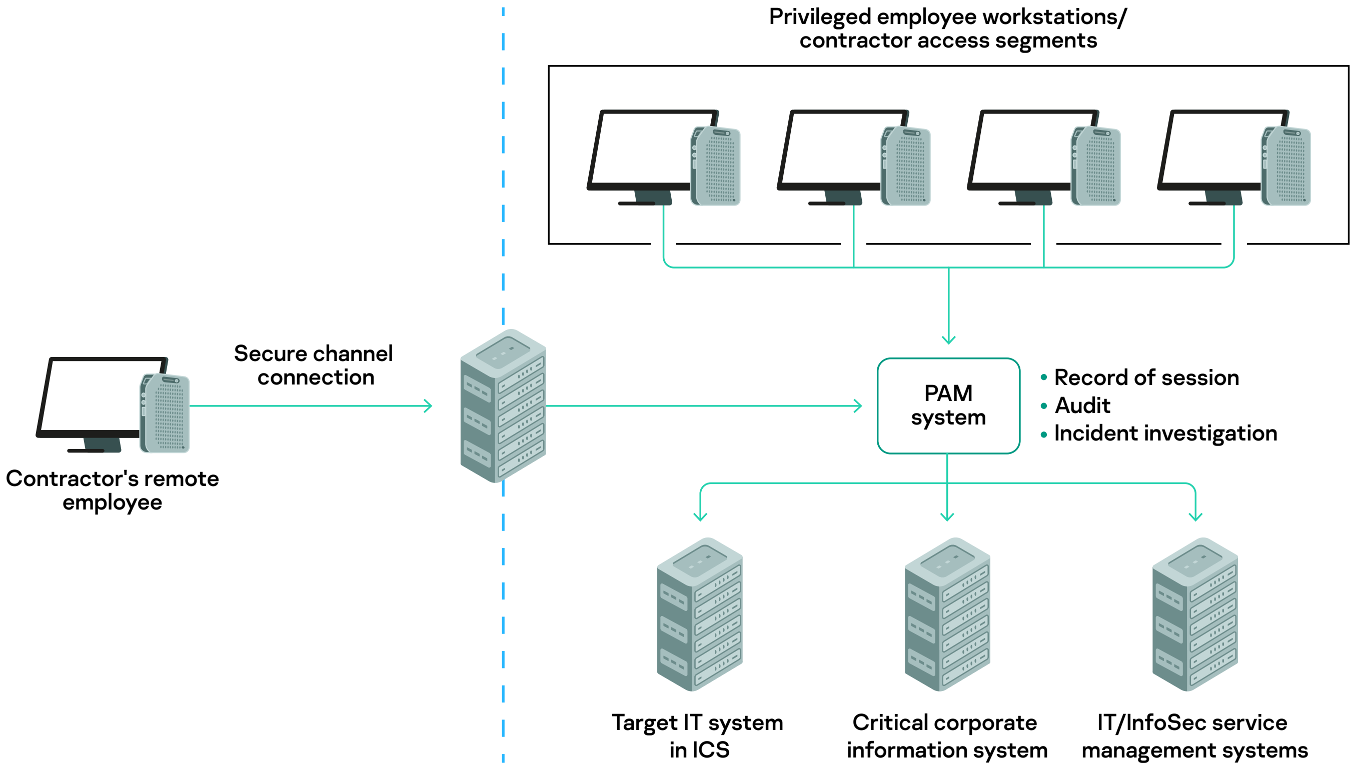

Students from different grades, streams and fields of study
Group 2
Group 1
Group N
Multipurpose classroom
Virtual desktop service with student profiles or virtual machines

3. Connecting to privileged access management systems

Privileged Access Management (PAM) systems allow you to audit the actions of specialists (both internal and external) with enhanced rights, record sessions as well as manage password protection settings and authorization and authentication processes. Such systems are used, among other things, where IT maintenance of key infrastructure is outsourced, and the objects that are accessed are critical (e.g., ICS).

Using **Kaspersky Secure Remote Workspace** in conjunction with PAM eliminates the use of employee-owned portable devices that can be used to attack the infrastructure. It also enables control over the connection of peripheral devices.

Pre-installed certificates on PAM servers and thin clients do not permit connections to the infrastructure that bypass the access management system.

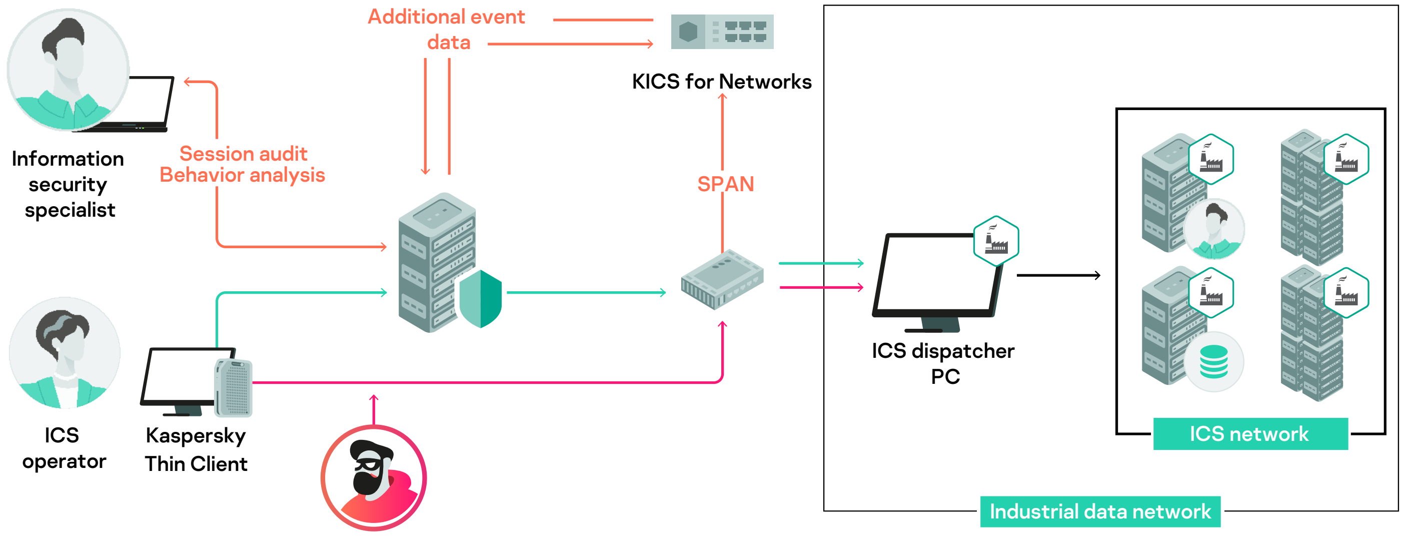


4. Segment isolation and provision of inherently secure access to CII

Secure and segmented access is implemented on the basis of an SKDPU NT system in conjunction with **Kaspersky Secure Remote Workspace**. This setup allows you to restrict access to only those devices necessary for operations, with the ability to limit the launch of arbitrary software on the target node.

The employee is provided with a remote workspace. Access to the protected segment is provided by thin clients with the Kaspersky Thin Client software product, based on KasperskyOS, installed on them. Collection and analysis of events within sessions is performed by SKDPU NT system tools.

At the same time, due to extended integration with **Kaspersky Industrial CyberSecurity for Networks**, additional functions are implemented to control access directly to the protected CII object's information system.



Additional information

Request an expert consultation to learn more about Kaspersky Secure Remote Workspace.
os.kaspersky.com/solutions/kaspersky-secure-remote-workspace

os.kaspersky.com
www.kaspersky.com

KasperskyOS