Building VDI infrastructure in government institutions

Orenburg Region's Ministry of Digital Development and Communications trusts Kaspersky solution to protect VDI infrastructure
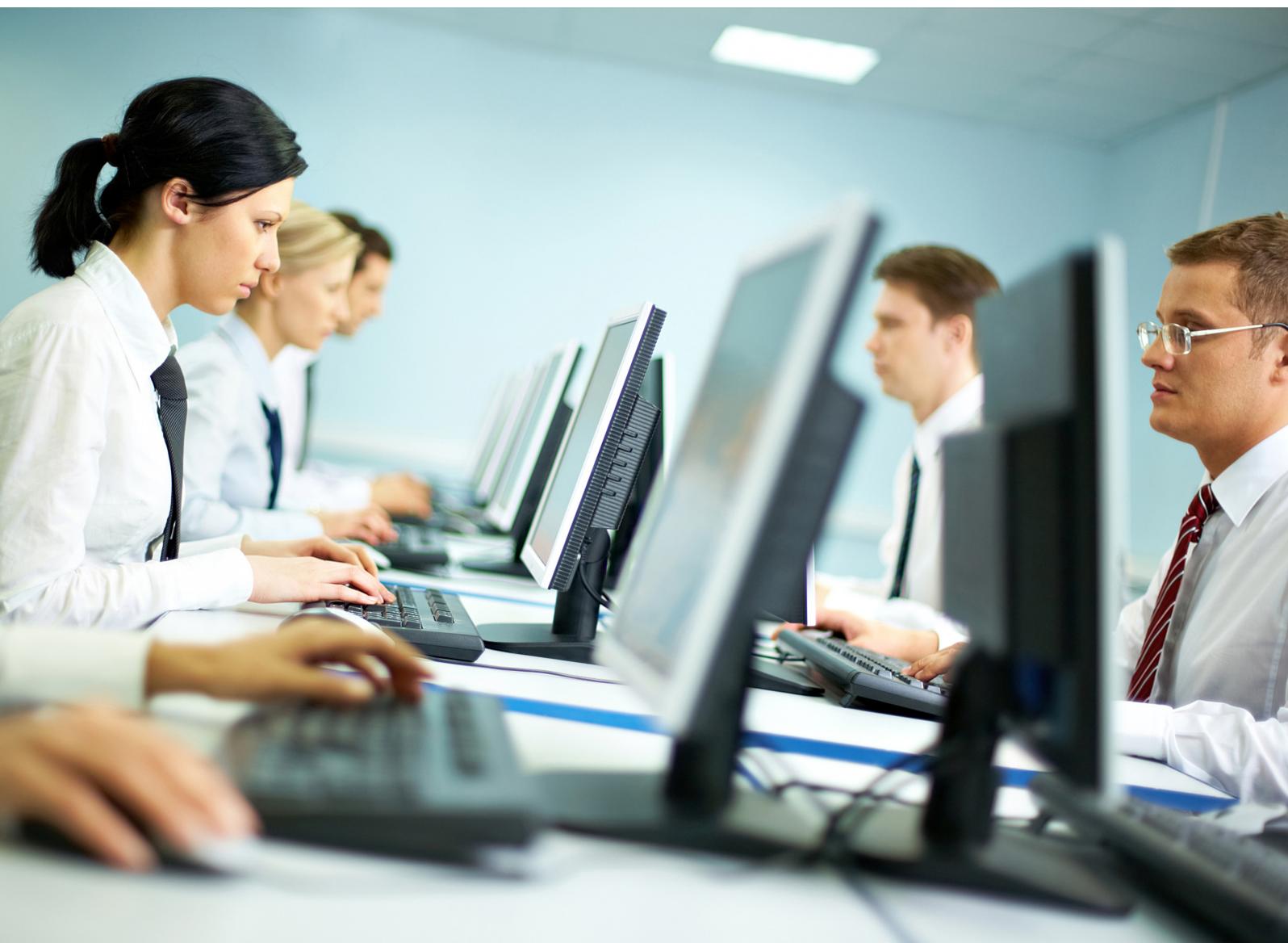
KasperskyOS

The public sector is actively integrating into the digital environment, trying to satisfy ever more requests from citizens and improve efficiency. This requires not only a restructuring of work processes, but also a reconsideration of the approach to cybersecurity. Following a request from the Orenburg Region's Ministry of Digital Development and Communications, we proposed a solution that both accelerates digital transformation and solves the problem of protecting new workspace infrastructure from cyberattacks.

Pilot project objectives

IT infrastructure in public sector institutions is becoming more complex, and it is being accessed by a large number of users. The volume of processed information that may be confidential is also growing. For this reason, more and more attention is being paid to cybersecurity issues. The following tasks were set before implementing the pilot project:

· simplify and standardize the IT infrastructure as much as possible and reduce maintenance costs;
· securely process data in the data center;
· ensure protection of information stored in the data center;
· provide a unified user device management system.

Solution

After studying the requirements for the pilot project, Kaspersky offered the Ministry a comprehensive solution – **Kaspersky Secure Remote Workspace** – designed to build a managed and functional thin client infrastructure based on the Cyber Immune operating system KasperskyOS. The solution consists of three complementary products:

Kaspersky Secure Remote Workspace

Kaspersky Thin Client

KasperskyOS-based software product installed on a hardware platform

Kaspersky Security Center

Unified console for managing thin clients and other Kaspersky products

Kaspersky Security Management Suite

Special add-on module for fleet administration

The project involved the implementation of a unified user device management system. In the **Kaspersky Secure Remote Workspace** solution, this is the **Kaspersky Security Center** console. It is also used to manage other Kaspersky products. It allows for more efficient and convenient administration and the creation of new workspaces. This increases reliability and reduces infrastructure maintenance costs. Using **Kaspersky Thin Client** for VDI access fully met the customer's requirement for simplified IT infrastructure and cost optimization, because of the favorable price and cost of ownership compared to classic desktops and laptops, as well as the long (7–10 years) service life. The project placed particular emphasis on the effectiveness of cybersecurity. Thanks to the KasperskyOS operating system that the Cyber Immune thin clients run on, the risk of attacks on remote workspaces is significantly reduced, which eliminates the likelihood of intruders accessing data from a data center. **Kaspersky Secure Remote Workspace** ensures:

· trusted connections to target servers are established using certificates;
· the integrity of data transmitted between the server and users;
· quick and secure thin client software updates.

The solution components have been entered into the unified register of Russian programs for electronic computers and databases:

· **Kaspersky Thin Client** —number 244652 dated 20.08.2021
· **Kaspersky Security Management Suite** —number 244657 dated 16.08.2021

Kaspersky Secure Remote Workspace therefore perfectly meets the requirements set by the ministry, and we proposed a pilot project based on it.

Result

The pilot project, launched in 2021, was deemed a success by the customer. Based on the results of the pilot, the Ministry of Digital Development and Communications of the Orenburg Region purchased:

· virtual desktop infrastructure based on the Basis.WorkPlace virtualization management system (formerly Scala-R VRM);
· thin clients with KasperskyOS-based software installed;
· operating systems for virtual machines (Alt Linux, Windows);
· office software.

In the future, the ministry plans to transfer all state organizations related to the administration of the city and region to a modern VDI infrastructure.

As a result of implementing **Kaspersky Secure Remote Workplace**, the customer received:

· a secure and functional remote workspace infrastructure with a competitive price, favorable cost of ownership and a long service life;
· the ability to scale infrastructure at minimal cost;
· quick and secure thin client software updates, as well as centralized thin client management;
· the ability to optimize cybersecurity and IT costs.

The solution is included in the list of standard automated workspaces that can be used by government agencies when building their infrastructure in accordance with Russian government decree No. 1236 of November 16, 2015, 'On establishing a ban on the admission of the software originating from foreign states for the purpose of procurement to meet state and municipal needs'.

At a meeting of the Commission on Digital Development and the Use of Information Technology in the Orenburg Region, a list of software was approved and the concept of a standard automated workspace was adopted. In the near future, the Orenburg Region authorities will start creating road maps for the transition to domestic solutions.

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

KasperskyOS