A managed and functional thin client infrastructure with Cyber Immunity

Kaspersky Thin Client

KasperskyOS

kaspersky cyber immunity

Using thin clients for workstations: advantages and challenges

This state-of-the-art approach to setting up remote workstations only requires that an employee workstation has a monitor, a keyboard and a thin client. A user uses the thin client to connect to a server-deployed operating system that runs only the applications required for the particular business. This approach has a number of advantages over traditional workstations, including:

- automates the process of creating desktops;
- moves away from storing and processing data on employee devices;
- recovers data quickly after an incident;
- manages remote desktops from one location;
- reduces the risk of attacks from remote workstations.

Thin clients connect to:

- terminal server;
- remote virtual machine;
- VDI infrastructure
- DaaS;
- remote physical PC/server;
- application server.

A user workstation is one of the most common points of access into a corporate network where sensitive data is stored. Potential vulnerabilities include the specific sets of network protocols of thin client operating systems, devices connected to thin clients, third-party applications, and thin client management servers. In addition, there are flaws and/or gaps in the code of remote environment delivery protocols.

According to data from Kaspersky ICS CERT, there are **at least** 25 known vulnerabilities in the Remote Desktop Protocol clients known as rdesktop and FreeRDP, which are used in Windows, Linux and macOS to allow users to connect to a remote desktop.

Threats affecting thin clients

RDP server spoofing

There are many tools that can be used to conduct a man-in-the-middle attack on RDP/VNC. All attacks exploit something from the following list:

- The client side is using a protocol without encryption (some VNC installations).
- The client side does not verify the server certificate.
- Weak encryption is used between the client and the server.

Vulnerabilities in RDP/VNC library code

When a connection is established with a malicious server, arbitrary code is remotely executed in the context of the user account that was used to start the RDP/VNC client. This could be used to acquire user accounts from other systems to expand an attack.

Attack on other thin client users

When a device is shared by various users, a legitimate user may exploit a vulnerability to elevate privileges and gain access to the user accounts of other users.

Attack on a management server

By exploiting a vulnerability in a management server or spoofing this type of server, cybercriminals can change the configuration or update the firmware of thin clients that connect to this server. Then the hacked devices can be used to acquire user accounts from other systems and use them for lateral movement to expand the attack.

Mandatory condition: Manageability of thin clients

The fleet of equipment used to connect to a remote workstation infrastructure can often be quite diverse. A company may employ PCs, laptops and thin clients at the same time. In terms of administrative costs, thin clients are the most optimal variant because even personnel with no special training can replace thin clients when these devices fail or malfunction.

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

- the absence of moving parts (fans and HDDs) 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, full-fledged management, configuration, updates and audits of a large fleet of thin clients can turn into a labor-intensive and high-risk process without proper centralization. The full benefits of thin clients are unlocked by a centralized management system that simplifies administration and support.

Cyber Immune approach to the protection and manageability of a thin client infrastructure

Potential threats can be prevented and your workstation infrastructure can be protected by utilizing the Cyber Immune approach employed in Kaspersky Thin Client. This is a specialized version of the KasperskyOS operating system designed for thin clients. An operating system that is secure by design lets you avoid having to use additional security tools on top of the OS. The single Kaspersky Security Center console for the solution lets you conveniently resolve potential problems concerning the manageability and monitoring of your thin client infrastructure.

Solution components

Cyber Immune Thin Client

Kaspersky Thin Client

Operating system that is designed for thin clients and is based on the KasperskyOS microkernel

Centerm F620

A single management platform for Kaspersky products

Kaspersky Security Center

Single console for centralized management of Kaspersky products

Kaspersky Security Management Suite

Kaspersky Security Center extension that lets you manage thin clients

Applicable use of Kaspersky Thin Client

Kaspersky Thin Client is suitable for many areas of activity in which a large number of workstations with similar tasks and a standard set of applications are used. There are many possible usage scenarios for various vectors of activity:

Finance and insurance

- Local offices of financial institutions
- Call centers
- Customer support services

Energy and manufacturing

- Access to SCADA/industrial control systems
- Engineer workstations

Public sector

- Access to electronic document management systems
- Public servant workplaces

Educational institutions

- Classrooms
- Testing grounds
- Academic competitions

Healthcare

- Reception areas
- Information boards
- Connection points for workstations of medical specialists

Retail and Warehouse logistics

- Cashier workplace
- Call center operator workplace
- Access to warehouse management systems (WMS)

Cyber Immunity

Approach to building systems to ensure that they have inherent protection against cyberattacks.

Cyber Immunity can be ensured only after clearly and precisely defining your security goals, separating your overall IT system into isolated segments, controlling the interaction between those segments, and minimizing the potential attack surface. Critical assets of a Cyber Immune system remain resistant even to unknown threats without additional security tools.

KasperskyOS

Proprietary microkernel operating system that was built from scratch by Kaspersky to support the development of Cyber Immune products. It was created based on best practices in the development of specialized, secure-by-design systems and the extensive, long-standing experience and expertise of Kaspersky in the field of information security.

Cyber Immune thin clients for secure connections to remote desktops

Kaspersky Thin Client has Cyber Immunity attributes that ensure the following:

- the integrity of data received from the user,
- the **Kaspersky Security Center** centralized management server, and connection broker servers;
- secure updates of thin clients
- confidentiality and integrity of data transmitted between **Kaspersky Thin Client**, a remote desktop, the **Kaspersky Security Center** server, a logging server, and the 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 the 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 by other Kaspersky products. This makes the integration of Kaspersky Thin Client into the existing ecosystem of corporate IT protection systems as seamless as possible, without the need to hire additional specialists.

Cyber Immunity in action: Kaspersky Thin Client compared to ordinary thin clients

Advantages of the Cyber Immune approach

A Cyber Immune thin client is not affected by this vulnerability because it does not connect over the RDP protocol without first establishing a mandatory TLS connection that completes authorization of the remote server. The connection is established by TLS Terminator, which is a component with a small attack surface that cannot be disabled, modified or bypassed because these attributes are guaranteed by the design of the operating system.

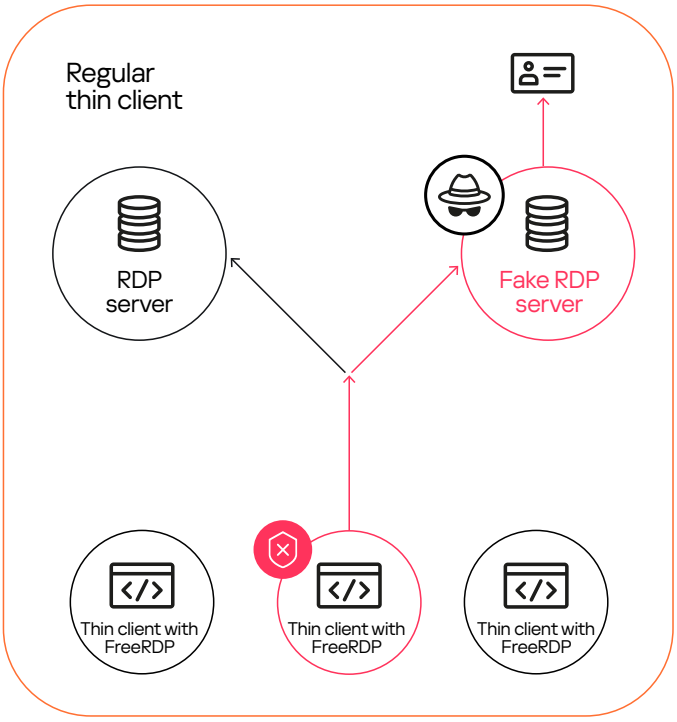
1. Attack on the RDP/VNC protocols

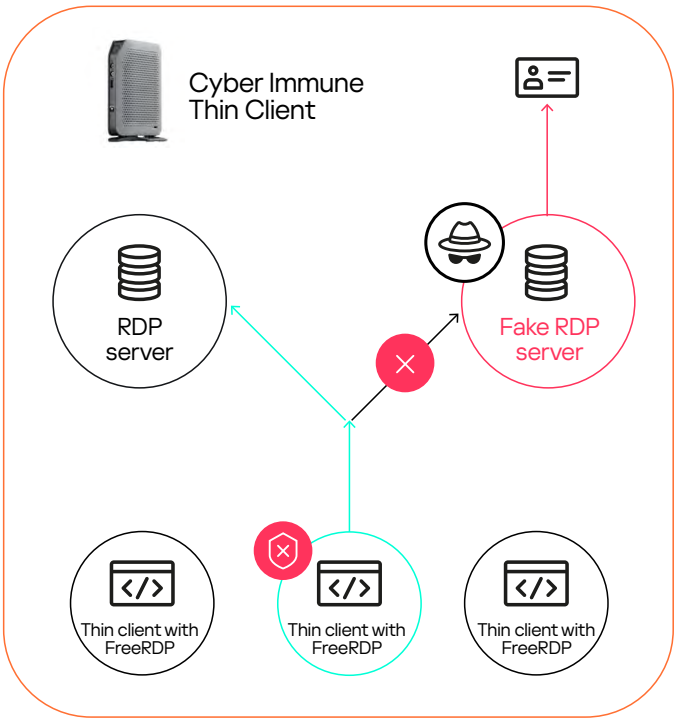
A cybercriminal gains access to the internal network of a company and conducts a man-in-the-middle attack using ARP Spoofing, for example. A victim connects to the spoofed RDP/VNC server and the cybercriminal captures the victim's user account credentials.

Then the cybercriminal can use these credentials to connect to a legitimate server for lateral movement to further expand the attack.

CVE-2005-1794

Vulnerability in Microsoft Terminal Server that enables a cybercriminal to conduct a successful man-in-the-middle attack.





Advantages of the Cyber Immune approach

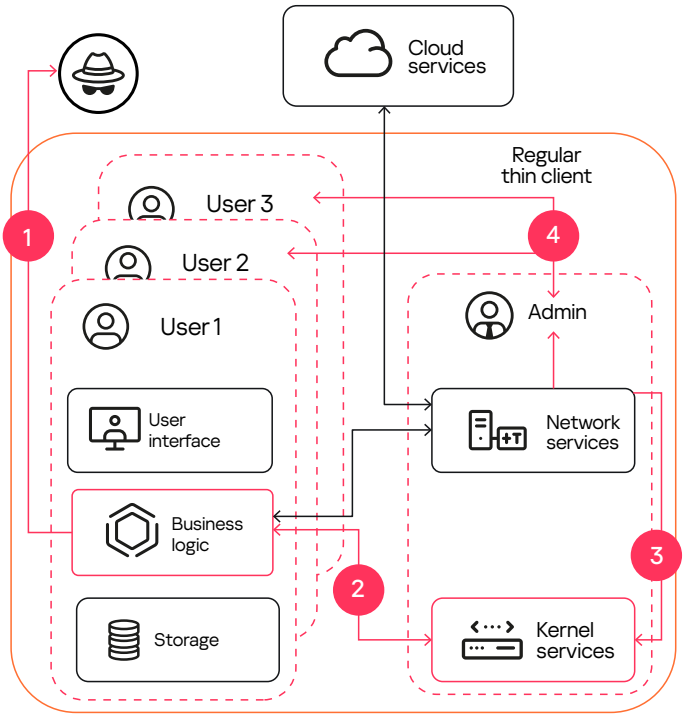
The concept of «users» is irrelevant to a Cyber Immune thin client. The system functions responsible for administration are allocated into separate, isolated components. Privilege elevation in a Cyber Immune thin client is fundamentally impossible even if a successful attack is conducted against one of its components.

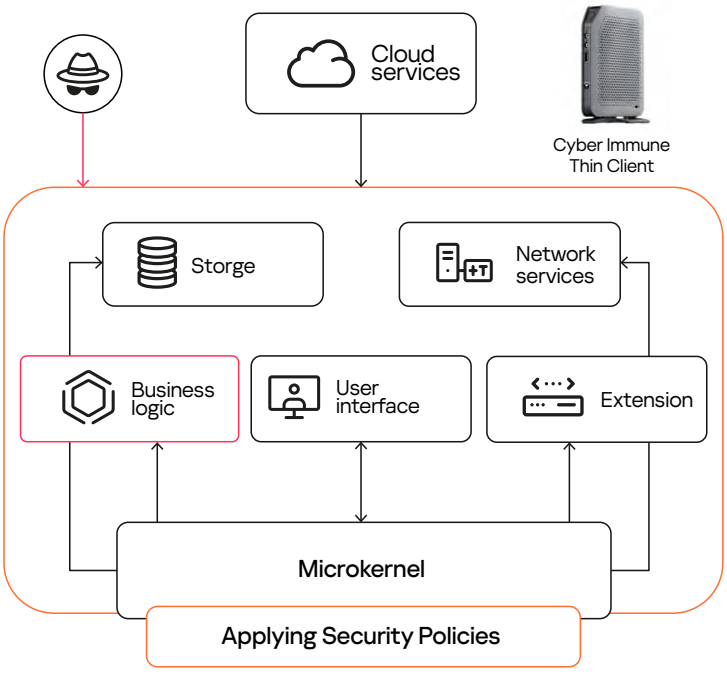
2. Attack on other users of a shared thin client

An otherwise legitimate user of a thin client exploits the privilege elevation exploit to gain administrator/root privileges and then uses this privileged access to steal the user accounts of other users of the shared thin client.

CVE-2016-2246

A local user can use a virtual keyboard to elevate their privileges.





Advantages of the Cyber Immune approach

Administration of a Cyber Immune thin client is conducted through the KSC server. The connection to this server is established with the mandatory use of a TLS connection just like any connection to a remote RDP server. If a cybercriminal deploys their own KSC server, its certificate will not be present in the trusted certificate store of the thin client and the attempted TLS connection will result in an error.

3. Attack on a thin client management server

A cybercriminal gains access to the internal network of a company and conducts a man-in-the-middle (MITM) attack. A victim connects to a spoofed management server and the cybercriminal changes the configuration of the device.

The goal of this attack is to establish persistence on the victim's computer to gather more information and move laterally through the network.

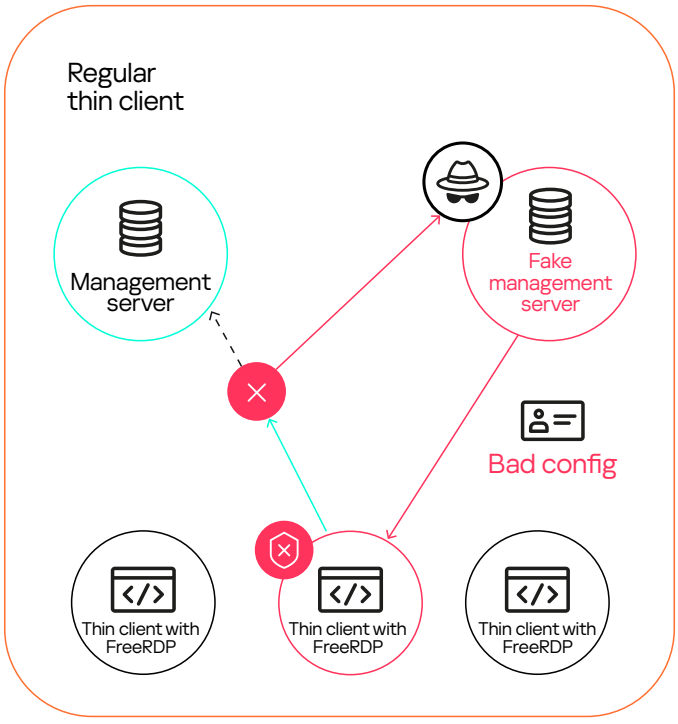
The cybercriminal exploits a vulnerability on the management server to change the configuration of thin clients or update their firmware. Then the cybercriminal uses the modified thin clients to acquire the user accounts from other systems and employs those user accounts for lateral movement to expand the attack.

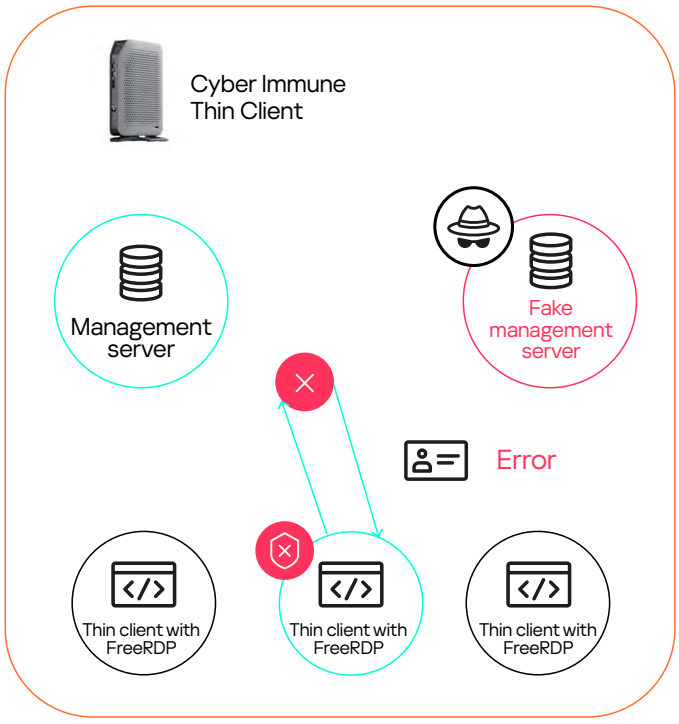
CVE-2021-21532

This vulnerability allows a cybercriminal to conduct an MITM attack between a thin client running an OS with a monolithic kernel and the management server to then change the configuration of a device.

CVE-2020-29492

An FTP server used to update the firmware of devices running an OS with a monolithic kernel allows an anonymous user to edit the INI file. This could allow arbitrary code to be executed on both the thin client itself and on a machine to which the thin client connects.





Role of Kaspersky Thin Client in the comprehensive workstation infrastructure protection provided by Kaspersky products

Additional information

Request an expert consultation to learn more about Kaspersky Thin Client and successfully implemented projects os.kaspersky.com/solutions/kaspersky-thin-client

Setting up a Cyber Immune workstation

Based on the KasperskyOS microkernel, Kaspersky Thin Client ensures a secure and trusted connection to remote desktops.

Protecting virtual and cloud infrastructures

Kaspersky Hybrid Cloud Security is an integrated solution that provides comprehensive protection of virtual machines against various types of information security threats, network attacks, and other fraudulent activity.

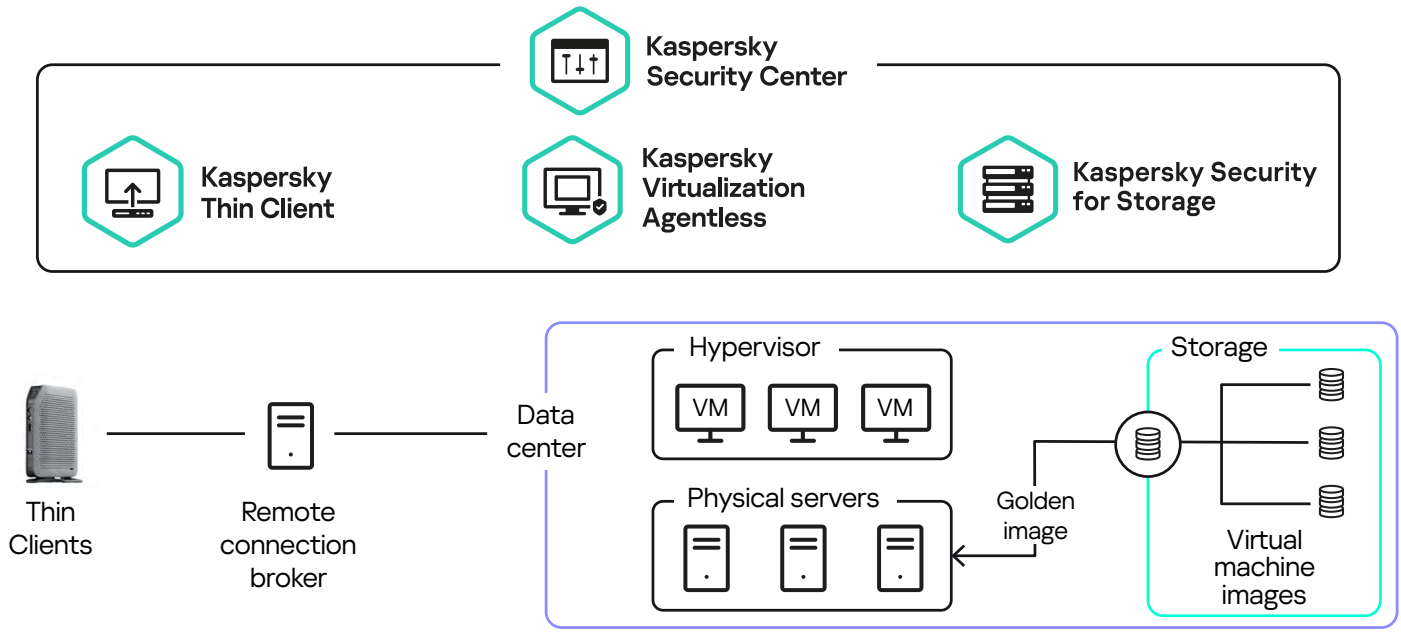
Remote workstation protection

Kaspersky Endpoint Security provides comprehensive protection of a computer against various types of threats, network attacks, and other fraudulent activity.

Centralized management

Kaspersky Security Center provides a single console for centralized management of all Kaspersky products.

All of these products are also managed through **Kaspersky Security Center**.



os.kaspersky.com
www.kaspersky.com

KasperskyOS