# Computer antivirus system

# General requirements:

# Systems support:

# • Windows workstations

# • Windows servers

# • Linux servers

# The computer antivirus system provided must be recognized by the following independent analytical agencies:

# • The Forrester Wave Endpoint Security Suites

# • Gartner Magic Quadrant for Endpoint Protection Platform (Leaders)

# Product licensing should be common, regardless of the number of servers.

# Quantity

# • 500 pieces

Protecting servers and workstations

Requirements for the management system

Platform support

• Windows Server 2012 R2 64 Standard / Datacenter

• Windows Server 2016 64 Standard / Datacenter

• Windows Server 2019 64 Standard / Datacenter

Database support

• Built-in database

• Microsoft SQL Server 2008 R2 Express SP2

• Microsoft SQL Server 2008 R2 / 2012/2014/2016

• Microsoft SQL Server Express SP1

The control panel should be based on web technologies and work through the HTTPS protocol.

Browser support:

• Microsoft Internet Explorer Windows

• Mozilla Firefox Windows / Mac

• Chrome Windows / Mac

• Microsoft Edge Windows

Automatic grouping should not interfere with manual placement.

In the event of a malfunction, the system should be able to collect information through the control panel for technical support from the manufacturer

Digital certificates should be used to protect agent-server communication

It should be possible to specify an individual communication port for each agent

Support for workstation operating systems:

* Windows 7 32/64 SP1
* Windows 7 32 /64 Thin PC/Thin PC SP1
* Windows 8.1 32/64 Standard/ Pro/ Enterprise
* Windows 10 32/64

Server operating system support:

* Windows Server 2008 R2 64 Standard SP1/ Enterprise SP1/ Datacenter SP1/ Web SP1/ Server Core SP1
* Windows Storage Server 2008 64 R2 Basic SP1/ Standard SP1/ Enterprise SP1/ Workgroup SP1
* Windows Server 2012 64 Standard/ Datacenter/ Server Core
* Windows Server 2012 R2 64 Standard/ Datacenter/ Server Core
* Windows Storage Server 2012 64 Standard/ Workgroup
* Windows Storage Server 2012 R2 64 Standard/ Workgroup
* Windows Server 2016 64 Standard/ Datacenter/ Server Core
* Windows Server 2019 64 Standard/ Datacenter/ Server Core

Install / uninstall

Methods of setting agents:

• From the control panel

• Logon Script

• The so-called gold image

• Monitor network segments and automate installation on vulnerable stations

• DHCP traffic monitoring and automatic installation on vulnerable stations

• Autonomous Distribution Generation:

• EXE 32 package generation

• EXE 64 package generation

• MSI package generation

• Create a self-generating package for agent updates (signature files and executable files)

Central uninstallation of agents should be possible.

Agent self-defense (with password):

• Remove the agent

• Protect settings changes (real time scanner)

• Protect settings changes (scheduled scanning)

• Protect settings changes (manually scan)

Updates

• Update signature files

• Update scan modules

Update sources:

• Manufacturer's servers

•control panel

Requirements for protection mechanisms

The agent must ensure protection against the following threats:

•virus

• Trojan virus

• "Network Worm"

• Advertising programs

• Spyware

• Calling programs

• Joke programs

• Pirate key generators

• Crypto-robber viruses

The agent should be able to implement the following protection mechanisms

• Heuristic analysis

• Behavioral analysis

Product protection technologies:

• Check the exploit file

• Block access to unsafe web resources (HTTP / HTTPS)

• Close programs if they have been attacked by exploits.

Malware protection modes:

• Real time (file creation / modification)

• At the request of the customer

• From the central control panel

• According to the schedule (message before checking, postponing the scan in case of insufficient charging of the laptop battery)

If the file is cured, the product should be able to produce automatic backups.

The system should be able to detect threats in the following formats: ARJ, UPX, MSCOMP, PKLite, ASPAC, DIET, LZEXE, ACE, BZIP, BZIP2, CAB, CHM, GZIP, LHA, RAR, TAR, ZIP, BIN, TD0

The system should be able to block / detect potentially dangerous actions below

• Create a system-like file name

• Change programs that belong to a certain extension

• Block access to DLL files from unreliable folders

External devices / network control:

• Block auto-start from USB devices

• Block programs from USB devices

• USB device content-only browsing mode

• Lock CD / DVD playback

• Block playback of CD / DVD files

• CD / DVD read only mode

• Block network drives

• Block programs running from network drives

• Network Disk Content Browsing Mode

External device controls must be configurable individually for users.

The system must have the following modes of mechanical containment of threats:

• Block file by name

• Block write to certain folders

• Block the interaction of certain network ports

• Block write to network folders

• Block access to the following format check files: Armadillo, Aspack, ASPR (Asprotect), AutoHotkey, Autoit, Enigma Protector, EXECryptor, EXE Stelth, eXPressor, FSG, MEW, MoleBox, MPRESS, NeoLite, NsPack, Packman, P , Telock, Themida, Upack, UPX

System response methods for malicious files.

• Stop the process

• Quarantine

• Rename

• Journal entry

• Display message to customers

The system must have and support the sandbox function, which can be purchased separately