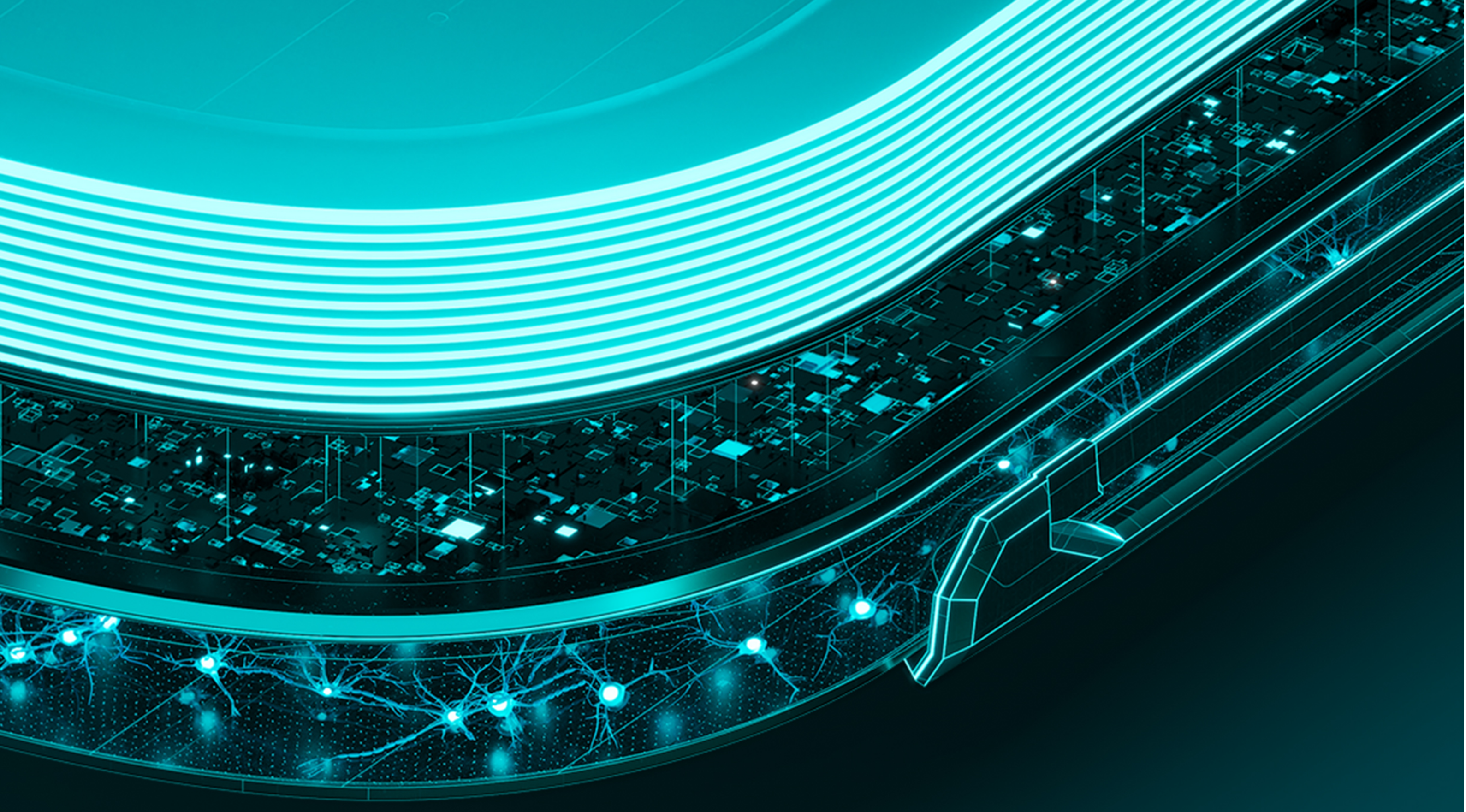
ESET PROTECT COMPLETE



Digital Security
Progress. Protected.

Content

Endpoint Protection 3
Server Protection 8
Mail Protection 11
Protection Management....................14
About ESET company....................17

Endpoint Protection

1. Provides protection against: viruses, Trojan horses, adware, phishing, and spyware.
2. Providing protection against malware - certain malicious code that is added to the beginning or end of the code of existing files on the computer. Malware detection should be performed by a detection engine in combination with a machine learning component.
3. Providing protection against potentially unwanted programs that cannot be unambiguously classified as malware by analogy with such definitely malicious programs as viruses or trojans, but these programs can install additional unwanted software, change system settings, and perform unexpected actions or actions not confirmed by the user.
4. Providing protection against potentially dangerous programs - a variety of software that can be used for malicious purposes, such as unauthorized remote access, password theft or cracking, keyloggers, etc.
5. Provide protection against suspicious programs - programs that are compressed with packers or protectors that are often used by malicious actors to prevent detection of malware.
6. Provides protection against dangerous rootkit programs that give attackers from the Internet unlimited access to the system while hiding their presence in the operating system.
7. The ability to customize separate response levels for different categories of threats for both protection and reporting.
8. The ability to exclude certain files from scanning that are not malicious, but whose scanning may cause abnormalities or affect system performance.
9. The ability to create exceptions for system-wide processes in order to improve the speed of system services and minimize interference with the OS.
10. The ability to scan boot sectors for viruses in the master boot record, including the UEFI interface.
11. Provide real-time antivirus protection.
12. Using heuristic technologies of our own design during scanning.
13. Antivirus scanning at the request of the user or administrator and according to the schedule.
14. Document protection module that allows you to check Microsoft Office macros for malicious code.
15. Ability to scan files at OS startup.
16. The ability to scan WMI and the system registry, all sections and subsections, which provides protection against malicious software code and malicious links that are distributed in the form of data.
17. The presence of a built-in tool that combines several utilities to clean the remnants of complex persistent threats, such as Conficker, Sirefef, Necurs, etc.
18. Scanning a computer when it is idle.
19. The ability to define detailed parameters of the anti-virus scanner, such as: defining objects and scanning methods, setting the maximum file size and scanning time, the maximum archive attachment depth and creating exceptions.

20. The use of a 64-bit kernel for scanning, which reduces the load on the system and allows for the fastest and most efficient scans.
21. The ability to use machine learning technologies for more in-depth code analysis to detect malicious behavior and malware characteristics.
22. An exploit protection module that provides protection against threats that can exploit vulnerabilities in various applications such as Java, Flash, etc.
23. A module that deeply analyzes running processes and their activities in the file system, which provides an additional level of protection against ransomware.
24. A RAM scanning module that can monitor the work of suspicious running processes, which helps prevent infection even with carefully encrypted and hidden threats.
25. The presence of an intrusion detection system (HIPS) that monitors program launches and changes in the system registry and protects the computer from malware and unwanted activity.
26. Ability to create custom rules to control running processes, executable files, and registry keys.
27. Additional verification of running processes in the cloud reputation service.
28. Ability to integrate workstation and server protection with a cloud sandbox (with an additional license), without the need to install additional software.
29. Automatic anti-virus scanning of removable media.
30. Availability of a tool that can control the connection of removable media to the workstation by creating access rules, namely: blocking, permission, read-only, read and write, warning.
31. The ability to control the connection of external devices to the workstation by device type, manufacturer, model or serial number of the device.
32. Ability to create groups of allowed or prohibited external devices.
33. The ability to disable or enable external device connections for all users, individual Windows users or groups, or a domain.
34. The ability to set time intervals, which allows you to more flexibly configure device control rules.
35. Provide an additional layer of protection for email traffic on the workstation by integrating with an email client, with the ability to check POP3, POP3S, SMTP, IMAP and IMAPS and verify email attachments, especially on PCs that are temporarily or permanently outside the corporate network.
36. Ability to automatically delete or move infected mail to a specified directory in the email client.
37. An in-house developed anti-spam module that can be integrated into an email client, which provides an additional level of protection against spam, especially on PCs that are temporarily or permanently outside the corporate network.
38. The ability to use both user-specific (flexible personalization of the intelligent spam module) and global white and black lists of spam recipients, which are updated from update servers.
39. Providing an additional level of Internet traffic protection by checking HTTP and HTTPS traffic, which makes it possible not only to block files transmitted by these protocols, but also to block the addresses of such dangerous resources as phishing sites, botnet servers, command and control (C&C) APT servers, and servers that distribute ransomware threats.
40. The ability to create lists of blocked, allowed, or excluded URLs.

41. The ability to block downloading files from the Internet with a specified extension, especially on PCs that are temporarily or permanently outside the corporate network.
42. Ability to check the SSL protocol in both automatic and interactive modes.
43. Verification of the validity and integrity of SSL traffic certificates.
44. Ability to manage lists of trusted certificates and certificates excluded from verification, as well as the ability to select an action when a certificate is determined to be invalid, uncertain or damaged.
45. Availability of an additional module that allows you to run browsers in protected mode in order to block attempts to interfere with the browser's memory area and the contents of its windows, as well as additional protection of critical Internet connections such as Internet payments and Internet banking, etc.
46. The ability to create exceptions to traffic inspection for individual programs and individual IP objects (IP addresses, IP address ranges, subnets).
47. Personal firewall for network filtering and protection against both external and local network attacks.
48. The personal firewall has an interactive mode that provides detailed information about a new unknown network connection and allows not only to create a new network filtering rule on the PC for the detected connection, but also to specify detailed settings for it.
49. The personal firewall has a learning mode that allows the administrator to remotely configure permission rules for network applications and equipment.
50. The rule editor allows not only to edit the created rules, but also to manage the built-in rules, which are sufficient for initial thorough protection against unauthorized network connections and local network attacks.
51. Ability to create network filtering rules for specific programs and services.
52. The ability to create different profiles for the personal firewall that can automatically switch, depending on which network the computer is connected to.
53. The ability to use additional network authentication in the personal firewall to prevent unauthorized connection of the PC to unknown dangerous networks.
54. Additional functionality of the personal firewall that allows you to view all the detailed information on all existing network connections, as well as warn the user about connecting to an unsecured Wi-Fi network.
55. The ability to configure additional parameters of the Intrusion Detection System (IDS) module in order to detect various types of possible network attacks on the computer.
56. The ability to use technology that provides protection against botnet threats.
57. Protection of network protocol vulnerabilities, which improves the detection of threats that exploit the shortcomings of network protocols such as SMB, RPC, RDP, etc.
58. Availability of implemented methods for detecting various attacks that try to exploit software vulnerabilities and providing more detailed information about CVE identifiers.
59. The ability to view automatically blocked network connections on a PC and, if necessary, temporarily allow specific secure network connections.

60. Additional personal firewall functionality that allows you to view a list of blocked IP addresses on your PC, provides information about the reasons for being blacklisted, and allows you to make exceptions for specific safe addresses.
61. Additional functionality of a personal firewall that can detect changes in network programs that have caused new unauthorized network connections.
62. Filtering of Internet traffic.
63. The presence of a web control module that allows you to restrict access to certain categories of sites.
64. 27 categories of Internet traffic filtering, in which more than 100 subcategories are distributed, as well as the ability to create groups of categories and subcategories.
65. Ability to create Internet traffic filtering rules for different users and groups of Windows or domain.
66. Ability to set time intervals, which allows you to customize web filtering rules more flexibly.
67. Regular update of virus databases at least 24 times a day.
68. Receiving client updates from local storage on the server, which allows you to keep anti-virus protection up-to-date in closed, isolated networks that do not have access to the Internet.
69. Ability to create an update mirror based on endpoint security solutions.
70. Ability to receive virus database updates from backup sources if the main source of updates is unavailable.
71. The ability for laptop computers to receive updates from the manufacturer's servers online when outside the corporate network.
72. Rollback of updates with the ability to revert to previous versions of virus signature databases and update modules, and the ability to temporarily suspend updates or install new ones manually.
73. Ability to update in the mode of receiving regular, test and delayed updates.
74. Monitoring, security assessment and response tools.
75. Availability of a mechanism for monitoring the security status and relevance of OS updates.
76. Availability of a system diagnostic tool that has the ability to create snapshots of the operating system state for further in-depth analysis of various aspects of the operating system, including running processes, registry content, installed software, network connections.
77. The ability to determine the criticality level (dangerous, unknown, little known, safe) of various operating system parameters in order to detect unauthorized and dangerous changes in the operating system.
78. The ability to compare different snapshots of the system state in order to identify changes that have occurred in the system over a certain period of time.
79. The ability to create and remotely execute scripts that will allow you to stop running processes and services on a remote PC, delete registry keys, and block network connections.
80. Local storage of logs on workstations.
81. The presence of a task scheduler that will allow you to create scheduled tasks, including: launching an external program, checking files at system startup, creating a snapshot of the system status, checking the computer, updating virus databases and program modules.

82. The ability to schedule tasks that will run once, periodically, and when specific events occur.
83. The ability to create several tasks of the same type in the scheduler with different frequency or different start conditions.
84. The ability to create a bootable disk on both CD and USB media with an installed antivirus product.
85. Ability to password protect the solution parameters to protect the endpoint.
86. Policy override mode, which allows the system administrator to temporarily change the antivirus software settings on the PC that are assigned by the policy and are not available for editing, in order to flexibly configure the antivirus software in a specific environment.
87. A graphical interface compatible with a high-resolution touch screen.
88. Ability to flexibly customize alerts and notifications about events on the user's desktop.
89. Possibility of remote installation on a client workstation.
90. Possibility of pre-installation on individual PCs or in a VDI image using a comprehensive installer, which will allow you to connect to the management server immediately after connecting to the network or launching in a VDI environment.
91. The ability to enable component updates in automatic mode, which makes it possible to download and install components without administrator or user intervention.
92. The ability to update components in manual mode, which makes it possible to update components on unmanaged workstations.
93. Ability to update some components without the need for a reboot to start functioning.
94. Support for programs running in full screen mode, with the ability to hide all messages from antivirus software.
95. The antivirus product should use its own technological developments, not borrowed ones, for the effective operation of all major modules and services. For example:
    - a detection kernel containing a variety of up-to-date detection methods,
    - cloud-based reputation service and timely detection system,
    - technology that reduces scanning time and OS load,
    - intelligent anti-spam kernel,
    - technology to reduce the use of virtual environment resources.
96. The ability to specify backup administration servers in addition to the main one.
97. Availability of a remote management tool.
98. Low consumption of PC resources by up-to-date antivirus products (all processes in total: graphical interface, comprehensive protection process, remote administration service): 50-100 MB of RAM, 2-35% of the CPU.
99. OS support: Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7, 8; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 and later: Android 5 (Lollipop) and later versions.
100. Support for Microsoft Windows 10 Multi-session and Azure virtualized Windows 10.

Server Protection

1. Automatic detection of server roles to create automatic exceptions for specific files, folders, programs, which minimizes the impact on the server operating system.
2. Providing protection against: malware, Trojan horses, keyloggers, adware, phishing, spyware, rootkits, scripts, potential unwanted and dangerous software.
3. Provide real-time protection.
4. Use of heuristic technologies during scanning.
5. Antivirus scanning at the request of the user or administrator and according to the schedule.
6. Hyper-V virus scanning, which allows you to scan Microsoft Hyper-V Server disks, i.e. virtual machines (VMs), without the need to install any agents on the corresponding virtual machines.
7. Microsoft Office Document Protection Module, which allows you to scan macros for malicious code.
8. Protection against exploits that provides protection against threats that can exploit vulnerabilities in Java, Flash and other applications
9. An additional level of user protection against ransomware monitors and evaluates all applications based on their behavior and reputation.
10. The ability to integrate workstation and server protection with a cloud sandbox (with an additional license), without the need to install additional software.
11. Scan the UEFI interface to check for malware in the master boot record.
12. Ability to scan files at the startup of the operating system.
13. Advanced memory scanner that monitors suspicious processes and scans them as soon as they occur, which helps prevent infection even with carefully encrypted and hidden threats.
14. Scan your computer when it is idle.
15. The ability to define detailed parameters of the anti-virus scanner, such as: defining objects and scanning methods, setting the maximum file size and scanning time, maximum archive attachment depth and creating exceptions.
16. Automatic anti-virus scanning of removable media.
17. A tool that can control the connection of peripheral devices to the workstation by creating access rules by device type, access level, manufacturer, model or serial number of the device. Rules can be created for all users, as well as for individual users or Windows groups.
18. The presence of an intrusion detection system (HIPS) that protects the computer from malicious programs and unwanted activity. This module also includes a wizard for creating rules and a rule editor for monitoring running processes, used files, and registry keys.
19. Additional check of running processes in the cloud reputation service.
20. Provide email client security on the workstation with the ability to integrate with the email client, check POP3, POP3S, SMTP, IMAP and IMAPS, and provide email attachment verification.
21. Ability to automatically delete or move infected mail to a specified directory in the mail client.

22. HTTP and HTTPS traffic scanning with the ability to create lists of excluded, blocked and allowed URLs.
23. Ability to block downloading files from the Internet by the specified extension.
24. Ability to check the SSL protocol and verify the validity and integrity of certificates. Ability to manage the lists of trusted certificates and certificates excluded from verification, as well as the ability to select an action when a certificate is determined to be invalid, uncertain or damaged.
25. Ability to create traffic inspection exceptions for individual programs and individual IP objects (IP addresses, IP address ranges, subnets).
26. The ability to configure additional parameters of the Intrusion Detection System (IDS) module to detect various types of possible network attacks on the computer.
27. Ability to use technology that provides protection against botnet threats.
28. Protection of network protocol vulnerabilities, which improves the detection of threats that exploit the flaws of network protocols such as SMB, RPC, RDP, etc.
29. Regular updating of virus databases at least 24 times a day.
30. Receiving client updates from a local mirror on the server.
31. Ability to create an update mirror using antivirus software.
32. Ability to receive updates of virus databases from backup sources if the main source of updates is unavailable.
33. Rollback of updates with the ability to revert to previous versions of virus signature databases and update modules, and the ability to temporarily pause updates or install new ones manually.
34. Ability to update in the mode of receiving regular, test and delayed updates.
35. Availability of a remote management tool.
36. Ability to specify backup administration servers in addition to the main one.
37. Availability of a mechanism for monitoring the relevance of operating system updates.
38. Availability of a system diagnostic tool that has the ability to create snapshots of the operating system state for further in-depth analysis of various aspects of the operating system, including running processes, registry content, installed software, network connections. Thanks to its ability to compare different snapshots of the system state, this tool can detect changes that have occurred in the system. It can also create and execute scripts, which will allow you to stop running processes, delete registry keys, and block network connections.
39. A task scheduler that allows you to create scheduled tasks, including: launching an external program, checking files at system startup, creating a system snapshot, scanning your computer, updating virus databases and program modules. You can schedule tasks that will run once, periodically, and when specific events occur.
40. The ability to create several tasks of the same type in the scheduler with different periodicity or different start conditions.
41. Ability to work in clusters of both domain and workgroup.
42. Ability to customize performance by specifying the number of scan threads.

43. Ability to customize the startup mode by disabling the graphical user interface for terminal users, which reduces the load on the server running in terminal server mode.
44. Ability to create a bootable disk on both CD and USB media with installed antivirus software.
45. Support for programs running in full-screen mode with the ability to hide all notifications from antivirus software.
46. Possibility of password protection from changing the settings and uninstalling the antivirus software.
47. Possibility of remote installation on a file server.
48. Possibility of pre-installation on individual file servers using a comprehensive installer, which will allow you to connect to the management server immediately after connecting to the network.
49. possibility of integration with Microsoft Azure cloud server.
50. OS support: Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12,SUSE Linux Enterprise Server (SLES) 15,Oracle Linux 8, Amazon Linux 2.

Mail Protection

1. Support for Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007, 2003.
2. Checking incoming and outgoing mail traffic at the transport protocol level.
3. Possibility of centralized management of antivirus protection of the entire network infrastructure.
4. The ability to build a hierarchical administration structure consisting of a master server and subordinate servers, which makes it possible to perform centralized management of antivirus protection of workstations, servers, and mobile devices belonging to both the main and regional divisions.
5. Inventory of equipment installed on workstations and servers running Windows, macOS, and Linux.
6. Inventory of software installed on workstations and servers running Windows, macOS and Linux.
7. Remotely install antivirus software for Windows, Linux, and Mac operating systems on multiple endpoints simultaneously.
8. Remote installation of custom software.
9. Ability to remotely uninstall installed user software.
10. Remote uninstallation of antivirus software for Windows, Linux and Mac operating systems.
11. The ability to perform additional network actions using the remote management tool, such as shutting down and rebooting, sending a computer wake-up signal, sending messages, executing specific command line instructions on the client computer, and starting an update of the client computer's operating system.
12. A tool for creating and editing installation packages for Windows, Linux, and Mac operating systems with preset configuration settings, which makes it possible to export installation packages for deploying full-fledged anti-virus protection on endpoints in an isolated network, as well as on endpoints that need protection but temporarily do not have a connection to the administration server.
13. The presence of a user manager that allows you to create different users of the administration server and assign them different access rights to individual sections, groups of computers on the administration server, which makes it possible to provide different access rights for regional system administrators of a branched anti-virus protection system.
14. Ability to authenticate console administrators using Active Directory security groups.
15. The ability to use two-factor authentication for administrator accounts, which makes it possible to prevent unauthorized connection to the centralized management server.
16. An audit log that records and tracks all configuration changes and all actions performed by users of the administration server.
17. The ability to remotely activate and deactivate security modules such as personal firewall, real-time protection, email client protection, Internet access protection, device control, web control, anti-spam on a single client.
18. Ability to create and edit static groups and the ability to import a computer tree from Active Directory.

19. Ability to configure automatic distribution of clients into dynamic groups according to many criteria, followed by the assignment of appropriate security policies, as well as the launch of the necessary tasks.
20. The ability to import users and groups from Active Directory, for further use to personalize device control rules and web control.
21. The ability to use both built-in and custom policies designed to continuously maintain the configuration settings of antivirus products. Ability to export/import policies.
22. The presence of a monitoring panel that provides all the necessary detailed information about the level of security protection of the infrastructure, the status of protected endpoints, as well as the status of the administration server itself.
23. Availability of about 100 pre-installed report templates that can be used both for the dashboard and for generating various reports.
24. The ability to create and edit report templates that are used both for the dashboard and for generating reports in PDF, CSV formats and further saving them to the specified path or sending them to the specified email.
25. The remote administration tool supports the following databases: MS SQL Server, MySQL.
26. Ability to export logs to syslog for further integration with SIEM.
27. Ability to customize log and report settings or choose from more than 50 templates for different systems/clients.
28. Ability to create a mirror of updates using an antivirus product, a special utility or a proxy server.
29. Ability to create an update mirror based on third-party HTTP servers.
30. Web-oriented interface that allows you to control the server through any browser using a certificate-protected connection.
31. The use of an independent agent that allows you to remotely manage the antivirus product on endpoints, as well as monitor the level of antivirus protection on workstations and the state of the operating system.
32. The ability to monitor all software installed on the workstation, as well as uninstall the installed software of your choice.
33. An additional component that allows you to manage antivirus protection on mobile devices.
34. A special component that detects unprotected workstations in the network for further deployment of antivirus protection.
35. Protecting connections between server components using both independently issued certificates and existing certificates.
36. A tool for managing license status (even without using the administration server.
37. The ability to deactivate the license of anti-virus products even on workstations to which there is no physical or remote access.
38. Ability to install the administration server on Windows and Linux
39. Delivery of the administration server in a deployed form, ready for use in such virtual environments as Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).

40. Support for virtualization systems such as VMware Horizon 8.x or Citrix XenCenter/XenServer 8+.
41. Ability to determine which virtual machine will be the source for copying or cloning in VDI systems.
42. Availability of a setup wizard to define detailed parameters for integration with VDI systems.
43. Ability to choose options for processing cloned computer identifiers, such as mapping to existing computers or creating new computers.
44. Ability to define VDI naming conventions for instant clones or machine directories.
45. Preset templates in the notification system to inform about incorrect identification of cloned machines, which makes it possible to notify about incorrectly configured integration with VDI systems.
46. Automatic updating of the management agent, which makes it possible to use the latest versions without the intervention of administrators.
47. Availability of a mechanism for distributing the automatic update process, which reduces the load on the network and computers in general.
48. Ability to install the management agent on ARM64 processors.
49. Availability of the functionality of creating sites in accordance with the company's branches, which allows you to assign a certain part of the license to individual branches.
50. Availability of the functionality of determining the administrator of a site or branch with the corresponding part of the license.

Protection Management

1. Possibility of centralized management of antivirus protection of the entire network infrastructure.
2. Inventory of equipment installed on workstations and servers running Windows, macOS, and Linux.
3. Inventory of software installed on workstations and servers running Windows, macOS and Linux.
4. Remote installation of antivirus software for Windows, Linux and Mac operating systems on multiple endpoints simultaneously.
5. Remote installation of custom software.
6. Ability to remotely uninstall installed user software.
7. Remote uninstallation of antivirus software for Windows, Linux and Mac operating systems.
8. The ability to perform additional network actions using the remote management tool, such as shutting down and rebooting, sending a computer wake-up signal, sending messages, executing specific command line instructions on the client computer, and starting an update of the client computer's operating system.
9. A tool for creating and editing installation packages for Windows, Linux, and Mac operating systems with preset configuration settings, which makes it possible to export installation packages for deploying full-fledged anti-virus protection on endpoints in an isolated network, as well as on endpoints that need protection but temporarily do not have a connection to the administration server.
10. The presence of a user manager that allows you to create different users of the administration server and assign them different access rights to individual sections, groups of computers on the administration server, which makes it possible to provide different access rights for regional system administrators of a branched anti-virus protection system.
11. Ability to authenticate console administrators using Active Directory security groups.
12. The ability to use two-factor authentication for administrator accounts, which makes it possible to prevent unauthorized connection to the centralized management server.
13. An audit log that records and tracks all configuration changes and all actions performed by users of the administration server.
14. The ability to remotely activate and deactivate security modules such as personal firewall, real-time protection, mail client protection, Internet access protection, device control, web control, anti-spam on a single client.
15. Ability to create and edit static groups and the ability to import a computer tree from Active Directory.
16. Ability to configure automatic distribution of clients into dynamic groups according to many criteria, followed by the assignment of appropriate security policies, as well as the launch of the necessary tasks.
17. The ability to import users and groups from Active Directory, for further use to personalize device control rules and web control.

18. The ability to use both built-in and custom policies designed to continuously maintain the configuration settings of antivirus products. Ability to export/import policies.
19. The presence of a monitoring panel that provides all the necessary detailed information about the level of security protection of the infrastructure, the status of protected endpoints, as well as the status of the administration server itself.
20. About 100 pre-installed report templates that can be used both for the dashboard and for generating various reports.
21. The ability to create and edit report templates that are used both for the dashboard and for generating reports in PDF, CSV formats and further saving them to the specified path or sending them to the specified e-mail.
22. Ability to customize log and report parameters or choose from more than 50 templates for different systems/clients.
23. Ability to create a mirror of updates using an antivirus product, a special utility or a proxy server.
24. Ability to create an update mirror based on third-party HTTP servers.
25. Web-oriented interface that allows you to control the server through any browser using a certificate-protected connection.
26. The use of an independent agent that allows you to remotely manage the antivirus product on endpoints, as well as monitor the level of antivirus protection on workstations and the state of the operating system.
27. The ability to track all software installed on the workstation and uninstall installed software of your choice.
28. An additional component that allows you to manage antivirus protection on mobile devices
29. A special component that detects unprotected workstations in the network for further deployment of antivirus protection.
30. Protection of connections between server components using both independently issued certificates and existing certificates.
31. A tool for managing the status of licenses (even without using the administration server.
32. The ability to deactivate the license of anti-virus products even on workstations to which there is no physical or remote access
33. Support for virtualization systems such as VMware Horizon 8.x or Citrix XenCenter/XenServer 8+.
34. Ability to determine which virtual machine will be the source for copying or cloning in VDI systems.
35. Availability of a configuration wizard to define detailed parameters for integration with VDI systems
36. Ability to choose options for processing cloned computer identifiers, such as mapping to existing computers or creating new computers.
37. Ability to define VDI naming conventions for instant clones or machine catalogs.

38. Preset templates in the notification system to inform about incorrect identification of cloned machines, which makes it possible to notify about incorrectly configured integration with VDI systems.
39. Automatic updating of the management agent, which makes it possible to use the latest versions without the intervention of administrators.
40. The presence of a mechanism for distributing the automatic update process, which reduces the load on the network and computers in general.
41. Ability to install the management agent on ARM64 processors.
42. Availability of the functionality of creating sites in accordance with the company's branches, which allows you to assign a certain part of the license to individual branches.
43. Availability of the functionality of determining the administrator of a site or branch with the corresponding part of the license.

About ESET company

ESET is a leading European cybersecurity company, protecting millions of customers and hundreds of thousands of enterprises worldwide with innovative antivirus and internet security solutions, an expert in the development of cyberthreat detection technologies.

The main mission of the company is to provide a safe IT environment for everyone with the help of innovative technologies and quality products. The ESET product portfolio includes security solutions for computers, laptops and mobile devices, file and mail servers, cloud applications, products for two-factor authentication, encryption, data leak prevention, network traffic analysis, and additional protection tools and services.

Founded in 1992 by Slovak programmers, the ESET company today has an extensive partner network and offices in more than 180 countries around the world. The main office of the company is located in Bratislava, Slovakia. The leading positions of ESET in the market are confirmed by the ratings of leading research companies, such as Kuppinger Cole, Radicati, Forrester Wave, Canalys, and Gartner.

Today the high quality of ESET products is recognized by more than 100 million users worldwide, independent experts and authoritative publications (AV-Test, AV-Comparatives, SE Labs and others). ESET solutions are used by major international companies and organizations. More detailed information about the ESET company and products is available on the official website: https://www.eset.com/md-ru.

Digital Security
Progress. Protected.