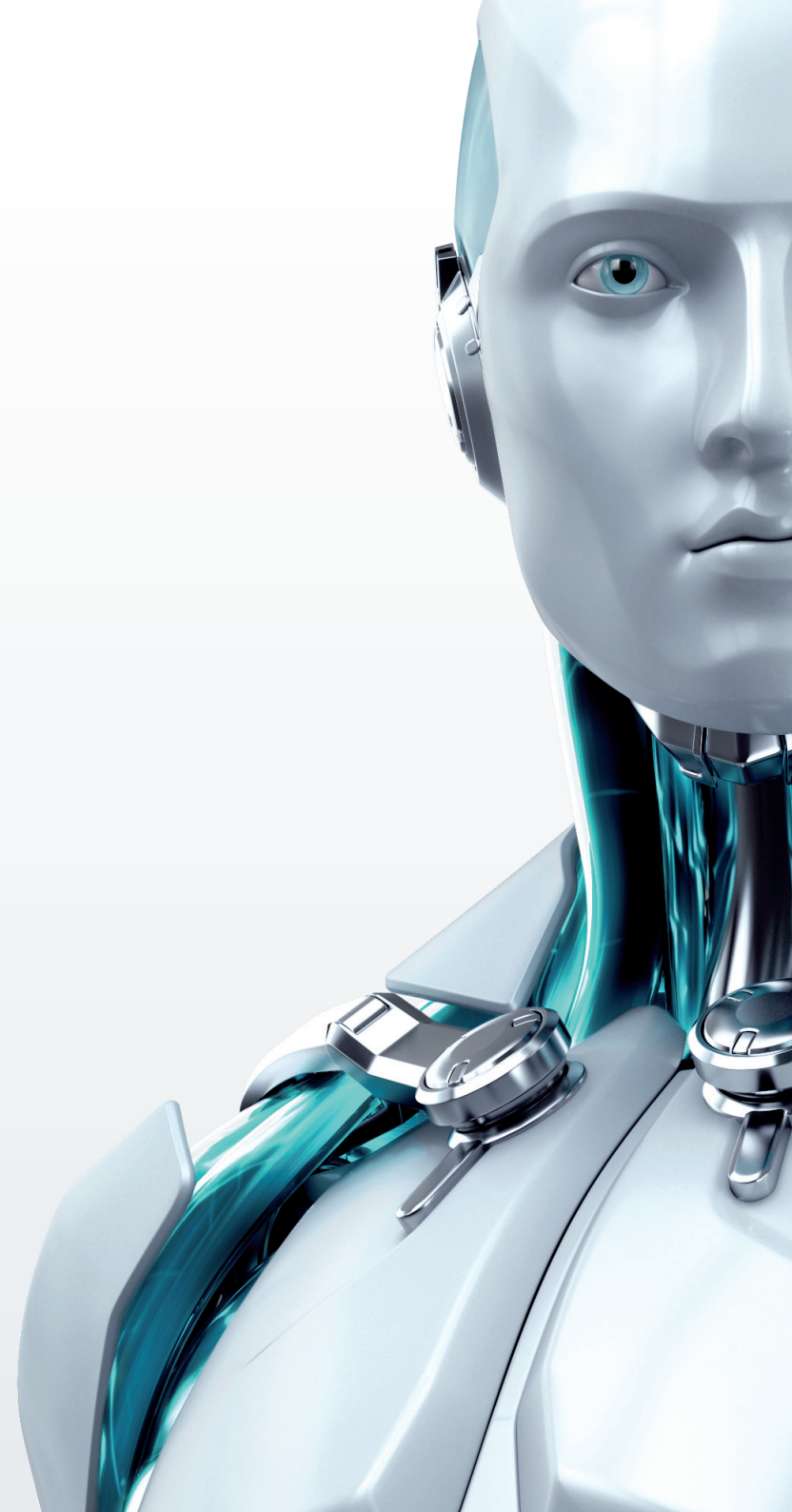


# ESET **ENDPOINT SOLUTIONS**

Features  
Business Perspective



[www.eset.com](http://www.eset.com)



## Endpoint Protection

| FEATURE  | WHAT IT DOES   | WHAT'S THE BENEFIT  |
|--|--|---|
| <b>Antivirus / Antispyware</b>                       | Eliminates all types of threats, including viruses, rootkits, worms and spyware<br><b>Optional cloud-powered scanning:</b><br>Whitelisting of safe files based on file reputation database in the cloud<br>Only information about executable and archive files sent to the cloud | Keep company data safe and prevent malware from infecting endpoints, no matter what operating system they target. Cloud-powered file reputation speeds up system scans and keeps false positives to an absolute minimum, while preserving confidentiality of your data. |
| <b>Auto-Scan of Removable Media</b>                  | Allows you to scan devices and media for malware immediately upon insertion<br>Scanning options include: start automatically/notify (prompt user)/do not scan  | Automatically scan USBs, CDs, and DVDs upon insertion to eliminate autorun and other removable media.   |
| <b>Host-based Intrusion Prevention System (HIPS)</b> | Enables you to define rules for system registry, processes, applications and files<br>Provides tampering protection<br>Detects threats based on system behavior  | Company endpoints are always safe as our HIPS behavioral scanner protects ESET security solutions against tampering. Critical system registry entries, processes, applications and files are protected from unauthorized access and changes.                            |
| ★ <b>Client Antispam</b>                             | Effectively filters out spam on the user's endpoint device<br>Scans all incoming emails for malware  | Automatically filter unwanted email to increase employee work efficiency and reduce the risk of phishing attacks. Customize settings by user type to meet your business' email communication requirements.  |
| <b>Cross-platform Protection</b>                     | Detects and eliminates malware targeting Windows, Mac and Linux operating systems  | Exchange files and email attachments between Windows, Mac and Linux endpoints knowing that malware targeting any of these platforms will be automatically detected and eliminated.  |
| <b>ESET SysRescue</b>                                | Allows you to create an automatically bootable OS image with installed security solution to clean deeply infected endpoints  | Boot and clean infected endpoints from CD or USB and increase the chance of data retrieval when no other options exist.   |

★ Features marked with an asterisk are available only for ESET Endpoint Security; all other listed features are available also for ESET Endpoint Antivirus.

## Data Access Control

| FEATURE                            | WHAT IT DOES  | WHAT'S THE BENEFIT  |
|------------------------------------|---|---|
| ★ <b>Two-way Firewall</b>          | Prevents unauthorized access to company network<br>Provides anti-hacker protection and data exposure prevention                       | Keep company data safe from foreign interference and protect your company's proprietary information from leaking through unauthorized unbound connections.  |
| <b>Device Control</b>              | Blocks unauthorized media and devices from the system<br>Lets you set rules/parameters for specific media, devices, users and clients | Prevent company data from unauthorized copying to USB, CD, DVD or other removable media. Flexible device control policies allow for access control by individual users or groups based on device parameters like serial number, manufacture ID, model and others. |
| ★ <b>Trusted Network Detection</b> | Provides stricter protection when clients connect to new/unauthorized network   | Maintain the confidentiality of company data as your mobile workforce hops from trusted networks to public hotspots at a café, airport or hotel. Prevent unauthorized persons "listening in" to company communication.  |

## Employee Effectiveness

| FEATURE                               | WHAT IT DOES  | WHAT'S THE BENEFIT   |
|---------------------------------------|---|--|
| ★ <b>Web Control</b>                  | Limits website access by category<br>Enables you to create rules for user groups to comply with your company policies   | Prevent unproductive web surfing and enforce your company's acceptable Internet use policy by blocking access to unauthorized web sites or categories. Keep employees off inappropriate, unwanted or non-work-related pages like social networks or freemail to prevent overloading the network. |
| <b>Low System Demands</b>             | Delivers proven protection while leaving more system resources for programs you regularly use   | Improve ROI by keeping company computers running smoothly and extending the lifetime of hardware. Increase employee effectiveness by not having to worry about computer slowdowns due to a bloated antivirus solution.   |
| <b>Presentation Mode</b>              | Blocks pop-up messages and postpones security tasks when in full-screen mode  | Prevent embarrassing moments or disruptions during slideshows, presentations or during any other full-screen applications.   |
| ★ <b>Component-based Installation</b> | Gives you the option to install any and all of the following security components: firewall, antispam, web control, device control, Microsoft NAP support, and web access protection | Extend hardware lifecycles and save money by minimizing CPU overheads and conserving memory and disk space used by the security solution.  |

★ Features marked with an asterisk are available only for ESET Endpoint Security; all other listed features are available also for ESET Endpoint Antivirus.

## Administrator Effectiveness

| FEATURE                       | WHAT IT DOES  | WHAT'S THE BENEFIT   |
|-------------------------------|---|--|
| <b>Centralized Management</b> | Lets you manage all ESET security solutions software from a central management tool   | Keep IT budgets under control - with ESET Remote Administrator for management of past, present and future ESET solutions. Easily manage all endpoints, servers, smartphones and even virtual machines from a single console, no matter if you are running Windows, Mac or Linux systems. |
| <b>Role-based Management</b>  | Assigns different privileges to different ESET Remote Administrator users<br>Audit users with ESET Remote Administrator<br>Enforce password complexity  | Role based administration makes it easy for your IT team to delegate responsibilities among different individuals or groups. Detailed audit logs simplify compliance reporting.  |
| <b>Dynamic Client Groups</b>  | Enables you to create static and dynamic clients groups and using different parameters for populating the groups  | The security rules are easily adjustable for different groups of employees. Dynamic groups can be created on-the-fly based on specified conditions to simplify identification and remediation of endpoints that trigger security events.   |
| <b>Event Notifications</b>    | Allows you to specify log and report parameters or choose from more than 50 templates available for different system/client events<br>Gives you the option to set threshold for event notifications   | Save your IT team's time by prioritizing notifications and setting up what type security event is important, how detailed it should be and in what interval it should be reported, so they get actionable information without being overloaded.  |
| <b>Remote Installation</b>    | Performs remote installation of ESET software to multiple endpoints at once   | Have your IT manage endpoint security with a few clicks by deploying ESET security software on all endpoints from one central location.  |
| <b>Export/Import Policies</b> | Enables you to import/export/edit policies in XML   | Save time and prevent errors by defining the configuration settings once, and then exporting and applying them to desired endpoints or groups.   |
| <b>Remote Module Switch</b>   | Remotely activates or deactivates protection modules installed on a given client, including firewall, anti-stealth, real-time file system protection, web-access and e-mail client protection<br><br>Automatic re-activation can be set for: 10 min, 30 min, 1 hour, 4 hours or never | Reduce potential downtimes during system maintenance by remotely enabling and disabling security modules.  |

## Reporting

| FEATURE                        | WHAT IT DOES  | WHAT'S THE BENEFIT   |
|--------------------------------|---|--|
| <b>Real-time Web Dashboard</b> | Ensures complete oversight of the company network and lets you check the security status from anywhere  | Oversee the security status of the entire network with real-time information about the server load and security. You can access critical information from outside the company network via web-based dashboard. |
| <b>Multiple Log Formats</b>    | Lets you save logs in common formats - CSV, plain text, Windows event log - readable by SIEM tools<br>Stores logs on endpoint side for later harvesting | Take advantage of data mining functions, making correlations of security events easy and quick. Make the data readable to 3rd party Security Information and Event Management (SIEM) tools.                    |
| <b>Device Control Reports</b>  | Device Control Reports deliver comprehensive logs and reports for all device-related events   | Monitor the usage of removable media and devices across the entire company, keeping all important information in one place.  |
| <b>RSA enVision Support</b>    | Integrates with the RSA enVision SIEM tool via a plug-in  | Support for RSA enVision ensures ease of integration with this popular 3rd party SIEM tool.  |
| <b>ESET SysInspector</b>       | Performs in-depth analysis of endpoint systems to identify possible security risks  | Give your IT admins all the tools to easily find potential security risks and take preventive actions proactively.   |

## Update Management

| FEATURE                          | WHAT IT DOES  | WHAT'S THE BENEFIT  |
|----------------------------------|---|---|
| <b>Randomized Task Execution</b> | Enables you to set random time periods for executing scheduled security tasks   | Prevent system slowdowns due to delayed response from servers or AV storms on virtual endpoints. This feature ensures that simultaneously scheduled security tasks will not cause network slowdowns or negatively impact its traffic.         |
| <b>Update Rollback</b>           | Lets you revert to a previous version of protection modules and virus signature database  | Address incompatibilities or other system disruptions by rolling back virus signature and module updates with a few simple clicks.  |
| <b>Postponed Updates</b>         | Provides an option to download from 3 specialized update servers: pre-release (beta users), regular release (regular users) and postponed release (approx. 12 hours after regular release)                          | Keep the company online systems working smoothly 24/7. Prevent outages of critical systems due to antivirus updates or any events that could impact the company's operations.   |
| <b>Local Update Server</b>       | Saves company bandwidth by downloading updates only once to a local mirror server<br><br>Secured (HTTPS) communication channel is supported   | Keep the connection available for work-related online services, by keeping the antivirus updates traffic to a minimum.  |
| <b>Faster Database Access</b>    | Provides an optimized and streamlined database access to endpoint security-related data   | Quick database response means faster reporting and data aggregation across your endpoints, increasing IT productivity.  |
| <b>Database Cleanup</b>          | Allows you to set database storage attributes such as time period and threshold values for entries to be kept in database   | Store only security logs that are important and up-to-date, ensuring a tidy database, without unnecessary server slowdowns.   |
| <b>Microsoft NAP Support</b>     | Deploys server side System Health Validator (SHV) plug-in and client side System Health Agent (SHA)<br><br>Grants full network access for compliant clients and limited/no network access for non-compliant clients | Control access to network resources based on a client computer's identity and compliance with corporate governance policy. Microsoft Network Access Protection (NAP) plug-in allows full integration with your company's compliance policies. |