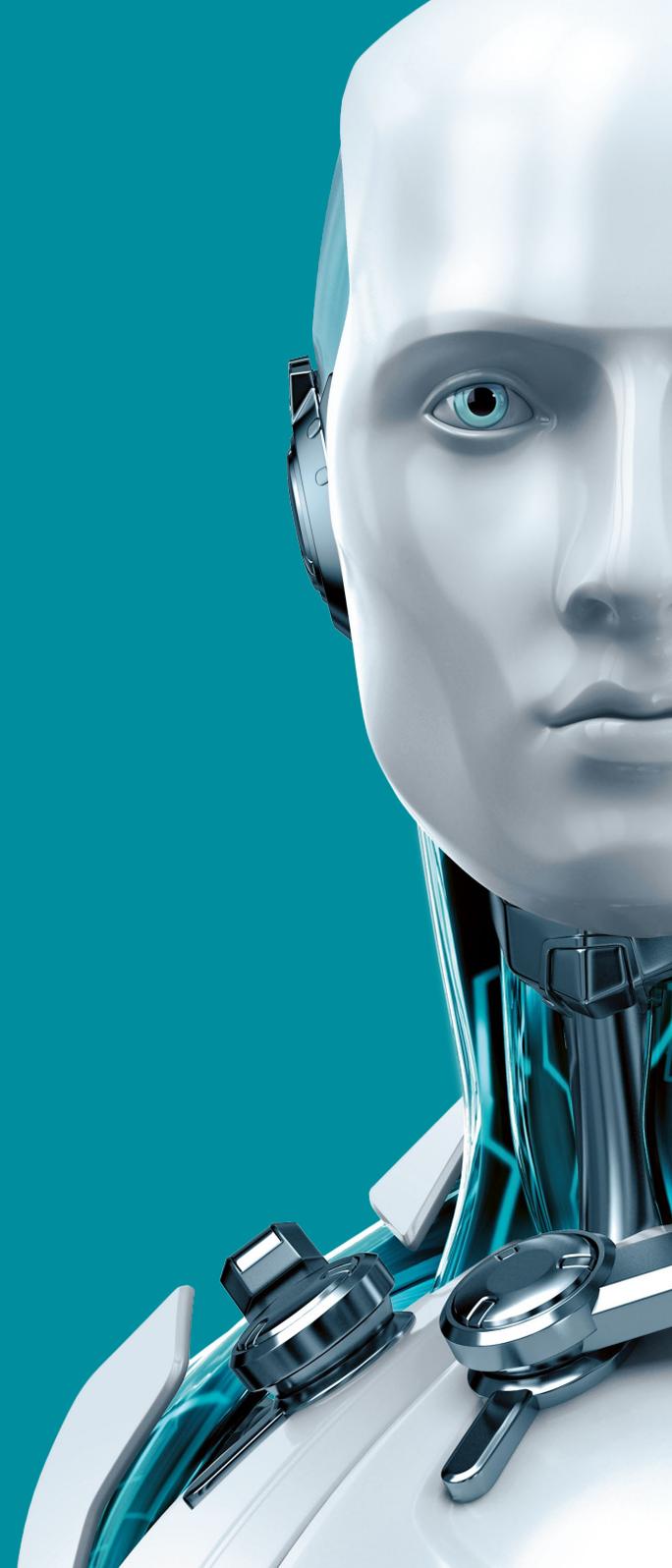# ESET®

ENDPOINT SECURITY

FOR WINDOWS

BUSINESS

ENJOY SAFER TECHNOLOGY™

ESET

ENDPOINT SECURITY
FOR WINDOWS

ESET Endpoint Security delivers comprehensive IT security for your business via multiple layers of protection, including our field-proven ESET NOD32® detection technology, complete data access protection and fully adjustable scanning and update options. Our multi-layered technology blocks ransomware attacks even before it reaches victim's computers.

Keep your system running at its best thanks to low system demands, virtualization support and optional cloud-powered scanning.

And oversee it all effortlessly with our completely redesigned, user-friendly remote administrator tool.

Endpoint Protection

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware **Optional cloud-powered scanning:** Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data are not personally attributable.
Virtualization Support	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so identical files are not scanned again, resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, so these don't have to be downloaded every time a virtual machine is reverted to default snapshot.
Host-Based Intrusion Prevention System (HIPS)	Enables you to define rules for system registry, processes, applications and files. Provides anti-tamper protection and detects threats based on system behavior.
Exploit Blocker	Strengthens security of applications such as web browsers, PDF readers, email clients or MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks that could be used by crypto-ransomware to enter the targeted system.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention, even from heavily obfuscated malware, often detecting crypto-ransomware prior to it encrypting valuable files.
Client Antispam	Effectively filters out spam and scans all incoming emails for malware. Native support for Microsoft Outlook (POP3, IMAP, MAPI).
Cross-Platform Protection	ESET security solutions for Windows are capable of detecting Mac OS threats and vice-versa, delivering better protection in multi-platform environments.

Ransomware protection with ESET's multi-layered technology

ESET's technology stops ransomware on network layer so it blocked before it reaches the computers, monitors running applications and uncovers the true nature of heavily obfuscated processes. Metadata from each of these layers can be sent to our ESET LiveGrid® cloud systems, providing further intelligence to our machine learning algorithms. These automated systems, in combination with the expertise of our researchers and engineers, enable us to prevent ransomware threats before they strike.

Data Access Protection

Web Control	Limits website access by category, e.g. gaming, social networking, shopping and others. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that the website is blocked giving him an option to access the website, with activity logged.
Anti-Phishing	Protects end users from attempts by fake websites to acquire sensitive information such as usernames, passwords or banking and credit card details.
Two-Way Firewall	Prevents unauthorized access to your company network. Provides anti-hacker protection and data exposure prevention. Lets you define trusted networks, making all other connections, such as to public Wi-Fi, in 'strict' mode by default. Troubleshooting wizard guides you through a set of questions, identifying problematic rules, or allowing you to create new ones.
Vulnerability Shield	Improves detection of Common Vulnerabilities and Exposures (CVEs) on widely used protocols such as SMB, RPC and RDP. Protects against vulnerabilities for which a patch has not yet been released or deployed.
Botnet Protection	Protects against infiltration by botnet malware – preventing spam and network attacks launched from the endpoint.
Device Control	Blocks unauthorized devices (CDs/DVDs and USBs) from your system. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that his device is blocked and gives him the option to access the device, with activity logged.

Scanning and Update Options

Idle-State Scanner	Aids system performance by performing a full scan proactively when the computer is not in use. Helps speed up subsequent scans by populating the local cache.
First Scan after Installation	Provides the option to automatically run low priority on-demand scan 20 minutes after installation, assuring protection from the outset.
Update Rollback	Lets you revert to a previous version of protection modules and virus signature database. Allows you to freeze updates as desired - opt for temporary rollback or delay until manually changed.
Postponed Updates	Provides the option to download from three specialized update servers: pre-release (beta users), regular release (recommended for non-critical systems) and postponed release (recommended for company-critical systems – approximately 12 hours after regular release).
Local Update Server	Saves company bandwidth by downloading updates only once, to a local mirror server. Mobile workforce updates directly from ESET Update Server when the local mirror is not available. Secured (HTTPS) communication channel is supported.

FREE LOCAL TECHNICAL SUPPORT

Do More with the help of our specialists. On call to provide technical support when you need it, in your language.

Usability

RIP & Replace	Other security software is detected and uninstalled during installation of ESET Endpoint solutions. Supports both 32 and 64-bit systems.
Customizable GUI Visibility	Visibility of Graphical User Interface (GUI) to end user can be set to: Full, Minimal, Manual or Silent. Presence of ESET solution can be made completely invisible to end user, including no tray icon or notification windows. By hiding the GUI completely, the "egui.exe" process does not run at all, resulting in even lower system resource consumption by the ESET solution.
ESET License Administrator	Makes it possible to handle all licenses transparently, from one place via web browser. You can merge, delegate and manage all licenses centrally in real-time, even if you are not using ESET Remote Administrator.
Touchscreen Support	Supports touch screens and high-resolution displays. More padding for and complete rearrangement of GUI elements. Basic frequently used actions accessible from tray menu.
Low System Demands	Delivers proven protection while leaving more system resources for programs that end users regularly run. Can be deployed on older machines without the need for an upgrade, thereby extending hardware lifetime. Conserves battery life for laptops that are away from the office, using battery mode.
Right-to-Left Language Support	Native right-to-left language support (e.g. for Arabic) for optimum usability.
Remote Management	ESET Endpoint solutions are fully manageable via ESET Remote Administrator. Deploy, run tasks, set up policies, collect logs, and get notifications and an overall security overview of your network – all via a single web-based management console.