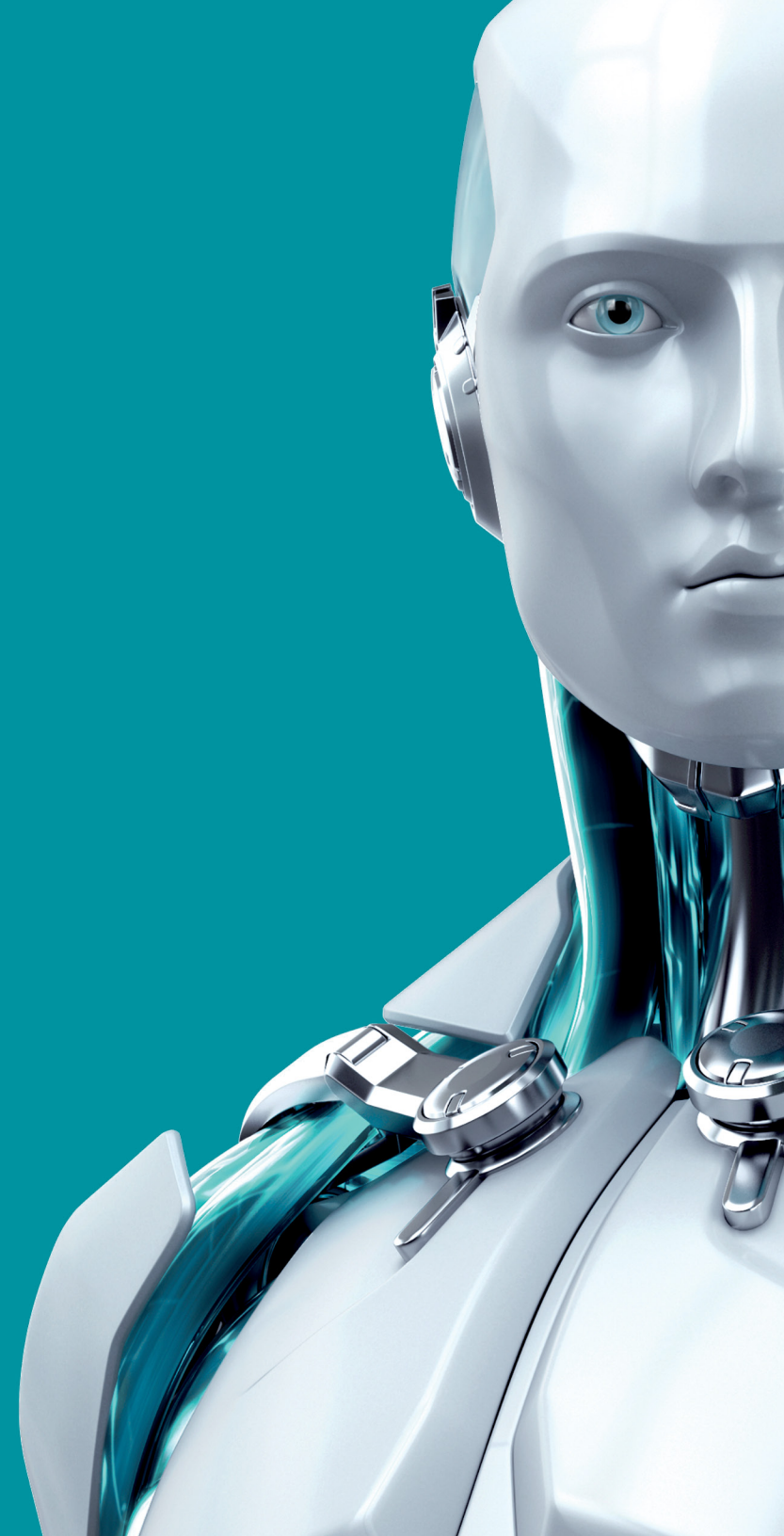# ESET®

FILE SECURITY

FOR MICROSOFT™ WINDOWS SERVER

ENJOY SAFER TECHNOLOGY®

ESET

FILE SECURITY
FOR MICROSOFT WINDOWS SERVER

ESET File Security for Microsoft Windows® Server provides superior protection for your company's data passing through the file server.

The solution utilizes the proven ESET NOD32® scanning engine at its core and combines high detection speed, smooth performance and stability to ensure a continuously high level of security.

Maintain more memory and CPU power for critical system tasks thanks to the solution's minimal resource usage. Stay on top of server security with detailed and comprehensive security logs, vital protection status information and system notifications.

File server 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 is 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.
Hyper-V storage scan	Agentless scanning for malware on Hyper-V based virtual servers; scans offline virtual server disks to save system resources.
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.
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.
Native Clustering support	Allows you to configure the solution to automatically replicate settings when installed in a cluster environment. An intuitive wizard makes it easy to interconnect several installed nodes of ESET File Security within a cluster and manage them as one, eliminating the need to replicate changes in configuration manually to other nodes in the cluster.
Storage scan	Allows you to easily set up on-demand scans of connected Network Attached Storage (NAS).
	Combined with ESET Shared Local Cache installed within the network, this can drastically reduce the amount of disk input/output operations on network drives.
Specialized cleaners	Provides most relevant critical malware standalone cleaners within the product interface for malware that cannot be removed by the regular cleaner.
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.

Data access protection

Anti-phishing	Protects you from attempts by fake websites to acquire sensitive information.
Device control	Blocks unauthorized portable devices from connecting to the server.
	Enables you to create rules for user groups to comply with your company policies.
	Soft blocking—notifies the end user that that the device is blocked and gives user the option of accessing 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.
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.

Usability

Process exclusions	The admin can define processes which are ignored by the real-time protection module—all file operations that can be attributed to these privileged processes are considered to be safe. This is especially useful for processes that often interfere with real-time protection, like backup or live virtual machine migration. Excluded process can access even unsafe files or objects without triggering an alert.
Windows management instrumentation (WMI) provider	Allows you to monitor key functionalities of ESET File Security via Windows Management Instrumentation framework. This allows integration of ESET File Server into 3rd party management and SIEM software, such as Microsoft System Center Operations Manager, Nagios and others.
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.
Component-based installation	Allows you to choose which components to install: —Real-Time File System Protection —Web Protocol Filtering —Device Control —Graphical User Interface (GUI) —E-mail Client Protection —ESET Log Collector —ESET SysInspector —ESET SysRescue —Offline Help
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.
ESET log collector	A simple tool that collects all logs relevant for troubleshooting, assisted by ESET's technical support, and bundles them into a single archive that can be sent via email or uploaded to a shared network drive to speed up the troubleshooting process.