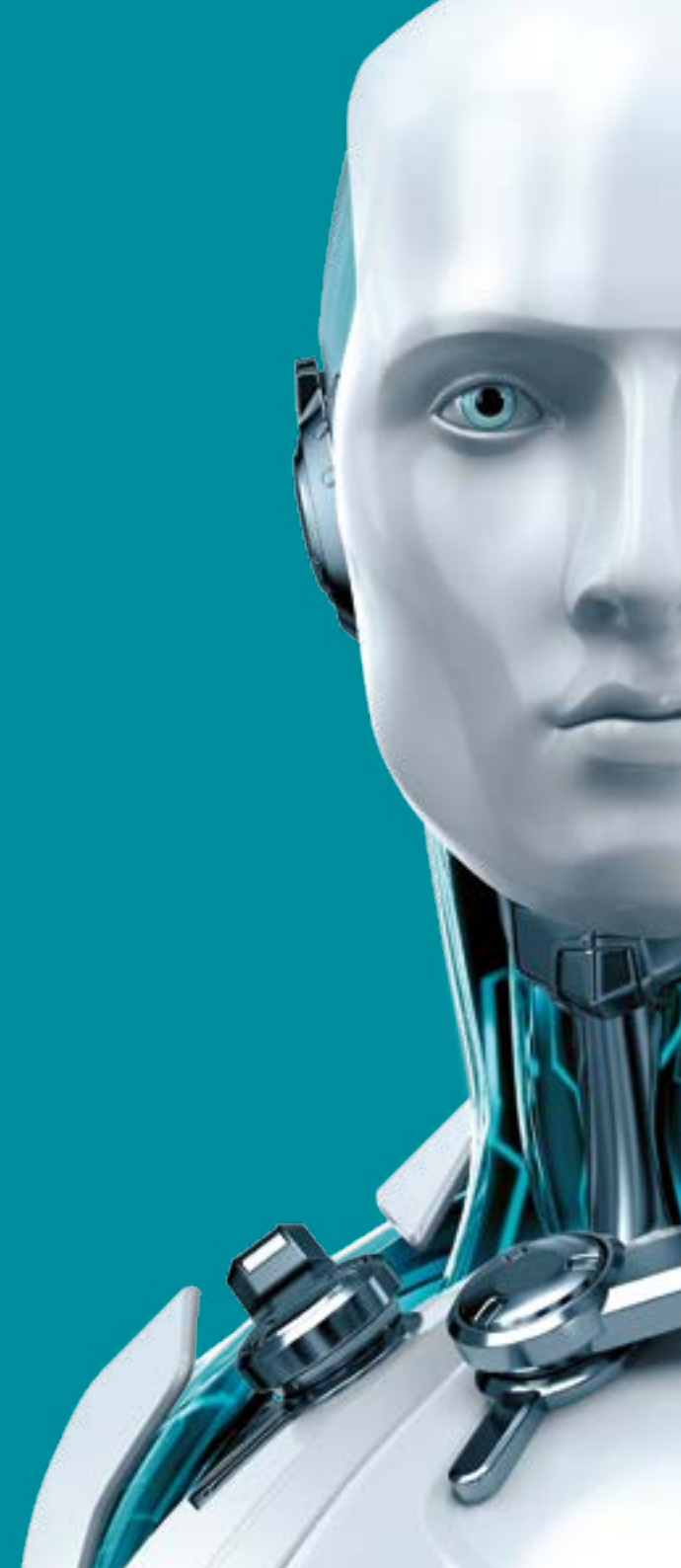
ENDPOINT ENCRYPTION

BUSINESS

ENJOY SAFER TECHNOLOGY™



ENDPOINT ENCRYPTION

ESET Endpoint Encryption is a simple-to-use encryption for companies large and small. Take advantage of the optimized setup that speeds up the time to adoption for admins. The client side requires no user interaction, increasing user compliance and the security of your company data.

Client side

Data is a critical part of every organization, but this most valuable asset often poses a huge risk when it travels or is transmitted beyond the corporate network. Full disk and removable media encryption protect laptop computers against the unexpected. File, folder and email encryption allow fully secure collaboration across complex workgroups and team boundaries, with security policy enforced at all endpoints via remote central management. Meet your data security compliance obligations with a single MSI package.

Zero User Interaction	The implementation of encryption is completely transparent for the users and requires no action on their part.
Full Disk Encryption	Encrypt only disks and partitions you want
	On-screen keyboard which allows encrypting of Windows tablets and convertible devices
	Transparent pre-boot security using FIPS 140-2 validated, 256 bit AES Encryption
	Encryption may be started and managed remotely
	Remote user-password recovery
	Enhanced workstation screening prior encryption, including Safe Start mode
	Fully compatible with Microsoft Windows 10, 8 and 8.1, with support for UEFI and GPT
	Support of Trusted Platform Module (TPM)
Removable Media Encryption	No extra space is reserved for encrypted content and the whole device capacity can be used by user
	Policy driven encryption includes "Go" portable encryption, on-device software for use on unlicensed systems
	Works with any USB drive, CD & DVD media
File & Folder Encryption	Encrypt only files and folders you want
	All files moved to encrypted folder are encrypted immediately
Email Encryption	Transparent email encryption for Outlook through a dedicated plugin
	The email can be decrypted only by recipients who share the same key as sender
	Text and clipboard encryption works with any e-mail client, including webmail

Desktop	Essential Edition	Standard Edition	Pro
Full Disk Encryption	-	-	✓
Removable Media Encryption	-	✓	✓
"Go" Portable Encryption	-	✓	✓
File & Folder Encryption	✓	✓	✓
Email Encryption	✓	✓	✓
Text & Clipboard Encryption	✓	✓	✓
Virtual Disks & Encrypted Archives	✓	✓	✓
Centralised Management Compatible	✓	✓	✓

A single install serves all licence types. Upgrading is silent and automatic for managed users, unmanaged users simply enter an activation code.

Mobile	Unmanaged Mode	Managed Mode
File Encryption	✓	✓
Email Encryption	✓	✓
Text & Clipboard Encryption	✓	✓
Encryption using Passwords	✓	✓
Encryption using Encryption Keys	-	✓

System Requirements

Client & Server Side
Microsoft® Windows® 10
Microsoft® Windows® 8, 8.1*
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® XP SP 3
Microsoft® Windows® Server 2003 – 2012

* Microsoft Windows RT is not supported;
Full Disk Encryption requires keyboard

Mobile Platforms
iOS

Certifications:
FIPS 140-2 level 1

Algorithms & standards:
AES 256 bit
AES 128 bit
SHA 256 bit
SHA1 160 bit
RSA 1024 bit
Triple DES 112 bit
Blowfish 128 bit

Server side

The Enterprise Server can manage users and workstations together or independently. Activation, and changes to security policy, software feature-set, encryption keys and endpoint status are all handled securely through the cloud, keeping your most high-risk endpoints under close control at all times.
Only **ESET Endpoint Encryption** offers full control wherever your users are.

Remote Central Management	Manage any user or workstation with a standard internet connection
	All commands, updates, status requests and responses posted via the Enterprise Proxy
	No dependency on Active Directory or any existing server architecture installation
	Secure connectivity allows control of endpoint encryption keys, security policy and software features beyond the corporate security boundary
	Full remote management, creation and removal of user accounts
Encryption Key Management	Patented technology
	Add or remove any or all encryption keys
	Change the encryption policy remotely and silently, without user interaction
Enterprise Server Proxy	By using the Enterprise Proxy as an intermediary, all connections from client and server are outgoing.
	All information is encrypted with either RSA or AES and the connection itself is SSL encrypted
	No need for own SSL certificate and additional hardware, network or firewall changes