



ENDPOINT ENCRYPTION

Simple and powerful encryption
for organizations of all sizes

CYBERSECURITY
EXPERTS ON YOUR SIDE

The ESET difference

MANAGE DEVICES ANYWHERE

ESET Endpoint Encryption can manage devices anywhere in the world without requiring VPNs or any firewall exceptions. Management is handled by utilizing HTTPS internet connectivity via a proxy. This eliminates the need for risky incoming connections, making management of encryption safe and simple for businesses of all sizes. All client and server connections are SSL encrypted, and all commands and data are end-to-end AES or RSA encrypted.

ZERO IMPACT ON PRODUCTIVITY

The implementation of encryption is completely transparent for the users and requires no action on their part, increasing their compliance. No extra overhead is created for either IT departments or users, and there's no need for user training.

UNIQUE ENCRYPTION KEY SYSTEM

Using centrally managed, shared encryption keys avoids problems encountered by encryption solutions, which typically use either shared passwords or public keys. The system used by ESET Endpoint Encryption mirrors the way that physical keys are used to lock our houses, apartments, cars, etc. Staff already understand this concept, and it only needs explaining once. Coupled with a premium remote-management system, shared encryption keys are both highly secure and practical.

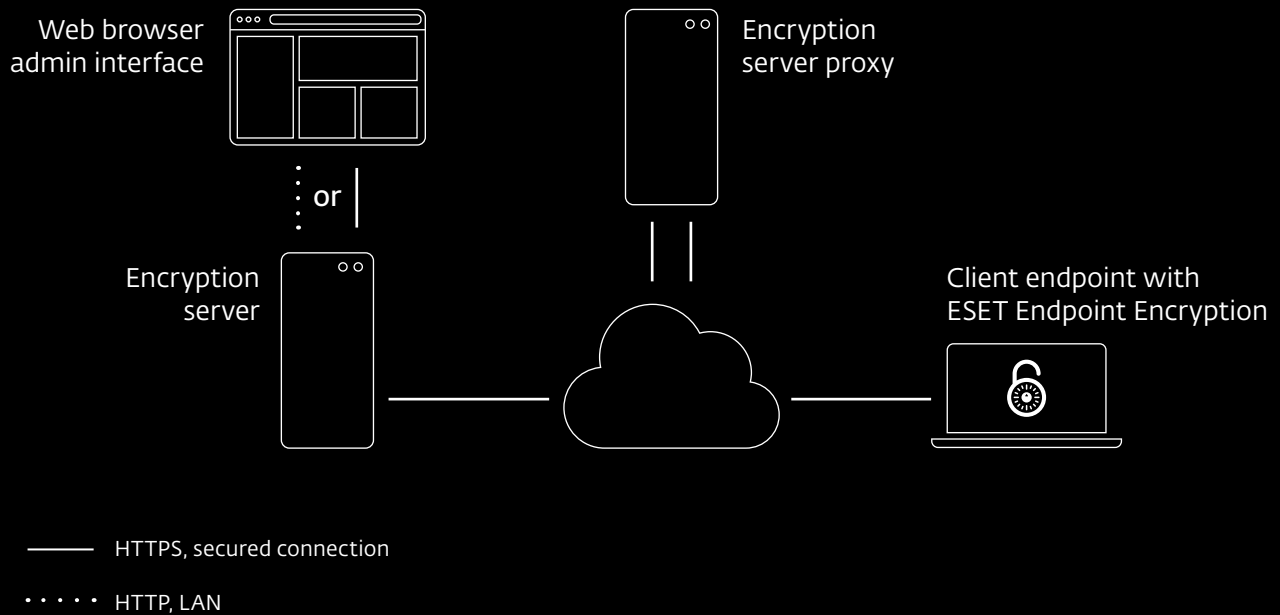
USER-PROOF REMOVABLE MEDIA

Management of removable media devices in a secure environment can sometimes be a hassle. ESET Endpoint Encryption protects drives of all sizes in seconds, creating an encrypted space which grows and shrinks as required. This means that any writable device is safe to use, user-owned devices are not locked for their private use, and whitelisting is not necessary. In addition, no shared passwords are required, which keeps it extremely simple for end-users and trouble-free for administrators.

REMOTELY DISABLE DEVICES

More companies are moving to a mobile workforce where employees not only work at airports or at home but also at coffee shops. Due to this, businesses need peace of mind and the ability to remotely disable or lock out devices in case the device is lost or stolen. ESET Endpoint Encryption provides a simple way to do this without the use of open, incoming Firewall ports, VPN access and critically, without any user interaction. If connected to a WiFi network, the laptop can have encryption keys wiped and be locked from the Windows login screen, with status reported back silently.

The shared encryption key system used by ESET Endpoint Encryption mirrors the way that physical keys are used to lock our houses, apartments, cars, etc. Staff already understand this concept, and it only needs explaining once.



The management of endpoints via server proxy requires no incoming connections, making it extremely safe and easy to set up. No firewall exclusions or open ports are required.

The encryption server can run on any Windows PC or server. All communication between the Encryption server and client endpoints is encrypted with 256bit AES or RSA 1024 meaning that the Encryption server proxy only holds transient, encrypted data packets with an anonymized index and no encryption keys.

Server installation of ESET Endpoint Encryption usually takes less than 10 minutes.

Complete setup of the solution typically lasts less than an hour. This significantly speeds up the time for adoption across the entire organization.

Technical features

ENCRYPTION TYPES SUPPORTED

Full disk encryption (FDE), file/folder encryption, USB encryption and email encryption are all supported features.

FULLY VALIDATED

ESET Endpoint Encryption is FIPS 140-2 validated with 256-bit AES encryption.

ALGORITHMS & STANDARDS

AES 256 bit, AES 128 bit, SHA 256 bit, SHA1 160 bit, RSA 1024 bit, Triple DES 112 bit, Blowfish 128 bit.

OS SUPPORT

Support for Microsoft® Windows® 10, 8, 8.1 including UEFI and GPT, 7, Vista, XP SP 3; Microsoft Windows Server 2003-2012; Apple iOS.

NO SPECIAL HARDWARE REQUIRED

TPM chips are optional but not required for using full disk encryption.

NO SERVER REQUIRED

ESET Endpoint Security requires no server to utilize and can seamlessly support encryption for remote users.

ENCRYPT EMAIL & ATTACHMENTS

Easily send and receive encrypted emails and attachments through Outlook.

TEXT & CLIPBOARD ENCRYPTION

Encrypt all or part of a text window—web browsers, database memo fields or web mail.

CENTRALIZED MANAGEMENT

Full control of licensing and software features, security policy and encryption keys.

VIRTUAL DISKS & ENCRYPTED ARCHIVES

Create a secure, encrypted volume on your PC or in another location or an encrypted copy of an entire directory tree and its files.

ESET IN NUMBERS

110M+

users
worldwide

400K+

business
customers

200+

countries &
territories

13

global R&D
centers



Bring ESET security solutions to your business today. Contact an Account Manager for more information.
1.800.800.0014 ■ www.connection.com/ESET