



# ENDPOINT ENCRYPTION

**Simple and powerful encryption**  
for organizations of all sizes

CYBERSECURITY  
EXPERTS ON YOUR SIDE



# What is an **Endpoint Encryption product?**

**Endpoint encryption is an essential tool for data security, providing encryption of files and disks on the organization's endpoint devices. This prevents the data from being readable and misused, should they fall in the wrong hands.**

ESET Endpoint Encryption is a simple-to-use encryption for companies large and small, which supports full disk encryption (FDE), file/folder encryption, email encryption and USB encryption.

# Why Endpoint Encryption?

## DATA BREACHES

Today's cybersecurity landscape has an increasing number of data breaches happening every day. When these breaches occur if encryption is not implemented, then the data is at risk of being released to the public or utilized for malicious purposes. Some companies may choose to not care about the release of data, but all companies have sensitive data such as customer lists, proprietary information, sales-related data, staff and HR information.

By implementing an encryption solution, businesses make it impossible for hackers to read the data that may have been stolen. The top industries for data breaches are traditionally ones that have valuable data such as financial, retail, healthcare and the public sector. However, that does not mean that other industries are safe—just that hackers typically weigh effort required versus the payoff.

## REMOTE EMPLOYEES

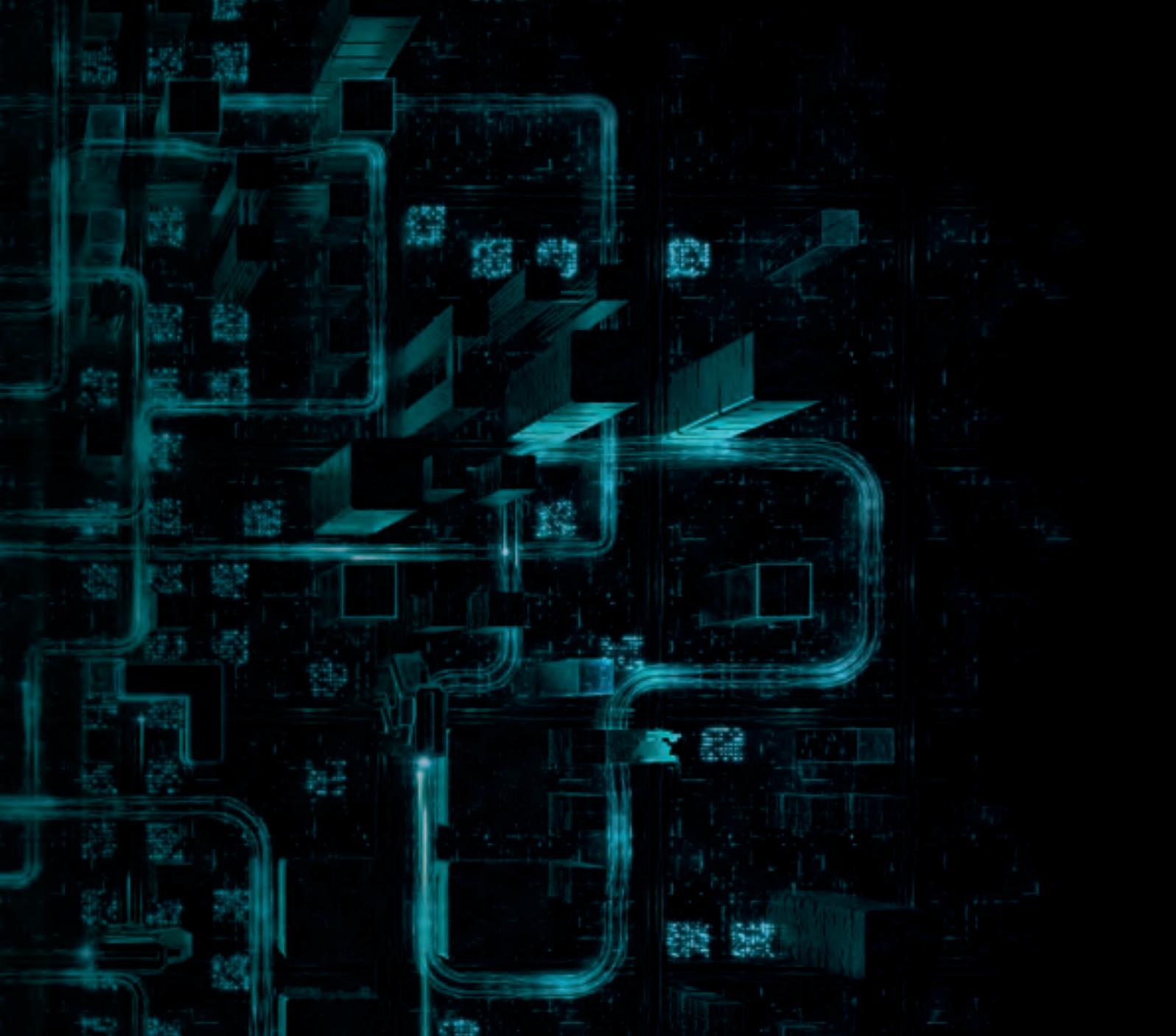
Remote employees or traveling users have become the norm of most businesses. Employees are now working out of coffee shops or, due to travel, working from airports. However, the more remote employees that you have the higher the risk of lost or stolen devices. Not only do businesses need to worry about simply lost or stolen devices, they need to think about the process of terminating remote users.

Unlike with other products, with ESET Endpoint Encryption you can disable a remote employee's laptop within seconds of their connection to the internet, without the need to wait for them to connect to the VPN or the corporate network.

## COMPLIANCE

When it comes to compliance, most businesses first need to understand whether they have to meet a compliance or not. Next, they have to review what requirements the compliance recommends and mandates that their business implement. When it comes to encryption, many regulations and laws, such as GDPR, PCI-DSS, HIPAA, SOX and GLBA, require that it be implemented.

Endpoint encryption is no longer an optional solution for most businesses that handle credit cards or health information, but rather a required solution. All businesses should do research and evaluate if they need to abide by certain compliances.



The more remote employees that you have the higher the risk of lost or stolen devices.

Endpoint encryption is no longer an optional solution for most businesses who handle credit cards or health information, but rather a required solution.



# 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.

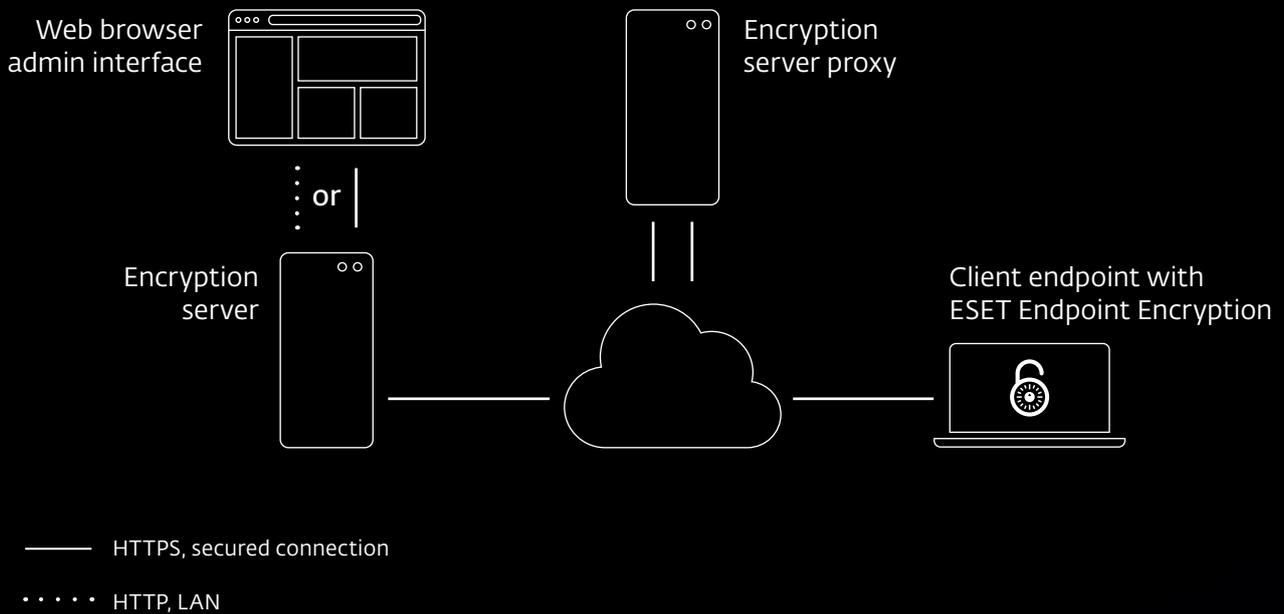
## USER-PROOF REMOVABLE MEDIA

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 to adoption across the entire organization.



# Use cases

## Prevent data breaches

### USE CASE

Businesses are in the news every single day notifying their customers that a data breach has occurred.

### SOLUTION

- ✓ Protect sensitive data with ESET Endpoint Encryption by means of full disk encryption (FDE).
- ✓ Protect vulnerable communications such as Remote Desktop by adding multi-factor authentication.
- ✓ Require multi-factor authentication in order to log in to devices that contain sensitive data.

### RECOMMENDED ESET SOLUTIONS

- ✓ ESET Endpoint Encryption
- ✓ ESET Secure Authentication

## Manage remote employees

### USE CASE

Companies need the ability to protect sensitive data in the case of employee termination or when devices are lost or stolen.

### SOLUTION

- ✓ Restrict access to company resources by leveraging multi-factor authentication.
- ✓ Utilize the remote lock-out functionality to protect devices that may be lost or stolen.
- ✓ Leverage the ability to remove users from remote devices in order to protect data in the case of employee terminations.

### RECOMMENDED ESET SOLUTIONS

- ✓ ESET Endpoint Encryption
- ✓ ESET Secure Authentication

*“As a service provider and working to service-level agreements, it is reassuring that we can recommend, procure, commission and support an encryption solution which helps keep continuity across Staffordshire educational establishments, reducing overall costs.”*

Andy Arnold, CS Team Leader of System Solutions,  
Staffordshire Learning Technologies (SLT), UK

# Prevent data leakage

## USE CASE

Every company utilizes removable media devices to move data from one computer to another, but most companies do not have a way to verify that the data is staying only on company devices.

## SOLUTION

- ✓ Implement user-proof removable media to restrict the moving of data outside of the company.
- ✓ Restrict access to removable media devices to selected users.

## RECOMMENDED ESET SOLUTIONS

- ✓ **ESET Endpoint Encryption**

*“The pilot was set up in a real-time environment and we found the solution be extremely user-friendly, with its web-based interface. The server was very good, even allowing control of devices over the internet, independent of network or directory structure.”*

Simon Goulding, Aster's Network Services Analyst, UK



# ESET Endpoint Encryption 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 Encryption 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.

All companies have sensitive data such as customer lists, proprietary information and sales-related data.

# About ESET

**ESET – a global leader in information security – has been named as a Challenger in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms\* two years in a row.**

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant,

comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

## ESET IN NUMBERS

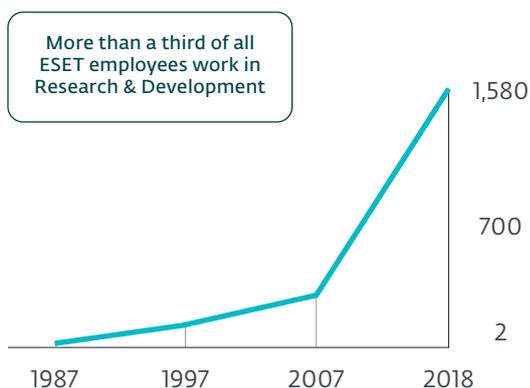
**110m+**  
users  
worldwide

**400k+**  
business  
customers

**200+**  
countries &  
territories

**13**  
global R&D  
centers

## ESET EMPLOYEES



## ESET REVENUE



\* Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

---

## SOME OF OUR CUSTOMERS

---



**MITSUBISHI  
MOTORS**

Drive your Ambition

protected by ESET since 2017  
more than 14,000 endpoints

**Canon**

Canon Marketing Japan Group

protected by ESET since 2016  
more than 9,000 endpoints

**Allianz**   
Suisse

protected by ESET since 2016  
more than 4,000 mailboxes



ISP security partner since 2008  
2 million customer base

---

## SOME OF OUR TOP AWARDS

---



*“Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions.”*

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018

