



OVERVIEW

MOBILE THREAT DEFENSE

Efficiently protect and manage
your company mobile fleet

Progress. Protected.

What is a mobile protection product?

A mobile protection product can be separated into two distinct categories: security and management.

The security features range from antimalware, anti-phishing, limiting access to unsecure connections, and much more.

The management includes remotely wiping devices, restricting application installs, preconfiguring devices for users, and other items related to IT management.

Mobile protection typically covers Android and Apple devices, the two most widespread mobile operating systems. As these OSes are different, also mobile protection capabilities can vary between these systems.

ESET solutions for mobile devices

✓ ESET Endpoint Security for Android

✓ ESET MDM for iOS & iPadOS

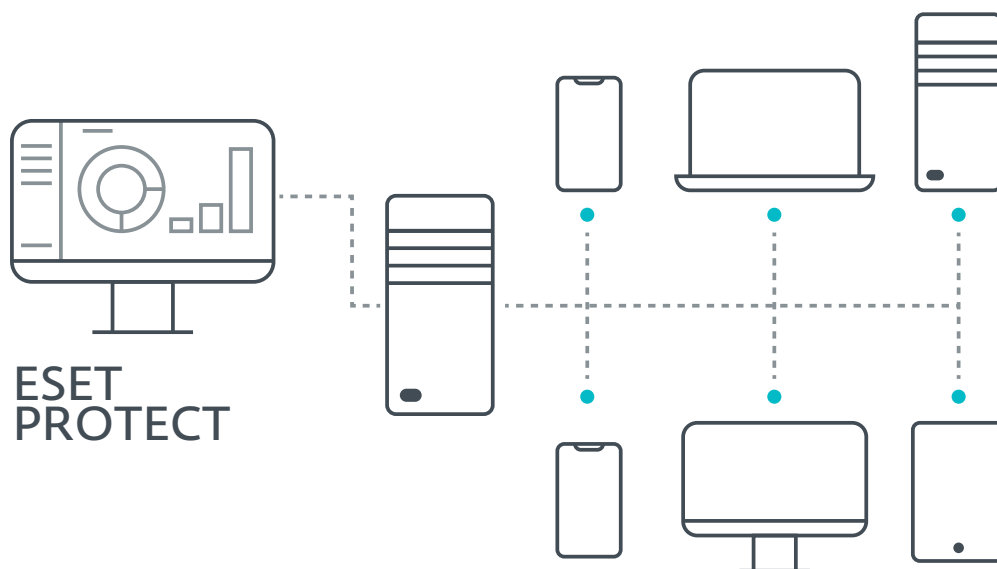
Supported MDM enrollment options

✓ Apple Business Manager (ABM)

✓ Microsoft Intune

✓ VMware Workspace ONE

✓ Microsoft Entra ID



With ESET PROTECT, you get a full visibility of the network, from mobiles to workstations and servers.

The ESET Difference

COST EFFECTIVE

No need for dedicated solutions for full Mobile Device Management. Oversee smartphones and other endpoint devices from a single point with ESET PROTECT.

MULTILAYERED PROTECTION

ESET combines multilayered technology, artificial intelligence and human expertise to provide its customers with the best level of protection possible. ESET technology is constantly updated to provide the best balance of detection, false positives and performance.

ESET CLOUD MALWARE PROTECTION SYSTEM

Whenever a zero-day threat such as ransomware is seen, the file is sent to the cloud-based system ESET LiveGrid®, where the threat is detonated and behavior is monitored. Results of this system are provided to all mobile endpoints without requiring any updates.

PROVEN AND TRUSTED

ESET has been in the security industry for over 30 years, and continues to evolve its technology to stay one step ahead of the newest threats. As a result, ESET technology protects over one billion internet users worldwide.

WORLDWIDE PRESENCE

ESET has offices in 13 countries worldwide, 11 R&D labs and a presence in 178 countries and territories. This helps provide us with data to stop malware before it spreads across the globe, as well as prioritize new technologies based on the most recent threats or new potential vectors.

Technical features

Android/ iOS

ANTI-THEFT

Easily remote lock or turn on a siren when a device is lost or stolen. In addition, send custom messages directly to devices, or set up lock screen information to help ensure devices get returned to proper owners. For iOS devices there is also the ability to perform a remote wipe.

APPLICATION CONTROL

Offers administrators the option to monitor installed applications, block access to defined applications, permissions, or categories and prompt users to uninstall particular applications.

DEVICE SECURITY

Left up to a user, device security is usually not implemented properly. So ESET enables admins to define password complexity requirements, prompt users to encrypt their device, and more.

UNIFIED MANAGEMENT CONSOLE

Manage all your endpoints, devices and servers from ESET PROTECT, our unified endpoint management (UEM) console, which delivers a full security overview of your network.

Android only

MULTILAYERED DEFENSE

A single layer of defense is not enough for the constantly evolving threat landscape. All endpoint products have the ability to detect malware pre-execution, during execution and post-execution, all while remaining optimized for mobile.

ARTIFICIAL INTELLIGENCE

All ESET endpoint products have been employing artificial intelligence alongside all other layers of defense since 1997. Specifically, AI is used in the form of consolidated output and neural networks.

ANTI-PHISHING

Protects users from fake websites that attempt to acquire passwords, banking data, and other sensitive information.

APPLICATION AUDIT

Tracks applications and their access to personal/company data sorted by categories, allowing administrators to monitor and control applications' access.

WEB CONTROL

Control or restrict websites that users of managed devices can access, in order to avoid inappropriate, harmful or productivity-impacting content. Use default report templates, or set up your own customized reports.

iOS only

A SINGLE POINT OF CONTROL

No need for dedicated solutions – oversee security of all company iOS devices from a single point with ESET PROTECT.

PUSH ACCOUNT AND DEVICE SETTINGS REMOTELY

Remotely push out settings such as Wi-Fi, VPN, Microsoft Exchange information, screen lock timers, and camera restrictions.

ABM COMPATIBILITY

APPLE BUSINESS MANAGER (ABM) is a powerful method of enrolling corporate iOS devices. With ABM compatibility you can enroll devices into ESET protection automatically, without needing direct contact with the device and with minimal interaction from the user. This allows complete customization of device setup, saving you time and money.

*The availability of the features above is dependent on Android/iOS system restrictions and the version of the mobile OS.



Use Cases

Ransomware

PROBLEM

Not only is ransomware a desktop and server threat, but it is also a threat on mobile devices. Businesses want to make sure that all of their data is protected from being ransomed.

SOLUTION

- ✓ Deploy ESET Endpoint Security for Android to all mobile devices to ensure that Android devices are protected from any type of malware.
- ✓ Restrict Android devices from installing applications from unknown sources to limit risk.

Data loss

PROBLEM

Organizations are not only concerned with devices being lost or stolen, but also concerned with data theft when an employment is terminated.

SOLUTION

- ✓ Enforce security policy that requires mobile devices to be encrypted.
- ✓ Implement security policies that require passcodes or pins to be set on all devices.
- ✓ Lock-out or remotely wipe devices when needed.

Device compliance

PROBLEM

Different organizations have different policies related to use of mobile devices, and administrators want to ensure that all devices and users remain in compliance.

SOLUTION

- ✓ Restrict which applications can be installed on devices.
- ✓ Restrict access to unsecured Wi-Fi networks.
- ✓ Ensure that security features of phones are enabled and implemented.

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats—targeted attacks, zero-day threats, ransomware, phishing, and more—with our AI-Native, prevention-first approach. ESET combines the power of AI and human expertise to deliver easy and effective protection.

Experience best-in-class, science-driven security, backed by over 30 years of in-house global cyber threat intelligence. Our extensive R&D network, led by industry-acclaimed researchers, powers our award-winning, cloud-first cybersecurity platform. ESET solutions are highly

customizable, include local support, and have minimal impact on performance.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+

protected
internet users

500k+

business
customers

178

countries

11

global R&D
centers

SOME OF OUR CUSTOMERS



protected by ESET since 2017
more than 9,500 devices



protected by ESET since 2019
1,200 devices & 2,700 mailboxes



protected by ESET since 2016
more than 23,000 devices



ISP security partner since 2008
2 million customer base

RECOGNITION



Winner of the **Best Enterprise Endpoint**
and **Best Small Business Endpoint**
awards at the SE LABS Awards 2025



Named a **Customers' Choice** in Gartner®
Peer Insights™ "**Voice of the Customer**"
Endpoint Protection Platforms report 2026



Named a **Leader** in Frost Radar: Endpoint
Security 2025, demonstrating excellence
in growth & innovation

Gartner and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.