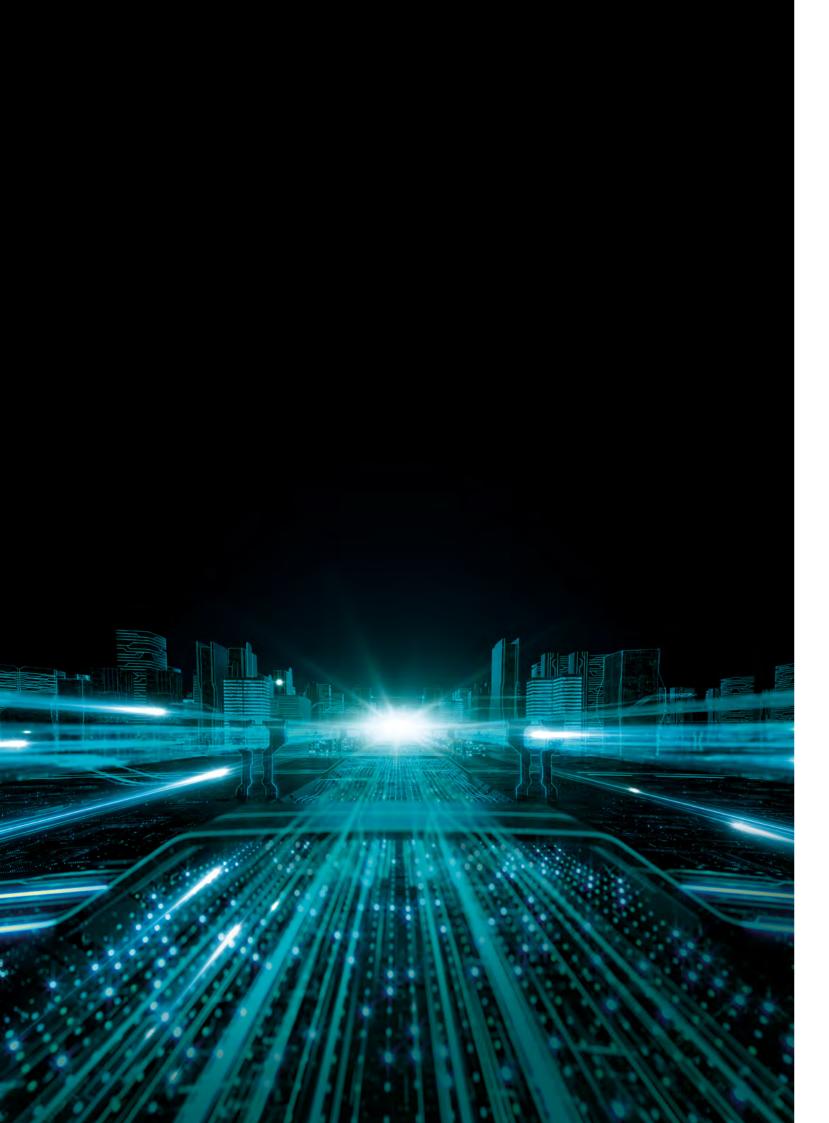# ESET®

MOBILE PROTECTION

Multilayered technology, machine learning and human expertise working together to provide comprehensive security for all platforms.

CYBERSECURITY
EXPERTS ON YOUR SIDE

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, pre-configuring 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.

Why **mobile protection?**

RANSOMWARE

Ransomware has traditionally been a major concern on desktops or servers, but since 2014 ransomware has also existed on Android devices. In 2014 we saw the first Android ransomware in the form of Simplocker. Just like the desktop variants, mobile ransomware has continued to evolve to employ new practices and new payload techniques to ransom mobile devices. When a business experiences a ransomware attack, they quickly realize that the backups they have are not recent enough, so the business feels as though they must pay the ransom.

With multiple layers of protection, ESET Endpoint Security for Android enables the prevention and detection of ransomware within an organization's mobile workforce. It is important for all businesses to prevent and detect ransomware, as every time a ransom is paid, it convinces the criminals to continue to utilize this attack method.

STOLEN OR LOST DEVICES

Nowadays, organizations are enabling employees to work from remote locations such as their home or coffee shops. By allowing employees to work remotely from the office, organizations have realized that this freedom brings with it a new set of challenges in the form of lost and stolen devices. These devices not only contain work related documents, files, and emails, but also can contain information that could harm an organization's reputation.

ESET security and Mobile Device Management (MDM) solutions for mobile platforms enable an organization to remotely lock or wipe devices. This ensures that sensitive information is not compromised when a device is lost or stolen, nor during an employee termination
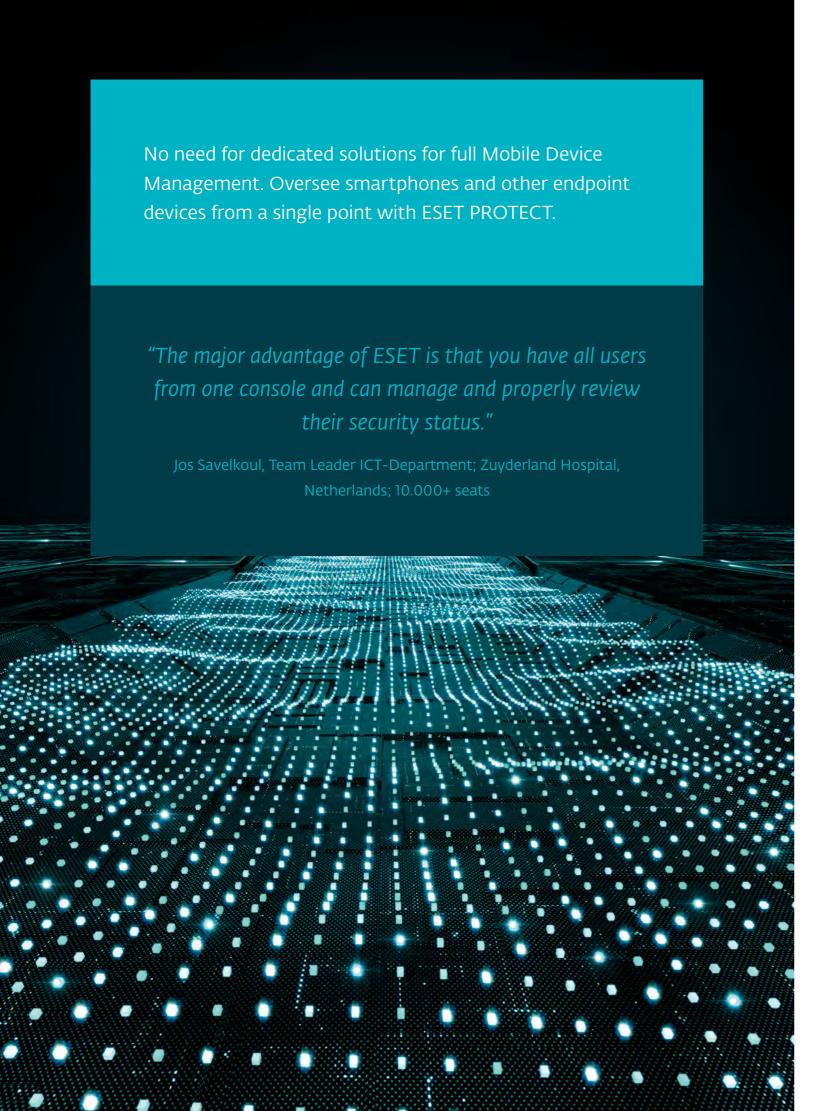
DEVICE MANAGEMENT

Organizations, due to liability reasons as well as time-management reasons, want to ensure that their employees are only using work-provided devices for work reasons. Also, mobile devices become more risky when they are allowed to connect to insecure networks or when they have certain features enabled.

ESET solutions for mobile platforms enable organizations to restrict users from certain applications, calling of certain numbers, as well as device features such as cameras, Wi-Fi, and Bluetooth. In addition, all of this functionality can be deployed as a time-based policy, so features are locked down only during work hours.

Allowing employees the freedom to work remotely from the office, organizations have realized that this freedom brings with it a new set of challenges in the form of lost and stolen devices. These devices not only contain work related documents, files, and emails, but also can contain information that could harm an organization's reputation.

It is important for all businesses to prevent and detect ransomware, as every time a ransom is paid, it convinces the criminals to continue to utilize this attack method.

In 2014 we saw the first Android ransomware in the form of Simplocker.

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

"The major advantage of ESET is that you have all users from one console and can manage and properly review their security status."

Jos Savelkoul, Team Leader ICT-Department; Zuyderland Hospital, Netherlands; 10.000+ seats

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, machine learning and human expertise to provide our customers with the best level of protection possible. Our technology is constantly adjusting and changing 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 our 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 our technology to stay one step ahead of the newest threats. This has led us to be trusted by over 110 million users worldwide.

UNPARALLELED PERFORMANCE

Countless times, organizations' biggest concern is the performance impact of a mobile protection solution. For example, in the May 2020 mobile security test by AV-Test, ESET got the best scores for performance and low impact on the system.

WORLDWIDE PRESENCE

ESET has 22 offices worldwide, 13 R&D facilities and presence in over 200 countries and territories. This helps to provide our customers with a worldwide perspective on all the most recent trends and threats.

"ESET security solutions have protected and alerted Primoris IT department on numerous occasions to serious threats and infections, most importantly ransomware."

Joshua Collins, Data Center Operations Manager; Primoris Services Corporation, USA; 4.000+ seats

Use cases

Ransomware

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

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

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.

"Centrally managed security on all endpoints, servers and mobile devices was a key benefit for us."

IT Manager; Diamantis Masoutis S.A., Greece; 6.000+ seats

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

Technical features

Android/iOS

ANTI-THEFT

Easily remote lock, wipe, or kick off a siren when a device may be 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.

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 allows admins to define password complexity requirements, set screen lock timers, prompt users to encrypt their device, block cameras and more.

CLOUD MANAGEMENT CONSOLE

Smartphones, along with desktops and servers, are fully managed from a single pane of glass cloud console, ESET PROTECT, for the complete 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.

MACHINE LEARNING

All ESET Endpoint products have been using machine learning in addition to all other layers of defense since 1997. ESET currently uses machine learning in conjunction with all of our other layers of defense. Specifically, machine learning 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.

iOS only

APPLE iOS MANAGEMENT FRAMEWORK

No need for dedicated solutions – take advantage of Apple iOS Management Framework and oversee security of all company iOS devices from a single point with ESET PROTECT.

PUSH ACCOUNT SETTINGS REMOTELY

Remotely push out account settings such as Wi-Fi, VPN and Exchange information.

MOBILE DEVICE MANAGEMENT

User and admin is automatically notified if the current device settings are not in compliance with corporate security policies and suggests the necessary changes.
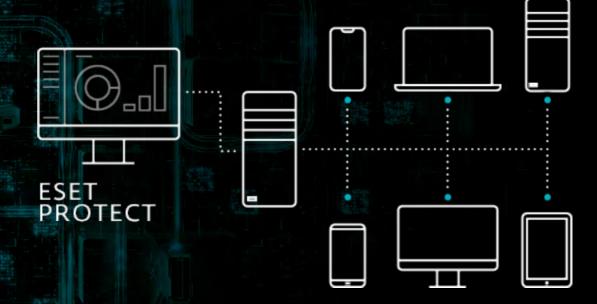
Choose your MDM deployment option

CLOUD MDM

This option comes as a ready-to-use solution, integrated with our cloud management console, ESET PROTECT CLOUD. It's easy to get started for organizations of any size, as it requires no prerequisites such as certificates or additional components. Cloud MDM covers Android, iOS and iPadOS devices.

ON-PREM MDM

In case you have both Android and iPhones in your mobile fleet, you may want to choose on-prem MDM. It is available from the on-prem version of ESET PROTECT. In order to implement, it requires the installation of a special mobile device connector.

ESET PROTECT

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

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

About ESET

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

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

Why choose ESET

ESET is compliant with ISO/IEC 27001:2013, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET's full compliance with industry-leading best practices.

ESET AWARDS

AV comparatives APPROVED Business Security DEC 2020

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION JAN-MAR 2020

AV-TEST av-test.org AWARD Best Usability ESET Endpoint Security

G2 Leader WINTER 2021

Gartner peerinsights customers' choice 2019

canalys CYBERSECURITY CHAMPION 2020

ANALYST RECOGNITION

Gartner

ESET was named the only Challenger in 2019 Gartner Magic Quadrant for Endpoint Protection Platforms, for the second year running.

FORRESTER®

ESET was rated a Strong Performer in the Forrester Wave(TM): Endpoint Security Suites, Q3 2019.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET was rated 'Top Player' in the 2019 Radicati Endpoint Security report according to two main criteria: functionality and strategic vision.

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.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

ESET ® ENJOY SAFER TECHNOLOGY™