



MOBILE PROTECTION

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

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, 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 organisation'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

Home working and remote working have now become the norm, rather than the exception. Organisations are working to facilitate this, but see that ensuring secure remote access brings with it a new set of challenges, including lost and stolen devices. These devices not only contain work related documents, files, and emails, but also can contain information that could harm an organisation's reputation.


ESET security and Mobile Device Management (MDM) solutions for mobile platforms enable an organisation 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

Organisations, 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 organisations 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.

As early as 2014, we saw the first Android ransomware in the form of Simplocker.



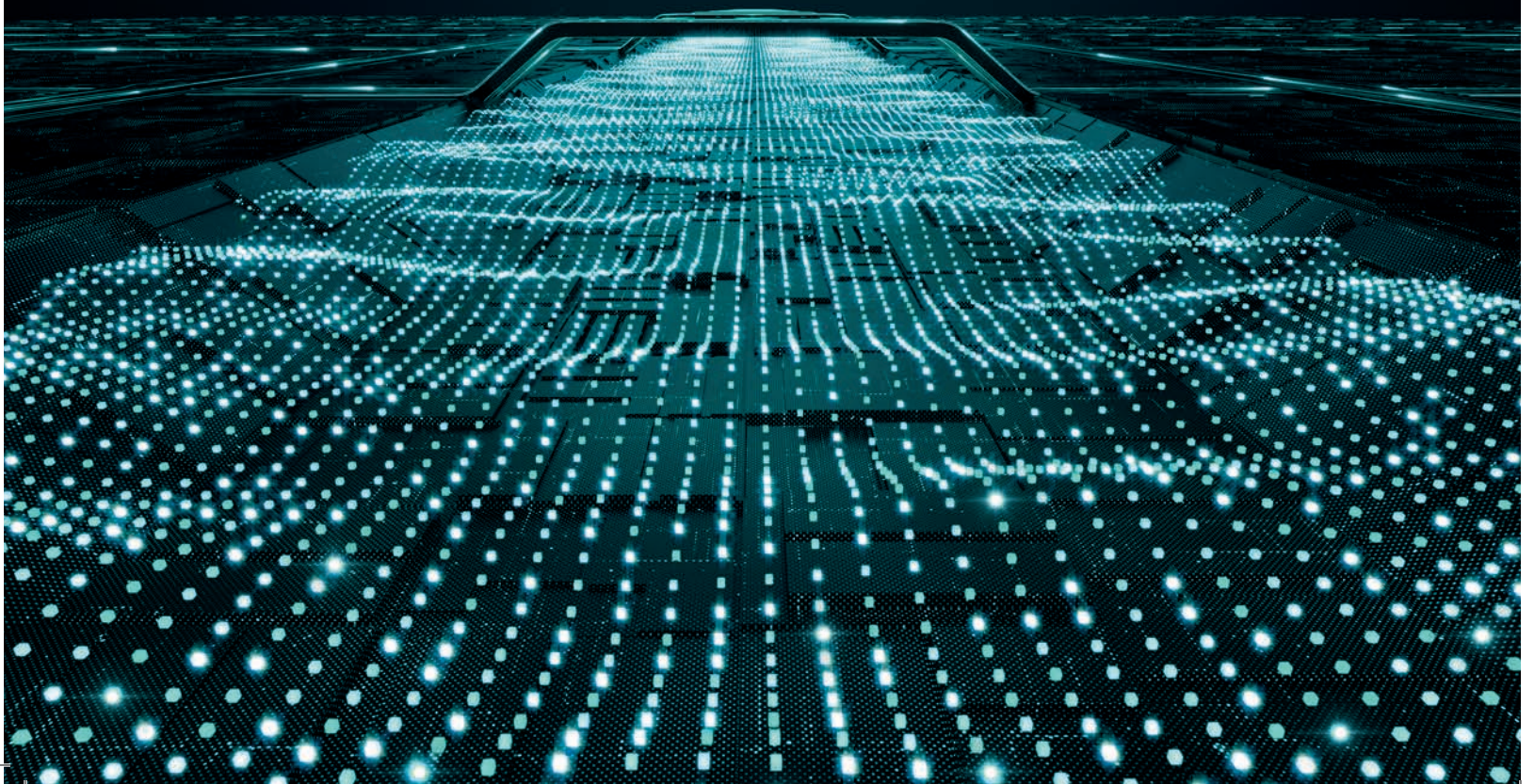
Remote working is now the norm, and organisations are working to give their employees the freedom and convenience it allows. But they realise that providing secure remote access brings with it a new set of challenges, including lost and stolen devices. These devices not only contain work-related documents, files and emails – they can also contain information that could harm an organisation’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 utilise this attack method.

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 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 behaviour 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 is now trusted by over 110 million users worldwide.

UNPARALLELED PERFORMANCE

Often, an organisations' biggest concern is the performance impact of a mobile protection solution. This is an area in which ESET has long excelled. For instance, in July 2021 ESET Endpoint Security 2.11 (Android) achieved a nearly perfect score in each of the three categories in AV-TEST's "Best Android antivirus for business users".

WORLDWIDE PRESENCE

ESET has 22 offices worldwide, 13 R&D facilities and presence in over 200 countries and territories. This helps to provide its 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

Organisations 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 organisations 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

Organisations 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.

FLEXIBLE CONSOLE MANAGEMENT

Manage all your endpoints, devices and servers from the ESET PROTECT console, which can be cloud-based or on-premises depending on your needs. ESET PROTECT is a unified endpoint management (UEM) console that delivers a full security overview of your network.

Android only

MULTILAYERED DEFENCE

A single layer of defence 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 optimised for mobile.

MACHINE LEARNING

ESET uses machine learning in conjunction with all its other layers of defence – and has done since 1997. Specifically, machine learning is used in consolidated outputs 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 customised 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 SETTINGS REMOTELY

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

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 customisation of device setup, saving you time and money.

Choose your MDM deployment option

CLOUD MDM

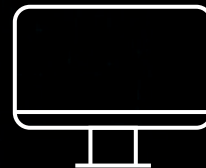
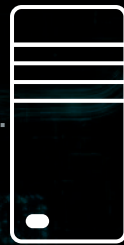
This option comes as a ready-to-use solution, integrated with ESET's cloud management console, ESET PROTECT CLOUD. It's easy to get started for organisations of any size, as it requires no prerequisites such as certificates or additional components. Cloud MDM covers Android, iOS and iPadOS devices.

ON-PREM MDM

If you prefer to deploy your console on-premises, ESET offers full support for this option. On-prem installation covers devices running Android, iOS and iPadOS. 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.



About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users
protected

400k+
business
customers

200+
countries &
territories

13
global R&D
centers

SOME OF OUR CUSTOMERS



protected by ESET
since 2017 more than
9,000 endpoints



protected by ESET
since 2016 more than
4,000 mailboxes



Canon Marketing Japan Group

protected by ESET
since 2016 more than
32,000 endpoints



ISP security partner
since 2008 2 million
customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS



ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2021.



ESET consistently achieves top rankings on the global G2 user review platform and its solutions are appreciated by customers worldwide.



ESET solutions are regularly recognized by leading analyst firms, including in "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" as a sample vendor.





eset[®] Digital Security
Progress. Protected.

