SOLUTION OVERVIEW

MOBILE PROTECTION

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

ENJOY SAFER TECHNOLOGY®

What is a **mobile protection product?**

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

The security features range includes 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.

One important distinction to note is that Apple mobile devices are unable to leverage security features such as antimalware due to restrictions placed on non-Apple applications. Therefore, Apple devices only have the management portion of mobile protection products.

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, it quickly realizes that the backups it has are not recent enough, so the business feels as though it must pay the ransom.

ESET Endpoint Security for Android provides layers of defense not just to prevent ransomware, but to detect it if it ever exists 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 homes or coffee shops. By allowing employees to work remotely, 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.

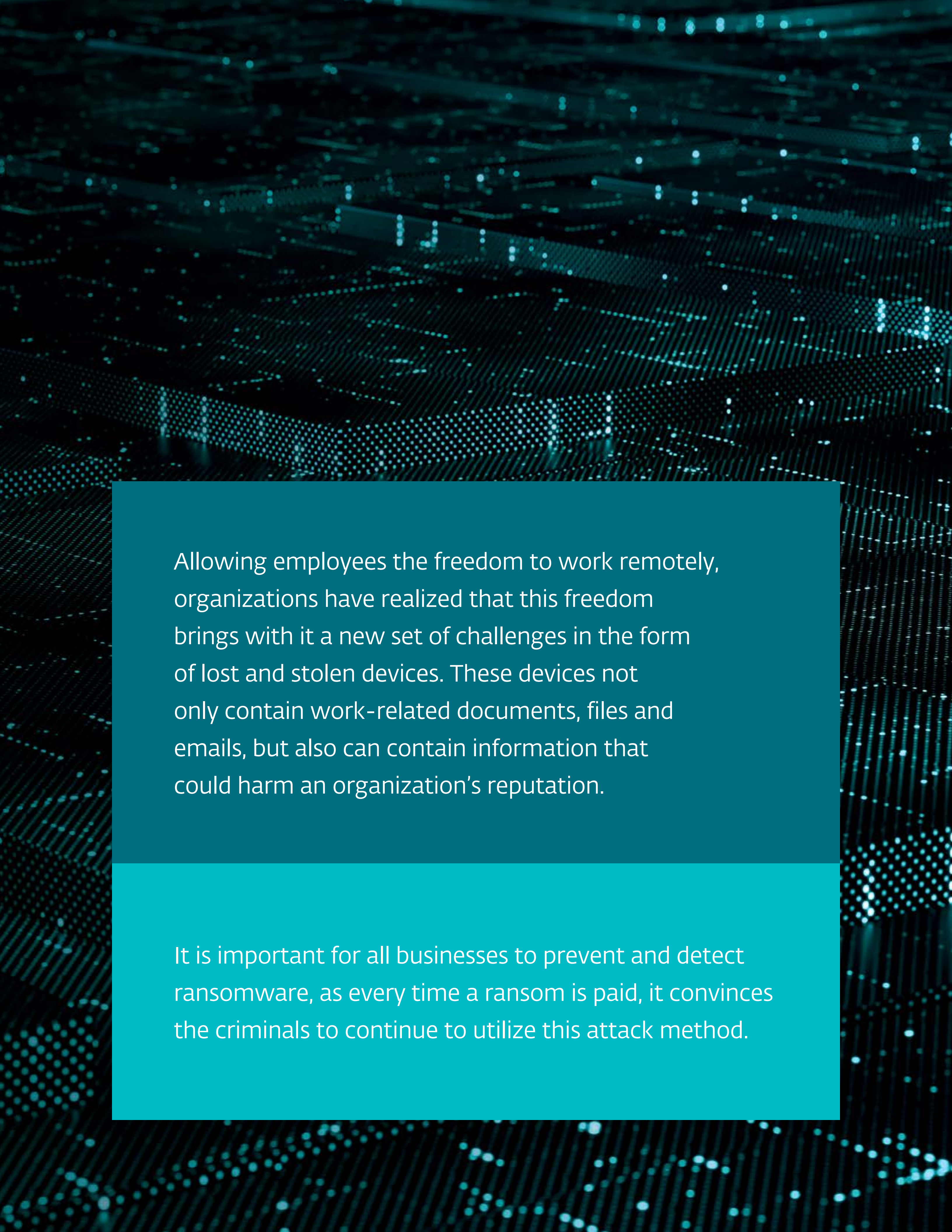
ESET security and mobile device management (MDM) solutions for mobile platforms provide an organization the ability to remotely lock or remotely wipe devices. This ensures that sensitive information is not compromised when a device is lost or stolen or during an employee termination.

DEVICE MANAGEMENT

Organizations, due to liability reasons as well as time-management reasons, want to ensure that their employees are using work-provided devices only 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 provide organizations the ability to restrict users from certain applications and from calling certain numbers, as well as restricting the use of 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.

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

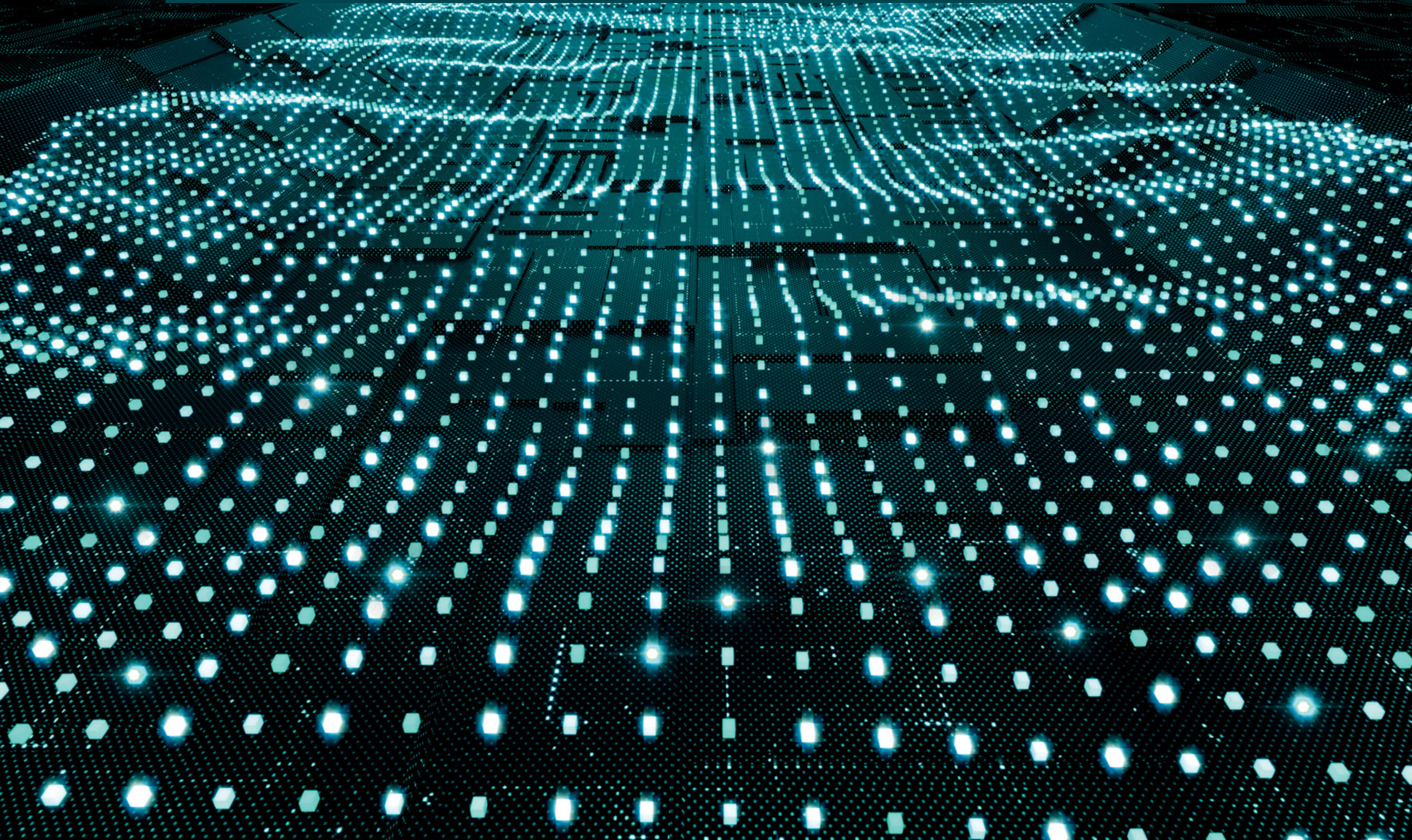


Allowing employees the freedom to work remotely, organizations have realized that this freedom brings with it a new set of challenges in the form of lost and stolen devices. These devices not only contain work-related documents, files and emails, but also can contain information that could harm an organization's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

No need for dedicated solutions for full mobile device management. Oversee all company iOS, Android and other endpoint devices from a single point with ESET Security Management Center.

> *"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 all company iOS, Android and other endpoint devices from a single point with ESET Security Management Center.

MULTILAYERED PROTECTION

ESET combines multilayered technology, machine learning and human expertise to provide its 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 its 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, an organization's biggest concern is the performance impact of a mobile protection solution. ESET products continue to excel in the performance arena and win third-party tests that prove how light-weight our endpoints are on systems.

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 with data theft when employment is terminated.

SOLUTION

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

Device compliance

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

SOLUTION

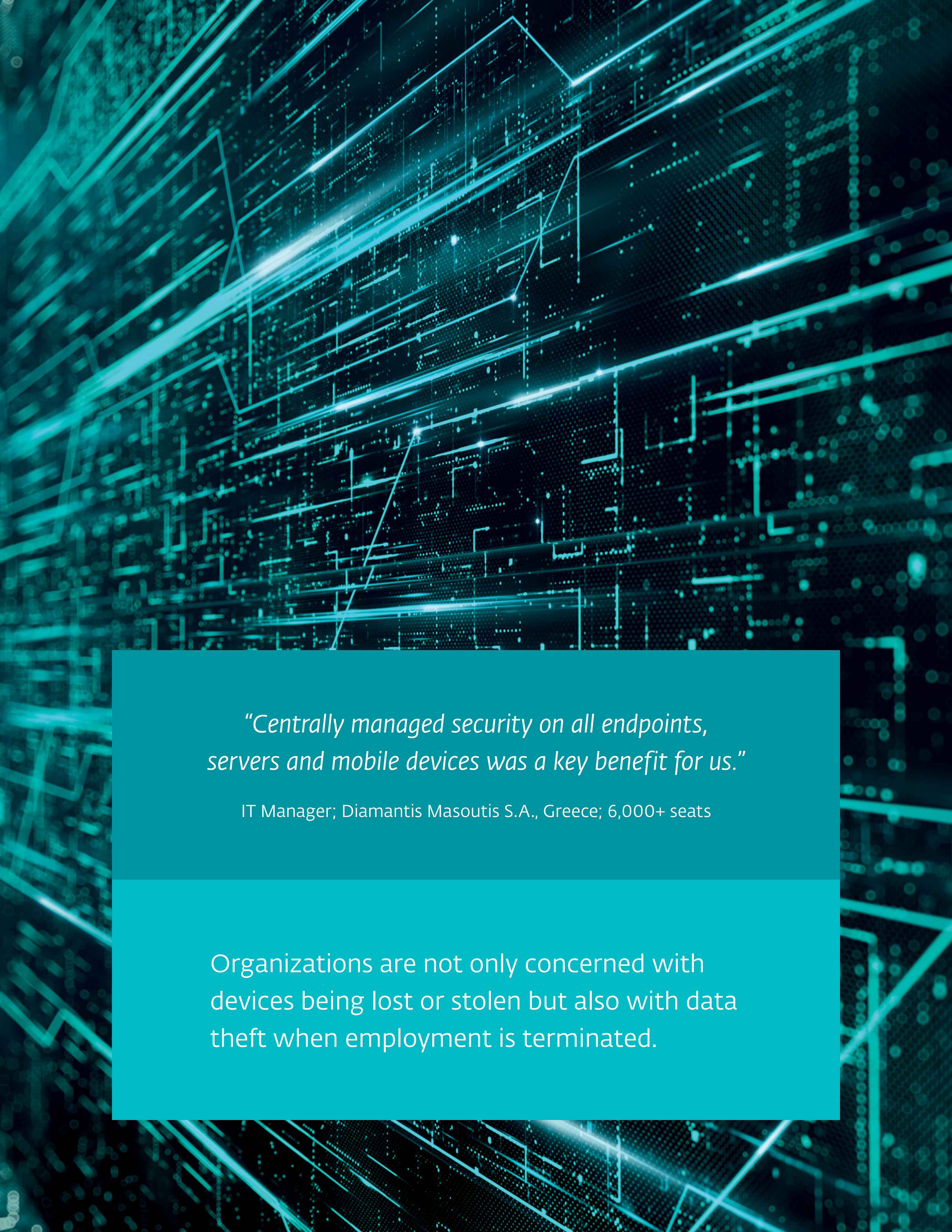
- ✓ Restrict which applications can be installed on devices.
- ✓ Restrict access to unsecured Wi-Fi networks.
- ✓ Ensure that security features of phones are enabled and implemented.

ESET®

ENDPOINT SECURITY
FOR ANDROID

ESET®

MOBILE DEVICE MANAGEMENT
FOR APPLE iOS



"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 with data theft when employment is terminated.

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 administrators to define password complexity requirements, set screen lock timers, prompt users to encrypt their devices, block cameras and more.

MANAGEMENT SERVER

Mobile products are fully managed from a single pane of glass that can be installed on Windows or Linux. In addition to installing, ESET has a virtual appliance that you can simply import for quick and easy setup.

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 its 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 Security Management Center.

PUSH ACCOUNT SETTINGS REMOTELY

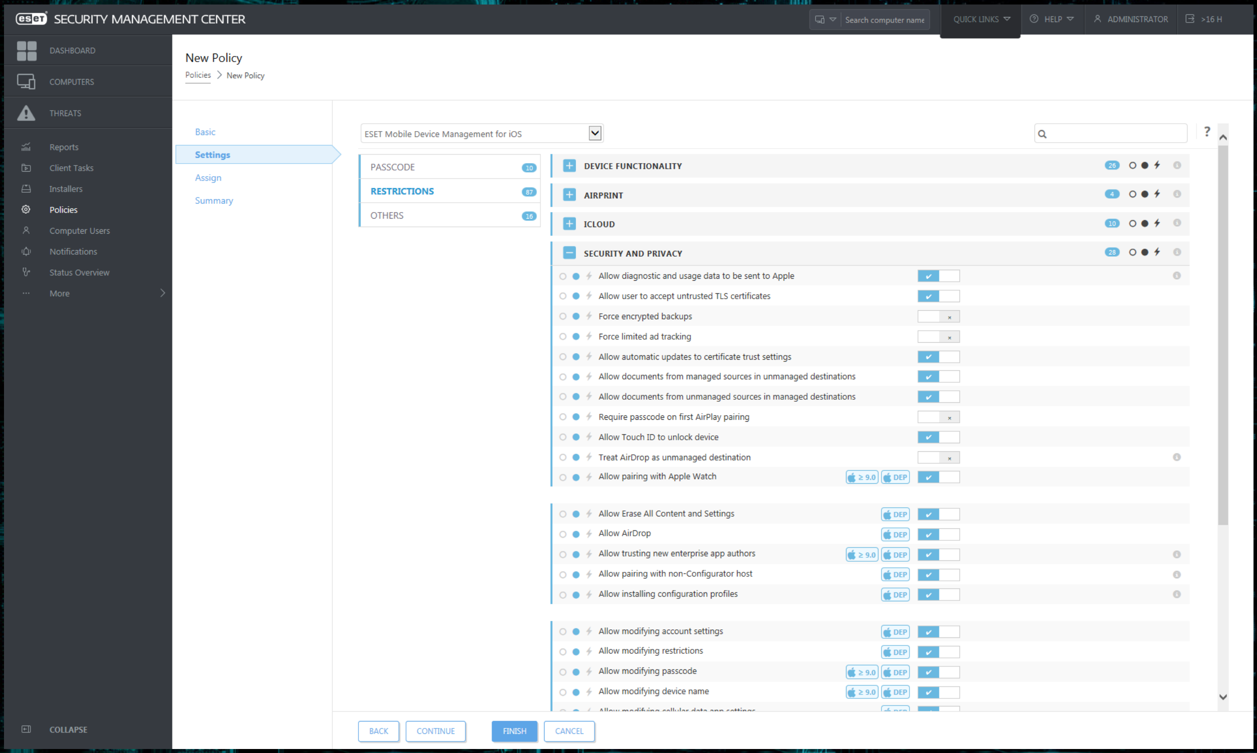
Remotely push out account settings such as Wi-Fi, VPN and Exchange information.

MOBILE DEVICE MANAGEMENT

The user and administrator are automatically notified if the current device settings are not in compliance with corporate security policies and suggests the necessary changes.

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

ESET SECURITY MANAGEMENT CENTER SETTINGS FOR IOS MDM



New Policy

Policies > New Policy

ESET Mobile Device Management for iOS

- PASSCODE 10
- RESTRICTIONS 87
- OTHERS 16

DEVICE FUNCTIONALITY 26

AIRPRINT 4

ICLOUD 10

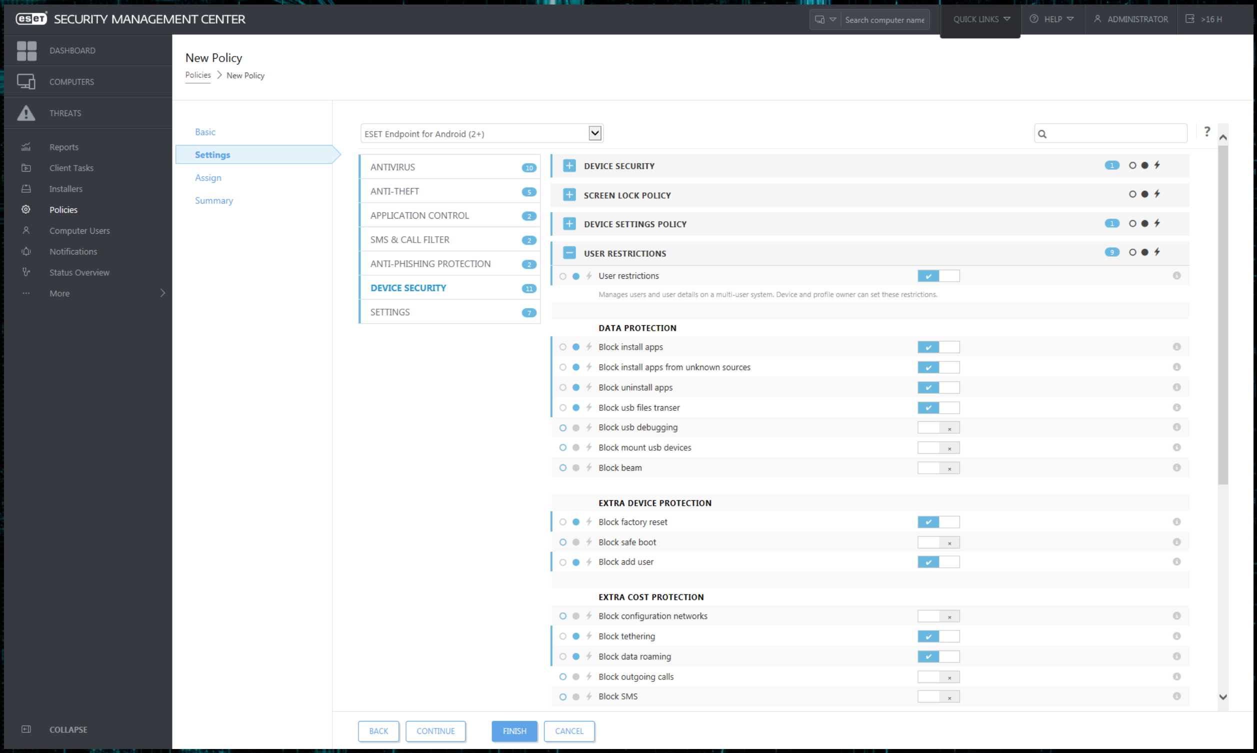
SECURITY AND PRIVACY 28

- Allow diagnostic and usage data to be sent to Apple ✓
- Allow user to accept untrusted TLS certificates ✓
- Force encrypted backups ×
- Force limited ad tracking ×
- Allow automatic updates to certificate trust settings ✓
- Allow documents from managed sources in unmanaged destinations ✓
- Allow documents from unmanaged sources in managed destinations ✓
- Require passcode on first AirPlay pairing ×
- Allow Touch ID to unlock device ✓
- Treat AirDrop as unmanaged destination ×
- Allow pairing with Apple Watch ≥ 9.0 DEP ✓

- Allow Erase All Content and Settings DEP ✓
- Allow AirDrop DEP ✓
- Allow trusting new enterprise app authors ≥ 9.0 DEP ✓
- Allow pairing with non-Configurator host DEP ✓
- Allow installing configuration profiles DEP ✓

- Allow modifying account settings DEP ✓
- Allow modifying restrictions DEP ✓
- Allow modifying passcode ≥ 9.0 DEP ✓
- Allow modifying device name ≥ 9.0 DEP ✓
- Allow modifying cellular data app settings

ESET SECURITY MANAGEMENT CENTER SETTINGS FOR ANDROID



New Policy

Policies > New Policy

ESET Endpoint for Android (2+)

- ANTIVIRUS 10
- ANTI-THEFT 5
- APPLICATION CONTROL 2
- SMS & CALL FILTER 2
- ANTI-PHISHING PROTECTION 2
- DEVICE SECURITY 11
- SETTINGS 7

DEVICE SECURITY 1

SCREEN LOCK POLICY

DEVICE SETTINGS POLICY 1

USER RESTRICTIONS 9

- User restrictions ✓

Manages users and user details on a multi-user system. Device and profile owner can set these restrictions.

DATA PROTECTION

- Block install apps ✓
- Block install apps from unknown sources ✓
- Block uninstall apps ✓
- Block usb files transer ✓
- Block usb debugging ×
- Block mount usb devices ×
- Block beam ×

EXTRA DEVICE PROTECTION

- Block factory reset ✓
- Block safe boot ×
- Block add user ✓

EXTRA COST PROTECTION

- Block configuration networks ×
- Block tethering ✓
- Block data roaming ✓
- Block outgoing calls ×
- Block SMS ×

About ESET

ESET—a global player in information security—has been named as the only challenger in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.*

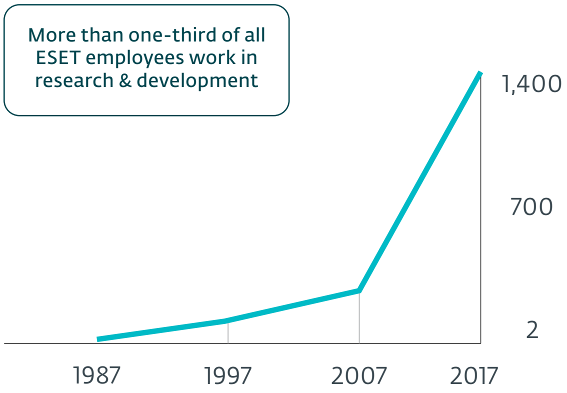
For more than 30 years, ESET has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

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.

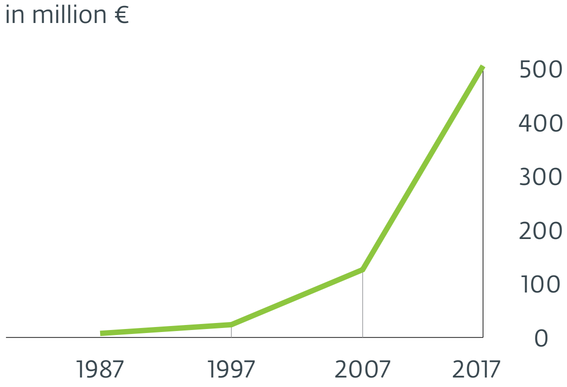
ESET IN NUMBERS

110M+	400K+	200+	13
users worldwide	business customers	countries & territories	global R&D centers

ESET EMPLOYEES


More than one-third of all ESET employees work in research & development

ESET REVENUE



*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

HONDA

protected by ESET since 2011

license prolonged 3 times and expanded 2 times

GREENPEACE

protected by ESET since 2008

license prolonged/expanded 10 times

Canon

protected by ESET since 2016

more than 14,000 endpoints

T · ·

ISP security partner since 2008

2 million customer base

SOME OF OUR TOP AWARDS

SE Labs AAA OCT-DEC 2017 ENTERPRISE ENDPOINT PROTECTION

THECHANNELCO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2017

AV comparatives Approved Business Product 2017

SC MEDIA RECOMMENDED

> *“Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the short list for consideration in enterprise RFPs for anti-malware solutions.”*
>
> KuppingerCole Leadership Compass
>
> Enterprise Endpoint Security: Anti-Malware Solutions, 2018