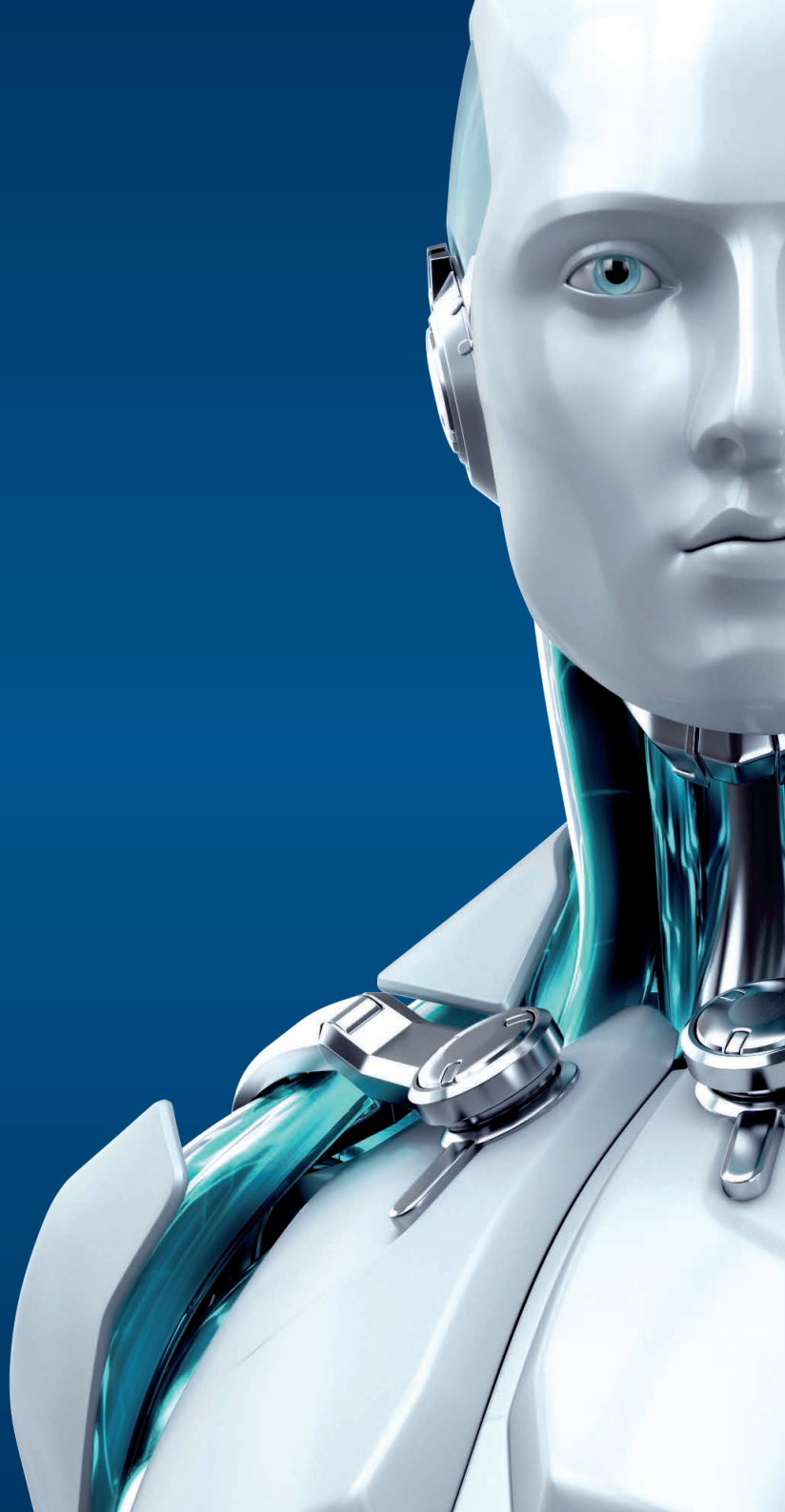
ENDPOINT SECURITY

FÜR ANDROID

ENJOY SAFER TECHNOLOGY™



ENDPOINT SECURITY
FÜR ANDROID

ESET Endpoint Security für Android bietet mit der vielfach ausgezeichneten ESET NOD32®-Technologie einen erstklassigen Schutz für die mobile Flotte Ihres Unternehmens.

Die Lösung prüft alle Anwendungen, Dateien und Speicherkarten auf Malware. Dank Anti-Theft behalten Sie selbst über verloren gegangene oder gestohlene Geräte die volle Kontrolle und mit dem SMS- und Anruffilter verhindern Sie unerwünschte Störungen. Administratoren können Sicherheitspolicies problemlos auf alle Geräte übertragen.

Endpoint-Schutz

Echtzeit-Schutz	Die proaktive Erkennungstechnologie ESET NOD32® ist jetzt auch in Kombination mit ESET LiveGrid® für mobile Geräte verfügbar und bietet somit noch mehr Schutz für Ihre Smartphone- und Tablet-Flotte.
On-Demand-Scan	Überprüft und säubert auf Wunsch den gesamten Speicher und Wechselmedien, ohne laufende Aktivitäten zu beeinträchtigen. Sie können Scans jederzeit anhalten oder Termine für eine automatische Ausführung festlegen.
Automatisches Prüfen beim Laden des Akkus	Wenn das Mobilgerät gesperrt ist und geladen wird, kann eine automatische Tiefenprüfung gestartet werden. So wird der Akku bei der Nutzung des Geräts nicht durch Routine-Scans belastet.
Anti-Phishing	Schützt Nutzer vor gefälschten oder manipulierten Webseiten, die auf persönliche Daten wie Benutzernamen, Passwörter oder Bankinformationen zugreifen wollen.
Deinstallationsschutz	Eine Deinstallation der App kann nur mit dem Administrator-Passwort vorgenommen werden.
SMS- und Anruffilter	Blockieren Sie unerwünschte Anrufe und Nachrichten* und erstellen Sie Regeln für unbekannte sowie unterdrückte Rufnummern, bestimmte Kontakte oder Zeiten, in denen Sie erreichbar sein wollen.

*Aufgrund von Änderungen, die Google im Android-Betriebssystem vorgenommen hat (Version 4.4 Kitkat und höher), ist die Blockierung von SMS nicht möglich.

Geräte-Sicherheit

Bietet dem Administrator die Möglichkeit, grundlegende Sicherheitspolicies für die gesamte mobile Flotte festzulegen. Die Anwendung informiert Nutzer und den Admin automatisch, wenn Einstellungen auf dem Gerät nicht mit den Unternehmenspolicies übereinstimmen und macht Änderungsvorschläge.

Sicherheitseinstellungen für Geräte	Bestimmen Sie die Anforderungen für komplexe Passwörter. Legen Sie eine maximale Anzahl an Entsperrungsversuchen fest, nach denen das Gerät automatisch auf die Werkseinstellungen zurückgesetzt wird. Bestimmen Sie die Gültigkeitsdauer von Passwörtern. Konfigurieren Sie die Dauer bis zur Displaysperre. Fordern Sie die Nutzer zur Verschlüsselung von mobilen Geräten auf. Blockieren Sie die Nutzung von eingebauten Kameras. Behalten Sie wichtige Einstellungen im Blick, wie z.B. USB-Debugging, NFC, WLAN, Verschlüsselung des Gerätespeichers, Roaming usw.

Anti-Theft

Auslösen von Remote Befehlen	Remote Kommandos können über den ESET Remote Administrator, per SMS mit Zwei-Faktor-Verifizierung oder direkt aus der Bedienoberfläche ausgeführt werden. Besonders hilfreich für Unternehmen ohne Remote Management oder bei Abwesenheit des Admins.
Remote Sperren	Sperren Sie verloren gegangene oder gestohlene Geräte aus der Ferne. So verhindern Sie unerlaubte Zugriffe auf gespeicherte Daten. Taucht das Gerät wieder auf, lässt es sich per Remote-Befehl wieder entsperren.
Ortung	Orten Sie ein vermisstes Gerät per Remote-Befehl und verfolgen Sie dessen Position anhand der GPS-Koordinaten.
Remote Löschen	Löschen Sie alle Kontakte, Nachrichten und Daten aus dem internen Gerätespeicher oder auf der Speicherkarte. Eine Wiederherstellung der gelöschten Daten ist nicht mehr möglich. ESET Endpoint Security für Android bleibt installiert und führt Anti-Theft-Befehle weiterhin aus.
Remote Signalruf	Mit dem Signalruf finden Sie auch ein stumm geschaltetes Smartphone in Ihrer Nähe wieder. Gleichzeitig wird das vermisste Gerät automatisch gesperrt.
Auf Werkseinstellungen zurücksetzen	Durch das Zerstören der Datei-Header und das Zurücksetzen auf die Werkseinstellungen werden alle sensiblen Daten auf dem Gerät entfernt.
Push-Benachrichtigungen	Der Administrator kann eine benutzerdefinierte Nachricht an ein einzelnes Gerät oder an eine ganze Geräte-Gruppe senden. Diese Nachricht wird dem Nutzer unübersehbar in Form eines Pop-Ups angezeigt.
Informationen bei aktiver Displaysperre	Ermöglicht dem Admin, wichtige Informationen, wie z.B. Name des Unternehmens oder Kontaktdaten, auf einem gesperrten Mobilgerät anzeigen zu lassen. So kann der Finder eines verloren gegangenen Geräts dessen rechtmäßigen Besitzer leichter ausfindig machen.
SIM-Schutz	Beim Einlegen einer fremden SIM-Karte wird das vermisste Gerät automatisch gesperrt. Die Informationen über diese SIM-Karte werden an den Administrator gesendet.
Admin-Kontakte	Ermöglicht Ihnen, eine Liste an Admin-Kontakten festzulegen, die mit einem Administrator-Passwort geschützt sind. Ausschließlich von diesen Kontakten aus können SMS-Befehle an die Geräte versendet werden. Darüber hinaus werden die Kontakte für die Anti-Theft-Funktionen verwendet.

KOSTENLOSER TECHNISCHER SUPPORT

Unsere deutschsprachigen IT-Spezialisten stehen Ihnen bei Fragen gern mit Rat und Tat zur Seite.

Anwendungskontrolle

Bietet Administratoren die Möglichkeit, installierte Anwendungen zu beobachten, den Zugriff auf bestimmte Anwendungen zu blockieren und Nutzer aufzufordern, einzelne Anwendungen zu deinstallieren.

Einstellungen für Anwendungskontrolle	Blockieren Sie unerwünschte Anwendungen anhand von: Kategorien - z.B. Spiele, Social Media usw. Berechtigungen einer App – z.B. Positionsbestimmung, Zugriff auf Kontakte usw. Quellen – Sperrt Anwendungen, die nicht aus den Standard-App-Stores installiert werden. Für blockierte Anwendungen können Ausnahmen festgelegt werden – App-Whitelist. Erstellen Sie eine Liste mit zwingend notwendigen Anwendungen.
Anwendungsprüfung	Anhand von Kategorien können Anwendungen und deren Zugriffe auf persönliche sowie Unternehmensdaten überprüft und kontrolliert werden.

Usability und Management

Einstellungen importieren/ exportieren	Selbst wenn Mobilgeräte nicht über den ESET Remote Administrator verwaltet werden, kann der Admin problemlos die Konfigurationen eines Mobilgeräts auf ein anderes Gerät übertragen, indem er die Einstellungen in eine Datei exportiert und diese dann auf den jeweiligen Geräten importiert.
Info Center	Nutzer können alle wichtigen Meldungen zentral aufrufen und erhalten zudem Informationen bezüglich der Lösung von Problemen. Hierdurch wird die Einhaltung von Unternehmenspolicies vereinfacht.
Lokale Administration	Nutzt das Unternehmen den ESET Remote Administrator nicht, kann der Admin Geräte lokal einrichten und verwalten. Alle Einstellungen der Anwendung sind mit einem Administrator-Passwort geschützt – damit behält der Admin die volle Kontrolle.
Sichere Geräte-Identifizierung	Bereits bei der Konfiguration werden mobile Geräte in einer Whitelist registriert, wodurch nur berechtigte Geräte eine Verbindung mit dem ESET Remote Administrator herstellen können. Die Unterscheidung verschiedener Geräte wird deutlich vereinfacht – über Name, Beschreibung und IMEI.
Einrichtungsassistent	Für ausgewählte Funktionen stehen nach der Installation Assistenten bereit, die die Konfiguration der Geräte erleichtern.
Zentrale Verwaltung	Alle ESET-Endpoint-Produkte können mit dem ESET Remote Administrator verwaltet werden. Über eine einzige webbasierte Management-Konsole können Sie Tasks aufsetzen und ausführen, Policies erstellen und alle Meldungen einsehen, um den Überblick über die Netzwerksicherheit zu behalten. Der Remote Administrator kann unter Windows oder Linux installiert werden und steht als Virtuelle Appliance bereit.
ESET License Administrator	Gibt Ihnen per Web-Browser die volle Übersicht über Ihre Lizenzen. Sie können sämtliche Lizenzen zentral und in Echtzeit bündeln, übertragen und verwalten, auch ohne ESET Remote Administrator.

Artikelnummer: M_Print2015_05
Stand: Februar 2015