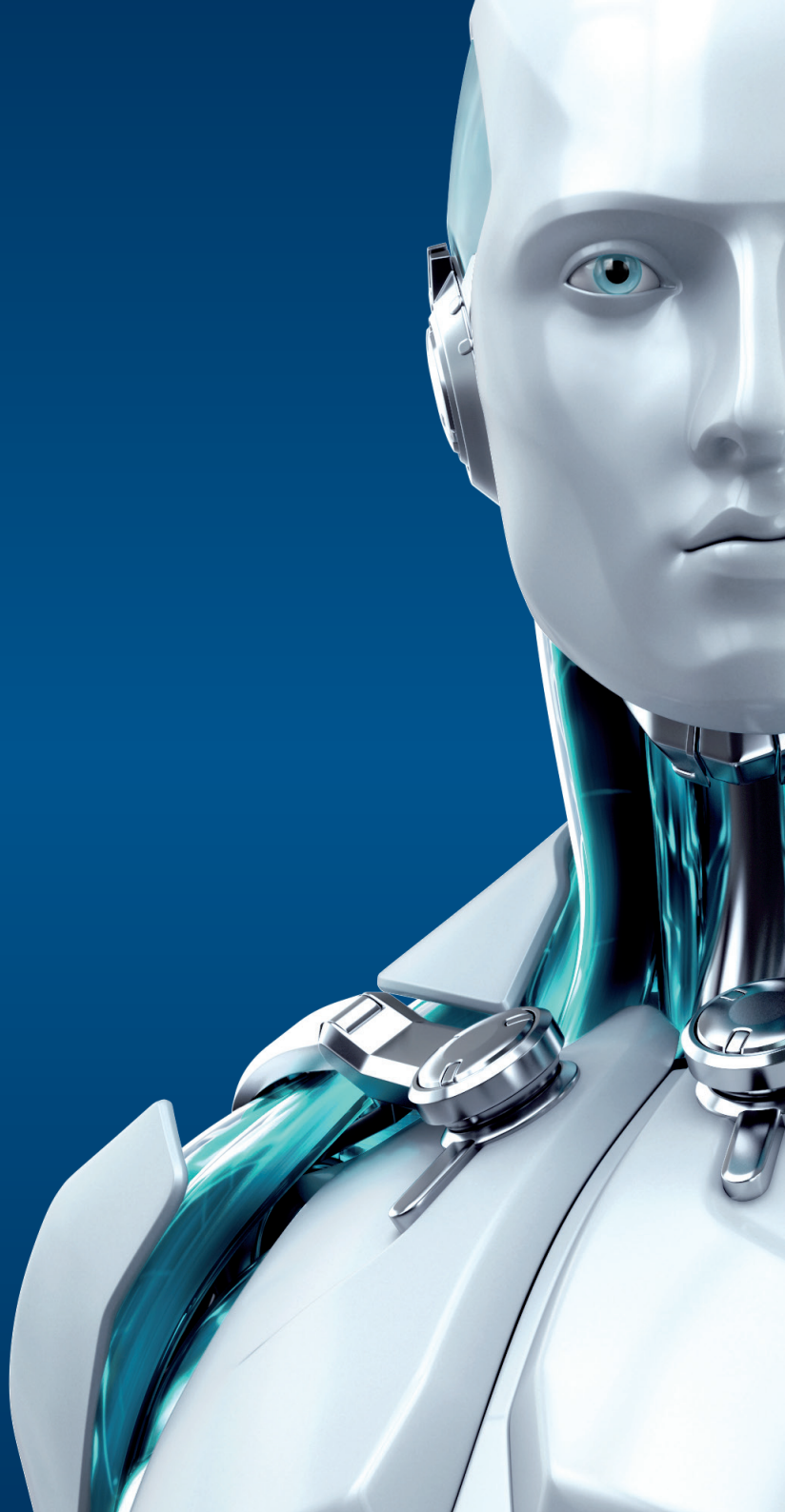
ENDPOINT SECURITY

PRO ANDROID

ENJOY SAFER TECHNOLOGY™



ENDPOINT SECURITY
PRO ANDROID

ESET Endpoint Security pro Android přináší na firemní mobilní zařízení technologii detekce škodlivého kódu ESET NOD32.

Kontroluje všechny aplikace, soubory a paměťové karty. Anti-Theft pomůže najít ztracené nebo ukradené zařízení, umožní zařízení vzdáleně zamknout nebo smazat soubory. Zároveň je možné vzdáleně uplatnit bezpečnostní politiky v souladu s firemní kulturou.

Ochrana koncových zařízení

Ochrana v reálném čase	Kontroluje všechny aplikace a navázané komunikace na přítomnost škodlivého kódu. Chrání před online i offline hrozbami, detekuje útoky USSD (protokol, který používají GSM telefony pro komunikaci s počítači poskytovatele).
Volitelná kontrola	Skenuje zařízení, paměť a výměnná média. Kontrola běží na pozadí a uživatel ji může přerušit. Je možné také kontrolu naplánovat na daný čas.
Kontrola při nabíjení	Umožňuje provést kontrolu v případech, kdy se zařízení nabíjí nebo je zamknutá obrazovka.
Anti-Phishing	Chrání před podvodnými stránkami, které se snaží získat citlivé informace jako je uživatelské jméno, heslo, podrobnosti o kreditních kartách nebo bankovnictví.
Ochrana před odinstalací	Pro odinstalaci je potřeba administrátorské heslo.
Filtr volání a SMS	Na zařízení se dovolá a pošle zprávu* jen určená osoba. Definovat lze také čas, kdy je zařízení dostupné.

*Díky změně, kterou provedla společnost Google v OS od verze 4.4, není blokování SMS dostupné.

Bezpečnost zařízení

Administrátor má možnost uplatňovat na zařízení základní bezpečnostní politiky pro mobilní zařízení.
Produkt automaticky upozorňuje uživatele a správce v případech, které nejsou v souladu s firemní politikou, a doporučuje provést změny.

Nastavení umožňuje	Definovat požadavek na silné heslo. Určit maximální počet pokusů pro odemknutí zařízení. Při překročení dojde automaticky k přechodu do továrního nastavení. Určit maximální dobu platnosti hesla. Určit čas pro zamknutí obrazovky při nečinnosti. Vyzvat uživatele k šifrování zařízení. Zablokovat integrovanou kameru.

Nastavení politik umožňuje správci monitorovat, zda je zařízení stále v požadovaném bezpečnostním stavu. Správce má přehled nad využitím paměti, Wi-Fi připojením, roamingem, instalacemi mimo Google Play, USB debug módem, NFC a šifrováním.

Anti-Theft

Události	Všechny vzdálené příkazy provádí správce pomocí ERA nebo přes SMS s dvoufaktorovou autentizací, případně přímo z grafického rozhraní.
Vzdálené zamknutí	Zamkne ztracené či ukradené zařízení. Po zamknutí se k uloženým datům může dostat pouze autorizovaná osoba. Po nalezení lze zařízení vzdáleně odblokovat.
Vzdálená lokalizace	Lokalizuje telefon a získá GPS souřadnice.
Vzdálené vymazání	Bezpečně vymaže všechny kontakty, zprávy a obsah telefonu i paměťové karty. Smazaná data nelze obnovit. Při vzdáleném smazání na telefonu produkt zůstává, takže lze pořád provádět další příkazy.
Zvukové upozornění	Pomůže najít zařízení spuštěním zvukové sirény a to i v případě, že je telefon v tichém režimu.
Tovární nastavení	Odstraní všechny data na zařízení a resetuje OS do továrního nastavení.
Zpráva na obrazovku	Odešle libovolnou zprávu např. s kontaktními informacemi na ztracené zařízení. Zpráva se zobrazí na obrazovce formou vyskakovacího okna, takže nelze přehlédnout.
Informace na zamknuté obrazovce	Správce může vytvořit a odeslat na zařízení vlastní zprávu (např. s kontaktními informace). Zpráva se zobrazí na obrazovce i v případě, že je zařízení zablokováno.
Kontrola SIM karty	Umožňuje kontrolu telefonu i po vložení neautorizované SIM karty. Správce obdrží informaci o vložené SIM kartě.
Admin kontakty	Obsahují seznam důvěryhodných telefonních čísel chráněných administrátorským heslem. SMS příkazy je poté možné odesílat jen z těchto čísel. Uvedené kontakty dostávají upozornění z Anti-Theftu.

SLUŽBY ZDARMA PRO ZÁKAZNÍKY S PLATNOU LICENCÍ

Technická podpora

K dispozici si nejen možnost konzultace po telefonu nebo e-mailem, ale také online pomocí vzdáleného připojení* a databáze znalostí.

Návštěva technika

V rámci platné licence nabízíme všem firemních zákazníkům s licencí na 25 počítačů a více jednou ročně návštěvu našeho technika. Zahrnuje max. 4 hodiny práce technika na místě + cestu. Možno čerpat jako školení, konzultaci nebo pomoc s instalací a nasazením.

Antivirová ambulance

Služba je poskytována online pomocí vzdáleného připojení po předchozí dohodě s technikem. Služba neslouží k odvirování všech počítačů ve firemním prostředí, ale jako konzultace, kdy je na základě vzorku postižených stanic technikem navržen optimální postup pro odvirování ostatních počítačů.

Školení a konzultace

Školení a konzultace vedené certifikovaným technikem v sídle společnosti ESET v maximálním rozsahu 4 hodiny.

* Po předchozí domluvě s technikem.

Kontrola aplikací

Umožňuje administrátorovi monitorovat instalované aplikace, blokovat přístup k definovaným aplikacím a vyzve uživatele k odinstalaci určité aplikace.

Nastavení kontroly aplikací	Umožňuje zablokovat definované aplikace podle a) kategorií - hry, sociální sítě atd. b) práv – kam aplikace přistupují c) zdroje – mimo Googleplay apod. Umí vytvořit výjimky na základě whitelistů a seznam povinně instalovaných aplikací.
Audit aplikací	Zobrazí přístupová práva všech nainstalovaných aplikací ve skupinách. Dozvíte se tak, k jakým informacím daná aplikace přistupuje.

Správa

Import a export nastavení	Umožňuje přenášet nastavení telefonů/ tabletů na jiná firemní zařízení. Nastavení se vyexportuje do souboru, který se následně použije pro import.
Centrum upozornění	Uživatel si může pročíst všechny důležitá upozornění i s doporučeným řešením.
Lokální administrace	Zařízení je možné spravovat i lokálně. Všechna nastavení jsou chráněna administrátorským heslem, proto nelze libovolně měnit kritické parametry.
Vylepšená identifikace zařízení	Při instalaci se zařízení zároveň dostane na whitelist, takže se do ERA mohou zapojit jen autorizovaná zařízení. To značně zjednodušuje jednotlivou identifikaci zařízení – podle jména, popisu a IMEI.
Průvodce nastavení	Vybrané funkce je možné nastavit pomocí jednoduchého průvodce po instalaci, což se hodí v případech, kdy se zařízení spravuje lokálně.
Vzdálená správa	Produkt podporuje připojení do nástroje vzdálené správy ESET Remote Administrator, který umožňuje nastavit a spravovat bezpečnostní politiky, sbírat logy, dostávat upozornění a mít přehled nad celkovou bezpečnostní situací v síti – vše pomocí jedné webové konzole.
Správce licencí	Umožňuje transparentně spravovat/spojovat/ delegovat všechny licence z jednoho místa pomocí webového prohlížeče v reálném čase, i mimo ESET Remote Administrator.