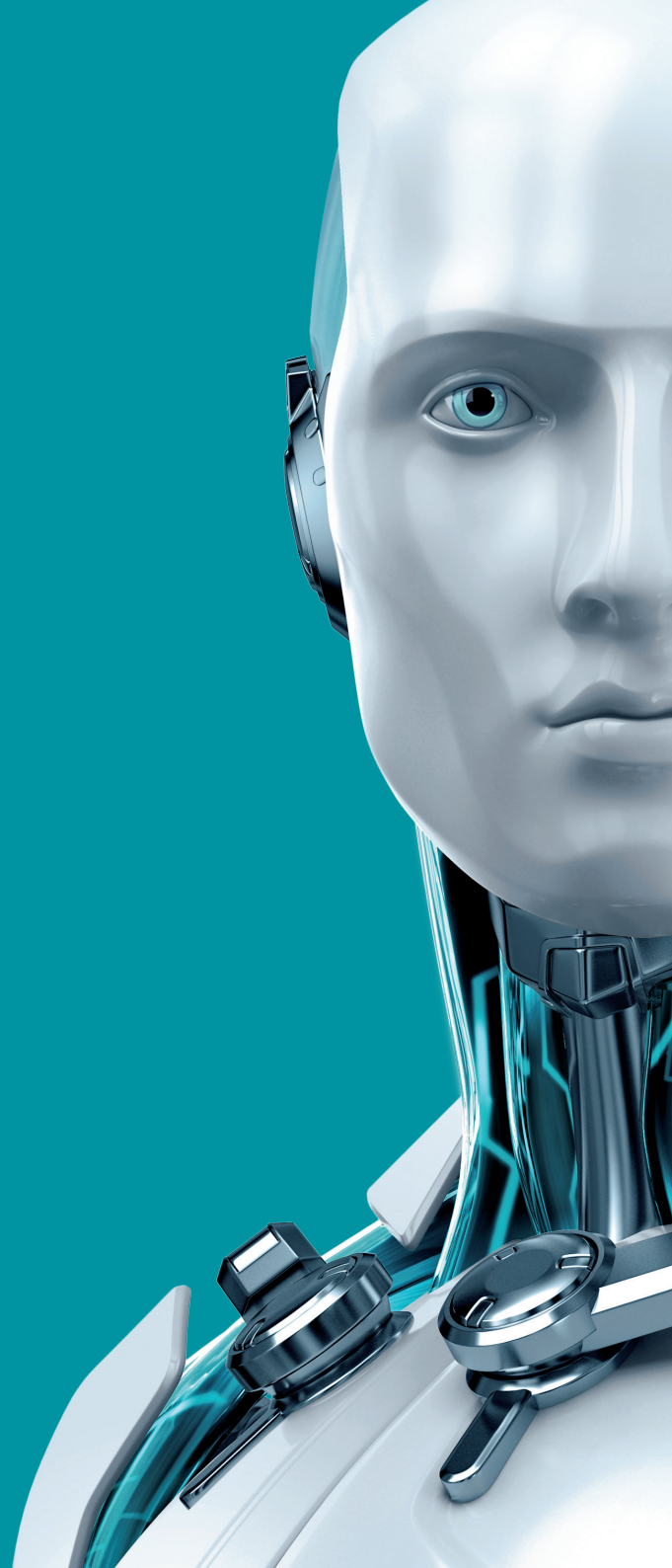
ENDPOINT SECURITY

FOR ANDROID

BUSINESS

ENJOY SAFER TECHNOLOGY™



ENDPOINT SECURITY
FOR ANDROID

ESET Endpoint Security for Android защитава мобилните устройства на компанията чрез доказалата се технология ESET NOD32®.

Предлагаме ви надеждно сканиране на всички приложения, файлове и карти памет. Системата против кражби защитава устройствата на физическо ниво и позволява отдалеченото им блокиране или изтриването на всички данни. Потребителите са защитени от нежелани обаждания и SMS съобщения, а администраторите могат да прилагат ограничения в съвместимост с фирмената политика.

Защита за крайни потребители

Защита в реално време	Защитава всички файлове и приложения в реално време чрез оптимизираната за мобилни платформи технология ESET NOD32®. Интегрираната система за анализ на заплахи ESET LiveGrid® , в комбинация с дълбокото сканиране, защитава всичките ви мобилни устройства от заплахи.
Сканиране	Предоставя надеждно сканиране и почистване на вътрешната памет и SD карти. Сканирането се извършва във фонов режим и може да бъде спряно. Можете също да създавате и график за сканиране.
Сканиране в режим на зареждане	Позволява напълното сканиране на устройството когато то не е заето и е в режим на зареждане, докато екранът е изключен.
Антифишинг	Защитава потребителите от измамни уебсайтове, които целят да придобият информация като пароли, данни за онлайн банкиране и други.
Защита против деинсталиране	Не позволява приложението да бъде деинсталирано без въвеждането на администраторска парола.
Филтър за обаждания и SMS	Защитава потребителите от нежелани обаждания и съобщения* от скрити номера или предварително зададени такива с възможност за настройка на забрани в определен времеви диапазон.
	*Поради промени в системата Android, направени от Google (от версия 4.4 Kitkat), функцията за SMS блокиране не е налична.

Сигурност на устройството

Позволява на администраторите да налагат основни политики за сигурност за всички мобилни устройства на фирмата. Приложението автоматично известява потребителя и администратора когато настройките на устройството са несъвместими с фирмените политики за сигурност и препоръчва промени.

Настройки за сигурността на устройството	Определяйте минималното ниво на сложност за пароли Настройте максимален брой опити за отключване преди изтриване на данните Задайте максимален срок за подменяне на кодове за отключване Задайте таймер за заключване на екрана Напомняйте на потребителите да криптират устройствата Забранете използването на камерата

Политика за настройките на устройствата – позволява на администраторите да наблюдават настройките, за да определят дали са съвместни с фирмената политика. Може да се наблюдават и използването на паметта, Wi-Fi свързаност, роуминг за повиквания и мобилни данни, източници на приложения, NFC и криптиране на вътрешната памет.

Система против кражби

Задействане на команди	Всички отдалечени команди могат да се задействат чрез ESET Remote Administrator, чрез SMS с код за дву-факторна оторизация или директно от администраторския интерфейс на продукта. Това е особено полезно за компании, които не използват отдалечена администрация или когато администраторът е извън офиса.
Отдалечено заключване	Позволява отдалеченото заключване на загубени или откраднати устройства. След заключване, данните на устройството стават недостъпни за външни лица. При намиране или връщане на устройството, то може да се отключи с отдалечена команда.
Отдалечена локализация	Определя местоположението на устройството и го следи чрез GPS.
Отдалечено изтриване	Безопасно унищожава всички контакти, съобщения и файлове в паметта на телефона по начин, който не позволява информацията да бъде възстановена. След изтриването, ESET Endpoint Security for Android остава инсталирано на устройството, позволявайки изпълнението на още команди.
Включване на сирена	Когато е включена, тази функция пуска сирена на устройството, без значение дали звукът е намален. Същевременно забранява изключването на звука.
Отдалечено връщане към фабрични настройки	Унищожава всички данни на устройството чрез изтриване на файловите хедъри и връща всички настройки към фабричните им стойности.
Показване на съобщения	Администраторът може да изпрати специфично съобщение към индивидуално устройство или група от такива. Съобщението ще бъде показано като поп-ъп, за да не бъде игнорирано.
Lock Screen информация	Позволява задаването на информация, която да се показва на екрана на телефона, когато е заключен (фирма, номер, съобщение). Така, при намиране на устройството, то може да бъде върнато по-лесно..
Доверени SIM карти	Когато непозната SIM карта бъде вкарана в устройството, то се заключва. Информация за картата не се изпраща към администратора.
Контакти на администратор	Съдържа списък с телефонни номера, защитени с администраторска парола. Устройството ще приема SMS команди само от тези номера. Номерата се използват и за известия от системата против кражби.

БЕЗПЛАТНА ТЕХНИЧЕСКА ПОДДРЪЖКА НА БЪЛГАРСКИ ЕЗИК

Постигнете повече с помощта на нашите експерти, които ще ви асистират и съветват по телефона.

Контрол над приложенията

Дава възможност на администраторите да наблюдават инсталираните приложения, да блокират достъпа до неодобрени такива и да съобщават на потребите, че трябва да деинсталират определено приложение.

Настройки за контрола	Ръчно определяйте кои приложения да бъдат блокирани. Блокирайте определени категории приложения - игри, социални мрежи и други. Блокиране на база разрешения - когато приложенията искат достъп до местоположение, списък с контакти и други. Блокиране на база източник - неофициалните приложения биват блокирани. Изключения при правилата за блокиране – позволявайте само определени приложения. Създайте набор от задължителни за инсталиране приложения.
Одит на приложения	Следи приложенията и техния достъп до лични/фирмени данни по категории, позволявайки на администраторите да контролират нивото на достъп.

Допълнителна функционалност и управление

Импортиране/експортране на настройки	Ако мобилните устройства не се управляват чрез ESET Remote Administrator, администраторът лесно може да сподели настройките от едно мобилно устройство към друго, като ги запази като файл и ги зареди в другите устройства.
Център за известията	Потребителят може да вижда всички известия на едно място, заедно със съвети за разрешаването на проблеми. Това прави спазването на фирмените политики още по-лесно.
Локална администрация	Администраторът може да управлява всички устройства локално, дори и да не използва ESET Remote Administrator. Всички настройки на локалното приложение за администрация се предпазват чрез парола, което ви осигурява пълен контрол.
Подобрено разпознаване на устройствата	При добавянето на устройства към ESET Remote Administrator, те автоматично биват добавени към списък с тяхното име, модел и IMEI номер. Това ви позволява много по-лесно да идентифицирате специфично устройство.
Помощници за настройка	След инсталацията, софтуерни помощници ще ви асистират при настройката на различни типове функционалност, което прави процесът по локално внедряване на настройките много по-бърз.
Отдалечено управление	Устройствата на крайните потребители могат лесно да бъдат управлявани чрез ESET Remote Administrator. Създавайте и изпълнявайте задачи, задавайте графици, събирайте логове и получавайте известия за цялостното състояние на мрежата ви – изцяло през достъпна уеб конзола.
Администратор за лицензи	Позволява ви да управлявате лицензите си централизирано, през уеб браузър. Можете да сливате, раздавате и контролирате всички лицензи в реално време, дори и да не използвате ESET Remote Administrator.