PRODUKTOVÝ LIST

MOBILE PROTECTION

Zabezpečení a správa firemních mobilních zařízení

ENJOY SAFER TECHNOLOGY™

Co je **ESET Mobile Protection?**

Produkty pro ochranu mobilních zařízení (Android, iOS) lze rozdělit do dvou kategorií: zabezpečení a správa.

Do zabezpečení řadíme funkce jako antimalware, anti-phishing, omezení přístupu k nezabezpečeným připojením a mnohé další. Funkce jako vzdálené smazání zařízení, pravidla pro instalaci aplikace, změny nastavení zařízení a podobně sice mobilní zařízení primárně nechrání, ale jsou důležité pro jeho celkové zabezpečení.

Je důležité poznamenat, že mobilní zařízení od společnosti Apple neumožňují využití všech bezpečnostních funkcí, jako je antimalware, a to z důvodu restrikcí na úrovni operačního systému. Z tohoto důvodu mají zařízení Apple k dispozici pouze část pro správu mobilního zařízení.

Proč **chránit mobilní zařízení?**

RANSOMWARE

Až do roku 2014 se ransomware týkal převážně klasických počítačů a serverů. V daném roce se poprvé objevil i na zařízeních s operačním systémem Android. Šlo o variantu škodlivého kódu Simplocker. A úspěch útočníky povzbudil natolik, že postupně do ransomwaru pro mobilní zařízení přidávali další techniky a funkce pro ještě efektivnější vydírání oběti.

ESET Endpoint Security pro Android chrání mobilní zařízení nejen před ransomwarem, ale také před ostatními hrozbami na internetu. Úspěšná detekce ransomwaru je základem boje proti tomuto škodlivému kódu, protože každé další zaplacení výpalného jenom povzbudí tvůrce k další aktivitě.

UKRADENÁ NEBO ZTRACENÁ ZAŘÍZENÍ

V současnosti firmy obvykle umožňují zaměstnancům pracovat mimo firmu (doma, v kavárně), což zvyšuje nejen nároky na zabezpečení, ale také pravděpodobnost, že dojde ke ztrátě nebo odcizení zařízení. Firemní mobilní zařízení mohou obsahovat kromě klasických dokumentů a e-mailů také další citlivá data, která může útočník zneužít a negativně ovlivnit reputaci firmy.

Produkty ESET určené k ochraně a správě mobilních zařízení (MDM) umožňují firmám je vzdáleně uzamknout nebo vymazat. Tím mají jistotu, že nedojde k zneužití citlivých firemních dat v případech krádeže zařízení nebo rozvázání pracovního poměru.

SPRÁVA ZAŘÍZENÍ

Organizace a firmy obvykle z bezpečnostních důvodů chtějí zajistit, aby zaměstnanci používali svěřená zařízení pouze k pracovním účelům. Proto je žádoucí, aby správci měli možnost zajistit, že se zařízení nepřipojí do nezabezpečené sítě a nemá zapnuté potenciálně nebezpečné funkce.

Řešení ESET pro mobilní platformy umožňují správcům definovat, jaké aplikace může uživatel instalovat, na jaká čísla může volat, zda je integrovaná kamera zapnutá nebo vypnutá a podobně. Tato nastavení může správce vynutit bezpečnostní politikou, kterou lze v případě potřeby časově omezit, například pouze na pracovní dobu.

První ransomware pro Android se objevil v roce 2014 v podobě Simplockeru.

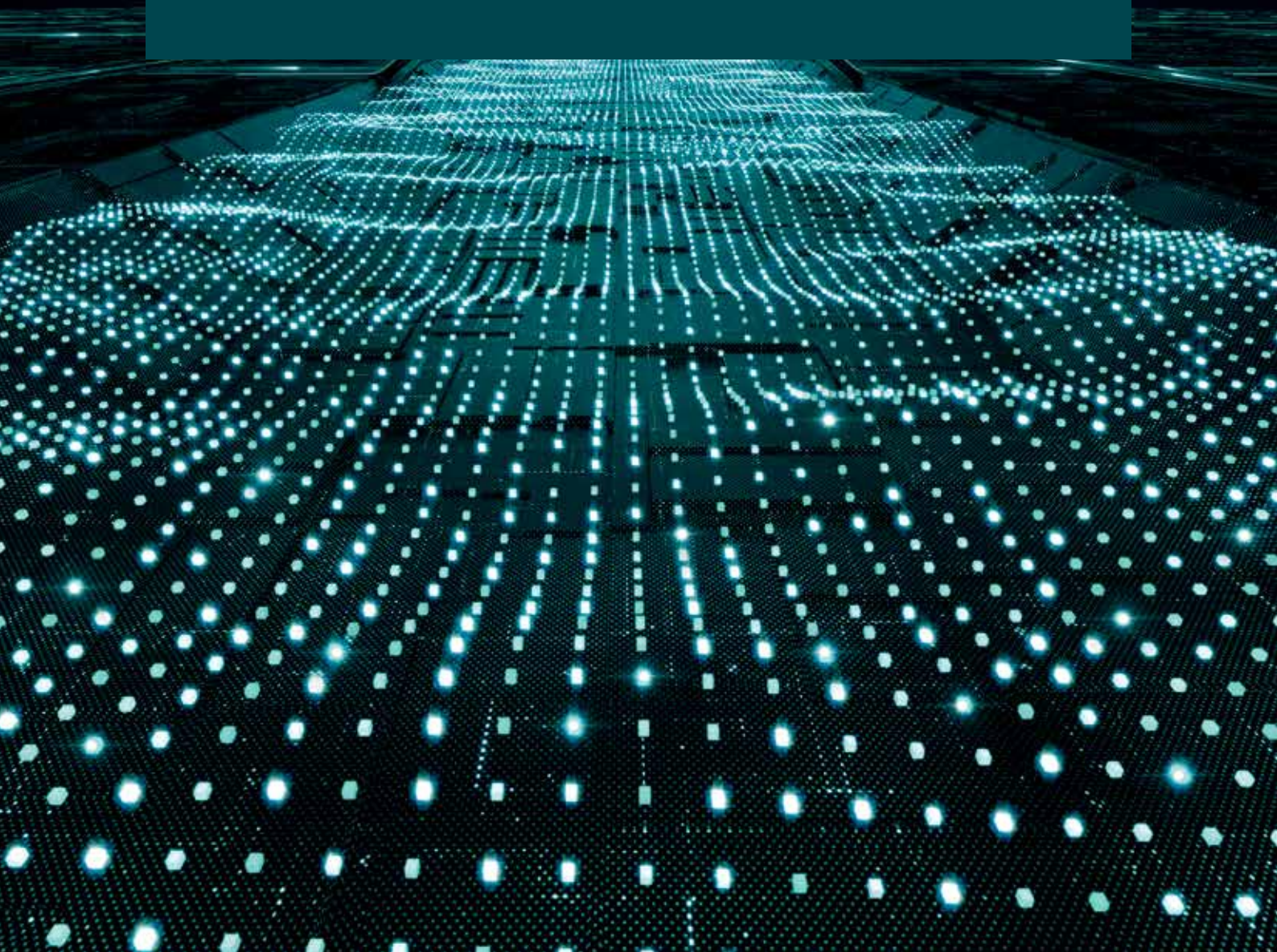
Možnost pracovat mimo firmu zvyšuje nároky na zabezpečení zařízení pro případ ztráty nebo odcizení. Zařízení totiž mohou obsahovat i citlivá data, která v případě zneužití mohou poškodit reputaci firmy.

Úspěšná detekce ransomwaru je základem boje proti tomuto škodlivému kódu, protože každé další zaplacení výpalného jenom povzbudí tvůrce k další aktivitě.

Pro správu mobilních zařízení není třeba žádné další dedikované řešení. Přehled o všech mobilních i dalších koncových zařízeních z jediného místa zajistí nástroj vzdálené správy ESET Security Management Center.

"Hlavní výhodou ESETu je, že máte všechny uživatele v jedné konzoli, kde je můžete spravovat a máte přehled o jejich bezpečnostním stavu."

Jos Savelkoul, Team Leader ICT-Department; Zuyderland Hospital, Netherlands; 10.000+ seats



Výhody ESETu

POŘIZOVACÍ NÁKLADY

Pro správu mobilních zařízení není třeba žádné další dedikované řešení. Přehled o všech mobilních i dalších koncových zařízeních z jediného místa zajistí nástroj vzdálené správy ESET Security Management Center.

KVALITNÍ OCHRANA

Společnost ESET kombinuje technologie ochrany, strojového učení a lidské odbornosti způsobem, který zajišťuje zákazníkům nejvyšší úroveň ochrany. Své technologie neustále vyvíjí a vylepšuje, aby dosáhl nejlepšího poměru mezi detekcí, falešnými poplachy a výkonem.

ESET LIVEGRID

Když dojde k detekci nového škodlivého kódu, odešle se podezřelý soubor do cloudového systému ESET LiveGrid, kde dojde k jeho podrobné analýze. Její výsledek je ihned poskytnut všem zapojeným mobilním zařízením, bez nutnosti čekat na aktualizaci virové databáze.

OVĚŘENÉ TECHNOLOGIE

Společnost ESET se pohybuje na trhu IT zabezpečení přes 30 let a neustále vyvíjí své technologie tak, aby byly před tvůrci škodlivého kódu vždy napřed. Výsledkem je důvěra více než 110 milionů uživatelů po celém světě..

NÍZKÉ SYSTÉMOVÉ NÁROKY

Při pořizování bezpečnostního řešení jsou důležitým kritériem také systémové nároky. Produkty ESET mnohokrát zvítězily v nezávislých testech třetích stran, které se týkaly dopadu na výkon operačního systému.

CELOSVĚTOVÁ PŮSOBNOST

ESET má po celém světě 22 poboček, 13 vývojových a výzkumných center a působí ve více než 200 zemích. Díky tomu může pružně reagovat na aktuální dění, trendy a vznikající IT hrozby na všech kontinentech.

"Bezpečnostní řešení ESET ochránila a upozornila naše oddělení na mnohé hrozby a infekce, hlavně na ransomware."

Joshua Collins, Data Center Operations Manager; Primoris Services Corporation, USA; 4.000+ seats

Příklady použití

Ransomware

Ransomware už není hrozbou jen pro klasické počítače a servery, od roku 2014 útočí i na mobilní zařízení. Firmy chtějí mít jistotu, že data na mobilních zařízeních nelze zneužít k požadování výpalného.

ŘEŠENÍ

- ✓ Instalace ESET Endpoint Security na všechna mobilní zařízení zajistí ochranu před všemi druhy škodlivého kódu, včetně ransomwaru.
- ✓ Zákaz instalace aplikací z neznámých zdrojů.

Ztráta dat

Firma požaduje, aby data na mobilních zařízeních byla chráněna i v případech ztráty nebo odcizení zařízení.

ŘEŠENÍ

- ✓ Zavedení bezpečnostní politiky, která vyžaduje šifrování zařízení.
- ✓ Zavedení politiky, která vynutí pro odemykání zařízení heslo nebo PIN.
- ✓ Správce musí mít možnost zařízení vzdáleně zamknout nebo vymazat.

Dodržování předpisů

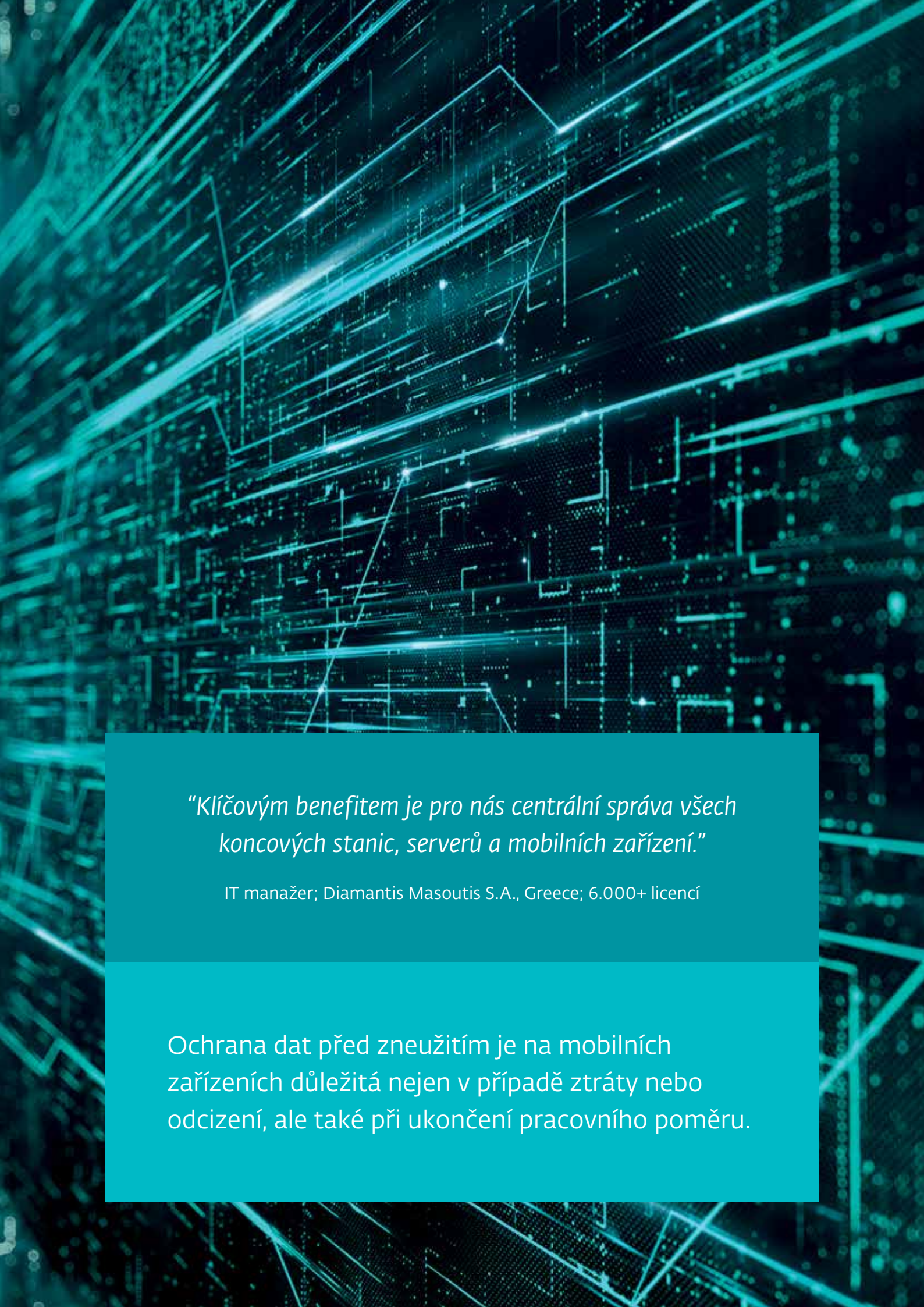
Jednotlivé organizace mají rozdílné politiky související s používáním mobilních zařízení. Jejich správci potřebují zajistit, že všechna zařízení zůstávají nastavena v souladu s definovanými požadavky..

ŘEŠENÍ

- ✓ Povolení instalace pouze vybraných aplikací.
- ✓ Zákaz připojení k nezabezpečené síti Wi-Fi.
- ✓ Zajištění implementace a zapnutí všech požadovaných bezpečnostních funkcí.

ESET ENDPOINT SECURITY
PRO ANDROID

ESET MOBILE DEVICE MANAGEMENT
PRO APPLE iOS



"Klíčovým benefitem je pro nás centrální správa všech koncových stanic, serverů a mobilních zařízení."

IT manažer; Diamantis Masoutis S.A., Greece; 6.000+ licencí

Ochrana dat před zneužitím je na mobilních zařízeních důležitá nejen v případě ztráty nebo odcizení, ale také při ukončení pracovního poměru.

Technické funkce

Android /iOS

ANTI-THEFT

Správce může v případě potřeby zařízení vzdáleně zamknout, smazat nebo zapnout zvukovou sirénu. Dále může na zařízení poslat zprávu s informacemi o majiteli, která se zobrazí na zamykací obrazovce.

KONTROLA APLIKACÍ

Umožňuje administrátorovi monitorovat instalované aplikace, blokovat přístup k definovaným aplikacím nebo jejich kategoriím či vyzvat uživatele k odinstalování určité aplikace.

ZABEZPEČENÍ ZAŘÍZENÍ

Administrátor může definovat požadavek na silné heslo, nastavit maximální počet pokusů pro odemknutí zařízení, vyzvat uživatele k šifrování zařízení, zablokovat integrovanou kameru a další.

VZDÁLENÁ SPRÁVA

Produkty je možné spravovat z jediného místa pomocí nástroje vzdálené správy, který je možné nainstalovat nejen na zařízení s Windows, ale také na linuxové servery nebo využít již připravenou Virtual Appliance.

Pouze Android

VÍCESTUPŇOVÁ OCHRANA

Jedna vrstva již na ochranu zařízení nestačí. Produkt dokáže detekovat škodlivý kód ve všech fázích útoku (před spuštěním, při spuštění a po nákaze).

STROJOVÉ UČENÍ

Všechny produkty ESET obsahují strojové učení od roku 1997. ESET v současné době využívá strojové učení ve spojení se všemi ostatními technologiemi ochrany.

ANTI-PHISHING

Chrání před podvodnými stránkami, které se snaží získat citlivé informace, jako je uživatelské jméno, heslo, podrobnosti o kreditních kartách nebo bankovnictví.

AUDIT APLIKACÍ

Zobrazí přístupová práva všech nainstalovaných aplikací ve skupinách. Dozvíte se tak, k jakým informacím daná aplikace přistupuje.

Pouze iOS

APPLE IOS MANAGEMENT FRAMEWORK

Integrace správy mobilních zařízení pro iOS do ESET Security Management Center umožňuje nastavení parametrů mobilních zařízení s operačním systémem iOS z jednoho centrálního místa.

PUSH ACCOUNT SETTINGS REMOTELY

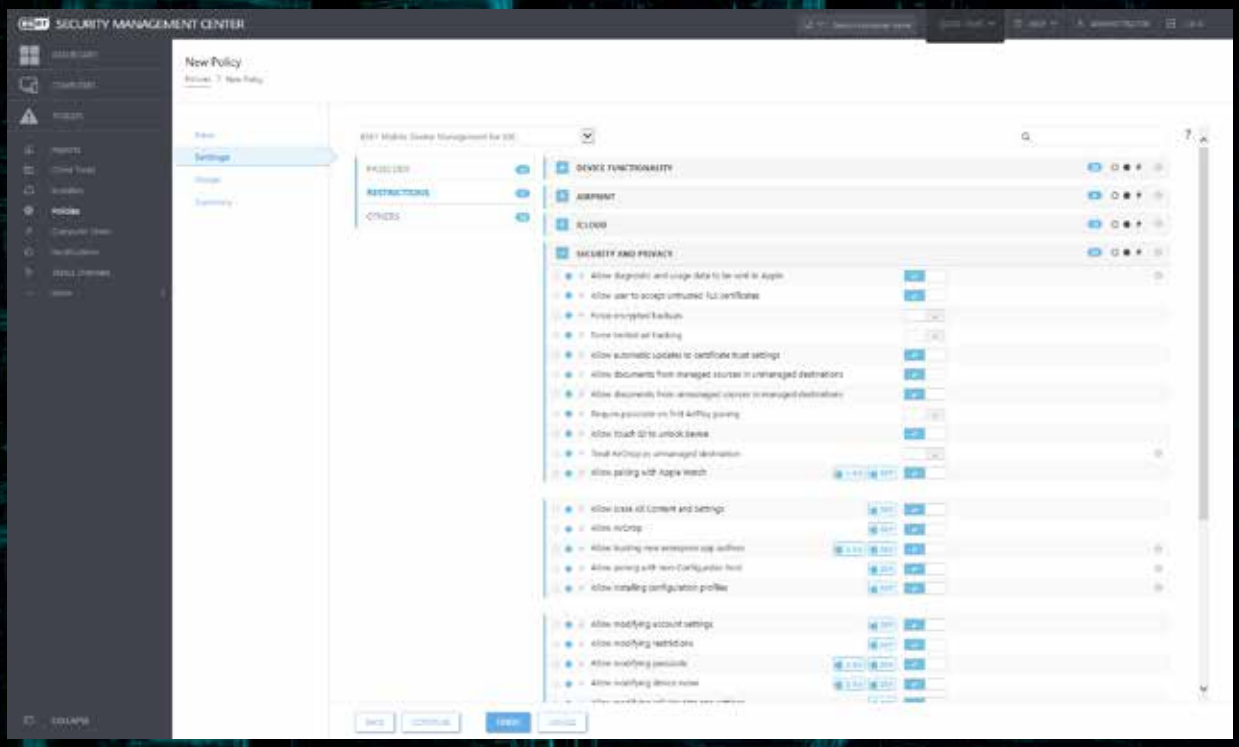
Umožňuje správci vzdáleně vynutit nastavení účtů pro Wi-Fi, VPN nebo Exchange.

MOBILE DEVICE MANAGEMENT

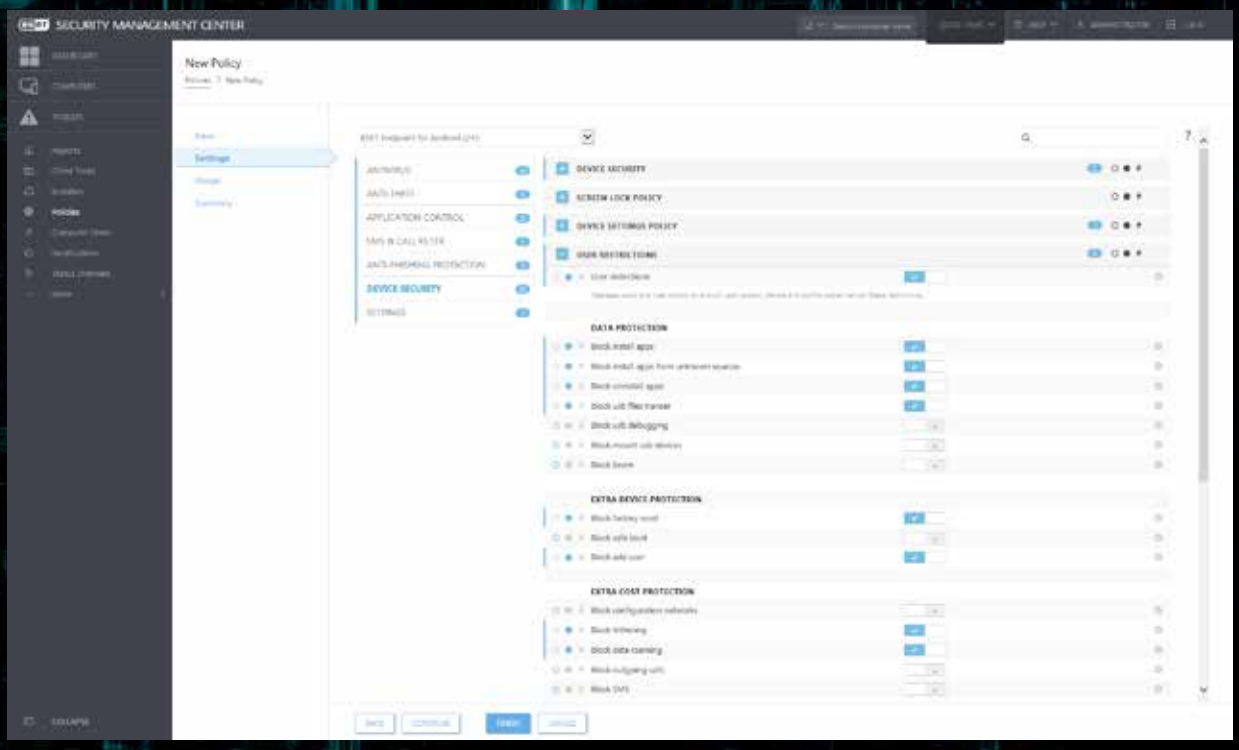
Správce automaticky dostane upozornění v případě, kdy zařízení není v souladu s firemní bezpečnostní politikou. Upozornění zároveň doporučí další postup.

Dostupnost výše uvedených funkcí závisí na omezeních systému Android / iOS a na verzi mobilního operačního systému.

ESET SECURITY MANAGEMENT CENTER
NASTAVENÍ PRO IOS MDM



ESET SECURITY MANAGEMENT CENTER
NASTAVENÍ PRO ANDROID



ENJOY SAFER TECHNOLOGY™