



# FIREMŇÍ ŘEŠENÍ



ENJOY SAFER TECHNOLOGY™



# Co jsou balíky **ESET Secure?**

**Při každodenním používání bezpečnostního softwaru jsou nejdůležitější jeho vlastnosti. V ESETu věříme, že firemní řešení má být rychlé, s kvalitní detekcí malwaru a vzdálenou správou. Proto jsme vytvořili balíky bezpečnostních řešení ESET Secure, ve kterých jsme zohlednili naše více než 30leté zkušenosti v oboru.**

V rámci jednotlivých balíčků je možné používat různé produkty podle aktuální potřeby na různých operačních systémech (Windows, Mac, Linux a Android) a zařízeních (počítače, smartphony, tablety a servery). Naše produkty byly navrženy s ohledem na nízké systémové nároky, které umožňují provozovat bezpečnostní řešení i na starším hardwaru. Produkty jsou optimalizované pro provoz ve virtuálním prostředí. Kompletní přehled o bezpečnosti koncových stanic lze získat s pomocí uživatelsky příjemného nástroje pro vzdálenou správu.

# Dostupné balíky

## ESET SECURE OFFICE

Chrání pracovní stanice (počítače, smartphony, tablety a souborové servery) před všemi typy hrozeb. ESET Secure Office poskytuje základní antivirovou ochranu firemních zařízení, jež je možné vzdáleně spravovat z jedné webové konzole.



## ESET SECURE OFFICE CLOUD

Jak už název napovídá, balík obsahuje stejné produkty a funkce jako ESET Secure Office. Vzdálená správa je umístěna v cloudu.

## ESET SECURE OFFICE+

ESET Secure Office+ přidává do firemní sítě oproti základnímu balíku další vrstvy ochrany, jako jsou Ochrana proti zapojení do botnetu, Antispam, Firewall nebo Kontrola přístupu na web. Vzdálená správa je snadno dostupná přes webové rozhraní.



## ESET SECURE OFFICE CLOUD+

Při zakoupení balíku můžete instalovat stejné produkty jako u ESET Secure Office+. Zařízení ale můžete vzdáleně spravovat v ESET Cloud Administratoru.

## ESET SECURE BUSINESS

ESET Secure Business obsahuje všechny bezpečnostní technologie a funkce řady Office+ a je vhodný pro firmy, které kromě pracovních stanic potřebují chránit i poštovní servery. Vzdálenou správu je možné naistalovat na zařízení s Windows, Linuxem nebo využít připravenou Virtual Appliance.



## ESET SECURE BUSINESS CLOUD

Pokud nepotřebujete nebo nechcete používat vzdálenou správu on-premise, pak vyberte tento balík. Produkty pro koncové stanice se neliší, jen vzdálená správa je v cloudu.



PRACOVNÍ STANICE



MOBILNÍ ZAŘÍZENÍ



PODPORA VIRTUALIZACE



SOUBOROVÝ SERVER



FIREWALL A ANTISPAM



POŠTOVNÍ SERVER



ADMINISTRACE V CLOUDU

ESET SECURE OFFICE  
 ESET SECURE OFFICE+  
 ESET SECURE BUSINESS  
 ESET SECURE BUSINESS CLOUD  
 ESET SECURE OFFICE+ CLOUD  
 ESET SECURE OFFICE CLOUD

	PRACOVNÍ STANICE	MOBILNÍ ZAŘÍZENÍ	PODPORA VIRTUALIZACE	SOUBOROVÝ SERVER	FIREWALL A ANTISPAM	POŠTOVNÍ SERVER	ADMINISTRACE V CLOUDU
ESET SECURE OFFICE	■	■	■	■	■	■	■
ESET SECURE OFFICE+	■	■	■	■	■	■	■
ESET SECURE BUSINESS	■	■	■	■	■	■	■
ESET SECURE BUSINESS CLOUD	■	■	■	■	■	■	■
ESET SECURE OFFICE+ CLOUD	■	■	■	■	■	■	■
ESET SECURE OFFICE CLOUD	■	■	■	■	■	■	■

# Rozdíl mezi produkty ESET Cloud Administrator a ESET Security Management Center?

ESET Cloud Administrator je určen pro SMB a nenabízí veškerou funkcionalitu jako ESET Security Management Center. Základ je identický, ale produkty se od sebe liší možnostmi správy, způsobem přidávání počítačů atp. V tabulce níže uvádíme zásadní rozdíly mezi cloudovou a on-premise variantou konzole pro vzdálenou správu.

Funkce	ESET Cloud Administrator	ESET Security Management Center
Prostředí	Běží v cloudu společnosti ESET	Běží na vámi spravovaném serveru
Údržba a aktualizace	Zajišťuje společnost ESET	Plně ve vaší kompetenci administrátora
Omezení počtu zařízení	5 až 250	Neomezeně (limitujícím faktorem je vámi použitý hardware)
Podporované koncové OS	Windows a macOS	Windows, Linux, macOS, Android, iOS
Synchronizace s Active Directory	Ne	Ano
Dynamické skupiny	Předdefinované společnosti ESET	Můžete si vytvářet vlastní
Oznámení	Předdefinované společnosti ESET	Můžete si vytvářet vlastní
Přehledy	Můžete si vytvářet vlastní	Můžete si vytvářet vlastní
Certifikáty	Spravuje společnost ESET	Plně ve vaší kompetenci administrátora
Přístupová oprávnění	Reflektují oprávnění z ESET Business Account	Plně ve vaší kompetenci, přístup můžete delegovat na konkrétní objekty

# Firemní řešení obsahují

## Pracovní stanice

**ESET ENDPOINT ANTIVIRUS PRO WINDOWS**

**ESET ENDPOINT ANTIVIRUS PRO MACOS**

**ESET NOD32 ANTIVIRUS BUSINESS EDITION PRO LINUX DESKTOP**

Antivirus a Antispyware	Odstraňuje všechny typy hrozeb včetně virů, rootkitů, červů a spywaru.
Anti-Phishing	Chrání uživatele před pokusy získat jejich citlivé informace, jako jsou hesla nebo bankovní data.
UEFI Skener	Chrání počítač před útoky již před startem Windows – na systémech s rozhraním UEFI.
Exploit Blocker	Chrání často zneužívané aplikace, jako jsou prohlížeče, čtečky PDF nebo poštovní klienti.
Pokročilá kontrola paměti	Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti.
Host-Based Intrusion Prevention	Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory.
Kontrola zařízení	Umožňuje blokovat nebo povolit konkrétní výměnná média, jako jsou CD, DVD, USB apod.
Ochrana proti zapojení do botnetu	Chrání počítač před připojením do škodlivé sítě, která může zneužít nakažené zařízení k rozesílání spamu a útokům na další počítače.
Ochrana proti ransomwaru	Produkty ESET obsahují několik na sobě nezávislých vrstev ochrany před ransomwarem. Vedle cloudového systému ESET LiveGrid a DNA detekcí i Ransomware Shield, který v reálném čase sleduje veškeré běžící procesy a pomocí behaviorální analýzy odhaluje škodlivý kód podle jeho chování.

## Podpora virtualizace

**ESET VIRTUALIZATION SECURITY PRO VMWARE**

**ESET SHARED LOCAL CACHE**

ESET Virtualization Security pro VMware vShield	Umožňuje standardní AV ochranu virtuálních strojů bez nutnosti instalace jakéhokoliv bezpečnostního produktu do jejich OS. Skenovací úlohy se zpracovávají pouze v centrálním skeneru uvnitř řešení.
ESET Shared Local Cache	Jednou kontrolované soubory na virtuálním stroji se už podruhé v rámci jednoho virtuálního prostředí na jiném stroji nekontrolují, což má značný dopad na rychlost skenování souborů.

Poznámka: Funkce se liší v závislosti na operačním systému.

# Mobilní zařízení

## ESET ENDPOINT SECURITY PRO ANDROID

## ESET MOBILE DEVICE MANAGEMENT PRO APPLE IOS

Ochrana v reálném čase	Kontroluje všechny aplikace a navázané komunikace kvůli možné přítomnosti škodlivého kódu.
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 bankovníctví.
Kontrola aplikací	Umožňuje správci monitorovat instalované aplikace, blokovat přístup nebo blokovat definované aplikace.
Anti-Theft	Chrání zařízení pomocí funkcí vzdáleného zamknutí, lokalizace, vzdáleného smazání a dalších.
Bezpečnost zařízení	Umožňuje správci uplatňovat základní bezpečnostní politiky na firemních mobilních zařízeních.
Filtr hovorů a volání	Na zařízení se dovolá a pošle zprávu jen určená osoba.
Správa mobilních zařízení s iOS	Umožňuje aplikovat vzdáleně jednotnou bezpečnostní politiku na všechna firemní mobilní zařízení s iOS.
Vzdálená správa	Nabízí správci celkový přehled o bezpečnostní situaci v síti pomocí jedné webové konzole.

# Souborový server

## ESET FILE SECURITY PRO MICROSOFT WINDOWS SERVER

## ESET FILE SECURITY PRO LINUX / BSD / SOLARIS

Antivirus a Antispyware Anti-Phishing	Odstraňuje všechny typy hrozeb včetně virů, rootkitů, červů a spywaru.
Exploit Blocker	Chrání často zneužívané aplikace, jako jsou čtečky PDF, poštovní klienti nebo MS Office.
Pokročilá kontrola paměti	Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti.
UEFI Skener	Chrání počítač před útoky již před startem Windows – na systémech s rozhraním UEFI.
Nativní podpora clusterů	Umožňuje nastavit řešení tak, aby docházelo k replikaci nastavení při instalaci v prostředí clusterů.
Kontrola úložiště	Dovolí jednoduše nastavit volitelné kontroly na připojených NAS discích.
WMI (Windows Management Instrumentation)	Poskytuje možnost monitorovat klíčové funkce produktu pomocí frameworku WMI.
Modulární instalace	Umožňuje zvolit, jaké moduly se mají nainstalovat.
Hyper-V Storage sken	Kontroluje Microsoft Windows servery s aktivní rolí Hyper-V na přítomnost malwaru, bez nutnosti mít další instanci antivirového produktu. Šetří čas a nabízí jednotlivé reporty v závislosti na výsledcích kontroly. Pro lepší výkon, menší spotřebu paměti a vytižení CPU je možné provádět kontroly na vypnutých virtuálních strojích.
Ochrana proti zapojení do botnetu	Technologie chrání počítač před připojením do škodlivé sítě, která může zneužít nakažené zařízení k rozesílání spamu a útokům na další počítače.

Poznámka: Funkce se liší v závislosti na operačním systému.

# Firewall a Antispam

## ESET ENDPOINT SECURITY PRO WINDOWS

## ESET ENDPOINT SECURITY PRO MACOS

Antivirus a Antispyware	Odstraňuje všechny typy hrozeb včetně virů, rootkitů, červů a spywaru.
Anti-Phishing	Chrání uživatele před pokusy získat jejich citlivé informace, jako jsou hesla, bankovní data.
Podpora virtualizace	Metadata souborů se v rámci daného virtuálního prostředí skenují pouze jednou.
Exploit Blocker	Chrání často zneužívané aplikace, jako jsou čtečky PDF, poštovní klienti nebo MS Office.
Pokročilá kontrola paměti	Monitoruje chování škodlivých procesů a kontroluje je ihned po rozbalení v paměti.
Ochrana proti zapojení do botnetu	Chrání před infiltrací botnetovým malwarem a zabraňuje šíření spamu a síťových útoků z daného zařízení.
Kontrola přístupu na web	Filtruje přístup k internetovým stránkám dle kategorií, např. hry, sociální sítě, nakupování a další.
Firewall	Brání neautorizovanému přístupu do firemní sítě a chrání firemní data před zneužitím.
Antispam	Efektivně filtruje nevyžádanou poštu a kontroluje příchozí zprávy na přítomnost škodlivého kódu.
HIPS (Host-based Intrusion Prevention)	Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory.
Odinstalace jiných řešení	Hledá a odstraní při instalaci jiný bezpečnostní software.

# Poštovní server

## ESET MAIL SECURITY PRO MICROSOFT EXCHANGE SERVER

## ESET MAIL SECURITY PRO IBM LOTUS DOMINO

## ESET MAIL SECURITY PRO LINUX / BSD / SOLARIS

## ESET SECURITY PRO KERIO

Antivirus a Antispyware	Odstraňuje všechny typy hrozeb včetně virů, rootkitů, červů a spywaru.
Antispam a Anti-Phishing	Blokuje nevyžádanou poštu a pokusy o phishing s vysokou úspěšností bez potřeby manuálně upravovat hodnoty SCL (Spam Confidence Level). Po instalaci je antispam plně funkční a není potřeba větší konfigurace.
Správa lokální karantény	Každý uživatel poštovní schránky může pomocí samostatného prohlížeče pracovat se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do poštovní schránky. V závislosti na povolených právech může uživatel třídít/prohledávat zprávy v karanténě a provádět povolené akce. Dostupné akce se liší v závislosti na důvodu uložení do karantény. Uživateli je také možné poslat pravidelný report se seznamem zpráv zařazených do karantény.
Volitelná kontrola databáze	Administrátor může vybrat, jaké databáze nebo poštovní schránky chce zkontrolovat. Kontroly je možné dále upřesnit, aby docházelo k co nejmenšímu využití systémových zdrojů.
Pravidla zpracování zpráv	Nabízejí široké možnosti kombinací, jak se mají zprávy zpracovat. Hodnotící parametry obsahují standardní volby, jako jsou předmět, odesílatel, tělo a hlavička, ale umožňují zvolit i další podmínky v závislosti na předchozím antispamovém filtrování a výsledcích antivirové kontroly. Porušené nebo heslem chráněné archivy jsou detekovány a obsah příloh je kontrolován pro nalezení skutečného typu souboru. Pravidla je možné měnit, aby bylo dosaženo ideálního výsledku.

Poznámka: Funkce se liší v závislosti na operačním systému.



# Vzdálená správa

## ESET SECURITY MANAGEMENT CENTER

<b>ESET Business Account</b>	Umožňuje spravovat všechny licence z jednoho místa skrze webové rozhraní i mimo ESET Security Management Center.
<b>Instalace na stanice</b>	Sestává ze dvou fází. První je instalace agenta, po které následuje instalace produktu. Agent automaticky vybere vhodnou architekturu podle operačního systému. Balíčky lze stahovat ze serverů ESET nebo lokálního úložiště.
<b>Správa založená na rolích</b>	Umožňuje hlavnímu správci vytvořit různé role, kterým lze přiřadit požadovaná oprávnění. Uživatel tak získává práva náležící aplikované roli. V případě instalace ve stromové struktuře může správce vytvořit „super admin“ účet, který může nadefinovat hlavní firemní politiky a práva pro lokální správce, kteří potom mohou spravovat jen svou část sítě. Režim "read only" poskytne správci přehled o bezpečnostní situaci v síti bez možnosti interakce.
<b>Přístup chráněný 2FA</b>	K ověření identity administrátora při přihlášení je možné zapnout dvoufaktorovou autentizaci přímo ve webové konzoli. Zdarma je možné chránit až 10 účtů. Po jednoduchém zápisu v konzoli, uživatel obdrží zprávu SMS s odkazem na stažení mobilní aplikace ESET Secure Authentication. Ta potom generuje náhodná jednorázová hesla, která doplňují a posilují proces autentizace.
<b>Integrovaný ESET SysInspector</b>	Je diagnostický nástroj, který pomáhá při řešení různých problémů u konkrétní koncové stanice. Všechny generované protokoly si správce může prohlédnout přímo ve webové konzoli. Při pravidelném ukládání protokolů, je možné například zpětně sledovat změny v operačním systému při bezpečnostních incidentech.
<b>MDM pro zařízení iOS</b>	Umožňuje administrátorovi udržet jednotnou bezpečnostní politiku na všech firemních mobilních zařízeních s operačním systémem iOS. Po registraci zařízení je možné měnit různá nastavení nebo je vzdáleně vymazat, zamknout či odemknout.
<b>Podpora prostředí VDI</b>	Algoritmus pro získání otisku hardwaru umožní automatickou detekci a řešení klonovaných stanic s operačním systémem Windows.
<b>Inventář hardwaru</b>	Agent dokáže sbírat informace o hardwaru zařízení běžících na Windows, macOS i linuxových systémech.
<b>Inventář softwaru</b>	V podrobnostech o daném počítači IT správce najde informace o veškerém instalovaném softwaru, včetně verze.
<b>Dynamické a statické skupiny</b>	ESET Remote Administrator pracuje na podobném principu jako Active Directory, jehož strukturu umí automaticky načíst a adaptovat. Klienty je možné zařadit do statických nebo dynamických skupin. Pro dynamické skupiny lze nadefinovat podmínky, za kterých dojde k zařazení do skupiny. Stejně tak je možné přiřadit politiku. Celý proces potom probíhá bez interakce ze strany administrátora.
<b>Politiky</b>	Správce může nadefinovat politiky pro každý produkt zvlášť a jednoduše určit jejich vzájemný vztah. Politiky jsou uplatňovány agentem, který je schopen příslušnou politiku uplatňovat i bez připojení k serveru. Správce může také využít předdefinované šablony podle svých potřeb.
<b>Reporty</b>	Správce může vybrat předdefinované šablony nebo vytvořit své vlastní. Stačí použít požadovaná data a hodnoty. ERA sbírá pouze data potřebná k vytvoření reportu, zbývající data zůstávají na klientské straně, což má pozitivní vliv na výkon databáze. Všechny reporty se zobrazují ve webové konzoli a poskytují tak správci přehled o bezpečnostní situaci v síti v reálném čase. Z konzole lze také rychle reagovat na vzniklé události. Reporty je možné uložit na definované místo nebo poslat e-mailem ve formátu PDF.

# Administrace v cloudu

## ESET CLOUD ADMINISTRATOR

<b>Snadné nastavení</b>	Po aktivaci ESET Cloud Administratoru jsou uživatelé v průvodci představeny základní funkce, jako je přidání počítačů, nasazení bezpečnostního produktu a vytvoření chráněné sítě. Po instalaci bezpečnostního produktu se počítače automaticky připojí do ESET Cloud Administratoru.
<b>Rychlé ovládání</b>	Produkt umožňuje provedení různých akcí pomocí jednoho kliknutí myši. Správce tak může rychle aktualizovat všechna bezpečnostní řešení v síti na poslední verzi, spravovat hrozby nebo řešit další úkoly typu aktivace, restart počítače nebo aktualizace operačního systému.
<b>Statické i dynamické skupiny</b>	<p>Každé zařízení je zařazeno do statické skupiny, kterou vytvoří správce dle svých potřeb. Statické skupiny lze řadit do stromové struktury.</p> <p>Dynamické skupiny sdružují zařízení na základě předdefinovaných kritérií. Pokud spravované zařízení kritériím dané skupiny vyhoví, jsou na něj automaticky aplikována příslušná pravidla.</p>
<b>Správa uživatelů</b>	Zařízení připojená do vzdálené správy je možné přiřadit specifickému uživateli. Tato funkce umožňuje správci filtrovat počítače dle uživatelů, prohlédnout si jejich detaily či zkontrolovat stav zařízení, která používají.
<b>Upozornění</b>	Správci potřebují vědět o vznikajících problémech uvnitř sítě v co nejkratším časovém intervalu. Jen tak mohou provést opatření. ESET Cloud Administrator umožňuje správci využít předdefinovaných upozornění, která se po výskytu incidentu ihned zobrazují v konzoli a odesílají na určenou e-mailovou adresu.
<b>Politiky, reporty a úlohy</b>	ESET Cloud Administrator obsahuje sadu vytvořených pravidel, která správce může použít. Pravidla je možné přiřadit skupinám nebo jednotlivým počítačům. Reporty jsou seřazeny do kategorií a rychle dostupné jedním kliknutím myši. Úlohy správce vytvoří z kontextových nabídek, panelů nebo přímo v sekci úloh. Naplňuje čas a podmínky spuštění.
<b>Přehled o incidentech</b>	Na hlavní nástěnce správce najde aktuální stav zabezpečení sítě, včetně informací o čase incidentu, skupinách a údajů o tom, jaké počítače detekovaly hrozbu, a o posledních deseti počítačích a uživateli, kteří zaznamenali bezpečnostní incident.
<b>Inventář hardwaru</b>	ESET Cloud Administrator sbírá a zobrazuje informace o hardwaru spravovaných koncových zařízení. Správce tak má možnost vidět informace o CPU, RAM, monitorech, discích, tiskárnách (včetně výrobce), sériových číslech a podobně. Produkt tak slouží i jako inventář používaného hardwaru.
<b>Detaily o stanicích</b>	Správce si může prohlédnout detailní informace o klientské stanici: do jaké dynamické skupiny je zařazena, jaké bezpečnostní řešení je nainstalované, jaký používá hardware a operační systém a kdo je uživatelem. Informace se zobrazují na interaktivních dlaždicích, které rovněž upozorňují na problémy k řešení.

# O ESETu

**Společnost ESET byla ve zprávě Magic Quadrant společností Gartner\* pro rok 2018 jmenována vyzyvatelem v segmentu Endpoint Protection. ESET byl v této zprávě uveden jako jediný vyzyvatel pro danou oblast a oceněn byl zejména za schopnost vytvářet a naplňovat své vize.**

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností,

kteřá díky dlouhodobě vysoké úrovni ochrany získala více než 100 ocenění prestižního magazínu Virus Bulletin VB100. Za těmito úspěchy stojí zejména dlouhodobé investice do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

