



FIREMŇÍ ŘEŠENÍ

Vylepřete si kybernetickou obranu pomocí proaktivního digitálního zabezpečení na bázi umělé inteligence

Progress. Protected.



30+ let
neustálých
inovací



Vlastněno
původními
zakladateli



Soukromá
společnost bez
dluhů



Silné hodnoty



Technologicky
zaměřená



Kontinuální růst
od založení

Jsme přesvědčeni, že jediným vhodným přístupem k účinné ochraně dat vaší organizace je zavedení více vrstev ochrany.

O ESETu

MALWAROVÉ HROZBY UMÍME ZASTAVIT, ALE PŘEDEVŠÍM JIM PŘEDCHÁZÍME.

Na rozdíl od běžných řešení, která se zaměřují na reakci na již aktivní hrozby, nabízí společnost ESET bezkonkurenční preventivní přístup využívající umělou inteligenci, lidské znalosti, renomovanou globální službu Threat Intelligence a rozsáhlou síť výzkumných a vývojových center.

Samozřejmostí je obchodní i technická podpora v českém jazyce.

NAŠI ZÁKAZNÍCI



Zákazníkem od roku 2017,
více než 9 000 licencí



Zákazníkem od roku 2016,
více než 4 000 mailboxů



Zákazníkem od roku 2016,
více než 32 000 licencí



ISP partnerem od roku 2008,
2 miliony zákazníků

ESET V ČÍSLECH

1mld+

chráněných uživatelů
na internetu

400k+

firemních
zákazníků

200

zemí
a teritorií

13

globálních výzkumných
center

Bezpečná firemní síť

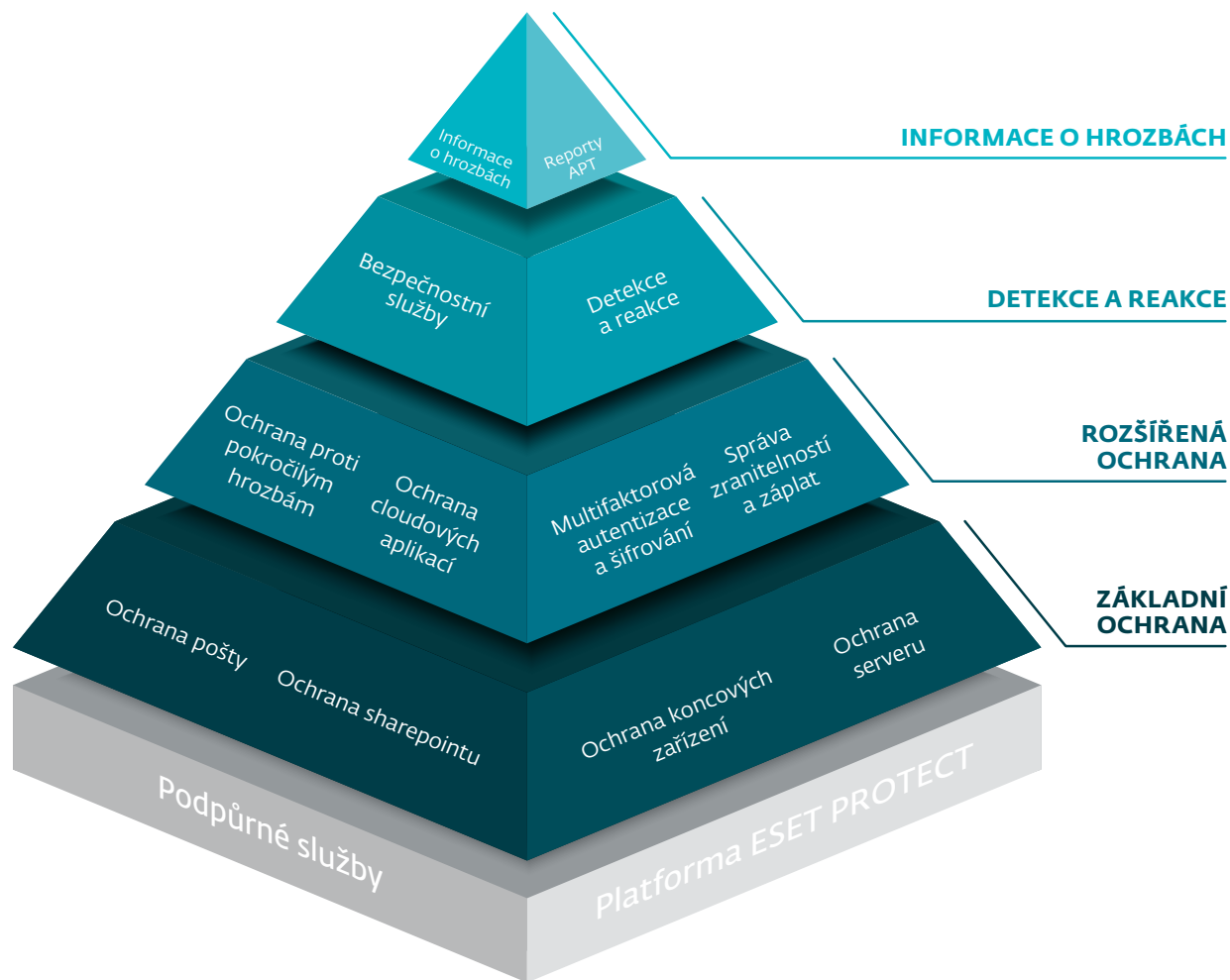
ESET preferuje proaktivní přístup k digitální bezpečnosti, kdy je prevence stejně důležitá jako detekce a reakce na hrozby.

Všechny vrstvy ochrany (každá používá vlastní technologii) fungují ve vzájemné součinnosti, zvyšují kybernetickou odolnost firmy a zajišťují bezpečnost sítě před všemi existujícími i dosud nepoznanými hrozbami.



„Komplexní řešení zabezpečení IT musí správně fungovat a snadno se používat. ESET tuto rovnováhu zvládá výborně.“

Stefan Pistorius, manažer informačních technologií, Kohlpharma



Ochrana napříč platformami



iOS



VRSTVY OCHRANY

INFORMACE O HROZBÁCH	Informace o hrozbách Zpravodajství ESET Threat Intelligence	Reporty APT Zpravodajství ESET Threat Intelligence PREMIUM
DETEKCE A REAKCE (EDR/XDR)	MDR služby ESET MDR ESET Detection & Response Ultimate (MDR Ultimate)	Detekce a reakce ESET Inspect (cloud nebo on-prem)
ROZŠÍŘENÁ OCHRANA	Ochrana proti pokročilým hrozbám ESET LiveGuard Advanced Ochrana cloudových aplikací ESET Cloud Office Security Správa zranitelností a záplat ESET Vulnerability & Patch Management	Autentizace ESET Secure Authentication Šifrování ESET Full Disk Encryption ESET Endpoint Encryption
ZÁKLADNÍ OCHRANA	Ochrana pošty ESET Mail Security (Exchange, IBM Domino) SharePoint Security ESET Security for Microsoft SharePoint Server	Endpoint Protection & Mobile Threat Defense ESET Endpoint Security (Win, macOS, Android) ESET Endpoint Antivirus (Win, macOS, Linux) ESET MDM (iOS and iPad OS) Server Security ESET Server Security (Win, Linux)

Podpůrné služby

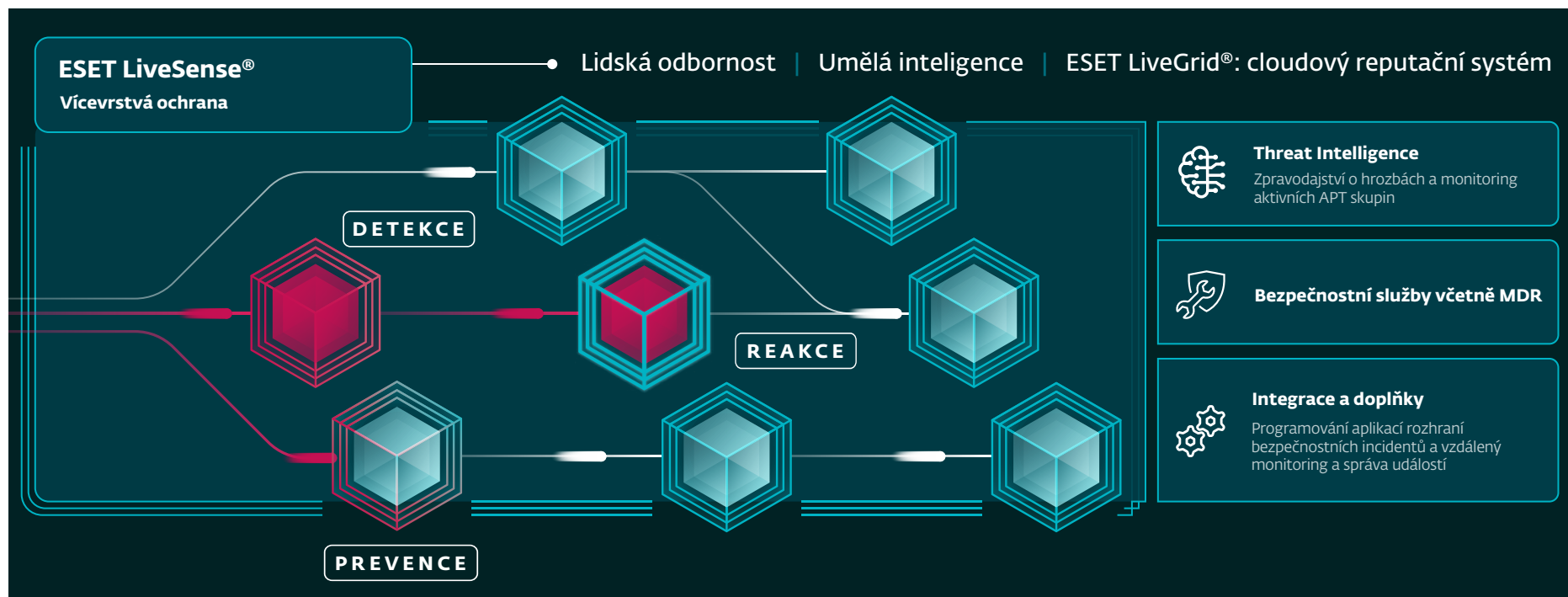
Technická podpora **ZDARMA**
ESET Extended Support
ESET Premium Support Essential
ESET Premium Support Advanced
ESET Deployment & Upgrade
ESET HealthCheck
ESET Micro Updates **ZDARMA**










Platforma ESET PROTECT

ESET PROTECT (cloud nebo on-prem konzole)
Naše jednotné rozhraní XDR platformy kybernetické bezpečnosti, poskytující vynikající přehled o bezpečnostní situaci v síti

PLATFORMA ESET PROTECT

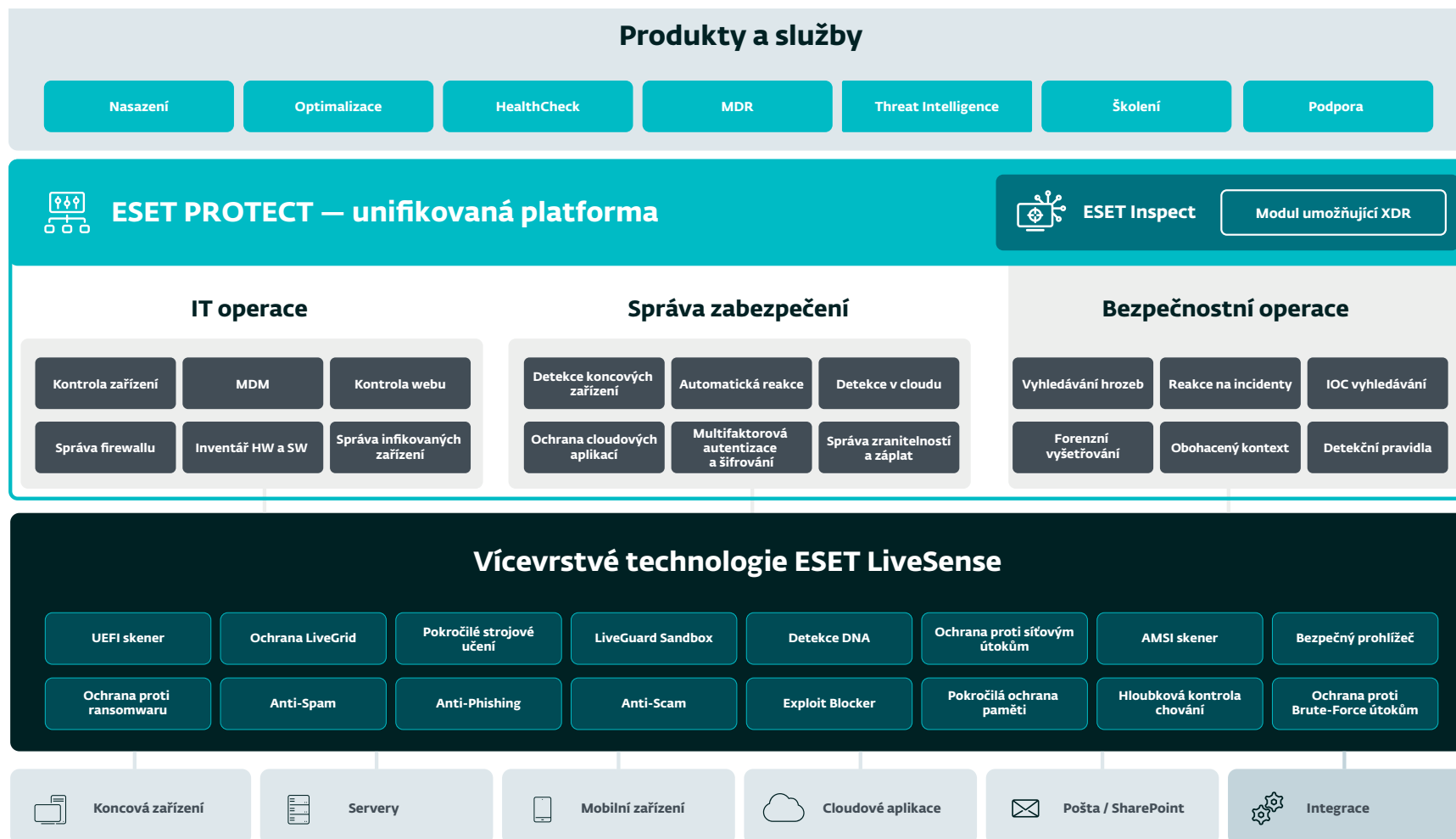
První cloudová platforma kybernetické bezpečnosti XDR, která kombinuje prevenci nové generace, detekci a proaktivní vyhledávání hrozeb a nabízí širokou škálu bezpečnostních služeb, včetně řízené detekce a reakce.



 Správa zabezpečení ESET PROTECT	 Detekce a reakce ESET Inspect	 Pokročilá ochrana proti hrozbám ESET LiveGuard	 Moderní ochrana koncových zařízení	 Šifrování
 Ochrana cloudových aplikací	 Vícefaktorová autentizace	 Správa zranitelností a záplat	 Ochrana pošty	možnost XDR

PLATFORMA ESET PROTECT







Platforma poskytuje bezproblémovou automatizovanou ochranu nad rámec koncových bodů a pokrývá další potenciální vektory útoku, včetně mobilních telefonů, e-mailu a webových a cloudových aplikací. To vše z jediné intuitivní konzole.



PLATFORMA ESET PROTECT

Rozšiřitelné a nastavitelné předplatné, snadná správa z cloudové nebo lokální konzole

Vlastnosti	KONZOLE (CLOUD/ON-PREM)
	MODERNÍ OCHRANA ZAŘÍZENÍ
	OCHRANA SERVERU
	OCHRANA MOBILNÍCH ZAŘÍZENÍ
	ŠIFROVÁNÍ CELÉHO DISKU
	POKROČILÁ OCHRANA PROTI HROZBÁM
	SPRÁVA ZRANITELNOSTÍ A ZÁPLAT
	OCHRANA POŠTY
	OCHRANA MICROSOFT 365 A GOOGLE WORKSPACE
	DETEKCE A REAKCE (XDR)
	VÍCEFAKTOROVÁ AUTENTIZACE
Služby	TECHNICKÁ PODPORA
	MDR
	MDR ULTIMATE
	PREMIUM SUPPORT ESSENTIAL
Volitelná řešení	PREMIUM SUPPORT ADVANCED
	ZPRAVODAJSTVÍ O HROZBÁCH A REPORTY
	OCHRANA SHAREPOINTU
	ŠIFROVÁNÍ KONCOVÝCH ZAŘÍZENÍ

	 PROTECT ENTRY	 PROTECT ADVANCED	 PROTECT COMPLETE	 PROTECT ELITE	 PROTECT MDR	 PROTECT MDR ULTIMATE
KONZOLE (CLOUD/ON-PREM)	●	●	●	●	●	●
MODERNÍ OCHRANA ZAŘÍZENÍ	●	●	●	●	●	●
OCHRANA SERVERU	●	●	●	●	●	●
OCHRANA MOBILNÍCH ZAŘÍZENÍ	○	●	●	●	●	●
ŠIFROVÁNÍ CELÉHO DISKU		●	●	●	●	●
POKROČILÁ OCHRANA PROTI HROZBÁM		●	●	●	●	●
SPRÁVA ZRANITELNOSTÍ A ZÁPLAT			●	●	●	●
OCHRANA POŠTY	○	○	●	●	●	●
OCHRANA MICROSOFT 365 A GOOGLE WORKSPACE	○	○	●	●	●	●
DETEKCE A REAKCE (XDR)				●	●	●
VÍCEFAKTOROVÁ AUTENTIZACE	○	○	○	●	●	●
TECHNICKÁ PODPORA	●	●	●	●	●	●
MDR				○	●	
MDR ULTIMATE				○		●
PREMIUM SUPPORT ESSENTIAL	○	○	○	○	●	
PREMIUM SUPPORT ADVANCED	○	○	○	○	○	●
ZPRAVODAJSTVÍ O HROZBÁCH A REPORTY	○	○	○	○	○	○
OCHRANA SHAREPOINTU	○	○	○	○	○	○
ŠIFROVÁNÍ KONCOVÝCH ZAŘÍZENÍ	○	○	○	○	○	○

● Obsahuje
○ Volitelné

ESET PROTECT ENTRY

Moderní vícevrstvá ochrana koncových bodů

Chraňte své firemní počítače, notebooky a chytré telefony. Špičková umělá inteligence a snadno použitelná správa v cloudu i lokálně. Multiplatformní řešení s ochranou serverů v ceně.



„Zjistili jsme, že ESET splňuje všechny naše požadavky. Řešení se snadno používalo, mělo příznivou cenu a pocházelo od lídra v oboru, kterého jsme hledali.“

Steven Thompson, manažer IT podpory, Totemic

OBSAHUJE

Konzole

Cloudové nebo lokální rozhraní jednotné platformy pro správu bezpečnostních řešení ESET pro firmy na všech operačních systémech. Umožňuje nasazení zabezpečení jedním kliknutím a cloudová konzole poskytuje přehled o síti bez nutnosti nákupu nebo údržby dalšího hardwaru, což snižuje celkové náklady.

Ochrana serveru

Vícevrstvá ochrana serverů pro všechny obecné servery a síťová úložiště souborů, která udržuje stabilní provoz a zajišťuje kontinuitu provozu.

Moderní ochrana zařízení

Chrání zařízení na několika vrstvách současně a detekuje malware před spuštěním, v jeho průběhu i po něm. Řešení jsou navržena tak, aby moderní technologie ochrany, jako jsou strojové učení, pokročilá analýza chování hrozeb a big data, dynamicky udržovaly co nejnvýhodnější poměr mezi výkonem, detekcí a falešnými poplarchy.

- Ochrana proti všem druhům malwaru
- Blokace cílených útoků
- Preventivní ochrana před podvodnými stránkami
- Blokace phishingových útoků
- Detekce pokročilých odolných hrozeb (APT)
- Včetně správy mobilních zařízení (MDM)

ESET PROTECT ADVANCED

Ochrana koncových zařízení proti ransomwaru

Špičková ochrana koncových bodů proti ransomwaru a hrozbám nultého dne. Multiplatformní řešení se snadno použitelnou cloudovou nebo lokální správou, zabezpečením serverů, pokročilou ochranou proti hrozbám a šifrováním celého disku.



„Výkon produktů ESET je robustní a efektivní. Zákaznický servis a produktová podpora jsou vynikající.“

Arun DeSouza, CISO & CPO, Nexteer Automotive Corporation

OBSAHUJE

Konzole

Ochrana serveru

Moderní ochrana zařízení

Obrana proti mobilním hrozbám

Robustní zabezpečení všech mobilních zařízení se systémy Android a iOS. Využijte na firemních mobilních zařízeních funkce Antimalware, Anti-Theft a MDM.

- Ochrana před mobilními hrozbami
- Ochrana firemních dat na přenosných zařízeních
- Blokování nežádoucích aplikací
- Včetně MDM pro iOS a iPadOS

Ochrana proti pokročilým hrozbám

ESET LiveGuard Advanced je cloudový sandbox (izolované zabezpečené testovací prostředí), ve kterém se analyzují nové a neznámé soubory. Na základě chování automaticky vyhodnotí, zda jde o hrozbu, či nikoli.

- Vyšší úspěšnost detekce nových, neznámých hrozeb
- Analyzuje chování podezřelého souboru a vyhodnotí jeho škodlivost
- Nemusíte nic instalovat, spravovat ani nic dalšího kupovat
- Jednoduchá aktivace a používání – nastavení v 5 minutách
- Funkční u zaměstnanců mimo firemní síť, např. při práci z domova

Šifrování celého disku

ESET Full Disk Encryption je doplňková funkce v konzoli vzdálené správy **ESET PROTECT**. Jedním kliknutím může správce nasadit a zašifrovat data na připojených zařízeních se systémy Windows a macOS. Šifrování výrazně zvyšuje úroveň zabezpečení firemních dat a pomáhá být v souladu s nařízením o ochraně dat.

- Správa šifrování na zařízeních s Windows a macOS
- Šifrování systémového disku, vybraných oddílů nebo celých disků
- Nasazení, aktivace a zašifrování jedním kliknutím

ESET PROTECT COMPLETE

Ochrana před více vektorovými útoky

Kompletní vícevrstvá ochrana koncových zařízení, cloudových aplikací a e-mailů (nejčastější zdroje hrozeb). Multiplatformní řešení se správou v cloudu, zabezpečením serverů, pokročilou ochranou proti hrozbám, šifrováním a záplatováním zranitelností.



„Je příjemné vědět, že naše koncové body jsou nyní zabezpečené a že dokážeme včas odhalit potenciální hrozby.“

Bob Kambora, manažer IT

OBSAHUJE

Konzole

Ochrana serveru

Moderní ochrana zařízení

Obrana proti mobilním hrozbám

Ochrana proti pokročilým hrozbám

Šifrování celého disku

Ochrana cloudových aplikací

Poskytuje pokročilou ochranu pro aplikace Microsoft 365 a Google Workspace. Obsahuje kombinaci filtrování nevyžádané pošty, antimalwarové kontroly a antiphishingové ochrany. Prostřednictvím webové konzole dokážete ochranu spravovat odkudkoli.

- Speciální vrstva ochrany pro aplikace Microsoft 365 a Google Workspace
- Zajišťuje ochranu firemní komunikace
- Minimalizuje nežádoucí efekt nevyžádaných zpráv na každodenní produktivitu
- Automatická ochrana nových uživatelů poštovních schránek
- Chrání před cílenými útoky přes e-mailové zprávy

Ochrana pošty

Chrání poštovní schránky uživatelů před nevyžádanou poštou. Používá interně vyvíjený antispam, antiphishing a další technologie, které kombinují strojové učení, analýzu dat a lidskou odbornost do jednoho celku.

- Správa karantény
- Technologie filtrování spamu a malwaru ve více vrstvách
- Antiphishingová ochrana

Správa zranitelností a záplat

Aktivně sleduje zranitelnosti operačních systémů a běžných aplikací a umožňuje automatické záplatování všech koncových zařízení.

- Stanovení priorit zranitelností na základě závažnosti
- Široká škála možností filtrování
- Možnosti automatického a ručního záplatování

ESET PROTECT ELITE

Komplexní kybernetická ochrana pro firmy všech velikostí

Komplexní řešení prevence, detekce a reakce kombinující XDR se špičkovou vícevrstvou ochranou e-mailů, dat a koncových zařízení.



„Díky datům z ESET Inspect víme o bezpečnostním incidentu téměř okamžitě a můžeme na něj ihned reagovat.“

Aleš Staněk, ředitel centra kybernetických operací

OBSAHUJE

Konzole

Ochrana serveru

Moderní ochrana zařízení

Obrana proti mobilním hrozbám

Ochrana proti pokročilým hrozbám

Šifrování celého disku

Ochrana cloudových aplikací

Ochrana pošty

Správa zranitelností a záplat

Detekce a reakce

ESET Inspect je sofistikovaný nástroj, který slouží k identifikaci nezvyklého chování a průniků a posouzení rizik, stejně jako k vyšetření bezpečnostních incidentů, jejich nápravě a odpovědi na ně. V reálném čase monitoruje a vyhodnocuje aktivity v síti (například chování uživatelů, soubory, procesy, registry, paměť a události), což organizacím umožňuje v případě potřeby rychle zareagovat.

- Sofistikovaný nástroj EDR/XDR analyzuje velké množství dat v reálném čase, potenciální hrozby nemají šanci uniknout detekci
- Synchronizovaná detekce a reakce na incident
- Jedno z nejlépe škálovatelných řešení XDR na trhu

Vícefaktorová autentizace

ESET Secure Authentication nabízí firmám všech velikostí možnost jednoduše implementovat vícefaktorovou autentizaci do běžně používaných systémů, jako jsou VPN, RDP, Microsoft 365, Outlook Web Access nebo přihlašování do systému.

- Prevence úniku dat
- Ochrana přístupu do sítě
- Provoz v cloudu
- Vzdálená správa
- Využití telefonu nebo hardwarového tokenu

ESET PROTECT MDR

Ochrana vše v jednom se službou MDR

Špičková ochrana na bázi umělé inteligence s nepřetržitým vyhledáváním a sledováním hrozeb. Získejte přístup ke špičkovým znalostem společnosti ESET a informacím o hrozbách prostřednictvím řízené detekce a reakce, poskytované jako služba 24 hodin denně, 7 dní v týdnu.



„Od nasazení ESETu u našich klientů jsme nezaznamenali jedinou epidemii. Je osvěžující mluvit s podporou, která se skutečně dokáže postarat o všechny problémy.“

Ed Bensinger, CEO, Bensinger Consulting

OBSAHUJE

Konzole

Ochrana serveru

Moderní ochrana zařízení

Obrana proti mobilním hrozbám

Ochrana proti pokročilým hrozbám

Šifrování celého disku

Ochrana cloudových aplikací

Ochrana pošty

Správa zranitelností a záplat

Detekce a reakce

Vícefaktorová autentizace

Služba MDR

Služba řízené detekce a reakce 24/7, která je určena k okamžitému vyšetřování a přerušení škodlivých aktivit a kyber útoků. Zajišťuje ochranu digitálních aktiv organizace před vyvíjejícími se kybernetickými riziky, aniž by bylo nutné zaměstnávat další pracovníky.

- Rychlá doba detekce a reakce na hrozby (průměrně 20 minut)
- Nepřetržité monitorování hrozeb
- Proaktivní vyhledávání hrozeb
- Týdenní nebo měsíční reporting

Služba Premium Support Essential

Zaručená, prioritní a rychlá technická podpora, včetně rychlé a podrobné analýzy všech problémů a následné přesné pomoci při řešení problémů v kteroukoli denní či noční hodinu.

- Okamžitá odezva
- Dostupnost podpory 365/24/7
- Certifikovaní specialisté

ESET PROTECT MDR Ultimate

Ochrana vše v jednom s prémiovou službou MDR

Maximální ochrana, vynikající řízení kybernetických rizik a detailní přehled o vašem IT prostředí. Buďte o krok napřed před všemi známými i nově vznikajícími hrozbami. Získejte přístup ke špičkovým odborným znalostem společnosti ESET prostřednictvím našich zahrnutých služeb Managed Detection and Response (MDR) a Premium Support.



„Reaktivní přístup nám nevyhovoval a rozhodli jsme se pro aktivní přístup. Proto jsme si vybrali službu MDR, která správu delegovala na ESET.“

Robert Heines, information security manager, Royal Swinkels Family Brewers

OBSAHUJE

Konzole

Ochrana serveru

Moderní ochrana zařízení

Obrana proti mobilním hrozbám

Ochrana proti pokročilým hrozbám

Šifrování celého disku

Ochrana cloudových aplikací

Ochrana pošty

Správa zranitelností a záplat

Detekce a reakce

Vícefaktorová autentizace

Služba MDR Ultimate

Služba kombinuje dovednosti špičkových výzkumných týmů a specialistů na řešení bezpečnostních incidentů a špičkové technologie společnosti ESET. Její pohotová, na míru šitá podpora snižuje riziko jakéhokoli přerušení kontinuity provozu.

- Garantovaná doba odezvy
- Nasazení a optimalizace XDR
- Vyšetřování podezřelého chování
- Digitální forenzní analýza
- Proaktivní vyhledávání a monitorování hrozeb

Služba Premium Support Advanced

Zaručená, prioritní a rychlá technická podpora, včetně rychlé a podrobné analýzy všech problémů a následné přesné pomoci při jejich řešení v kteroukoli denní či noční hodinu.

- Okamžitá odezva
- Dostupnost podpory 365/24/7
- Certifikovaní specialisté

Výhody cloudového sandboxu

OCHRANA VE VÍCE VRSTVÁCH

ESET LiveGuard Advanced používá ke zkoumání zaslaných vzorků hned tři různé modely strojového učení. Poté spustí testovaný soubor v sandboxu, který simuluje chování uživatele. S použitím neuronové sítě s hlubokým učením dojde k porovnání chování vzorku s dostupnými historickými daty. Nakonec skenovací jádro ESET analyzuje všechny části vzorku na přítomnost čehokoli neobvyklého.

KOMPLETNÍ PŘEHLED

Všechny analyzované vzorky se zobrazují v nástroji vzdálené správy s různými informacemi o vzorku samotném i jeho původu. V přehledu jsou uvedeny nejen ty odeslané do ESET LiveGuard Advanced, ale také vše, co bylo odesláno do cloudového reputačního systému ESET LiveGrid®.

MOBILITA

V současné době není nic neobvyklého, že zaměstnanci pracují i mimo firmu. Proto ESET LiveGuard Advanced může analyzovat příchozí vzorky nezávisle na místě, kde se zaměstnanec nachází. A navíc, pokud dojde k detekci škodlivého souboru, je ihned chráněna celá firemní síť.

RYCHLÁ ANALÝZA

V případě nákazy je důležitá každá minuta, proto ESET LiveGuard Advanced dokáže analyzovat většinu příchozích vzorků v řádu minut. Pokud již vzorek byl v minulosti analyzován, jsou všechna firemní zařízení chráněna během pár vteřin.

Výhody cloudu

UŠETŘENÍ NÁKLADŮ

Kompletní přechod do cloudu se může na první pohled jevit jako velmi nákladná záležitost. Ale když vezmete v potaz, že se nemusíte starat o servery a udržovat je, řešit aktualizace, záplaty nebo restarty a podobně, pak už to tak jednoznačné není.

PŘIPRAVENO ZA PÁR MINUT

Cloudovou konzoli můžete používat téměř okamžitě po přihlášení. Stačí jen připojit koncové stanice. Nemusíte čekat na instalaci jednotlivých komponent nebo odkládat aktualizace serveru na vhodnou chvíli mimo běžný pracovní provoz firmy.

VŽDY AKTUÁLNÍ VERZE

Aktualizace konzole probíhá v naší režii. Děje se na pozadí a budete mít vždy nejnovější verzi všech komponent. K připojení stačí oblíbený prohlížeč a funkční připojení k internetu. Ano, stejně se dá připojit i ke konzoli „on premise“, nemusíte nicméně řešit problémy s výjimkami ve firewallu a nastavování VPN.

RYCHLÉ ŘEŠENÍ PROBLÉMŮ

Při používání cloudové konzole vám naši odborníci mohou v případě potřeby velmi rychle a efektivně pomoci. A to jen díky tomu, že přesně vědí, jakou verzi konzole používáte.

Výhody šifrování

VŠECHNY PRODUKTY V JEDNÉ KONZOLI

IT správce používá vzdálenou správu každý den. ESET Full Disk Encryption je integrován do konzole vzdálené správy ESET PROTECT, takže se správce pohybuje v dobře známém prostředí.

VZDÁLENÝ PŘEHLED A SPRÁVA

Možnost vzdálené správy šetří administrátorovi čas a ulehčuje každodenní práci. ESET Full Disk Encryption je plně integrován do obou dostupných konzolí vzdálené správy, takže správa šifrování i zabezpečení probíhá v jediné konzoli. Pokročilé šifrovací řešení ESET Endpoint Encryption využívá vlastní hybridní vzdálenou správu založenou na cloudu.

SOULAD S NAŘIZENÍMI

Šifrování citlivých dat je velmi užitečné opatření, které vám značně pomůže v případě odcizení notebooku a vzniku bezpečnostního incidentu. Pokud jsou totiž uniklá data řádně chráněna šifrováním, je velmi pravděpodobné, že incident nebude posuzován jako nedodržení souladu s nařízeními o ochraně dat typu GDPR a podobně.

SNADNÁ INSTALACE

ESET Full Disk Encryption je možné instalovat na koncová zařízení podobně jako ostatní produkty ESET. Správce může v ESET PROTECT přidat plné šifrování disku do instalačního balíčku „all-in-one“, a to včetně požadovaných politik (např. délka hesla, maximální počet pokusů o přihlášení a podobně).

Výhody konzole ESET PROTECT

SPRÁVA ZALOŽENÁ NA ROLÍCH

Umožňuje hlavnímu správci vytvořit různé role, kterým lze přiřadit odlišná oprávnění. V případě instalace ve strojové struktuře může správce vytvořit „superadministrátorský“ účet. Ten pak umožňuje definovat hlavní firemní politiky a práva pro lokální správce, kteří potom mohou spravovat jen svou část sítě. Režim „read only“ dovolí správci získat přehled o bezpečnostní situaci v síti bez možnosti interakce.

FLEXIBILNÍ INSTALACE

ESET PROTECT je možné nainstalovat nejen na Windows, ale také na Linux nebo využít virtual appliance. Správa probíhá prostřednictvím webové konzole, která správcům umožňuje získat celkový přehled o bezpečnostní situaci ve firemní síti. Spravovat firemní infrastrukturu je možné odkudkoli. Stačí jen funkční webový prohlížeč.

INVENTÁŘ HARDWARU A SOFTWARE

V ESET PROTECT má správce přehled nejen o nainstalovaném softwaru ve firemní síti, ale také o používaném hardwaru. Všechny parametry (např. operační systém, model, procesor, RAM atd.) je možné použít pro tvorbu dynamických skupin.

WEBOVÁ KONZOLE

Všechny produkty ESET (nezávisle na operačním systému) je možné spravovat z jediné instance ESET PROTECT, a to včetně mobilních zařízení s Androidem a iOS.

BEZPEČNOSTNÍ POLITIKY

Správce může definovat politiky pro každý produkt zvlášť a jednoduše určit jejich vzájemný vztah. Politiky jsou uplatňovány agentem, který je schopen fungovat samostatně i bez připojení k serveru ESET PROTECT. Správce může také podle potřeby využít předdefinované šablony.

PODPORA SIEM

ESET PROTECT plně podporuje nástroje SIEM a umožňuje exportovat informace do běžně akceptovaných formátů JSON nebo LEEF.

RYCHLÉ OVLÁDÁNÍ

Správce může pouhým jedním kliknutím vytvořit výjimku z kontroly, odeslat soubor k další analýze nebo třeba spustit kontrolu počítače. Výjimky lze vytvořit podle názvu hrozby, URL, hashe nebo kombinací dostupných parametrů.

AUTOMATIZACE

Stanice je možné řadit do dynamických skupin dle aktuálního bezpečnostního stavu nebo jiných předdefinovaných podmínek. Zařazení stanice do dynamické skupiny může spustit definované úlohy, jako je např. antivirová kontrola, změna bezpečnostní politiky, instalace softwaru a podobně.

Volitelné produkty

ESET Cloud Office Security

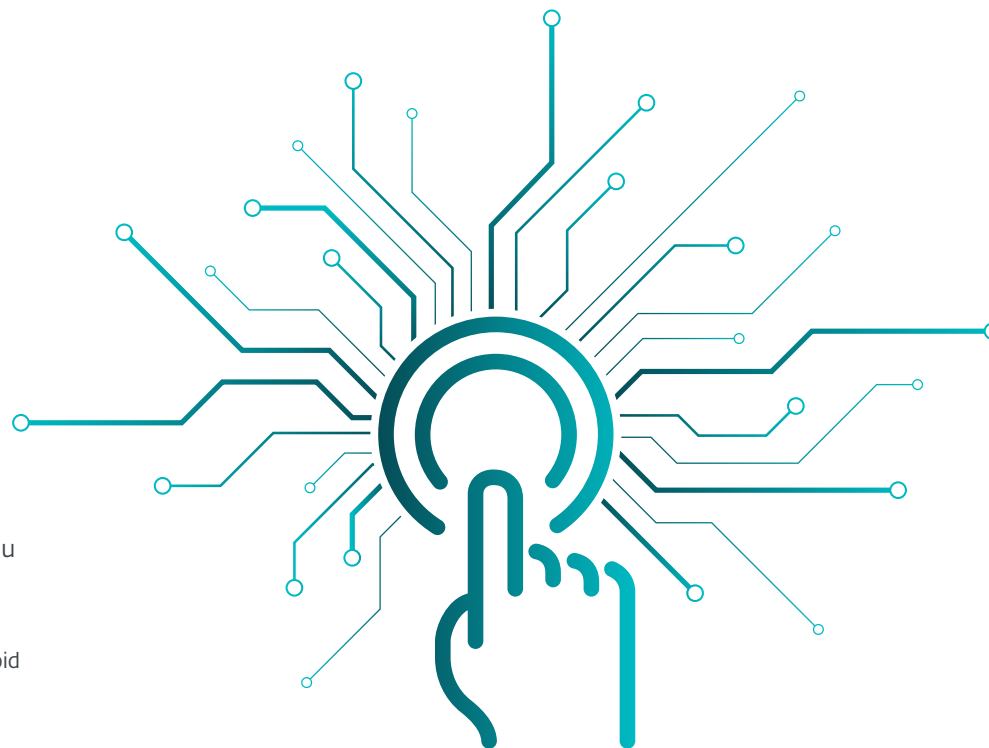
Poskytuje preventivní ochranu pro aplikace Microsoft 365 a Google Workspace. Obsahuje kombinaci filtrování nevyžádané pošty, antimalwarové kontroly a antiphishingové ochrany. Prostřednictvím webové konzole dokážete ochranu spravovat odkudkoli.

- Antimalware
- Antiphishing
- Antispam
- Ochrana proti pokročilým hrozbám
- Cloudová konzole
- Ochrana Exchange Online, OneDrive, Teams, SharePoint Online, Gmail a Google Drive
- Automatická ochrana uživatelů
- Nastavitelné reporty

ESET Secure Authentication

Nabízí firmám všech velikostí možnost jednoduše implementovat vícefaktorovou autentizaci do běžně používaných systémů, jako jsou VPN, RDP, Microsoft 365, Outlook Web Access nebo přihlašování do systému.

- Podporuje mobilní aplikace, push notifikace a hardwarové tokeny, bezpečnostní klíče FIDO, vlastní metody doručení
- Push notifikace fungují na iOS a Android
- Není potřeba žádný další hardware
- Včetně plné API a SDK
- Konzole správy přístupná z prohlížeče



ESET Security pro Microsoft SharePoint Server

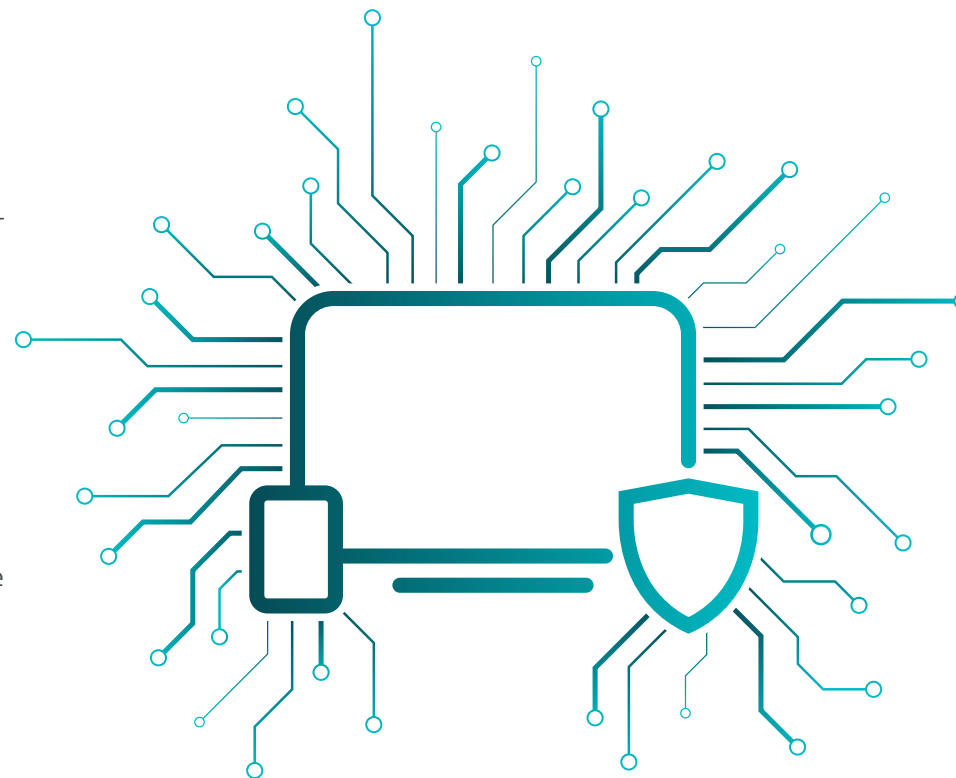
Pokročilá ochrana proti škodlivým uploadům a nechtěným souborům pro sharepointové servery. Stabilní a spolehlivé řešení pro serverové prostředí.

- Antivirus
- Antispyware
- Ochrana proti síťovým útokům
- Ochrana proti botnetu
- Volitelná kontrola
- Integrace s platformou ESET PROTECT

ESET Endpoint Encryption

ESET Endpoint Encryption je samostatné řešení pro šifrování dat, které umožňuje úplnou vzdálenou kontrolu nad šifrovacími klíči a politikou zabezpečení pevných disků, přenosných zařízení a e-mailů na koncových zařízeních.

- Bezpečné sdílení citlivých dat mimo vlastní organizaci
- Prevence úniku dat
- Zajištění souladu s nařízením
- Bezproblémové šifrování



SLUŽBY ESET

EXPERTI VÁM POMŮŽOU VYLEPŠIT ÚROVEŇ OCHRANY

Komplexní nabídka služeb společnosti ESET je navržena tak, aby vám pomohla využít plný potenciál řešení ESET, zajistila ochranu proti všem druhům nově vznikajících hrozeb a zabránila šíření problematického kódu v síti.

Threat Intelligence

Rozšířte své bezpečnostní informace z lokálních sítí do globálního kyberprostoru a získajte přístup k informacím a odborným znalostem IT týmu společnosti ESET. Získejte hloubkové a aktuální globální znalosti o konkrétních hrozbách a zdrojích útoků.

Managed Detection and Response

Analýza, identifikace a řešení všech hrozeb, které proniknou standardní obranou. Tato komplexní služba zahrnuje vše od základního zkoumání a odstraňování malware přes automatizovanou a ruční analýzu souborů až po vyšetřování/řešení incidentů a digitální forenzní analýzu. Službu nabízíme ve třech úrovních, Essential, Advanced a Ultimate, které se liší množstvím nabízených garantovaných úkonů.

Premium Support

Služba je navržena tak, aby zákazníci neprodleně dostali odpovědi na všechny dotazy, rychle vyřešili nastalé problémy a mohli naplno využít potenciál produktu ESET. Službu nabízíme v úrovních Essential a Advanced, které se opět liší množstvím nabízených garantovaných úkonů.

600+

Vývojářů a výzkumníků

20 minut

Průměrná doba reakce

365/24/7

Podpora certifikovanými specialisty

Rozdíl mezi ESET PROTECT MDR a ESET PROTECT MDR ULTIMATE*

	MDR	MDR ULTIMATE
Garantováno smlouvou SLA		
Malware: CHYBĚJÍCÍ detekce	●	●
Malware: Problém s odstraněním	●	●
Malware: Nákaza ransomwarem	●	●
Falešný poplach	●	●
Obecné: Analýza podezřelého chování	●	●
Základní analýza souborů	●	●
Podrobná analýza souborů	●	●
Digitální forenzní analýza	●	●
Digitální forenzní analýza při reakci na incidenty	●	●
Podpora – pravidla	○	●
Podpora – výjimky	○	●
ESET Inspect – otázky související s bezpečností	○	●
Počáteční optimalizace	○	●
Vyhledávání hrozeb (na vyžádání)	○	●
Sledování hrozeb	○	●
Vyhledávání hrozeb (proaktivní)	○	●
Nasazení a upgrade	○	●

	ESET PREMIUM SUPPORT ESSENTIAL	ESET PREMIUM SUPPORT ADVANCED
Doba reakce na kritickou událost (A)	2 hodiny	2 hodiny
Doba reakce na závažnou událost (B)	4 hodiny	4 hodiny
Doba reakce na běžnou událost (C)	1 pracovní den	1 pracovní den
Dostupnost podpory	365/24/7	365/24/7
Kontaktní místo pro volajícího	Specialisté u partnera společnosti ESET nebo centrála společnosti ESET	Specialisté u partnera společnosti ESET nebo centrála společnosti ESET
Kontakty zákazníka	Neomezené	Neomezené
Řazení přednostních hovorů do fronty	Ano	Ano
Tikety s nárokem na přednostní vyřízení	Omezené	Neomezené
Manažer vyhrazený pro konkrétního klienta		Ano
Přednostní přístup k vývojovým týmům		Ano
Proaktivní informační služby		Ano
Nasazení a upgrade		1
Kontrola stavu		1

* Tabulka navazuje na porovnávací řešení na straně 8.

Špičková technologie společnosti ESET

Náš jedinečný vícevrstvý přístup k digitálnímu zabezpečení

Bezpečnostní technologie ESET LiveSense® spolu s našimi znalostmi v oblasti strojového učení, cloudovým reputačním systémem ESET LiveGrid® a našimi lidmi vytváří velmi výkonnou platformu pro prevenci kybernetických hrozeb ve světě, jejich detekci a reakci na ně.



ESET LiveGrid®

Kdykoli dojde k detekci podezřelého souboru, např. hrozby nultého dne a ransomwaru, odešle se soubor do našeho cloudového systému ochrany ESET LiveGrid®. Tam se hrozba aktivuje a systém sleduje a vyhodnocuje její chování. Výsledky analýzy jsou poskytovány všem koncovým bodům globálně během několika minut, aniž by vyžadovaly jakékoliv aktualizace.



Strojové učení

Pro správné vyhodnocení přichozích vzorků (čistý, potenciálně škodlivý, nežádoucí) využívá kombinaci neuronových sítí a ručně vybraných algoritmů. Strojové učení spolupracuje s dalšími technologiemi, jako je DNA, sandbox a analýza paměti a chování, aby bylo dosaženo vysoké míry detekce při co nejnižším počtu falešných poplachů.



Lidská odbornost

Nejde jen o technologie. ESET velmi investuje do vzdělávání zaměstnanců. Odborníci ve 13 výzkumných centrech po celém světě analyzují každý den tisíce nových nalezených hrozeb. Jen tak je možné držet krok s dynamickým prostředím kybernetických hrozeb, kde jsou klíčem k úspěchu aktuální informace o malwaru.

ESET LiveSense®

Vysoce efektivní ochrana

V dnešním prostředí neustále se vyvíjejících hrozeb již pouze jediná vrstva obrany nestačí. ESET LiveSense® využívá množství patentovaných technologií, které dalece přesahují schopnosti základního antiviru.

PŘED SPUŠTĚNÍM

Reputace
a cache

Ochrana proti
síťovým útokům

Skener
UEFI

Pokročilé strojové
učení

Ochrana proti útoku
brute force

Kontrola
zařízení

Detekce
DNA

Integrovaný
sandbox

PŘI SPUŠTĚNÍ

Ochrana proti
ransomwaru

Skript a AMSI
skener

Pokročilá kontrola
paměti

Exploit
Blocker

Hluboká kontrola
chování

PO SPUŠTĚNÍ

Ochrana
LiveGrid®

Bezpečný
prohlížeč

Ochrana
proti botnetu

Toto jsou některé z klíčových technologií ESET a zobrazení, kdy a kde přibližně dochází k detekci a zablokování hrozby během jejího životního cyklu v systému.

