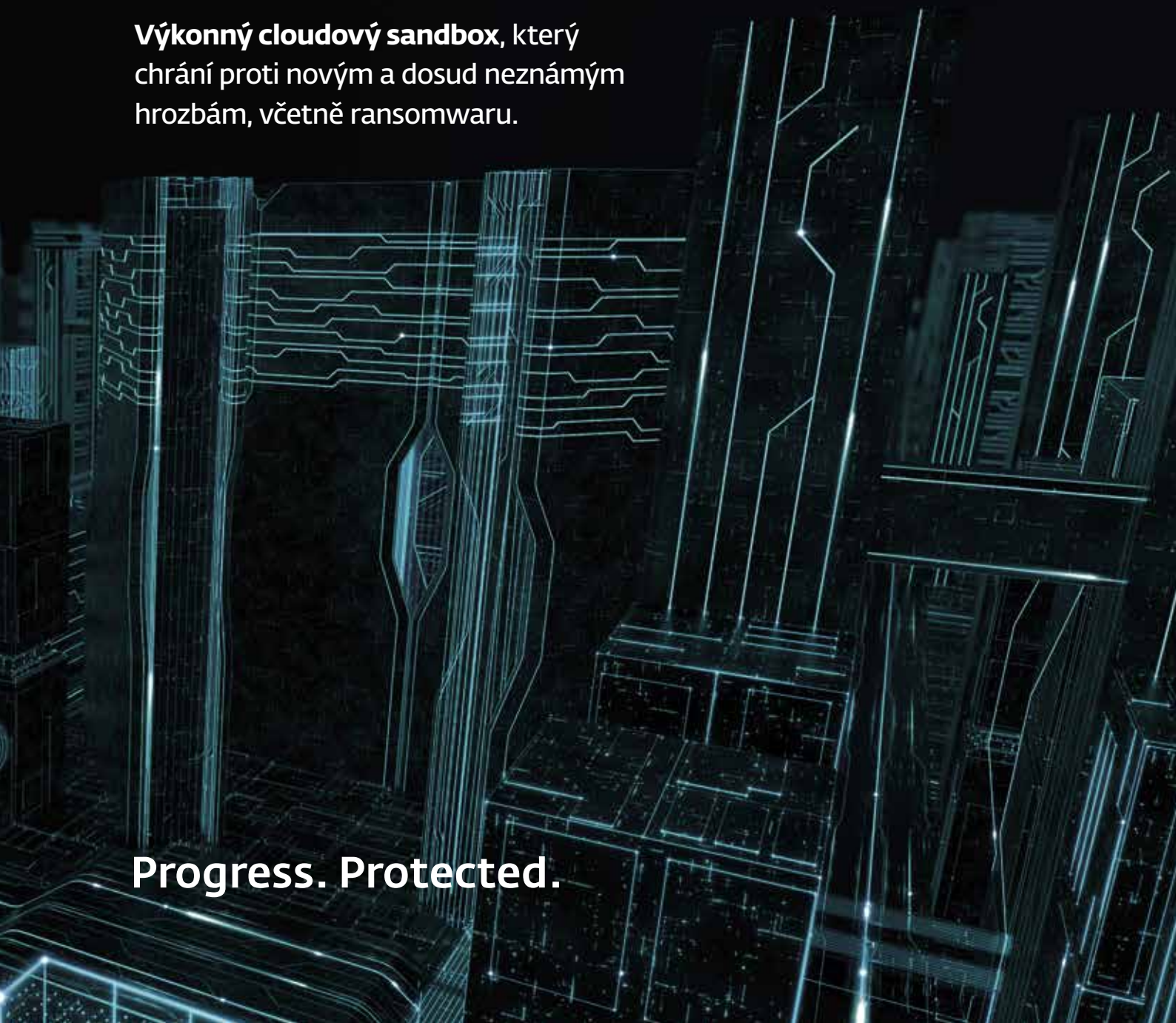
LIVEGUARD ADVANCED

Výkonný cloudový sandbox, který chrání proti novým a dosud neznámým hrozbám, včetně ransomwaru.



Progress. Protected.

Co je **ESET LiveGuard Advanced?**

Cloudový sandbox je izolované zabezpečené testovací prostředí, ve kterém se spouštějí podezřelé soubory, monitoruje a analyzuje jejich chování, a následně automaticky vyhodnocuje.

ESET LiveGuard Advanced poskytuje další vrstvu ochrany pro bezpečnostní produkty ESET, jako jsou ESET Mail Security, ESET Endpoint Security a ESET File Security, a to díky zapojení cloudové sandboxové technologie umožňující detekovat nové, dosud neznámé hrozby, včetně ransomwaru. Tento sandbox je složen z více typů algoritmů, které provádějí statickou analýzu kódů, hloubkovou inspekci vzorků pomocí strojového učení a behaviorální detekci.

Proč **ESET LiveGuard Advanced?**

RANSOMWARE

Ransomware představuje od příchodu Cryptolockeru v roce 2013 pro společnosti globální a trvalou hrozbu. I když existoval dávno předtím, nikdy nepatřil mezi hlavní nebezpečí. Jeden úspěšný ransomwarový útok může zcela ochromit chod firmy znepřístupněním důležitých či nezbytných souborů. Po útoku mohou firmy také zjistit, i když zálohují, že uložená data nejsou dostatečně aktuální. A musí zaplatit útočníkovi výpalné.

Cloudový sandbox poskytuje další vrstvu ochrany mimo firemní síť a zabraňuje ransomwaru ve spuštění v produkčním prostředí.

CÍLENÉ ÚTOKY A ÚNIKY DAT

Prostředí moderních hrozeb je velmi dynamické, neustále dochází k vývoji nového malwaru a způsobů útoku. Na většinu kybernetických útoků postižená firma reaguje v lepším případě se zpožděním, v horším útok ani nezaznamená. I po objevení útoku obvykle správce pouze reaktivně implementuje opatření na daný typ škodlivého kódu. Takový přístup však nezajistí ochranu v případě, kdy útočník zvolí jiný vektor útoku.

Cloudový sandbox je v boji s moderními hrozbami efektivnější, protože v zabezpečeném prostředí umožňuje analyzovat, jak se potenciální hrozba chová. Na základě analýzy chování rozhodne, zda je vzorek hrozba nebo jen neškodný soubor.

ESET LiveGuard Advanced poskytuje další vrstvu ochrany mimo firemní síť.

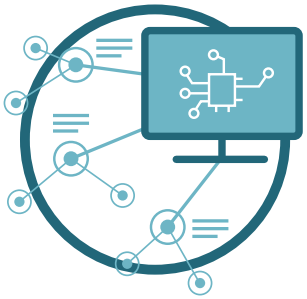
Je efektivnější, protože analyzuje chování potenciální hrozby.

Technologie

3 základní pilíře našich produktů

ESET LIVEGRID®

Při nalezení nového druhu škodlivého kódu, resp. podezřelé činnosti na počítači s instalovaným produktem ESET, se podezřelé soubory odešlou do cloudového systému ESET LiveGrid, kde dojde k pokročilé analýze. Pokud je vzorek detekován jako škodlivý, odešle se informace o nově nalezené hrozbě do všech počítačů po celém světě. To vše v řádu minut.



STROJOVÉ UČENÍ

ESET používá sílu neurálních sítí a pokročilých algoritmů k analýze podezřelých souborů, které vyhodnotí jako čisté, potenciálně nechtěné nebo škodlivé.

LIDSKÁ ODBORNOST

Odborníci ve 13 výzkumných centrech analyzují každý den tisíce nových nalezených hrozeb. Získané informace se ihned odesílají prostřednictvím ESET LiveGrid do všech počítačů s nainstalovaným řešením ESET.

Výhody ESETu

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 vzorky 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.

SOUKROMÍ

Společnost ESET bere ochranu soukromí velmi vážně. Prostřednictvím specifických nastavení může uživatel zadat, aby byl vzorek smazán ihned po analýze.

RYCHLÁ ANALÝZA

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

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 napřed. Výsledkem je důvěra 110 milionů uživatelů po celém světě.

PROAKTIVNÍ OCHRANA

Pokud je vzorek vyhodnocen jako podezřelý, je zablokován a čeká na analýzu v ESET LiveGuard Advanced. Tím se zabrání tomu, aby potenciální hrozby prováděly na zařízení škodlivou aktivitu. Po dokončení analýzy a v případě zjištění hrozby na jednom koncovém bodě je daná informace během několika minut předána všem koncovým bodům ve firemní síti.

Příklady použití

Ransomware

PŘÍKLAD

Ransomware se snaží infikovat firemní síť přes poštovní schránky uživatelů.

ŘEŠENÍ

- ✓ ESET Mail Security automaticky odešle podezřelou přílohu e-mailu do ESET LiveGuard Advanced.
- ✓ K analýze vzorku a odeslání výsledku zpět do ESET Mail Security dojde obvykle do pěti minut.
- ✓ ESET Mail Security detekuje a automaticky zablokuje škodlivý kód v přílohách e-mailů.
- ✓ Škodlivé přílohy se nedostanou k zaměstnancům.

Různá úroveň ochrany

PŘÍKLAD

Každá pozice vyžaduje rozdílnou úroveň ochrany. Vývojáři a IT zaměstnanci potřebují jiná bezpečnostní omezení než manažeři a ředitelé.

ŘEŠENÍ

- ✓ Nastavení unikátní politiky dle počítače nebo serveru v ESET LiveGuard Advanced.
- ✓ Automatické uplatnění politiky v závislosti na zařazení počítače do statické skupiny nebo skupiny v Active Directory.
- ✓ Automatická změna politiky, pokud dojde k přeřazení uživatele do jiné skupiny.

Neznámé soubory

PŘÍKLAD

Zaměstnanci potřebují zjistit, zda je soubor legitimní.

ŘEŠENÍ

- ✓ Jakýkoli uživatel může odeslat soubor k analýze přímo z řešení ESET.
- ✓ ESET LiveGuard Advanced soubor analyzuje v řádu minut.
- ✓ Pokud je soubor vyhodnocen jako škodlivý, jsou chráněny všechny počítače v síti.
- ✓ Administrátor má kompletní informace o tom, kdo soubor odeslal a jak dopadla analýza.

ESET LiveGuard technické funkce

AUTOMATICKÁ OCHRANA

Po nastavení už není potřeba žádné další interakce ze strany správce nebo uživatele. Řešení na koncových stanicích a serverech automaticky rozhodují, zda je vzorek v pořádku, infikovaný nebo neznámý. V případě neznámého souboru se v ESET LiveGuard Advanced provede analýza. Po dokončení se výsledek sdílí s ostatními bezpečnostními řešeními, které provedou odpovídající akci.

VLASTNÍ NASTAVENÍ

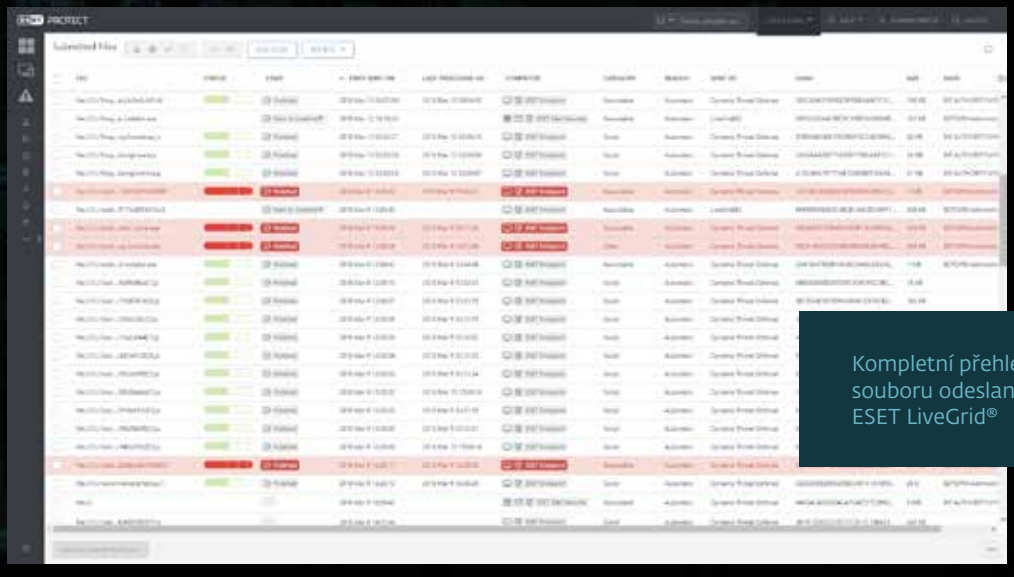
V rámci ESET LiveGuard Advanced může správce nastavit politiky pro jednotlivé počítače, takže má kontrolu nad tím, co se do systému odesílá a jaká akce se provede pro dokončení analýzy.

MANUÁLNÍ ODESLÁNÍ

Uživatel i správce můžou s pomocí instalovaného bezpečnostního řešení ESET kdykoli odeslat vzorek k analýze a dostat výsledky. Správce v nástroji vzdálené správy vidí, kdo vzorek odeslal a jaké akce byly provedeny.

OCHRANA POŠTY

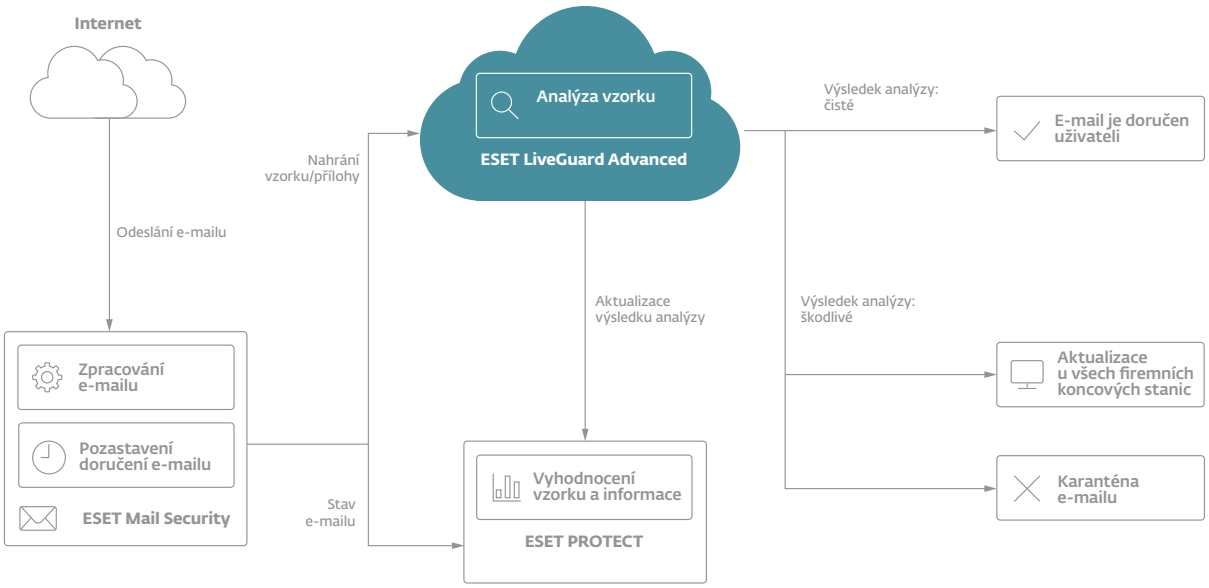
Přímá spolupráce mezi ESET LiveGuard Advanced a ESET Mail Security zajišťuje, že nedojde k infikování sítě prostřednictvím škodlivé přílohy e-mailů.
Pro zajištění efektivity je možné do ESET LiveGuard Advanced odesílat pouze e-maily, které přišly z vnější sítě mimo firmu.



Kompletní přehled všech souboru odeslaných do ESET LiveGrid®

Jak **ESET LiveGuard Advanced funguje**

S ESET Mail Security



ESET LiveGuard Advanced je kompatibilní s produkty ESET pro zabezpečení koncových stanic, serverů a cloudových aplikací (Microsoft 365) a je plně integrován do konzolí vzdálené správy ESET PROTECT.

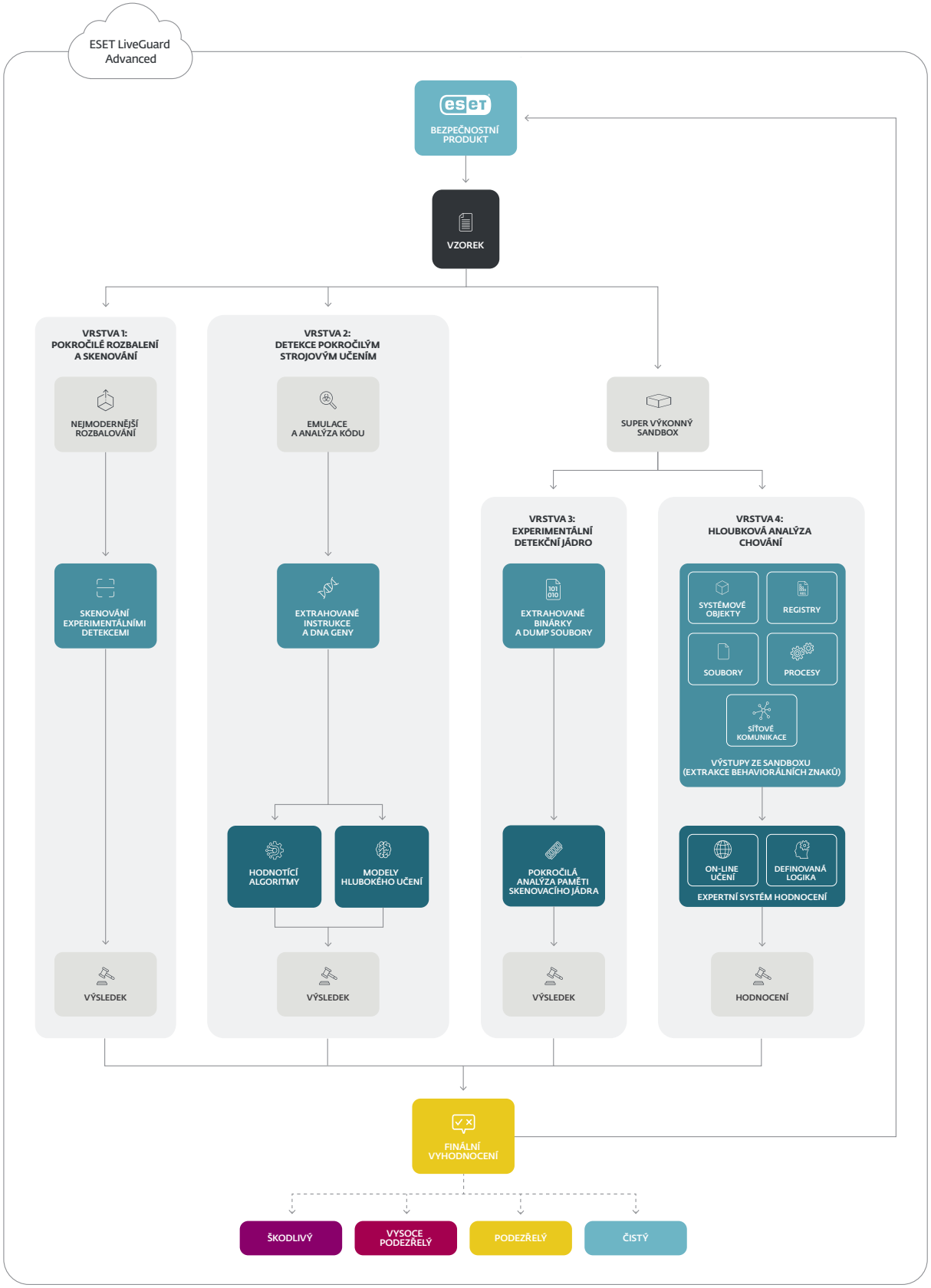
"Úžasný produkt!"

Co se vám líbí nejvíce?

"Líbí se mi, jak snadno jsem ho nasadil na všechny pracovní stanice a jak rychle zabezpečil mou síť. Našel jsem nežádoucí software a denně vidím e-maily o zastavení síťových chyb, dříve než stačí způsobit problém. Lépe spím, když je moje síť chráněna ESETem."

— Michael P. / Správce sítě / Střední trh (51-1 000 zaměstnanců)

Jak funguje pokročilá analýza



ESET LiveGuard Advanced využívá 4 samostatné detekční vrstvy, které zajišťují nejvyšší možnou míru detekce. Každá vrstva používá jiný přístup a poskytuje verdikt o vzorku. Konečné hodnocení zahrnuje výsledky všech informací o vzorku.

VRSTVA 1

Pokročilé rozbalování a skenování

Vzorky procházejí statickou analýzou a nejmodernějším rozbalováním a poté jsou porovnávány s bohatou databází hrozeb.

VRSTVA 2

Pokročilá detekce pomocí strojového učení

Statickou a dynamickou analýzu provádí řada algoritmů strojového učení, které využívají techniky včetně hlubokého učení.

VRSTVA 3

Experimentální detekční jádro

Vzorky jsou vkládány do velmi výkonných sandboxů, které se velmi podobají plnohodnotným uživatelům. Následně jsou sledovány jakékoli známky škodlivého chování.

VRSTVA 4

Hloubková analýza chování

Všechny výstupy ze sandboxu jsou podrobeny hloubkové analýze chování, která identifikuje známé škodlivé vzorce a řetězce akcí.

ŘEŠENÍ KOMBINUJE VŠECHNY DOSTUPNÉ VERDIKTY Z DETEKČNÍCH VRSTEV A VYHODNOCUJE STAV KAŽDÉHO VZORKU. VÝSLEDKY JSOU NEJDŘÍVE DORUČENY DO BEZPEČNOSTNÍCH PRODUKTŮ ESET A INFRASTRUKTURY SPOLEČNOSTI.

VYSOKÁ RYCHLOST

Analýza v sandboxu do 5 minut

VÝHODA DETEKCE

ESET LiveGuard ZAPNUTO

ESET LiveGuard VYPNUTO

+ 135min

Průměrná úspora času

O ESETu

Společnost ESET již od roku 1987 vyví-jí bezpečnostní software pro domácí i firemní uživatele. ESET se stal první společností, která díky vysoké úrovni ochrany získala více než 100 oceně-ní prestižního magazínu Virus Bulletin VB100.

Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvěto-vou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

ESET V ČÍSLECH

1mld+
uživatelů po celém světě

400k+
firemních zákazníků

200+
zemí a teritorií

13
vývojových center

NAŠI ZÁKAZNÍCI

MITSUBISHI MOTORS
Drive your Ambition

Zákazníkem od roku 2017, více než 9 000 licencí

Allianz Suisse

Zákazníkem od roku 2016, více než 4 000 mailboxů

Canon
Canon Marketing Japan Group

Zákazníkem od roku 2016, více než 32 000 licencí

T

ISP partnerem od roku 2008, 2 miliony zákazníků

VYBRANÁ OCENĚNÍ

AV comparatives APPROVED Business Security DEC 2021

ESET získal ocenění „APPROVED" za ochranu koncových řešení v Business Security Testu v prosinci 2021 společnosti AV-Comparatives.

G2 Leader WINTER 2022

ESET trvale dosahuje špičkových výsledků v celosvětovém platformě hodnocení uživatelů G2 a jeho řešení jsou oceňována zákazníky po celém světě

FORRESTER®

Řešení ESET jsou pravidelně oceněno předními analytiky firmami, včetně "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021".

eset® Digital Security
Progress. Protected.

220406