ENJOY SAFER TECHNOLOGY™

Update nie je upgrade

Július Selecký, Senior Technical Pre-Sales Representative

ENJOY SAFER TECHNOLOGY™

Harmonogram prezentácie

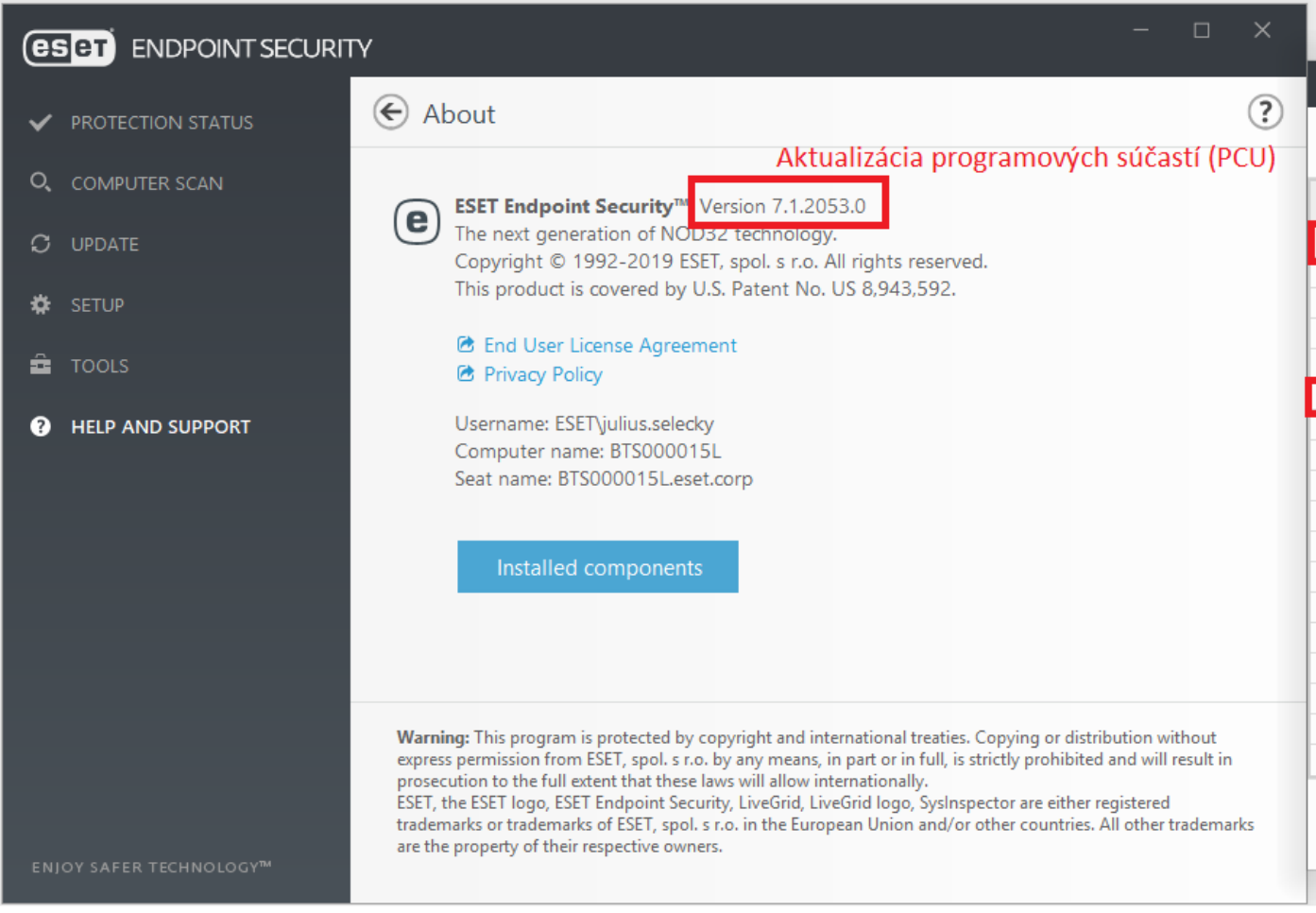
- Dôvody prechodu na novšie verzie
- Vysvetlenie pojmov „Upgrade“ a „Update“
- Čo je nové?
- New Life for ESET

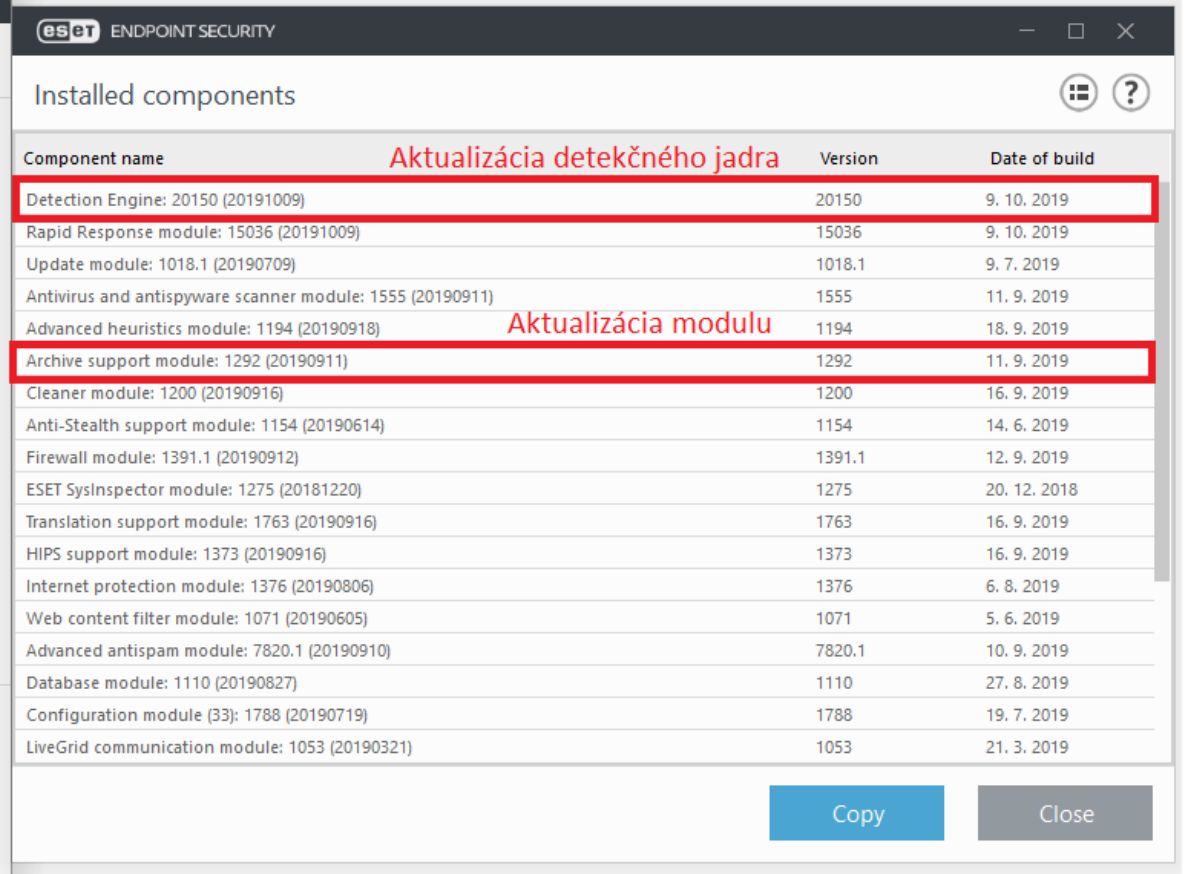

1BN+ INTERNET USERS
PROTECTED BY OUR TECHNOLOGY

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™


NOKIA
16:52
Menü
Vs.

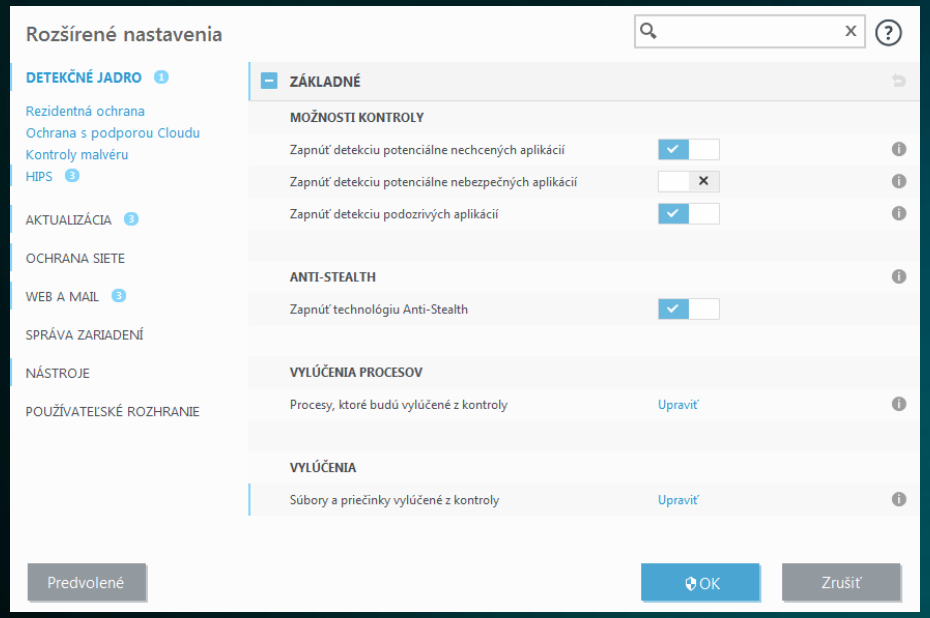
Pravidelné aktualizácie detekčného jadra vs. aktualizácia programových súčastí





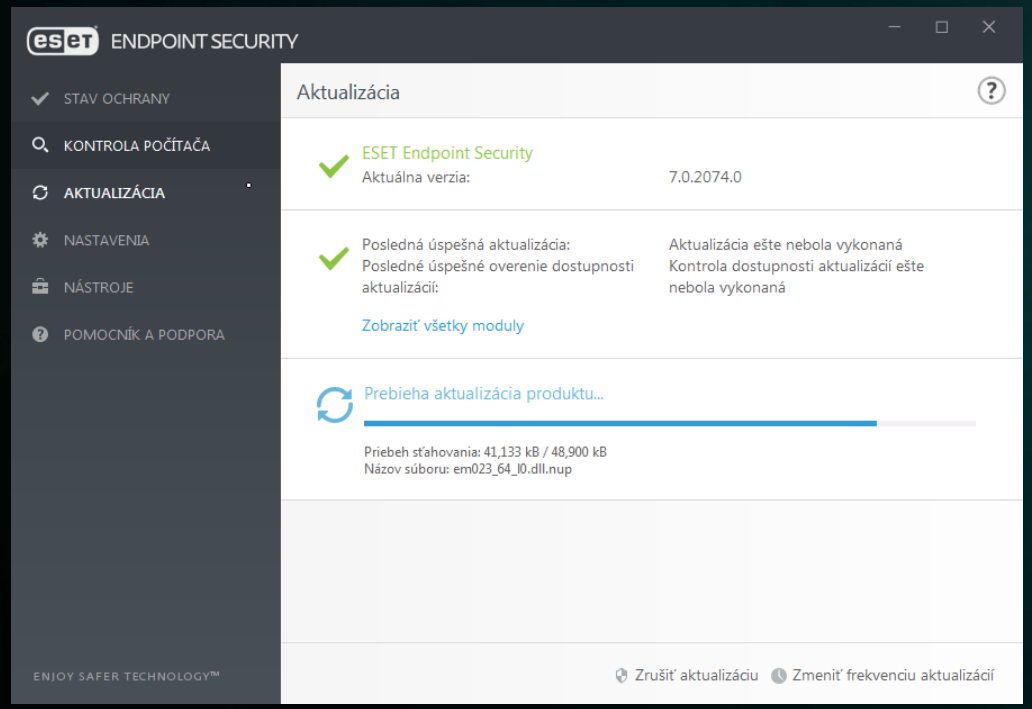
Detekčné jadro

- kontrola súborov, emailov a internetovej komunikácie
- eliminácia hrozby, zablokovanie, vyliečenie, zmazanie alebo presun do karantény
- využívanie najnovších technológií ako DNA detekcia, strojové učenie a heuristika
- technológia Anti-Stealth (rootkity)
- ThreatSense



Aktualizácia programových komponentov

- aktualizácia samotného programu ESET (nové funkcie)
- aktualizácie sprístupnené priamo v produkte rovnako ako detekčné jadro a moduly



Čo je nové? (alebo vylepšené, verzie 6.x, 7.x)

- Grafické prostredie
- Ochrana pred botnetmi
- Vylepšená správa zariadení
- Anti-Phishing ochrana
- Pokročilá kontrola pamäte
- Rozšírený Exploit blocker
- Nový Smart režim pre HIPS
- Aplikácia pravidiel podľa časových období

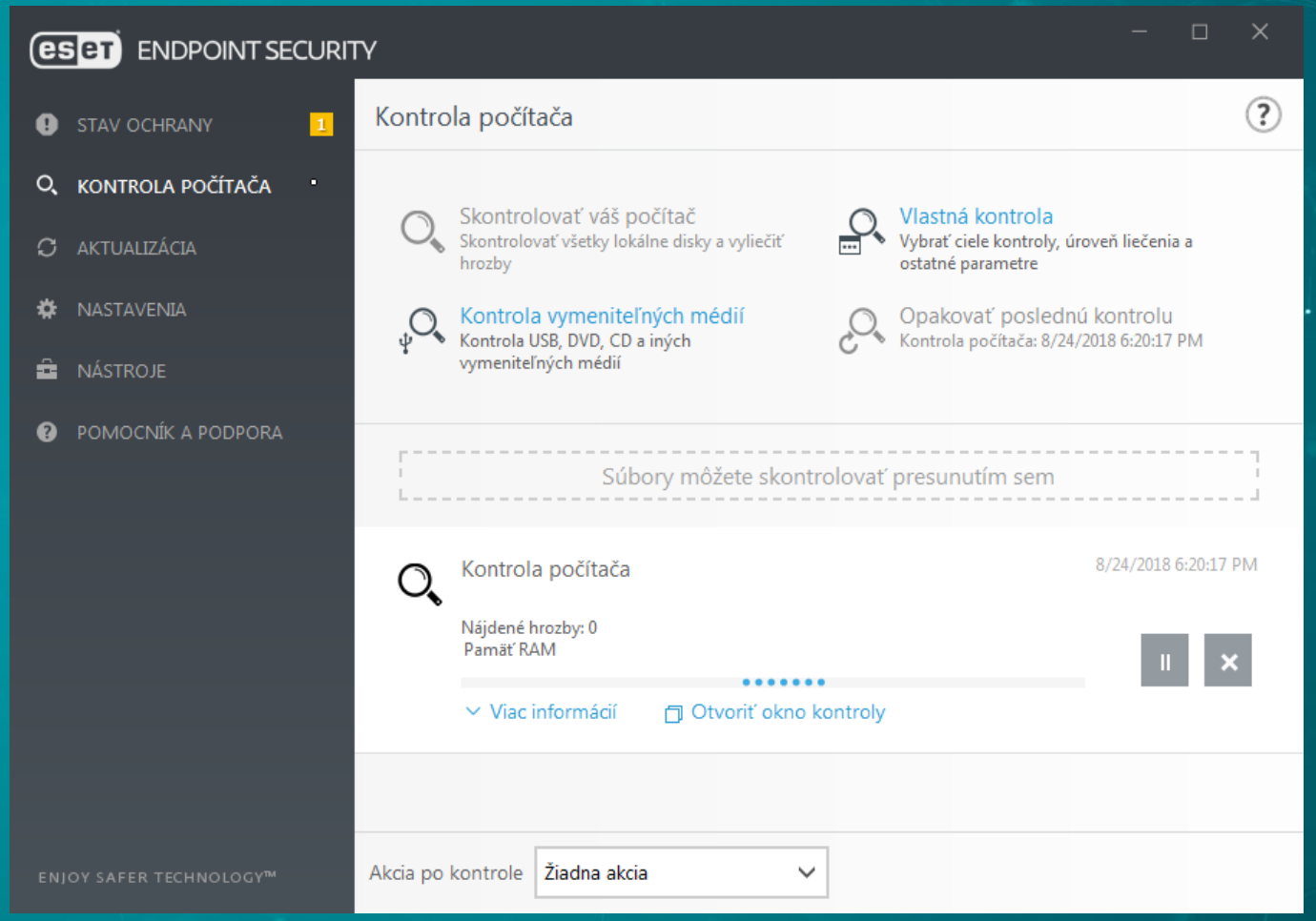
Čo je nové? (alebo vylepšené, verzie 6.x, 7.x)

- Ochrana pred sieťovými útokmi dostupná aj v ESET Endpoint Antivirus
- Nový typ zápisu do protokolov
- Vylepšená webová kontrola
- Personálny firewall (pravidlá priamo z protokolov a IDS
- Vylepšená detekcia a odstraňovanie bezpečnostných programov
- Kontrola UEFI
- Ransomware Shield
- Pokročilé strojové učenie
- Interaktívne upozornenia
- Vylúčenia

ESET Endpoint Antivirus 7 for Linux

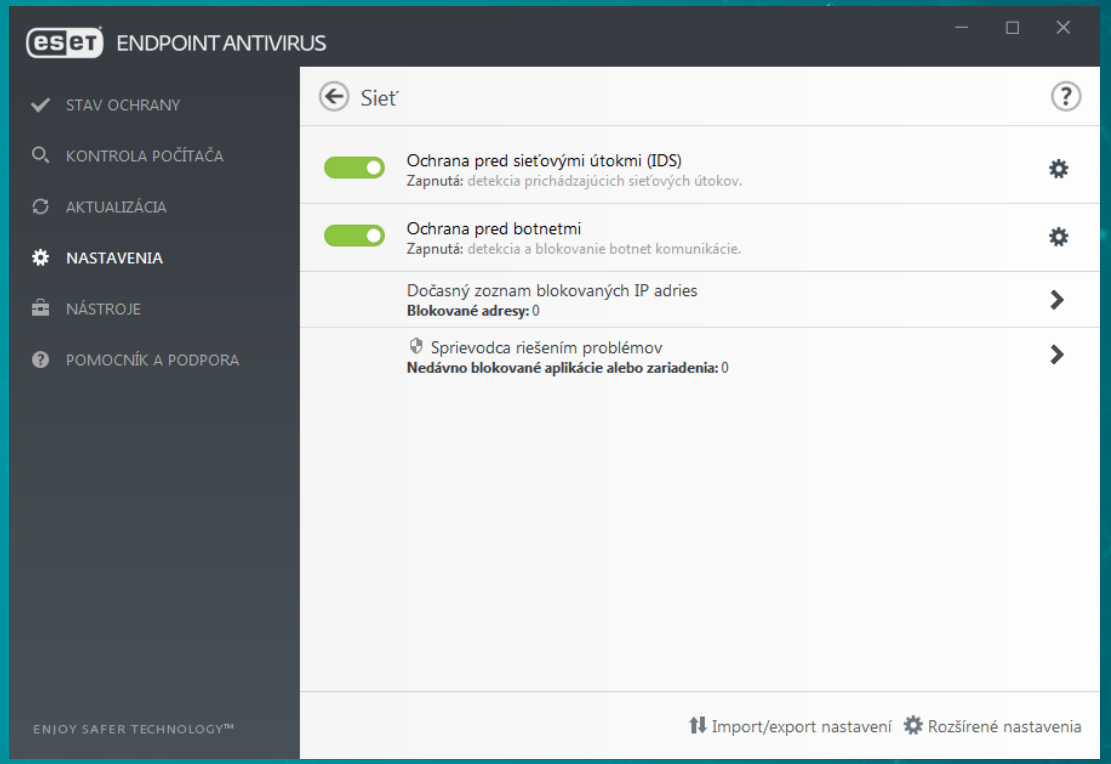
Nové grafické prostredie

- prepracované grafické prostredie
- jednoduchosť použitia
- súčasný dizajn aj na základe pripomienok zákazníkov v rámci celého sveta



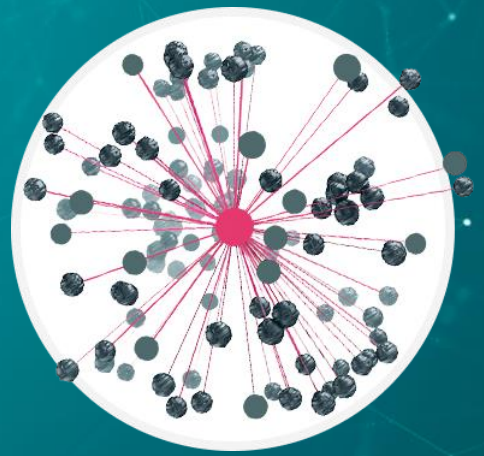
Ochrana pred sieťovými útokmi dostupná aj v ESET Endpoint Antivirus

- ochrana pred sieťovými útokmi (IDS) – analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi, zablokovanie komunikácie
- rozšírenie firewallu – vylepšuje detekciu tzv. exploitov (SMB, RPC, RDP)
- Informácie o nezabezpečených sieťach



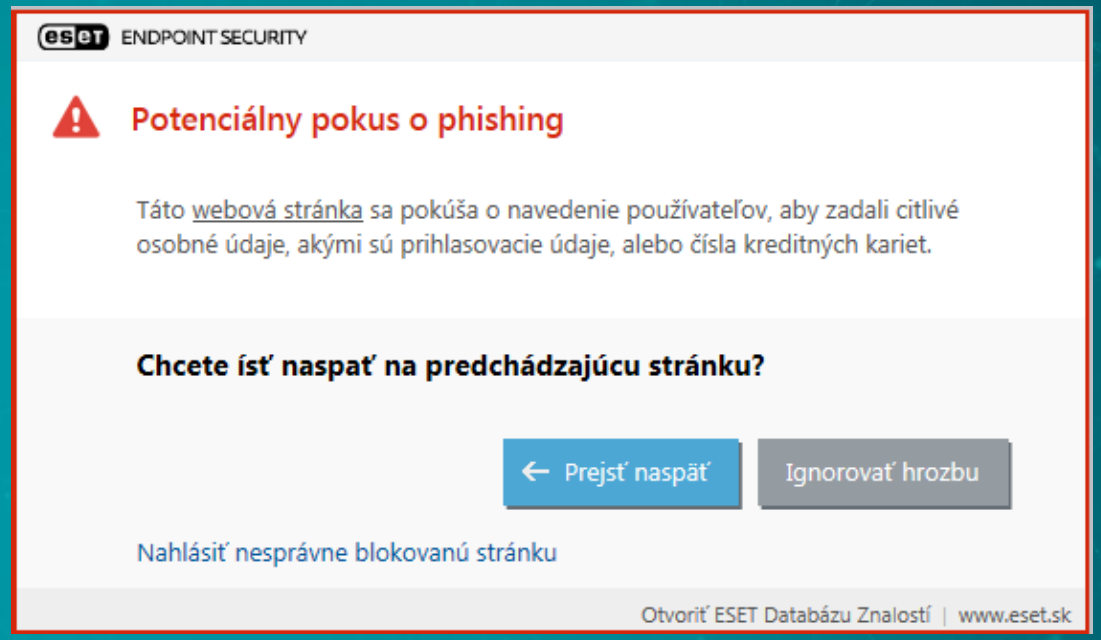
Ochrana pred botnetmi

- Bot/webový robot – škodlivý program prechádza sieťové adresy a infikuje zraniteľné počítače
- deteguje a blokuje komunikáciu s riadiacimi C&C servermi rozpoznávaním charakteristík
- V rámci spolupráce s FBI, Interpolom, Europolom niekoľko rozbitých botnetových sietí a zatknutia páchateľov



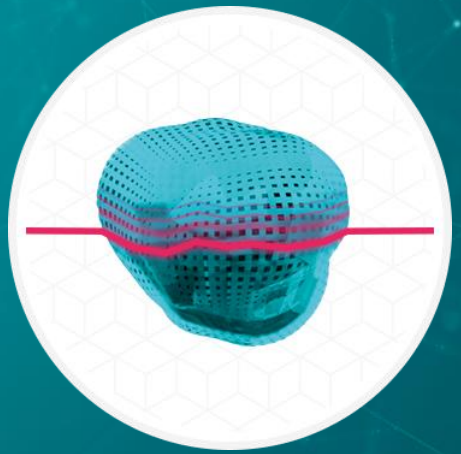
Anti-Phishing ochrana

- ochrana pred sociálnym inžinierstvom (získavanie citlivých údajov – heslá k bankovým účtom, PIN kódy, ...)
- falošný email s odkazom na webovú stránku s phishingovým odkazom
- nedajte sa nachytať
- nahlasovanie phishingových stránok https://phishing.eset.com/



Pokročilá kontrola pamäte

- Čo ak heuristika neodhalí hrozbu?
- v spolupráci s Exploit Blocker zvyšuje ochranu proti malvéru
- identifikuje podozrivé správanie a deteguje hrozby v pamäti systému
- „bezsúborové“ hrozby – parazitujú v pamäti
- dodatočná vrstva ochrany

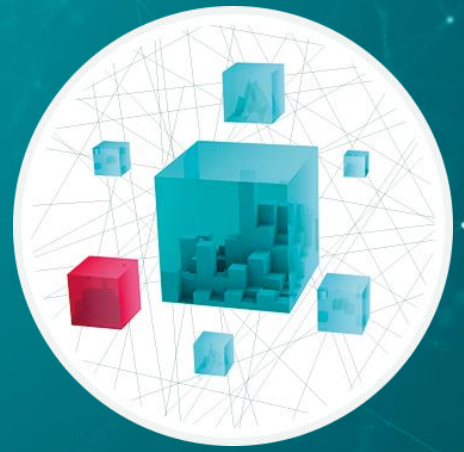


Rozšírený Exploit blocker

- monitorovanie často zneužívaných aplikácií (web prehliadač, prehliadač PDF dokumentov, e-mailový klient, flash, java,...)
- sledovanie techník zneužitia namiesto identifikátorov CVE
- analýza správania sa procesu
- spolupráca s ESET LiveGrid® cloud systém

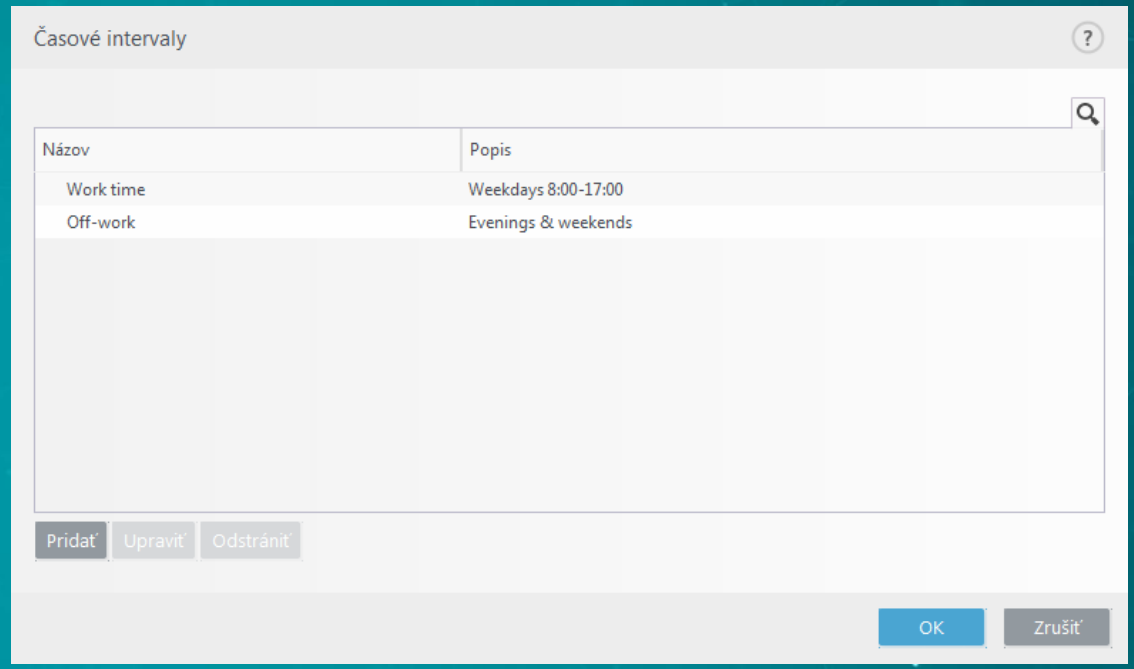
Nový Smart režim pre HIPS

- Host-based Intrusion Prevention System – chráni pred malvérom a nechcenou aktivitou v systéme
- pokročilá analýza správania
- Smart režim – upozornenia len v prípade skutočne podozrivých udalostí
  - Automatický režim
  - Interaktívny režim
  - Režim politík
  - Učiaci sa režim



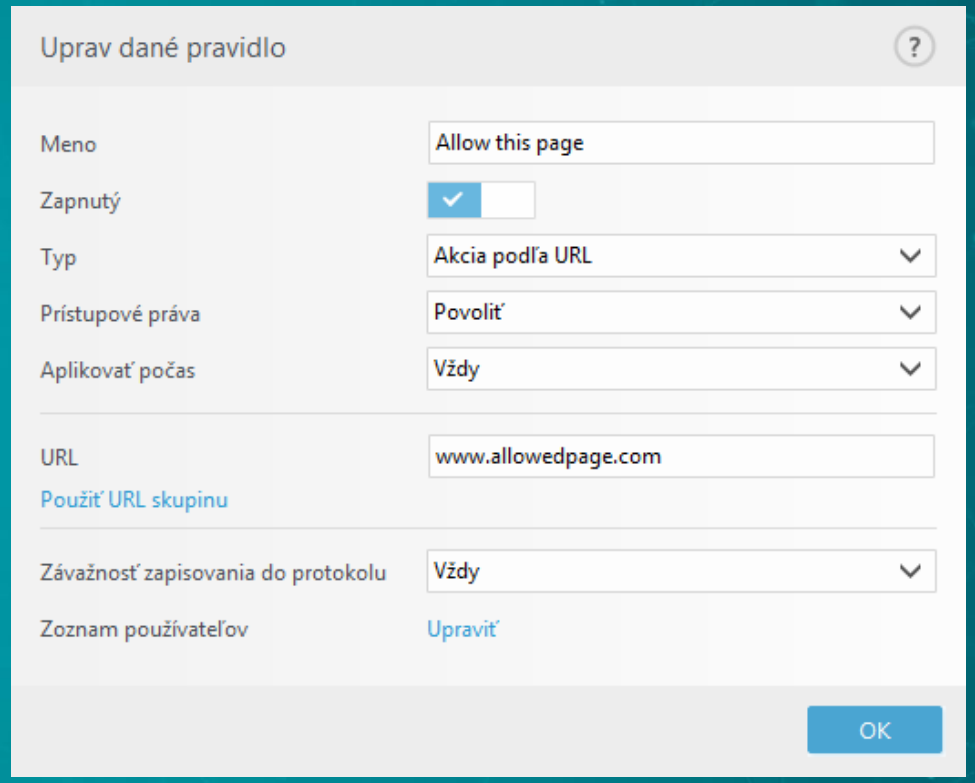
Aplikácia pravidiel podľa časových období

- pravidlá správy zariadení a webovej kontroly možné aplikovať na konkrétne časové obdobie
- často využívané časové intervaly (pracovná doba, víkendy, ...)
- priraďovanie časových intervalov ku konkrétnym pravidlám



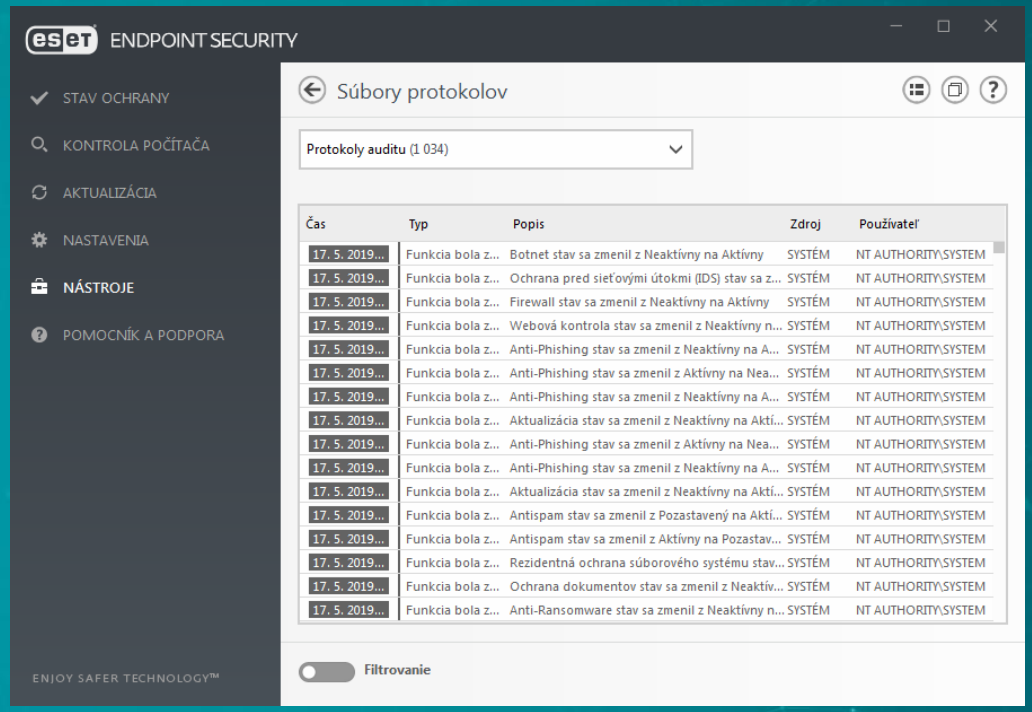
Vylepšená webová kontrola

- riadi prístup k webovým stránkam s potenciálne neprístojným obsahom alebo porušovaním intelektuálneho vlastníctva
- definícia pravidiel podľa URL adresy alebo politiky pre sieťové lokácie
- “soft” politiky blokovania



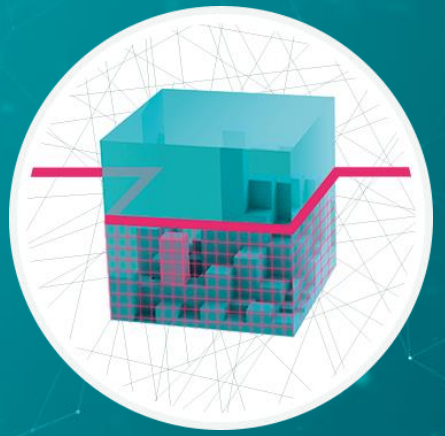
Nový typ zápisu do protokolov

- protokoly obsahujú informácie o všetkých systémových udalostiach
- silný nástroj systémovej analýzy, odhaľovania problémov, rizík a hľadaní riešení



Kontrola UEFI

- UEFI nahrádza BIOS
- ESET používa špeciálnu vrstvu na ochranu UEFI
- Monitoruje a vynucuje zabezpečenie prostredia pred štartom (integrita firmvéru)
- LoJax – už nie len koncept. Identifikovali sme zrejme prvý škodlivý kód, ktorý infikuje náhradu BIOSu.
- skupina Sednit – v pozadí útoku na Demokratickú stranu v USA pred voľbami (2016), úniky emailov Svetovej antidopingovej agentúry, ...
- Používajte Secure Boot

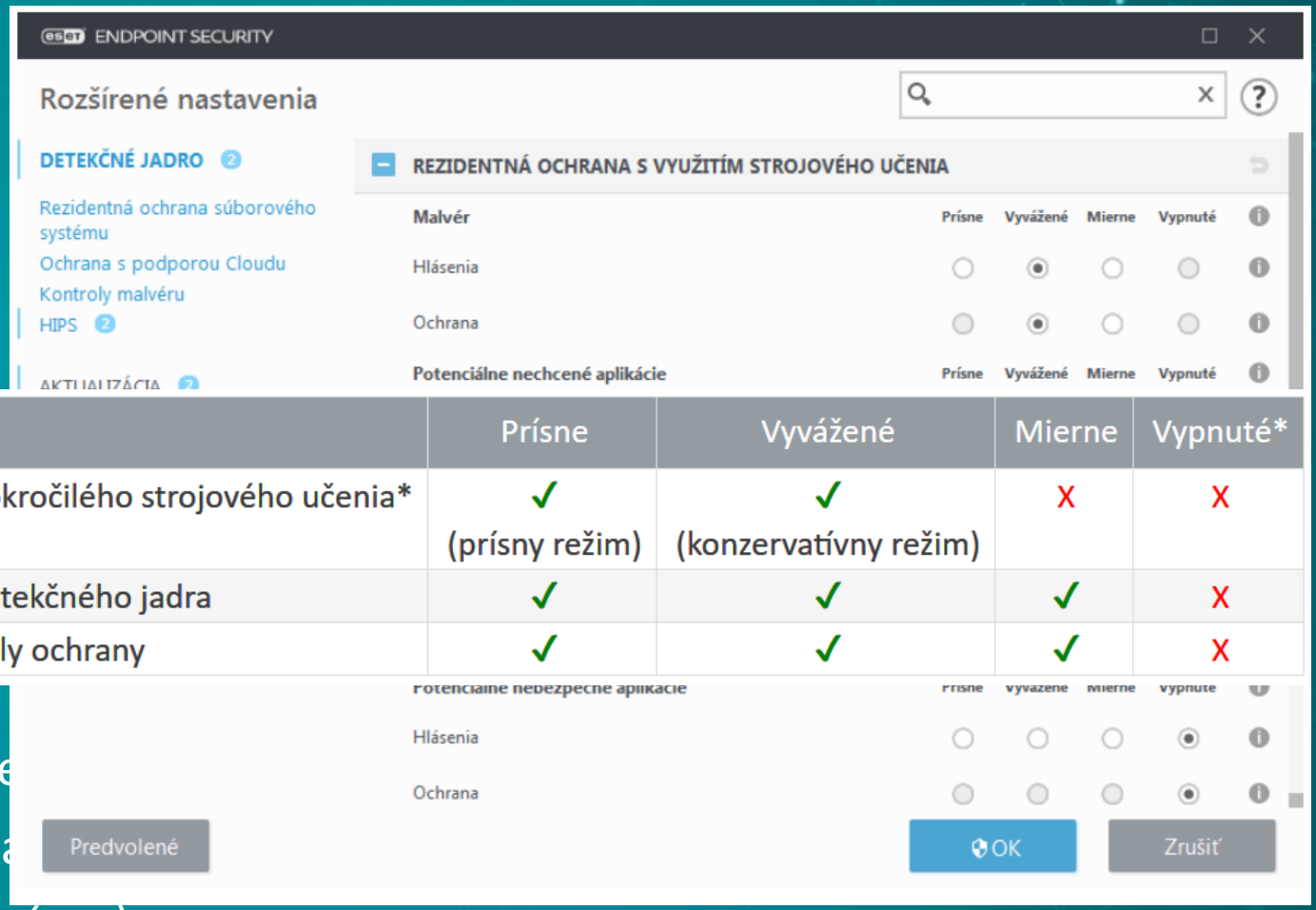


Ransomware Shield

- Ransomware – malvér, ktorým útočníci uzamknú zariadenie alebo zašifrujú jeho obsah s cieľom vymôcť peniaze
  - Screen locker
  - PIN locker
  - Disk coding
  - Crypto
- Ďalšia vrstva chrániaca používateľov pred ransomware
- Monitoruje a vyhodnocuje všetky spustené aplikácie na základe ich správania a reputácie
- Škodlivé/podozrivé správanie je blokované, prípadne je vyzvaný používateľ na reakciu

Pokročilé strojové učenie

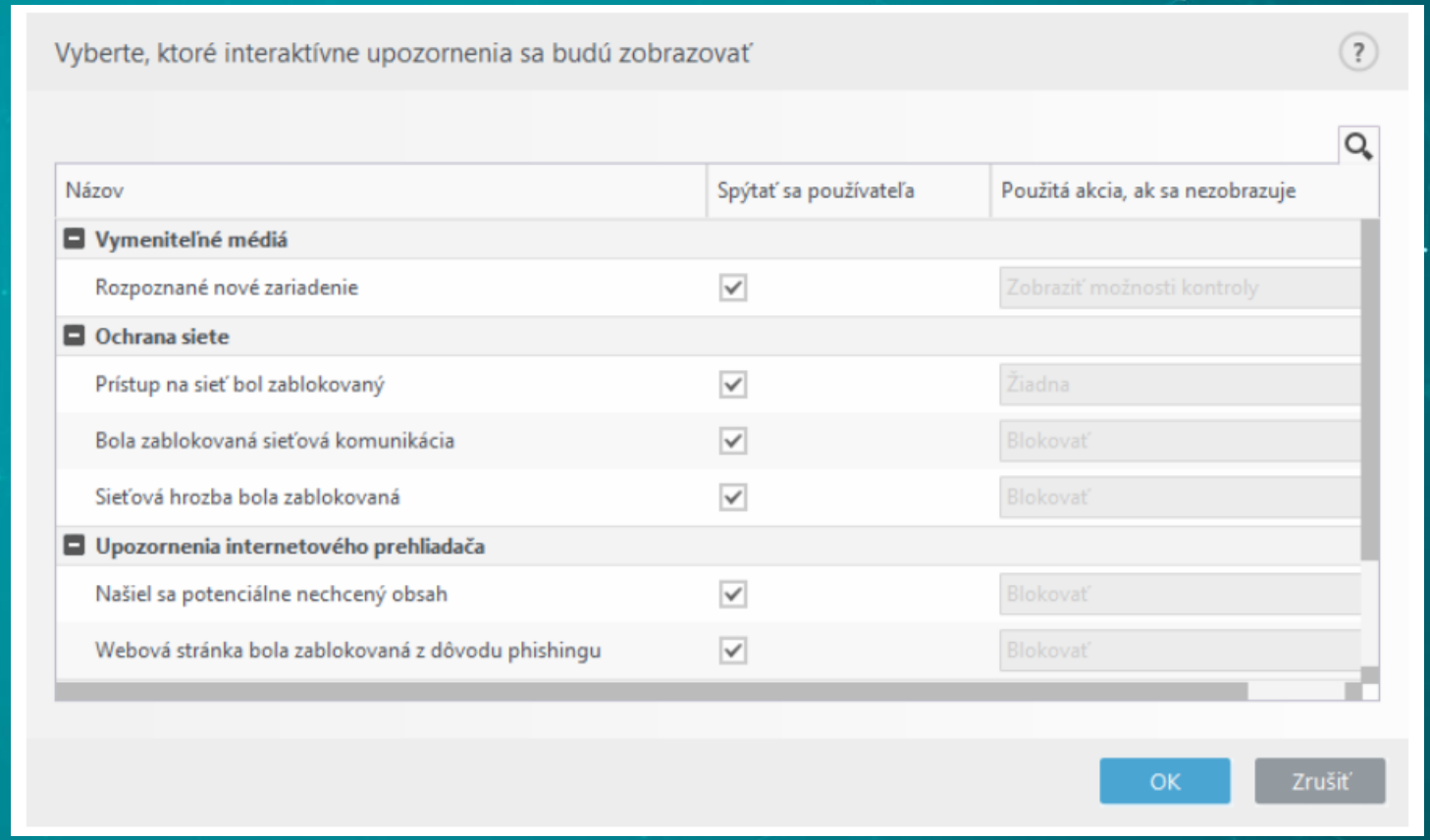
- ESET with ML – 1990
- ESET with NN – 1998
- Rezidentná ochrana s využitím strojového učenia
- Rozšírené nastavenia detekčného jadra
- Odporúčané postupy
  - 1. počiatočná fáza (vyvážené, mierne
  - 2. prechodná fáza (implementácia na
  - 3. produkčná fáza (vyvážené alebo prísne)



	Prísne	Vyvážené	Mierne	Vypnuté*
Modul pokročilého strojového učenia*	✓ (prísny režim)	✓ (konzervatívny režim)	X	X
Modul detekčného jadra	✓	✓	✓	X
Iné moduly ochrany	✓	✓	✓	X

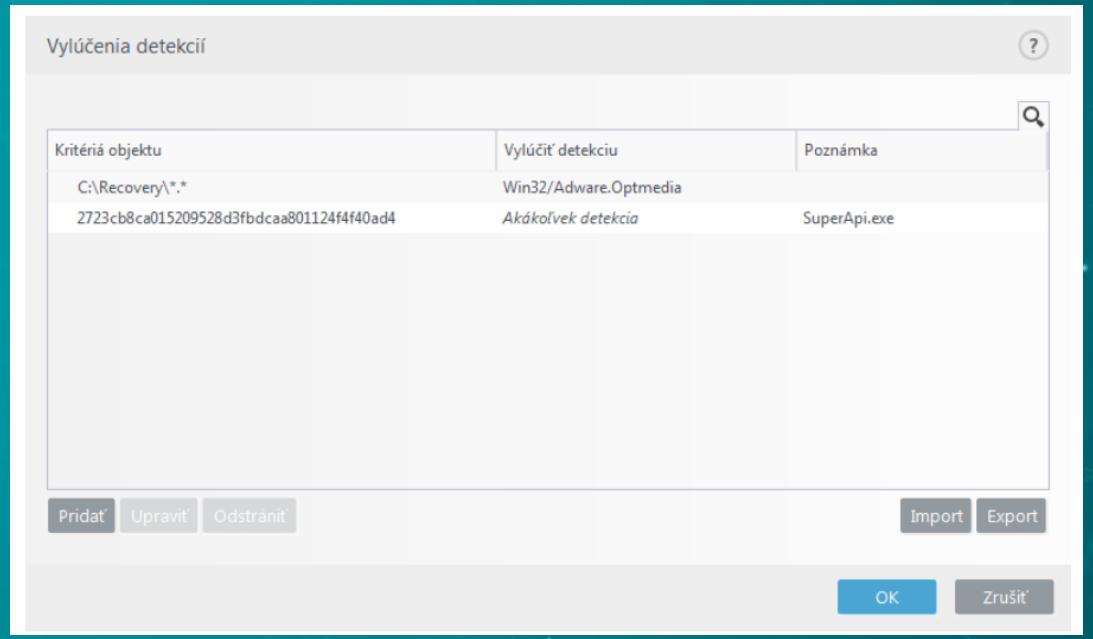
Interaktívne upozornenia

- Prispôsobenie správania interaktívnych upozornení
  - Vymeniteľné média
  - Ochrana siete
  - Upozornenia internetového prehliadača



Vylúčenia

- Výkonnostné vylúčenia – vylúčenie súborov/priečinkov
  - napr. veľké databázové súbory (zvážiť použitie)
- Vylúčenia detekcii – vylúčenie detegovaných objektov z procesu liečenia
  - Kritéria pre vylúčenie (cesta, názov detekcie, HASH)




Key takeaways?

ESET Endpoint ochrana

	verzia 5.x	verzia 6.x	verzia 7.x
Pokročilé strojové učenie/pokročilá vrstva ochrany	-	-	✓
Kontrola UEFI	-	-	✓
IDS dostupné aj pre Endpoint Antivirus	-	-	✓
Aplikácie časových období	-	-	✓
Výkonnostné a detegované vylúčenia	-	-	✓
Nový prehľadný dizajn	-	-	✓
Webová kontrola (pravidlá)	-	✓	✓
Pokročilá ochrana pred botnetmi	-	✓	✓
Anti-Phishing	-	✓	✓
Exploit Blocker	-	✓	✓
Antivirus/Antispyware/Firewall	✓	✓	✓

New Life for ESET

ESET Endpoint Security

Version	Release Date	Latest build	Updated	Status	Next Status	Expected EOL
7.x	16-Aug-18	7.2.2055.0	2019-11-12	Full Support	Limited Support	TBA
6.6	25-Feb-15	6.6.2089.2	2018-11-13	Full Support	Limited Support	TBA
6.5	14-Mar-17	6.5.2123.5	28-Nov-17	Limited Support	Basic Support	TBA
6.4	7-Jun-16	6.4.2014.0	7-Jun-16	Basic Support	End of Life	TBA
6.3	21-Jan-16	6.3.2016.0	21-Jan-16	Basic Support	End of Life	TBA
6.2	25-Feb-2015	6.2.2033.0	29-Jul-2015	Basic Support	End of Life	Feb 2020
6.1	11-Dec-2014	6.1.2227.0		Basic Support	End of Life	Feb 2020
5.x	29-May-12	5.0.2272.7	2018-05-22	Basic Support	End of Life	Dec 2020

Július Selecký

ESET Senior Technical Pre-Sales Representative

julius.selecky@eset.sk

/ESET @ESET

ENJOY SAFER TECHNOLOGY™