



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



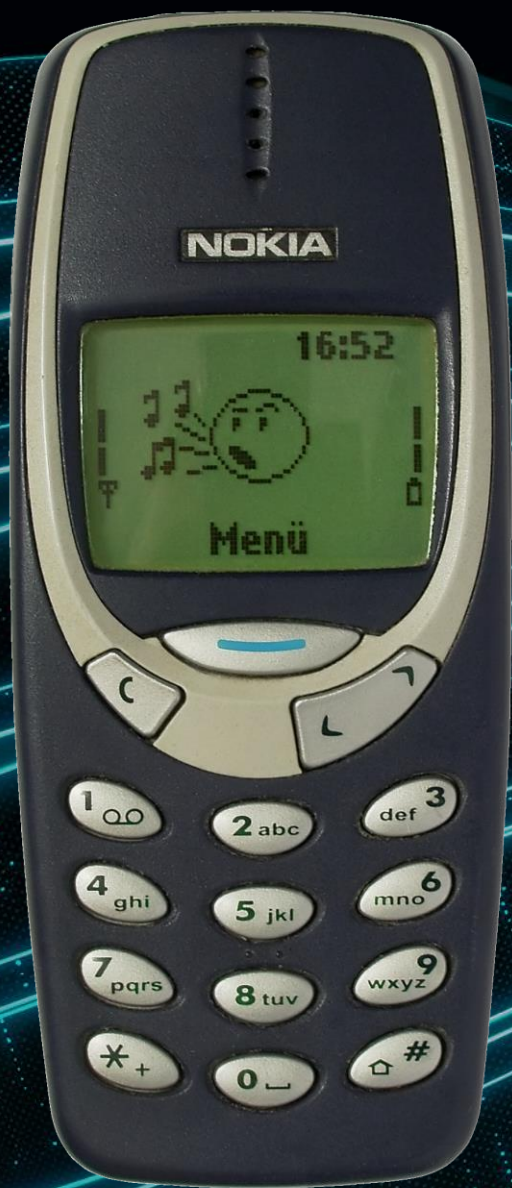


1BN+ INTERNET USERS
PROTECTED BY OUR TECHNOLOGY



UŽÍVAJTE SI BEZPEČNĚJŠIE
TECHNOLÓGIE™

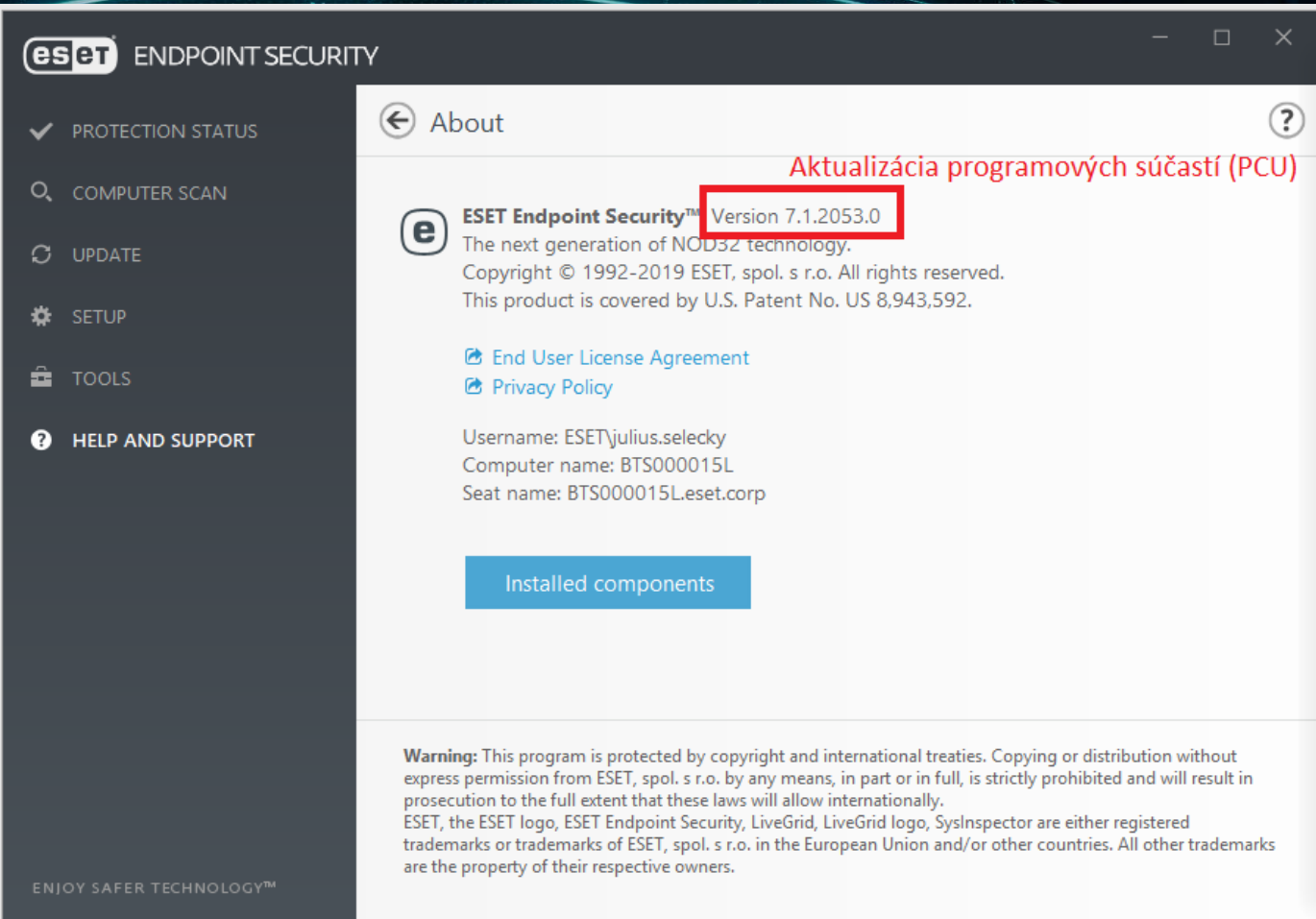




Vs.



Pravidelné aktualizácie detekčného jadra vs. aktualizácia programových súčastí



e **ESET Endpoint Security™** Version 7.1.2053.0

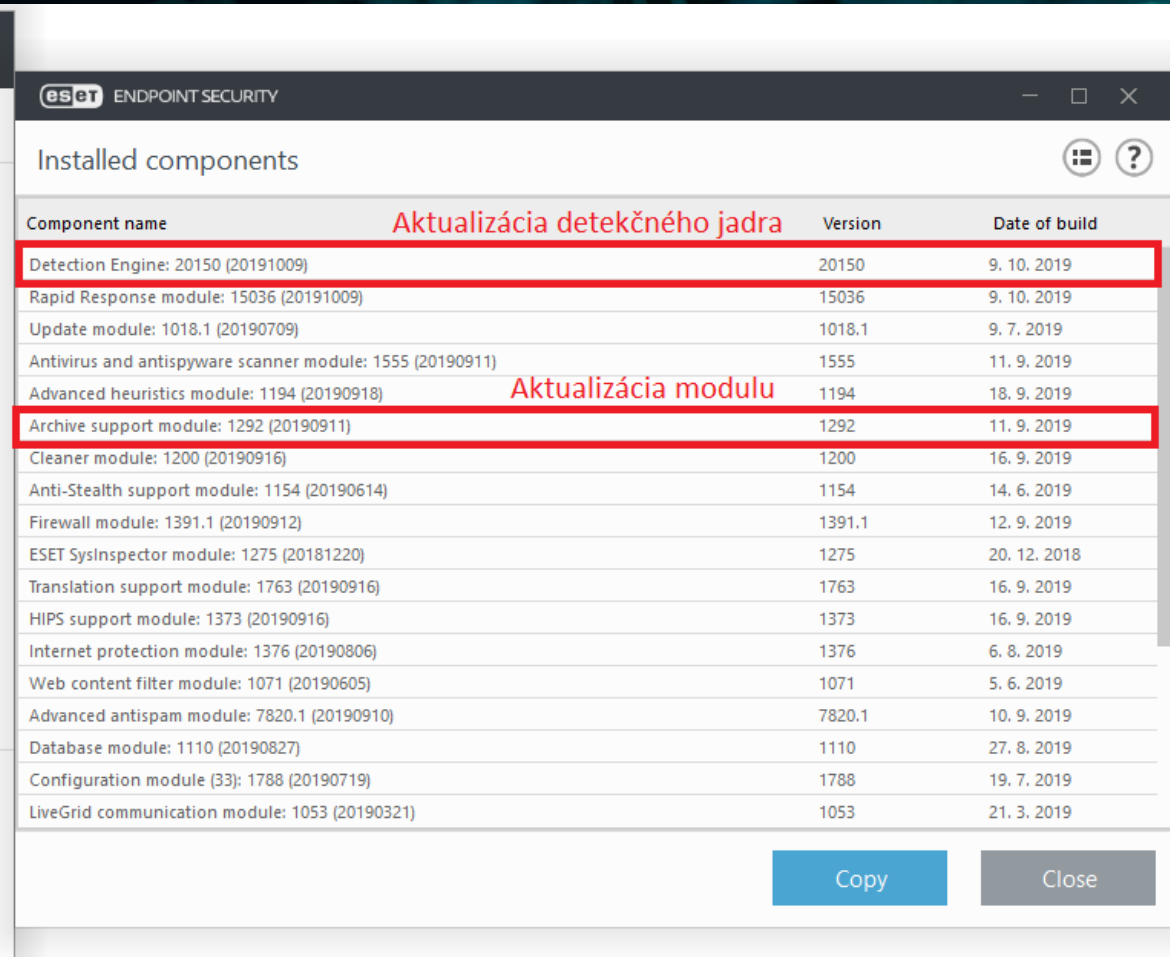
The next generation of NOD32 technology.
Copyright © 1992-2019 ESET, spol. s r.o. All rights reserved.
This product is covered by U.S. Patent No. US 8,943,592.

[End User License Agreement](#)
[Privacy Policy](#)

Username: ESET\julius.selecky
Computer name: BTS000015L
Seat name: BTS000015L.eset.corp

[Installed components](#)

Warning: This program is protected by copyright and international treaties. Copying or distribution without express permission from ESET, spol. s r.o. by any means, in part or in full, is strictly prohibited and will result in prosecution to the full extent that these laws will allow internationally.
ESET, the ESET logo, ESET Endpoint Security, LiveGrid, LiveGrid logo, SysInspector are either registered trademarks or trademarks of ESET, spol. s r.o. in the European Union and/or other countries. All other trademarks are the property of their respective owners.



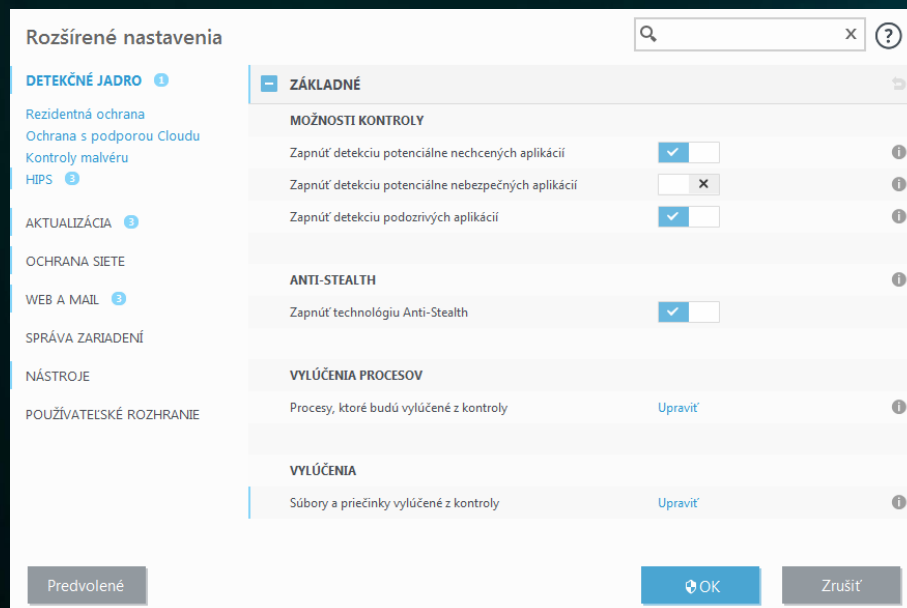
Installed components

Component name	Aktualizácia detekčného jadra	Version	Date of build
Detection Engine: 20150 (20191009)		20150	9. 10. 2019
Rapid Response module: 15036 (20191009)		15036	9. 10. 2019
Update module: 1018.1 (20190709)		1018.1	9. 7. 2019
Antivirus and antispymware scanner module: 1555 (20190911)		1555	11. 9. 2019
Advanced heuristics module: 1194 (20190918)	Aktualizácia modulu	1194	18. 9. 2019
Archive support module: 1292 (20190911)		1292	11. 9. 2019
Cleaner module: 1200 (20190916)		1200	16. 9. 2019
Anti-Stealth support module: 1154 (20190614)		1154	14. 6. 2019
Firewall module: 1391.1 (20190912)		1391.1	12. 9. 2019
ESET SysInspector module: 1275 (20181220)		1275	20. 12. 2018
Translation support module: 1763 (20190916)		1763	16. 9. 2019
HIPS support module: 1373 (20190916)		1373	16. 9. 2019
Internet protection module: 1376 (20190806)		1376	6. 8. 2019
Web content filter module: 1071 (20190605)		1071	5. 6. 2019
Advanced antispam module: 7820.1 (20190910)		7820.1	10. 9. 2019
Database module: 1110 (20190827)		1110	27. 8. 2019
Configuration module (33): 1788 (20190719)		1788	19. 7. 2019
LiveGrid communication module: 1053 (20190321)		1053	21. 3. 2019

[Copy](#) [Close](#)

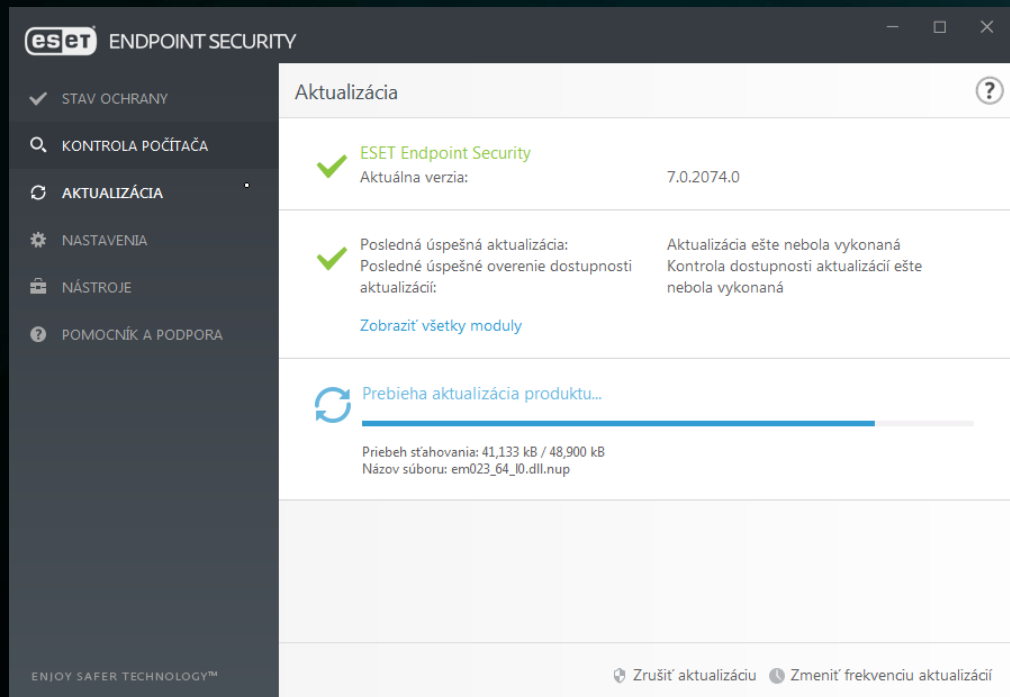
Detekčné jadro

- 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)

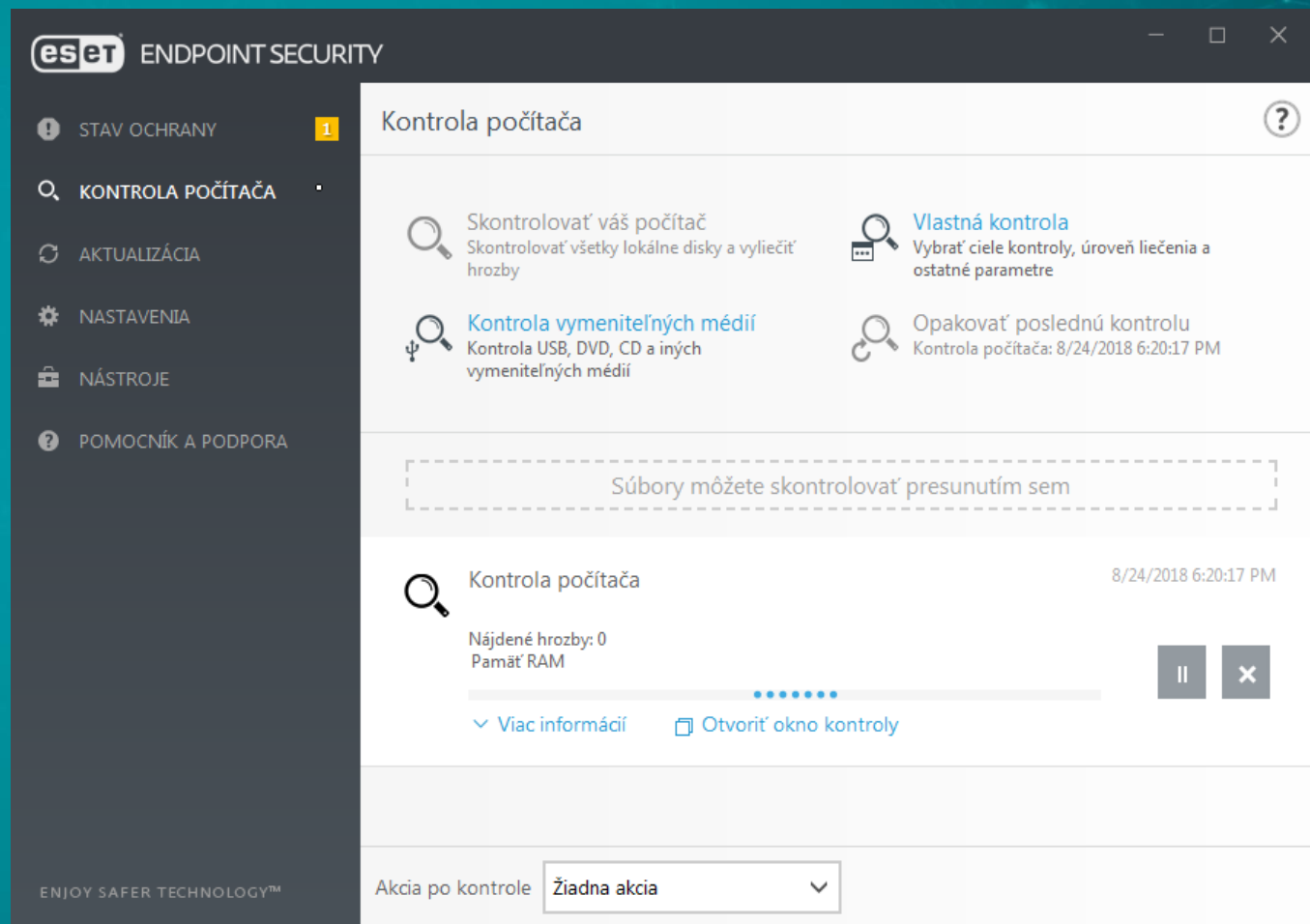
- Ochrana pred sieťovými útokmi dostupná aj v ESET Endpoint Antivirus
- Nový typ zápisu do protokolov
- Vylepšená webová kontrola
- Personálny firewall (pravidlá priamo z protokolov a IDS)
- Vylepšená detekcia a odstraňovanie bezpečnostných programov
- Kontrola UEFI
- Ransomware Shield
- Pokročilé strojové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



ESET Endpoint Antivirus 7 for Linux

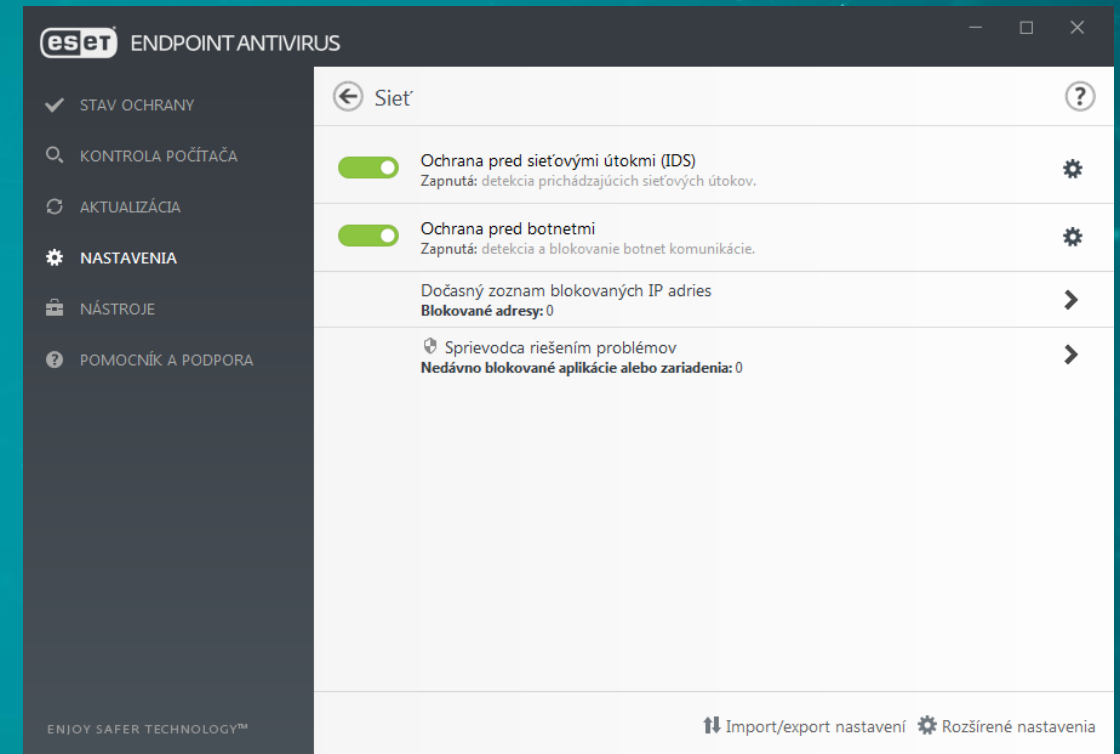
Nové grafické prostredie

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



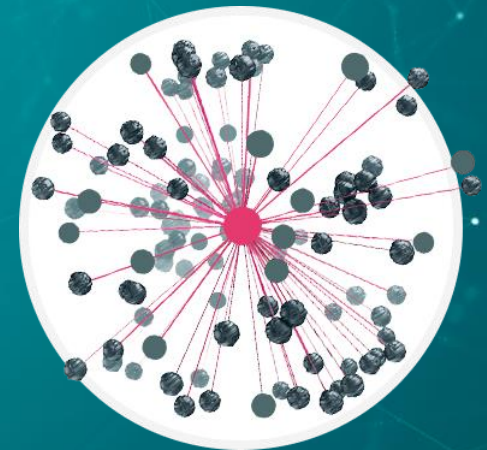
Ochrana pred sieťovými útokmi dostupná aj v ESET Endpoint Antivirus

- 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



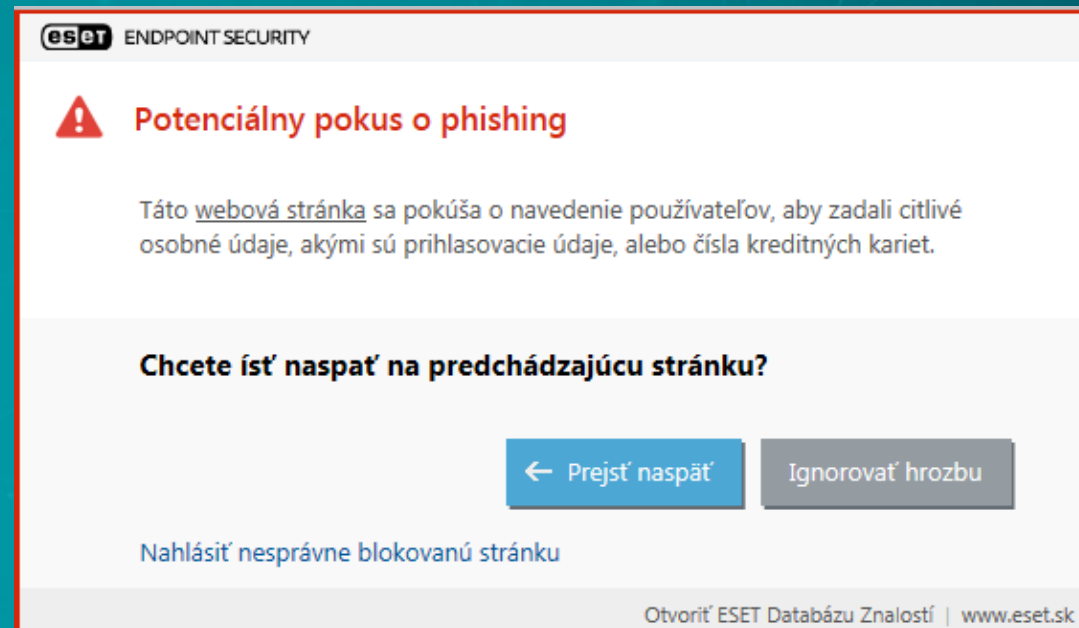
Ochrana pred botnetmi

- 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 páchatel'ov



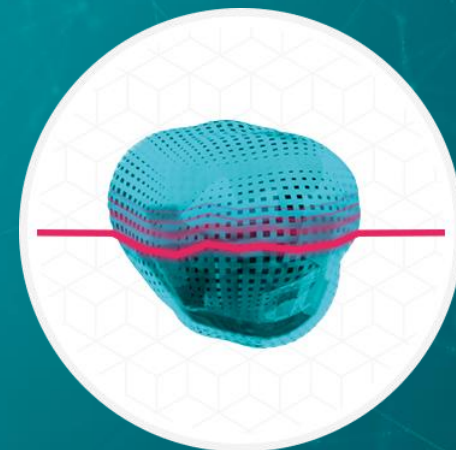
Anti-Phishing ochrana

- 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
- „bez súborové“ hrozby – parazitujú v pamäti
- dodatočná vrstva ochrany



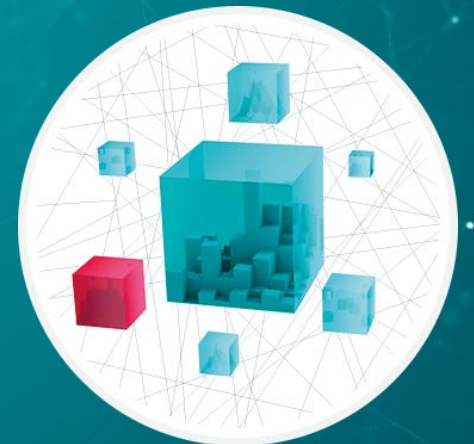
Rozšířený Exploit blocker

- 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 politik
 - 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, ...)
- priradovanie časových intervalov ku konkrétnym pravidlám

Časové intervaly

Názov	Popis
Work time	Weekdays 8:00-17:00
Off-work	Evenings & weekends

Pridať Upraviť Odstrániť

OK Zrušiť



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

Uprav dané pravidlo

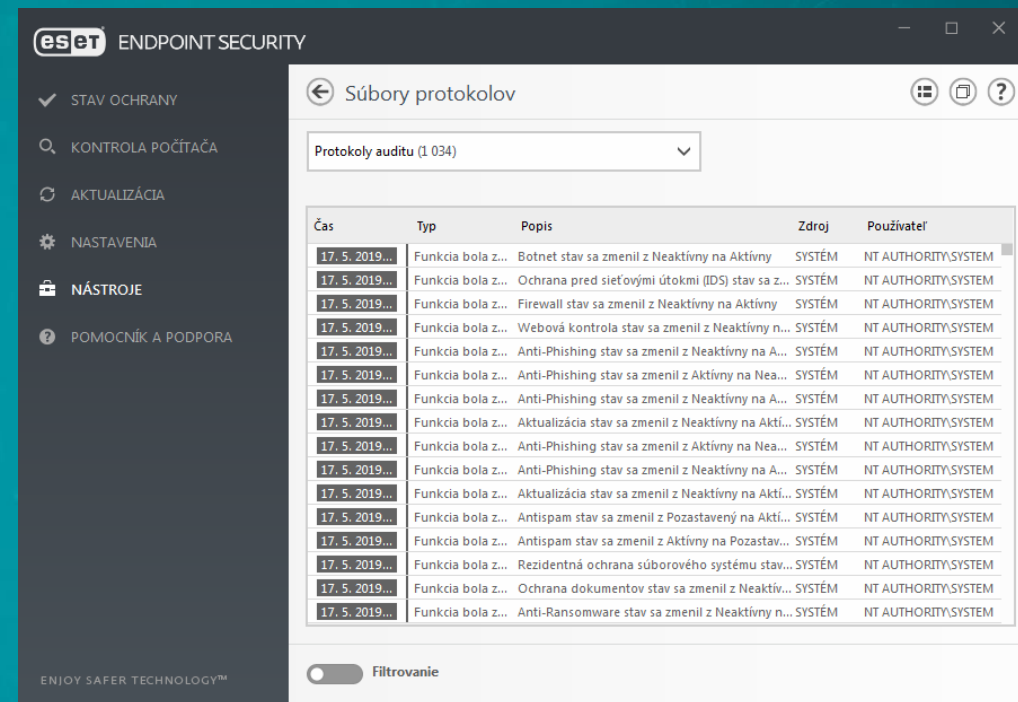
Meno	Allow this page
Zapnutý	☒
Typ	Akcia podľa URL
Prístupové práva	Povolit'
Aplikovať počas	Vždy
URL	www.allowedpage.com
Použiť URL skupinu	
Závažnosť zapisovania do protokolu	Vždy
Zoznam používateľov	Upraviť

OK



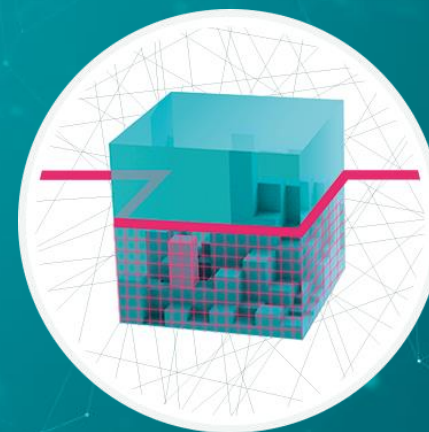
Nový typ zápisu do protokolov

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



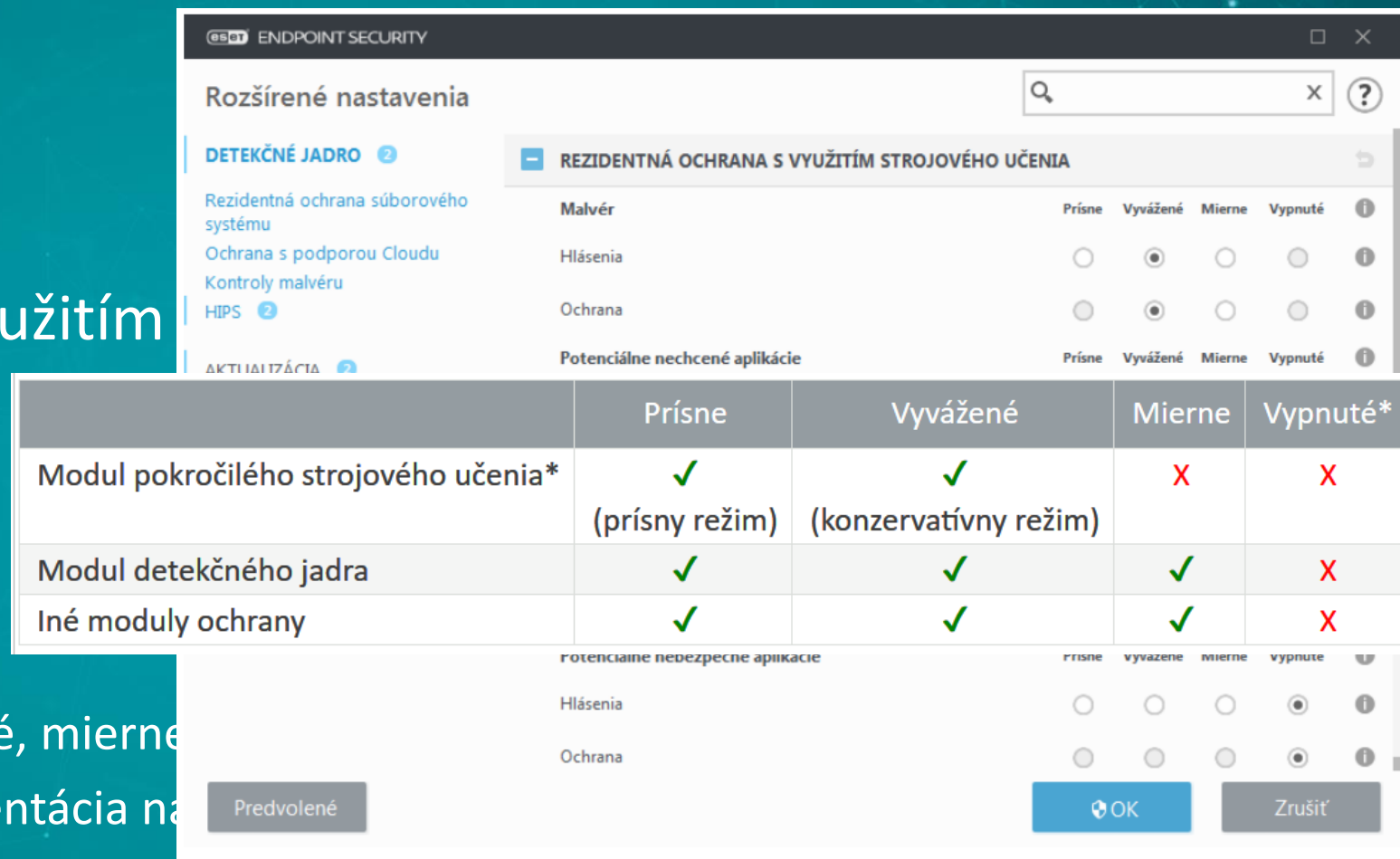
Ransomware Shield

- 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)



Interaktívne upozornenia

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

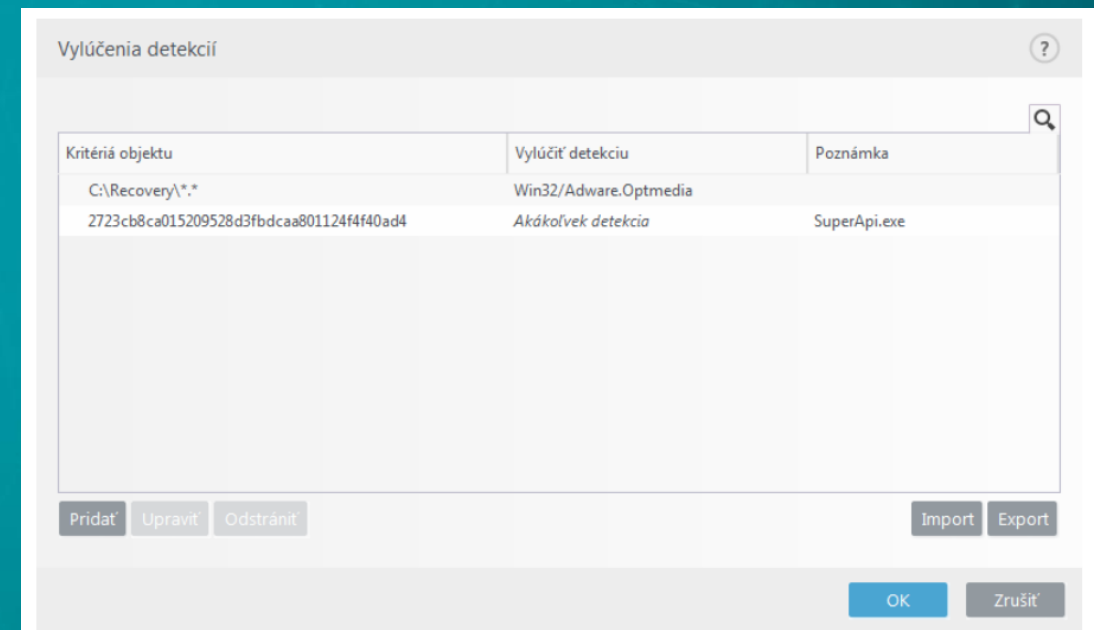
Vyberte, ktoré interaktívne upozornenia sa budú zobrazovať

Názov	Spýtať sa používateľa	Použitá akcia, ak sa nezobrazuje
Vymeniteľné médiá		
Rozpoznané nové zariadenie	☒	Zobraziť možnosti kontroly
Ochrana siete		
Pristup na sieť bol zablokováný	☒	Žiadna
Bola zablokovávaná sieťová komunikácia	☒	Blokovať
Sieťová hrozba bola zablokovávaná	☒	Blokovať
Upozornenia internetového prehliadača		
Našiel sa potenciálne nechcený obsah	☒	Blokovať
Webová stránka bola zablokovávaná z dôvodu phishingu	☒	Blokovať

OK Zrušiť

Vylúčenia

- Výkonnostné vylúčenia – vylúčenie súborov/priečinkov
 - napr. veľké databázové súbory (zvážiť použitie)
- Vylúčenia detekcií – 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