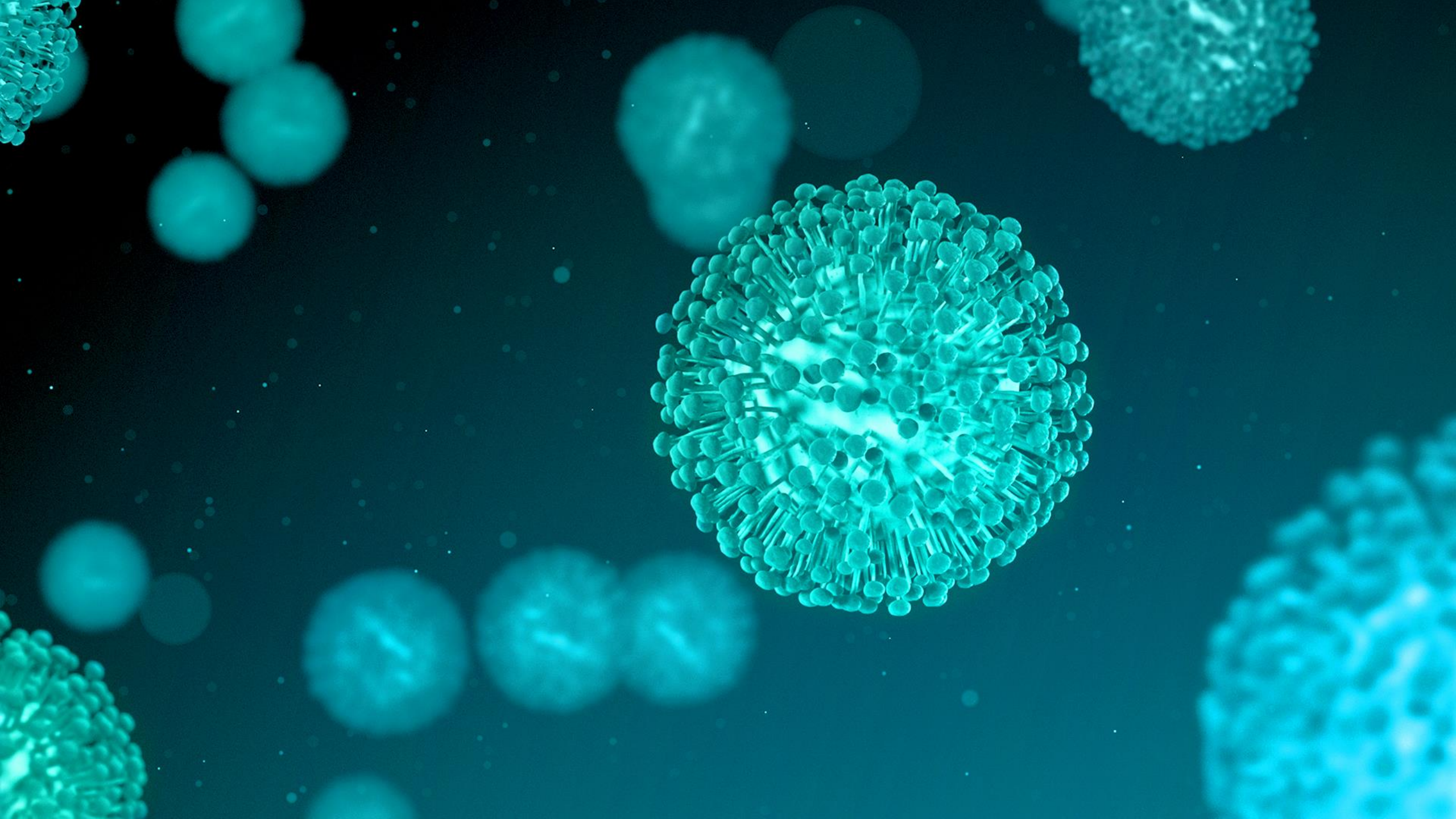
ENJOY SAFER TECHNOLOGY™

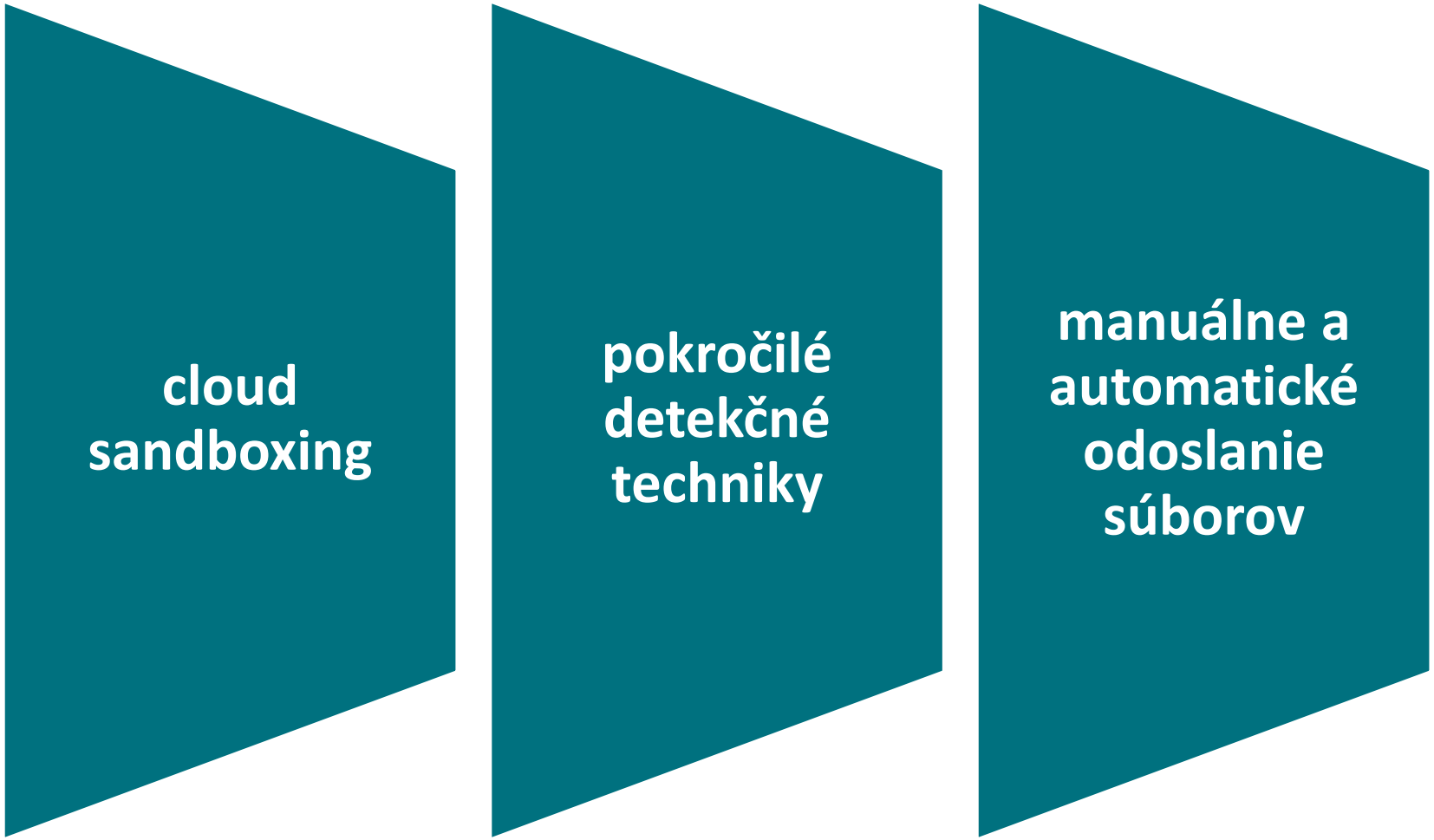
ESET Security Days

2020




ESET Dynamic Threat Defense

Čo je to ESET Dynamic Threat Defense (EDTD)



Hlavné výhody

1. automatizovaná ochrana proti 0-day zraniteľnostiam
2. využitie metód strojového učenia
3. ochrana staníc aj mimo LAN
4. priama podpora v produktoch od v.7
5. kompletný prehľad o odoslaných súboroch
6. možnosť regulovať odosielanie súborov

FILE BEHAVIOR REPORT

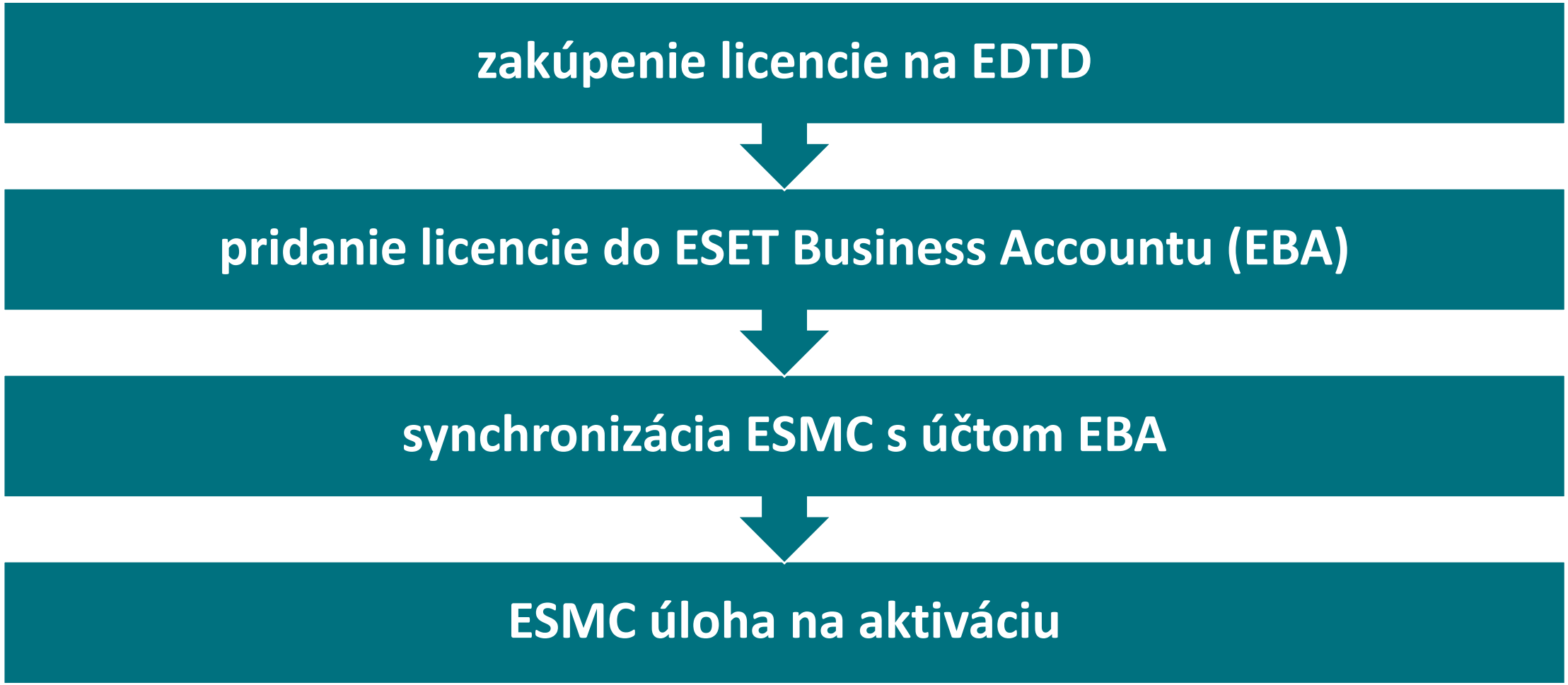
STATUS	**Malicious**
SHA-1	FED6A67C97B461A0DF1332AF61A89EA9FB5A540F
SIZE	436736B
CATEGORY	Executable

Detected Behaviors

BEHAVIOR	**Malware detected after execution**
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware detected with ESET scanning engine after execution

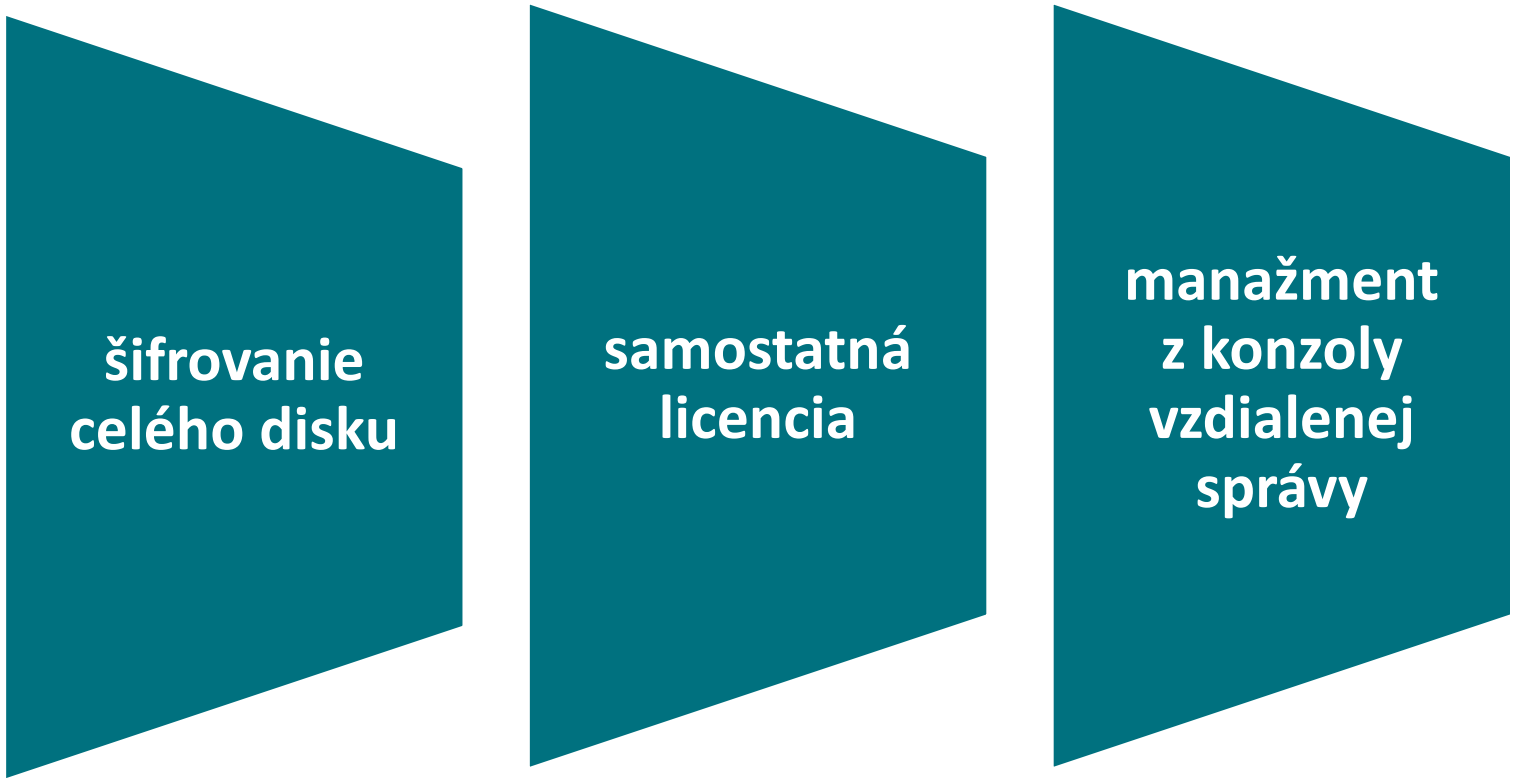
BEHAVIOR	**New files created in the Windows folder**
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence

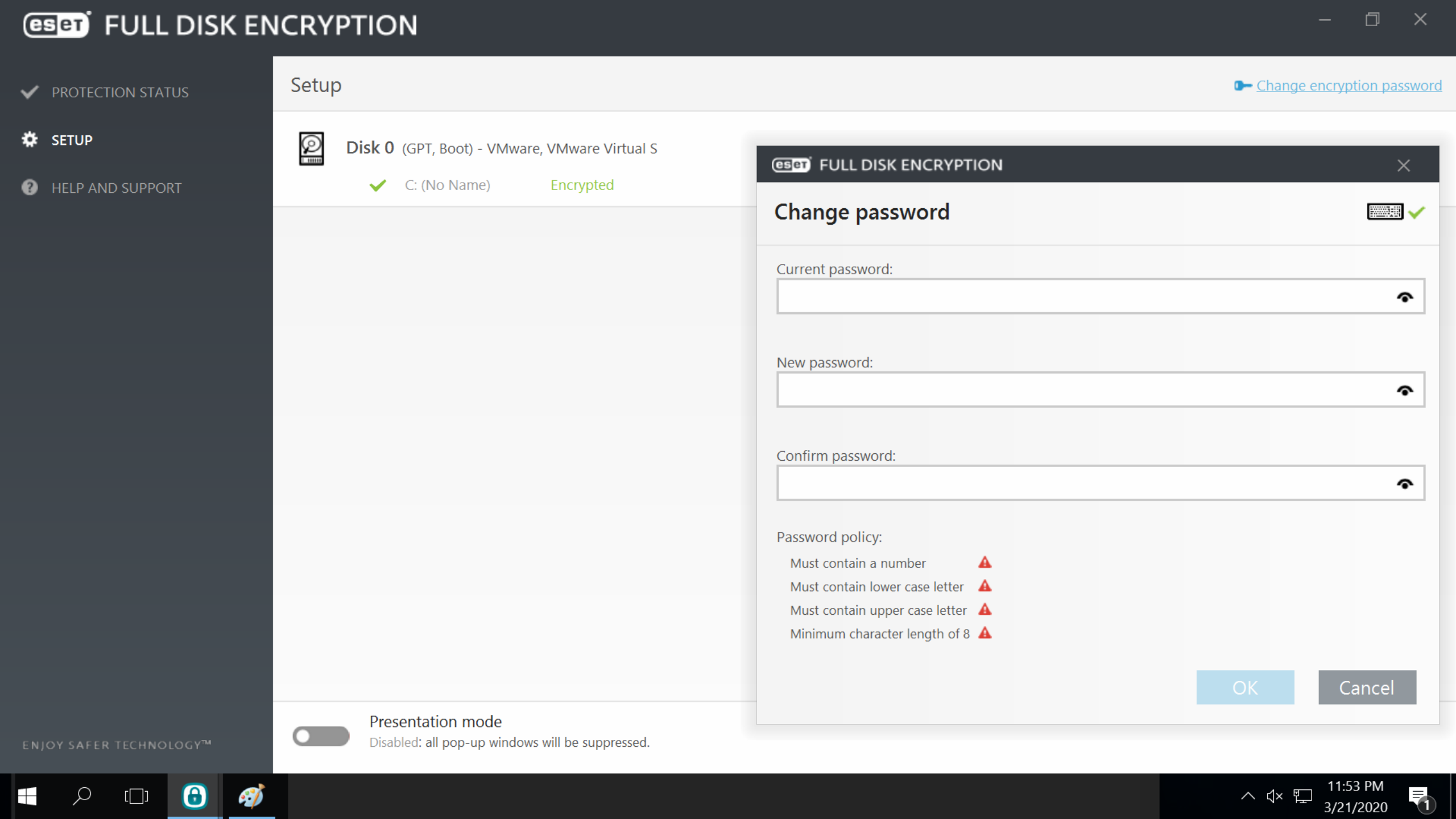
Použitie EDTD

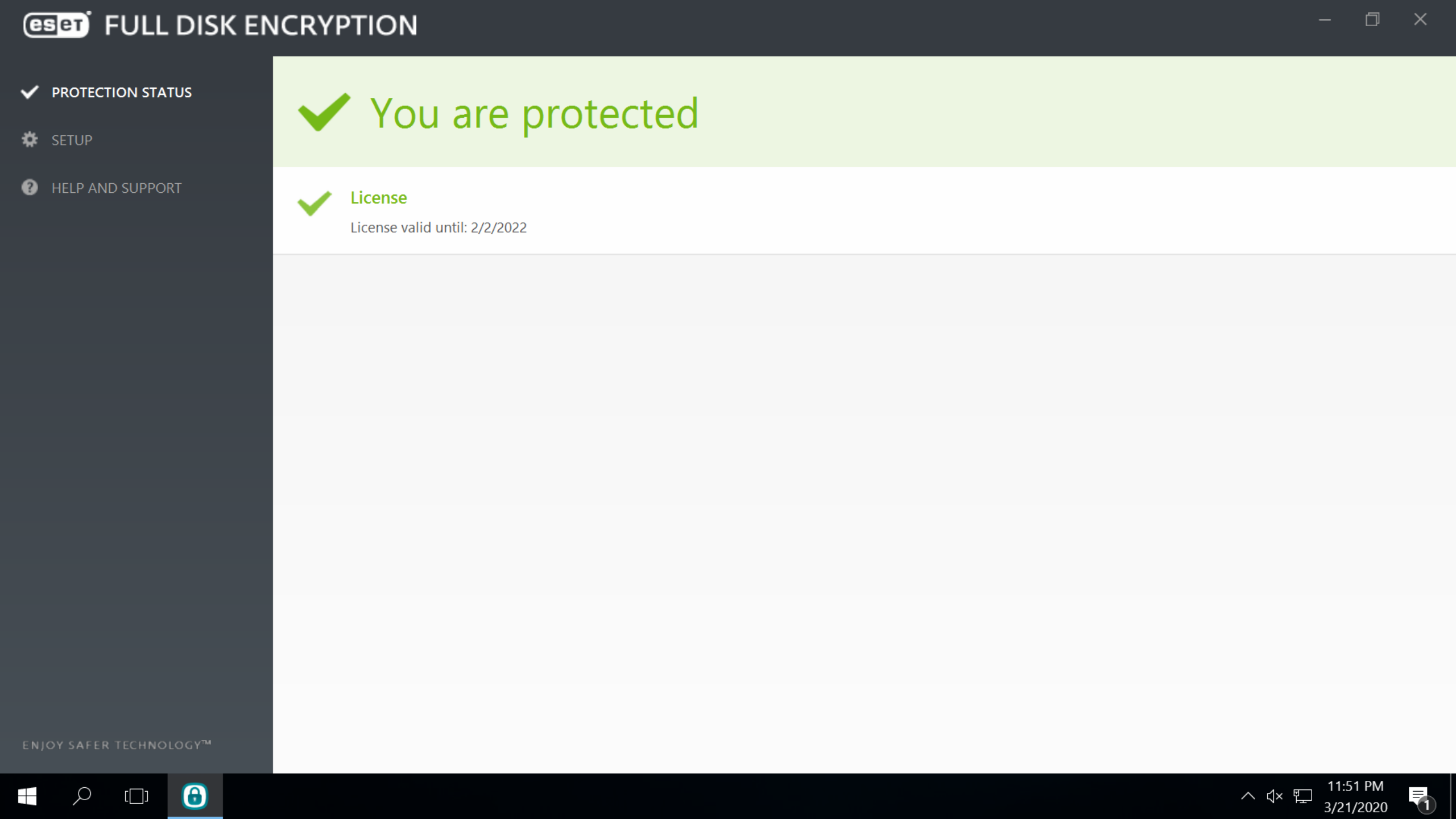


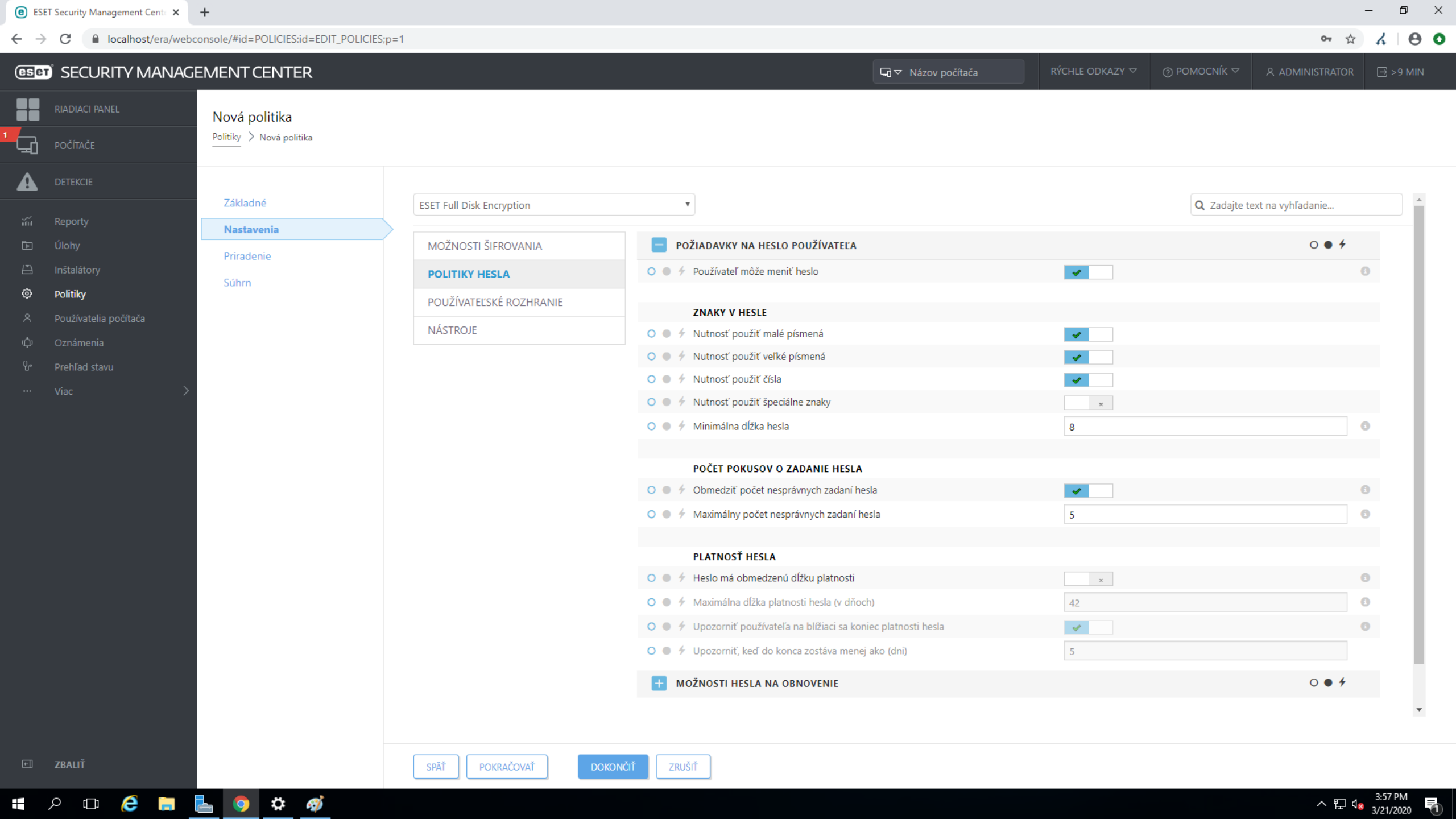

ESET Full Disk Encryption

EFDE


šifrovanie celého disku
samostatná licencia
manažment z konzoly vzdialenej správy


FULL DISK ENCRYPTION
PROTECTION STATUS
SETUP
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Setup
Change encryption password
Disk 0 (GPT, Boot) - VMware, VMware Virtual S
C: (No Name)
Encrypted
Presentation mode
Disabled: all pop-up windows will be suppressed.
FULL DISK ENCRYPTION
Change password
Current password:
New password:
Confirm password:
Password policy:
Must contain a number
Must contain lower case letter
Must contain upper case letter
Minimum character length of 8
OK
Cancel
11:53 PM
3/21/2020


FULL DISK ENCRYPTION
PROTECTION STATUS
SETUP
HELP AND SUPPORT
You are protected
License
License valid until: 2/2/2022
ENJOY SAFER TECHNOLOGY™
11:51 PM
3/21/2020


ESET Security Management Cent
localhost/era/webconsole/#id=POLICIES:id=EDIT_POLICIES;p=1
ESET SECURITY MANAGEMENT CENTER
Názov počítača
RÝCHLE ODKAZY
POMOCNÍK
ADMINISTRATOR
>9 MIN
RIADIACI PANEL
POČÍTAČE
DETEKCIE
Reporty
Úlohy
Inštalátory
Politiky
Používatelia počítača
Oznámenia
Prehľad stavu
Viac
ZBALIŤ
Nová politika
Politiky > Nová politika
Základné
Nastavenia
Priradenie
Súhrn
ESET Full Disk Encryption
Zadajte text na vyhľadanie...
MOŽNOSTI ŠIFROVANIA
POLITIKY HESLA
POUŽÍVATEĽSKÉ ROZHRANIE
NÁSTROJE
POŽIADAVKY NA HESLO POUŽÍVATEĽA
Používateľ môže meniť heslo
ZNAKY V HESLE
Nutnosť použiť malé písmená
Nutnosť použiť veľké písmená
Nutnosť použiť čísla
Nutnosť použiť špeciálne znaky
Minimálna dĺžka hesla
8
POČET POKUSOV O ZADANIE HESLA
Obmedziť počet nesprávnych zadaní hesla
Maximálny počet nesprávnych zadaní hesla
5
PLATNOSŤ HESLA
Heslo má obmedzenú dĺžku platnosti
Maximálna dĺžka platnosti hesla (v dňoch)
42
Upozorniť používateľa na blížiaci sa koniec platnosti hesla
Upozorniť, keď do konca zostáva menej ako (dni)
5
MOŽNOSTI HESLA NA OBNOVENIE
SPÄŤ
POKRAČOVAŤ
DOKONČIŤ
ZRUŠIŤ
3:57 PM
3/21/2020


Personal data
EU
GDPR
Digital economy
Protection
Privacy
Regulation

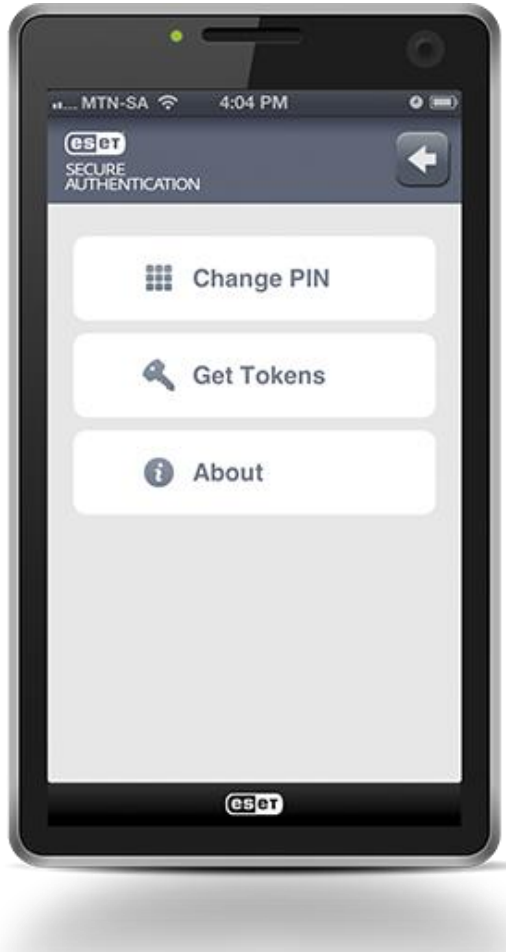

ESET Secure Authentication 2FA

ESET Secure Authentication

Mobilné riešenie využívajúce dvojfaktorovú autentifikáciu s jednorázovými heslami (2FA OTP).

Výhodou je:

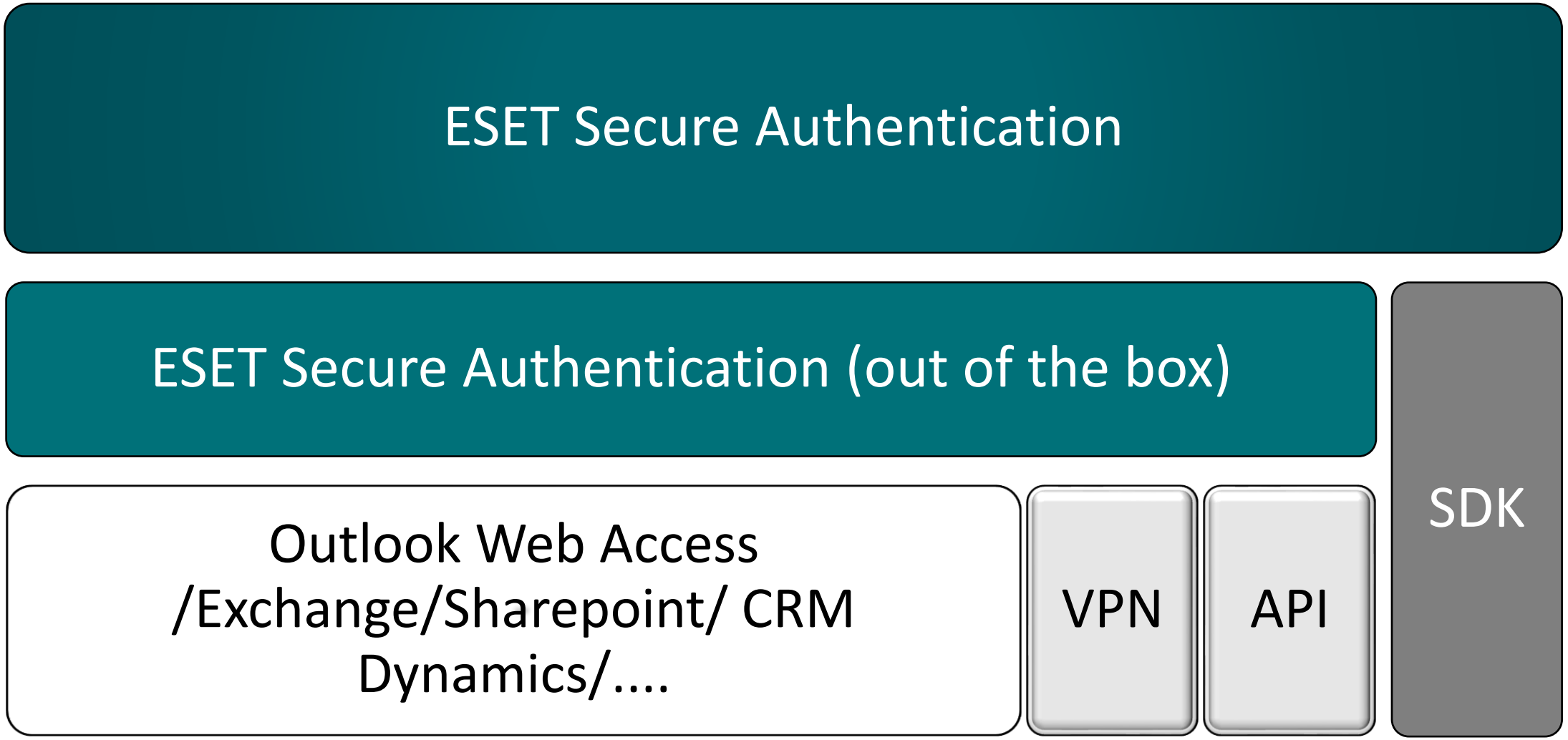
- náhodnosť
- nepredvídateľnosť
- unikátnosť



Typické problémy

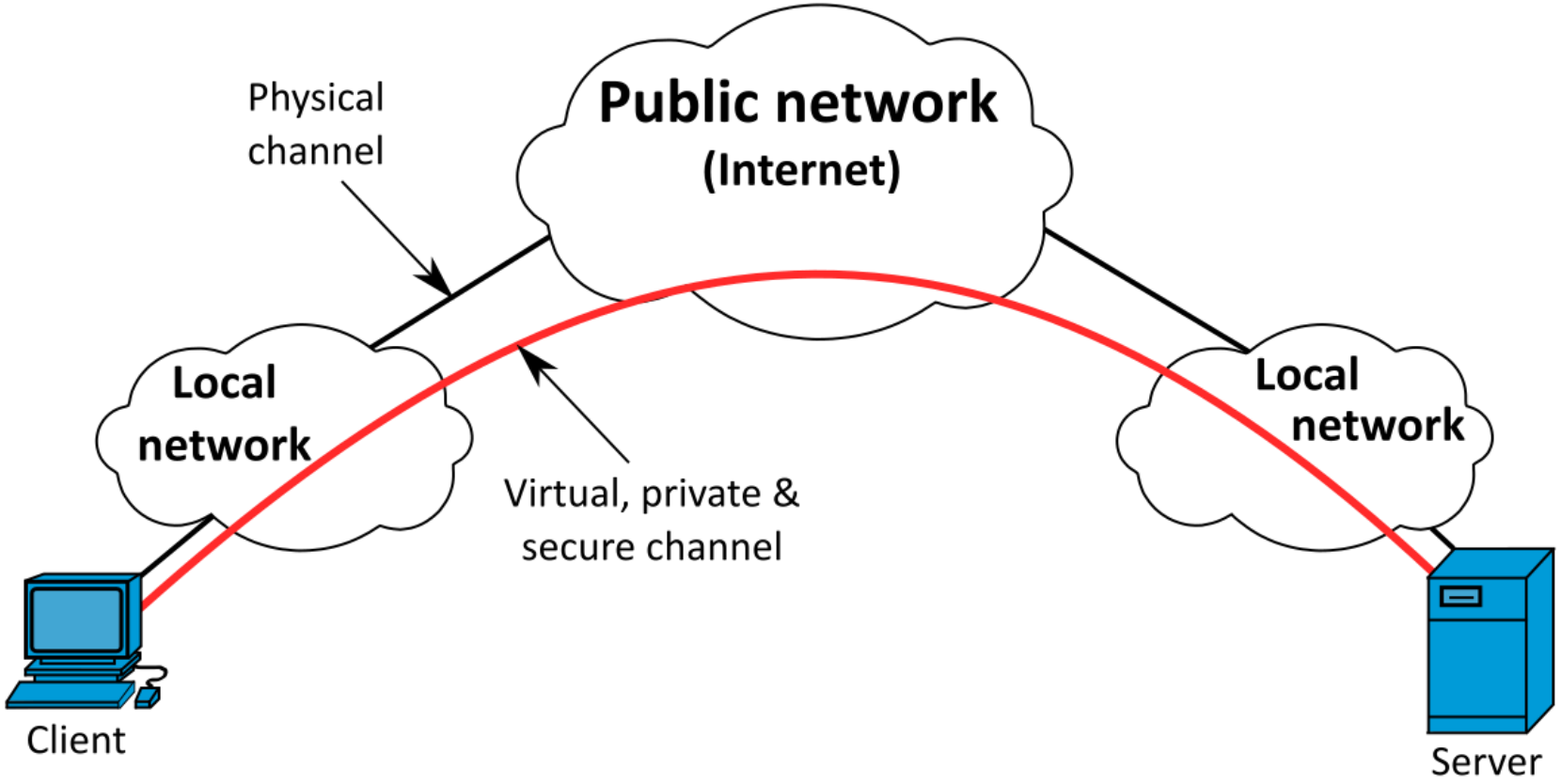
- slabé alebo ukradnuté heslá
- statické heslá
- nenáhodné heslá
- rovnaké heslá pre firemné aj privátne účty
- jednoduché vzorce pre nové heslá „peter1, peter2 ....“

Možnosti použitia ESA



VPN (Virtual Private Network)

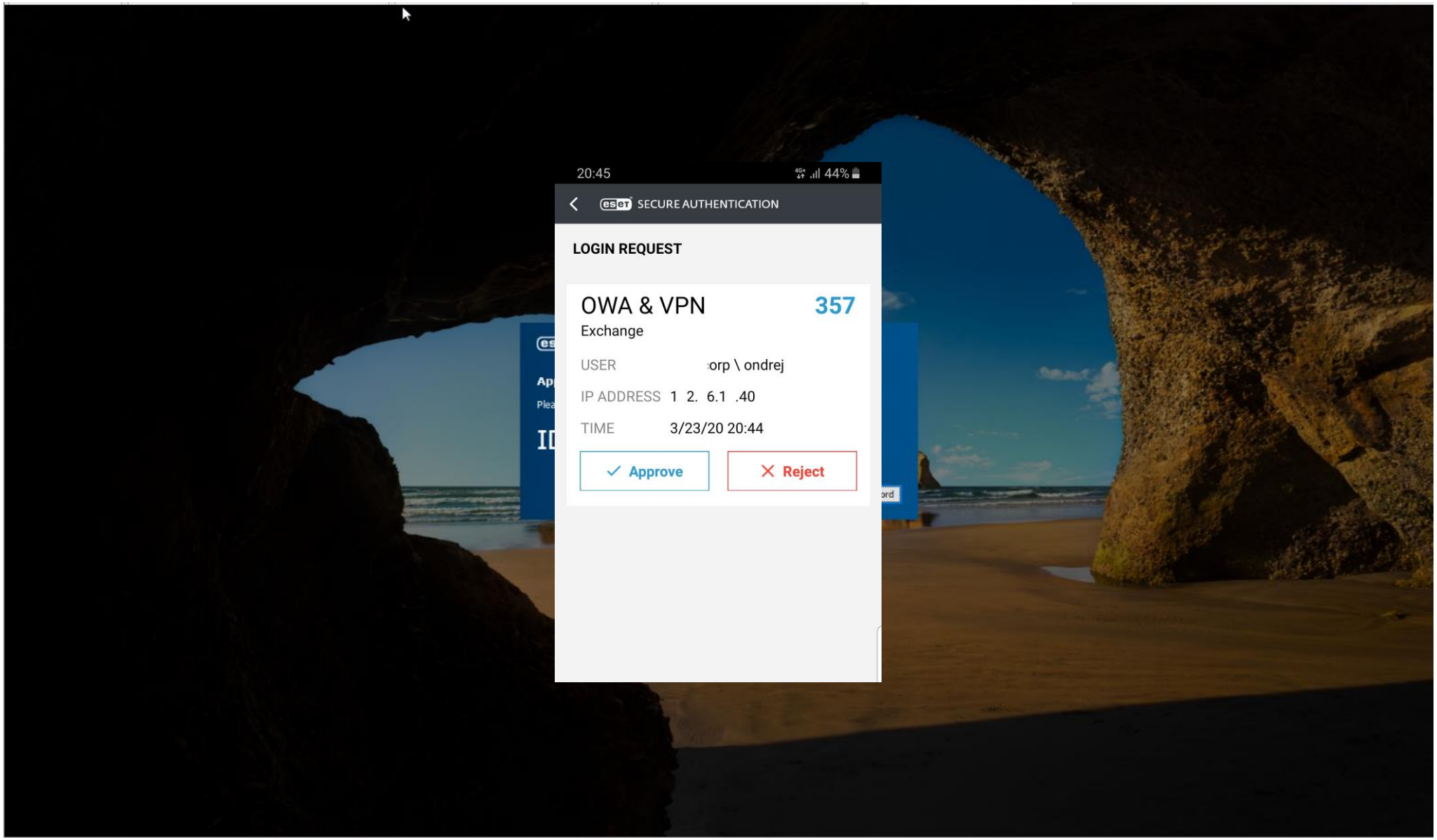
Radius IP / IPv6



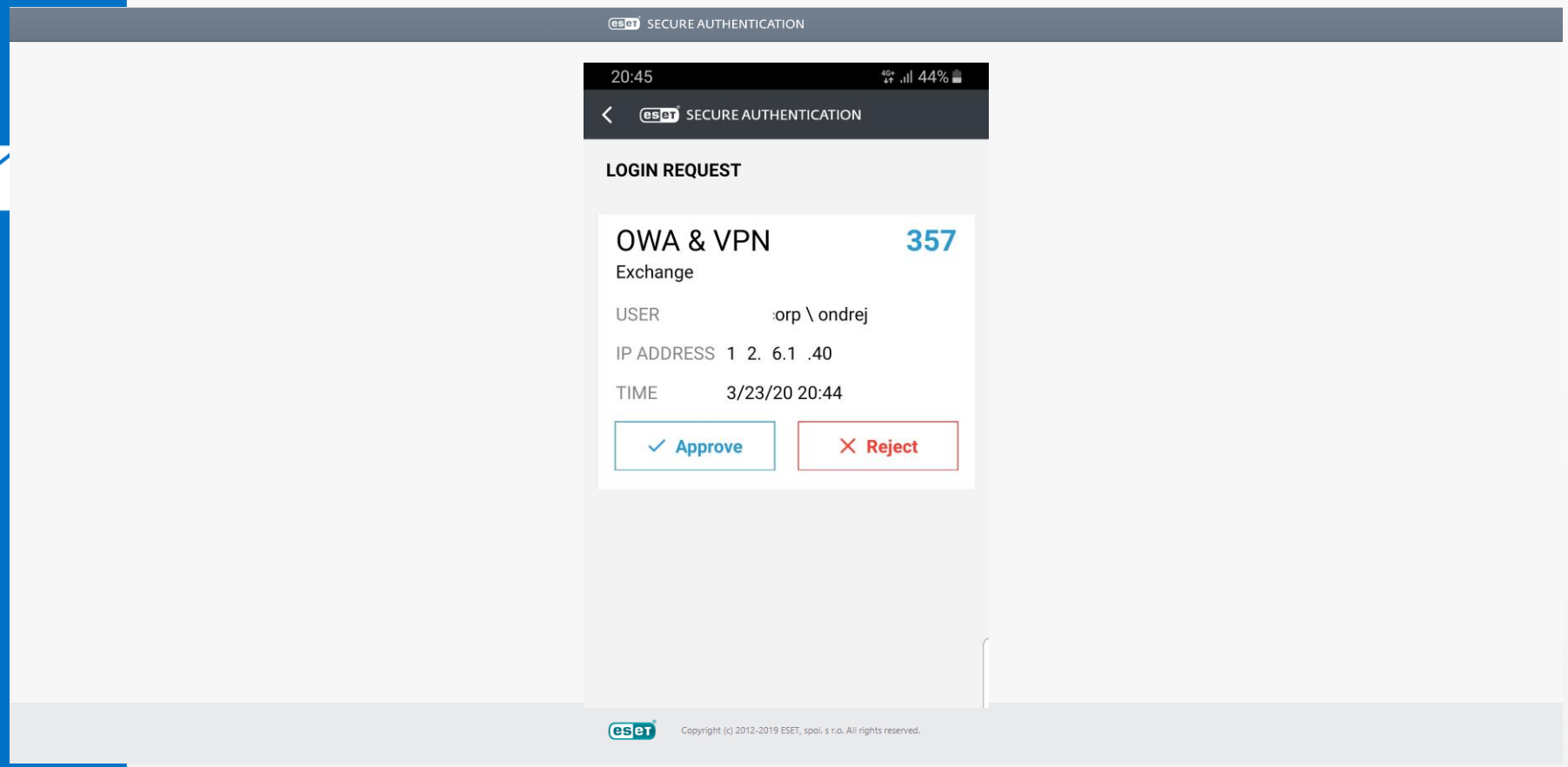
Integrácia s Microsoft službami

- Remote Desktop
- AD FS 3/4 (Office 365 login)
- Exchange control center 2007 / 2010 / 2013 / 2016
- Dynamics CRM 2011 / 2013 / 2015 / 2016
- SharePoint 2010 / 2013 / 2016
- SharePoint Foundation 2010 / 2013
- Remote Desktop Web Access
- Terminal Services Web Access

OS Login (Windows/Linux/MacOS)



Exchange OWA



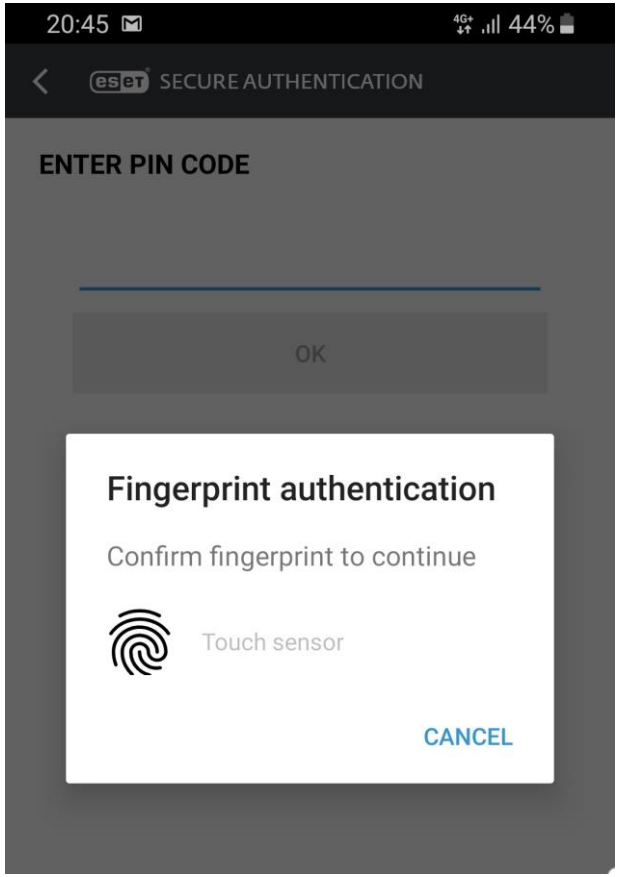
Funkcionality

- AD FS integrácia
- push autentifikácia
- master recovery key (MRK)
- geolokalizovana podpora DNS
- podpora 2FA mobilnej aplikácie pre Google a Facebook

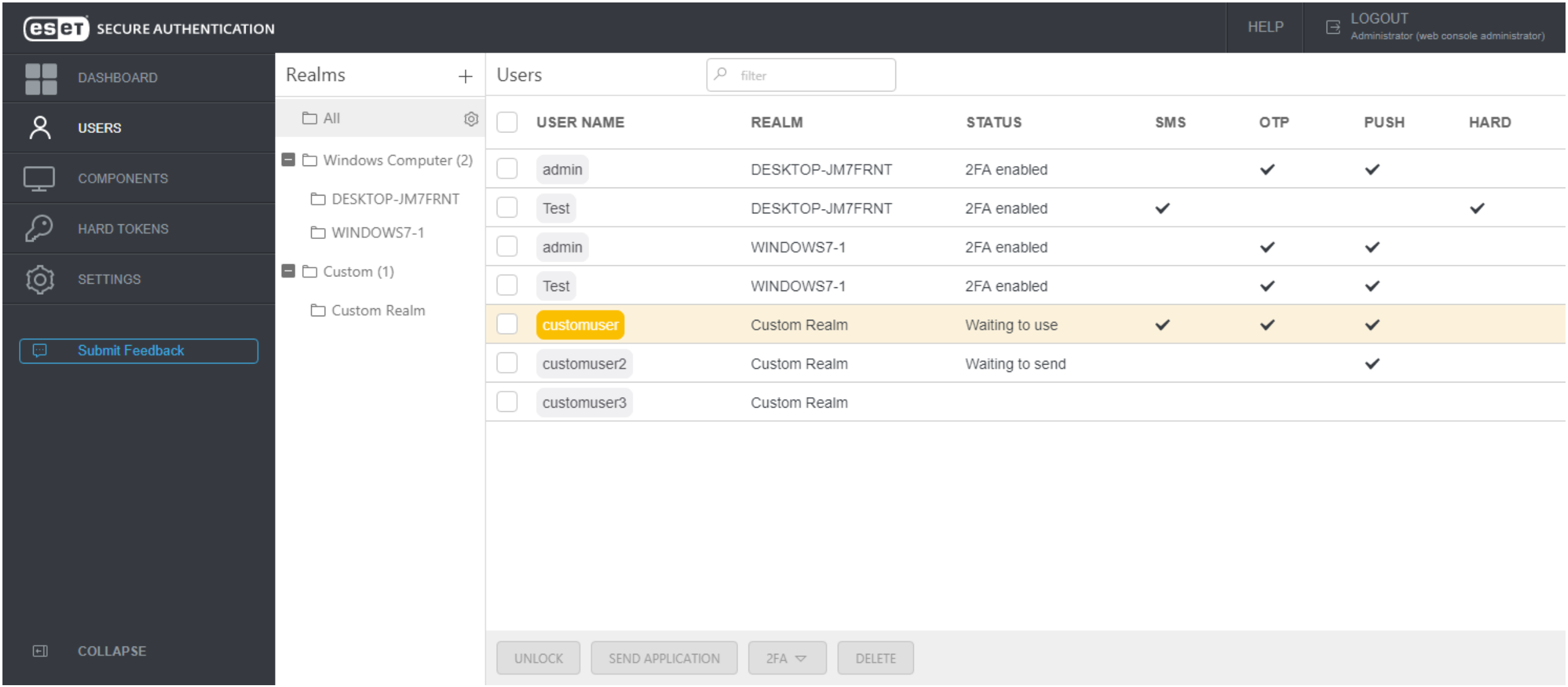
Nové funkcionality

- podpora FIDO / FIDO2 / FIDO U2F
- podpora copy/paste token
- podpora TOTP
- podpora Elasticsearch v.7
- notifikácie

Podpora biometrie v telefóne



Manažment užívateľov (web konzola)



Identity provider connector

Service Provider	ESA	Identity Provider
• Dropbox • Confluence • Google accounts • Office 365 • Salesforce • Webex •		• Azure AD • AD FS • Okta • OpenAM • Shibboleth • Keycloak

Spôsoby doručenia OTP

Podporované mobilné platformy

iOS	Android	Windows Mobile


via ako 100 dní


ESET Enterprise Inspector

Problém: cielené útoky / APTs

modifikácie hrozieb	dlhá doba	iné ako spustiteľné súbory

ESET Enterprise Inspector

detekcia

prehľad

reakcia

Nutné predpoklady

incident management	security tím	patch management

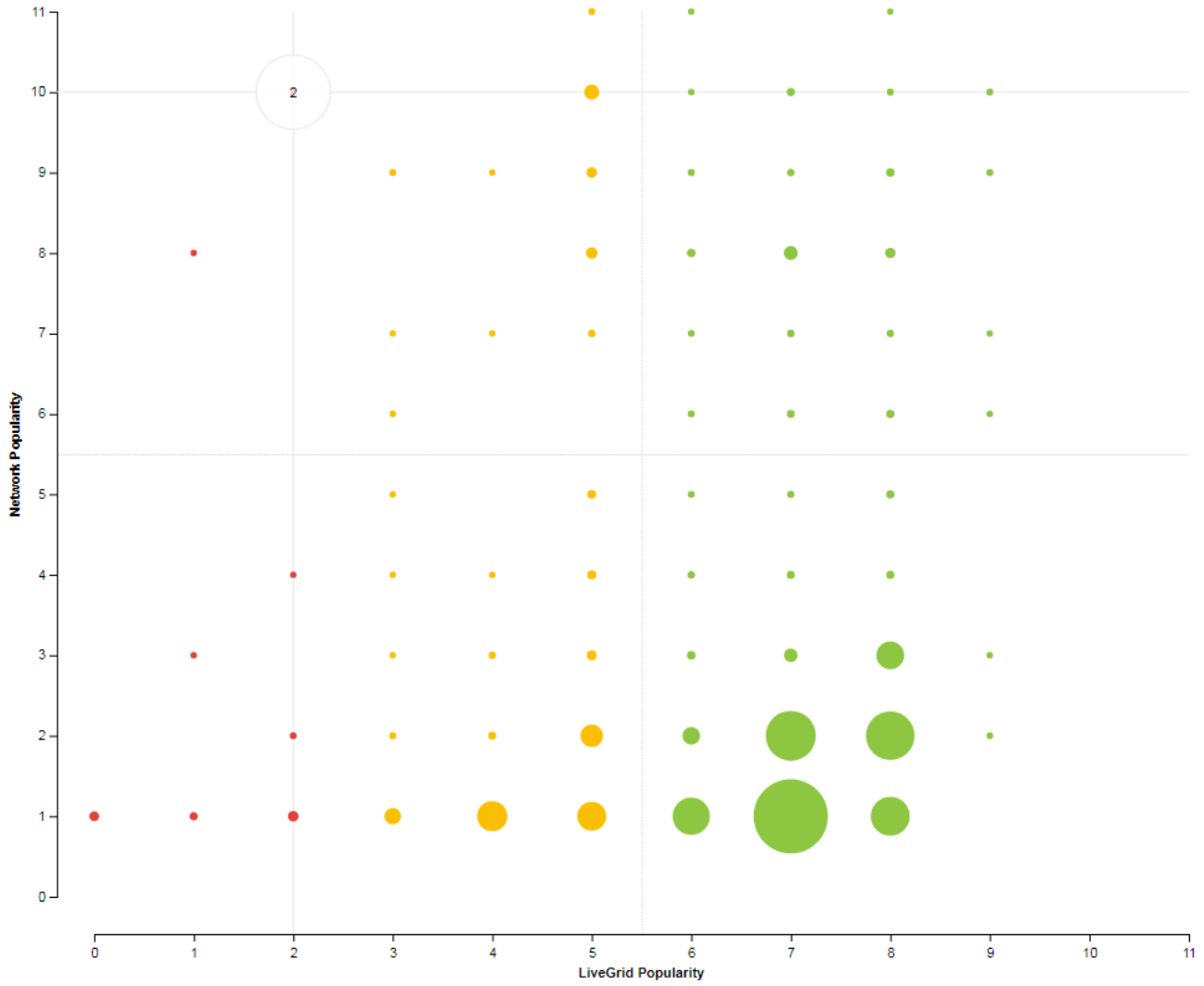
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU

Dashboard

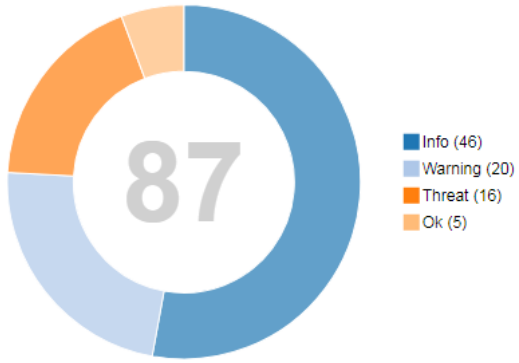
Alarms | Executables | Computer | Computers & Alerts | Server Status

ADD FILTER

Module Popularity

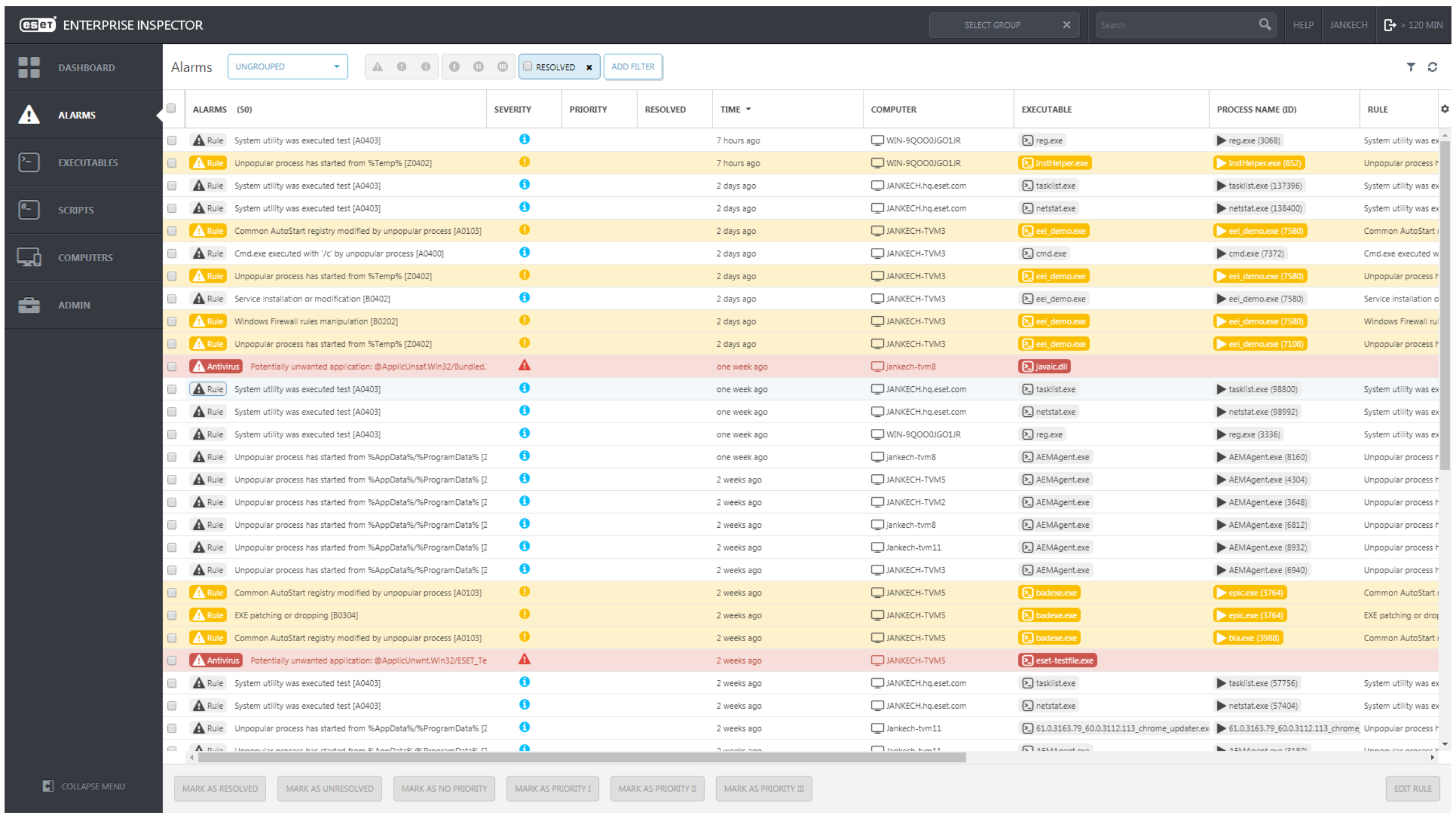


Module statuses



Problematic Executables

EXECUTABLE (BY SHA-1) (20)	UNRESOLVED ALARMS (UNIQUE)	UNRESOLVED ALARMS
eei_demo.exe	4	
badexe.exe	2	
apt 4.0.exe	2	
cmd.exe	1	
avira_antivir_personal_en_10.2.0.703	1	
cmd.exe	1	
cmd.exe	1	
cmd.exe	1	
cmd.exe	1	
reg.exe	1	


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
JANKECH
> 120 MIN
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU
Alarms
UNGROUPED
RESOLVED
ADD FILTER
ALARMS (50)
SEVERITY
PRIORITY
RESOLVED
TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
RULE
Rule System utility was executed test [A0403] 7 hours ago WIN-9QOO0JGO1JR reg.exe reg.exe (3068) System utility was ex
Rule Unpopular process has started from %Temp% [Z0402] 7 hours ago WIN-9QOO0JGO1JR InstHelper.exe InstHelper.exe (852) Unpopular process h
Rule System utility was executed test [A0403] 2 days ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (137396) System utility was ex
Rule System utility was executed test [A0403] 2 days ago JANKECH.hq.eset.com netstat.exe netstat.exe (138400) System utility was ex
Rule Common AutoStart registry modified by unpopular process [A0103] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Common AutoStart
Rule Cmd.exe executed with '/c' by unpopular process [A0400] 2 days ago JANKECH-TVM3 cmd.exe cmd.exe (7372) Cmd.exe executed w
Rule Unpopular process has started from %Temp% [Z0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Unpopular process h
Rule Service installation or modification [B0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Service installation o
Rule Windows Firewall rules manipulation [B0202] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Windows Firewall rul
Rule Unpopular process has started from %Temp% [Z0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7108) Unpopular process h
Antivirus Potentially unwanted application: @ApplicUnsaf.Win32/Bundled. one week ago jankech-tvm8 javaic.dll
Rule System utility was executed test [A0403] one week ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (98800) System utility was ex
Rule System utility was executed test [A0403] one week ago JANKECH.hq.eset.com netstat.exe netstat.exe (98992) System utility was ex
Rule System utility was executed test [A0403] one week ago WIN-9QOO0JGO1JR reg.exe reg.exe (3336) System utility was ex
Rule Unpopular process has started from %AppData%/%ProgramData% [Z one week ago jankech-tvm8 AEMAgent.exe AEMAgent.exe (8160) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM5 AEMAgent.exe AEMAgent.exe (4304) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM2 AEMAgent.exe AEMAgent.exe (3648) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago jankech-tvm8 AEMAgent.exe AEMAgent.exe (6812) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago Jankech-tvm11 AEMAgent.exe AEMAgent.exe (8932) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM3 AEMAgent.exe AEMAgent.exe (6940) Unpopular process h
Rule Common AutoStart registry modified by unpopular process [A0103] 2 weeks ago JANKECH-TVM5 badexe.exe epic.exe (3764) Common AutoStart
Rule EXE patching or dropping [B0304] 2 weeks ago JANKECH-TVM5 badexe.exe epic.exe (3764) EXE patching or drop
Rule Common AutoStart registry modified by unpopular process [A0103] 2 weeks ago JANKECH-TVM5 badexe.exe bia.exe (3988) Common AutoStart
Antivirus Potentially unwanted application: @ApplicUnwnt.Win32/ESET_Te 2 weeks ago JANKECH-TVM5 eset-testfile.exe
Rule System utility was executed test [A0403] 2 weeks ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (57756) System utility was ex
Rule System utility was executed test [A0403] 2 weeks ago JANKECH.hq.eset.com netstat.exe netstat.exe (57404) System utility was ex
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago Jankech-tvm11 61.0.3163.79_60.0.3112.113_chrome_updater.ex 61.0.3163.79_60.0.3112.113_chrome Unpopular process h
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS NO PRIORITY
MARK AS PRIORITY I
MARK AS PRIORITY II
MARK AS PRIORITY III
EDIT RULE

DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU

Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

61.0.3163.79_60.0.3112.113_chrome_updater.exe
Google Chrome Installer

SIGNATURE TYPE	Trusted
SIGNER NAME	Google Inc
SEEN ON	1 computer
FIRST SEEN	2 weeks ago - Sep 6, 2017, 1:04:35 AM
LAST EXECUTED	2 weeks ago - Sep 6, 2017, 1:04:40 AM

ESET LiveGrid®

REPUTATION	
POPULARITY	
FIRST SEEN	2 weeks ago

Jankech-tvm11

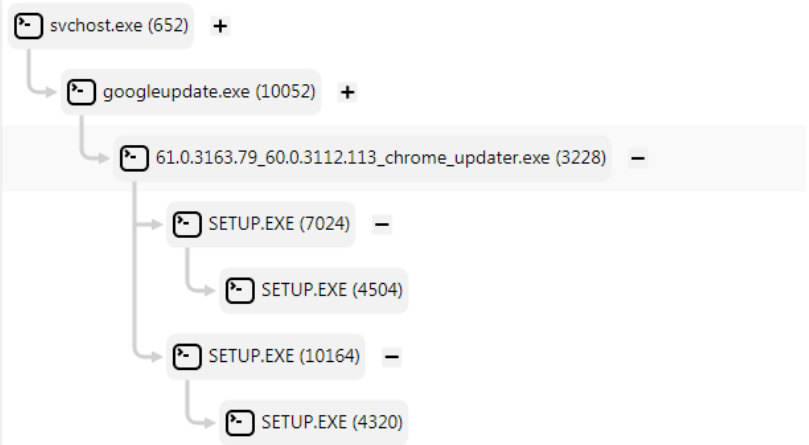
PARENT GROUP	Desktops
LAST CONNECTED	Sep 22, 2017, 4:11:16 PM
LAST EVENT	Sep 22, 2017, 4:11:07 PM
AGENT VERSION	1.0.503
OS	Windows 7

Events

File	Registry	Network
6	1	0

PROCESS	61.0.3163.79_60.0.3112.113_chrome_updater.exe (3228)
COMMAND LINE	"c:\users\admin\appdata\local\google\update\install\{ad95bcab-3cfc-42ed-8a69-65220924176f}\61.0.3163.79_60.0.3112.113_chrome_updater.exe" --verbose-logging --do-not-launch-chrome
PATH	%LOCALAPPDATA%\\google\update\install\{ad95bcab-3cfc-42ed-8a69-65220924176f}\
USER	admin
STARTED	Sep 6, 2017, 1:04:40 AM
ENDED	Sep 6, 2017, 1:18:04 AM
PARENT PROCESS	googleupdate.exe (10052)
COMPUTER	Jankech-tvm11

DOWNLOAD FILE | KILL PROCESS



DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU

< BACK

Bad extension - filecoders (ext. A - C) [C0607]

Edit rule

```
<?xml version="1.0" encoding="utf-8"?>
<rule>
  <description>
    <explanation>Process writes files with suspicious extensions. The rule contains list of common extensions used by ransomware starting with A-C. Seldom the rule may trigger on clean application (e. g. while performing backup of encrypted files).</explanation>
    <maliciousCauses>Filecoder is encrypting files.</maliciousCauses>
    <benignCauses>Backup process or administrator is copying encrypted files.</benignCauses>
    <recommendedActions>1. Scan the related process with AV.
2. If not detected then submit the executable for analysis.
3. Search for encrypted files. Shares on network may be affected.
4. Restore encrypted files from backup (backup encrypted files for future decryption)
</recommendedActions>
    <category>Filecoders</category>
    <guid> 86a47275-746e-4b38-8b7a-4509d033349a </guid>
    <name>Bad extension - filecoders (ext. A - C) [C0607]</name>
    <severity>Threat</severity>
  </description>
  <definition>
    <!-- rev 20170825 -->
    <Process>
      <operator type="AND">
        <Condition component="LiveGrid" condition="less" property="Reputation" value="8"/>
      </operator>
    </Process>
    <operations>
      <operation type="WriteFile">
        <operator type="OR">
          <!-- only extensions with size more than 3 are included starting with A-C -->
          <!-- extensions without comments are gathered from external resources -->
          <!-- Win32/Filecoder.FV -->
          <condition component="FileItem" condition="ends" property="Extension" value="A1crypt"/>
          <!-- MSIL/Filecoder.C/AC/BU -->
          <condition component="FileItem" condition="ends" property="Extension" value="adamlars"/>
          <!-- more variants use this -->
          <condition component="FileItem" condition="ends" property="Extension" value="AES256"/>
          <!-- Win32/Filecoder.AESNI -->
          <condition component="FileItem" condition="ends" property="Extension" value="aes_ni"/>
          <condition component="FileItem" condition="ends" property="Extension" value="aes_ni_0day"/>
          <!-- Win32/Filecoder.NKP -->
          <condition component="FileItem" condition="ends" property="Extension" value="aleta"/>
          <!-- Win32/Filecoder.AU -->
          <condition component="FileItem" condition="ends" property="Extension" value="amba"/>
          <!-- Win32/Filecoder.Crysis -->
          <condition component="FileItem" condition="ends" property="Extension" value="arena"/>
          <!-- Win32/Filecoder.FS -->
          <condition component="FileItem" condition="ends" property="Extension" value="badnews"/>
          <condition component="FileItem" condition="ends" property="Extension" value="bart"/>
          <!-- Win32/Filecoder.ED -->
          <condition component="FileItem" condition="ends" property="Extension" value="better_call_saul"/>
          <condition component="FileItem" condition="ends" property="Extension" value="bitcrypt"/>
          <condition component="FileItem" condition="ends" property="Extension" value="bitstak"/>
          <condition component="FileItem" condition="ends" property="Extension" value="bleepYourFiles"/>
          <condition component="FileItem" condition="ends" property="Extension" value="blocatto"/>
          <!-- MSIL/Filecoder.C/AC/BU -->
          <condition component="FileItem" condition="ends" property="Extension" value="block"/>
          <!-- Win32/Filecoder.RotoCrypt -->
          <condition component="FileItem" condition="ends" property="Extension" value="blockage42"/>
          <!-- more variants use this -->
          <condition component="FileItem" condition="ends" property="Extension" value="blocked"/>
```

Syntax Reference

The general structure of rule looks like this:

```
<rule>
    <name>example's name </name>
    <process />
    <operations />
</rule>
```

Process element defines which processes meet the rule conditions. Similarly, operations element defines operations which need to be executed by a process to meet the rule conditions. Both these elements are optional but one of them needs to be present in the rule. If there is no process element operations of all processes in the system are checked. If there is no operations element rule become active as soon as process which meets condition is started. If both are present a process needs to execute operations described by operations element to activate the rule. Conditions are defined using operator and condition elements. Operator element is a logical OR or AND operator. Condition element checks if a property has a required value.

```
<process>
    <operator type="AND">
        <condition component="FileItem" pr
        <condition component="FileItem" pr
    </operator>
</process>
```

This example checks if process with a name svchost was started from temp folder or its subfolders. Currently the following components and properties are supported: FileItem (Name, Extension, Path), Executable (SHA-1), LiveGrid® (Age, Reputation, Popularity), Enterprise (Popularity), NetworkAddress (RemoteAddressIpV4, RemotePort) The condition attribute can be: is, isnot, starts, notstarts, contains, notcontains, less, lessOrEqual, greater, greaterOrEqual.
Operations element contains one or more operation elements. Operation element has a type attribute and body which defines condition for this operation's argument. Here is an example checking if VBS file was written to the disk:

```
<operations>
    <operation type="WriteFile">
        <condition component="FileItem" pr
    </operation>
</operations>
```

The following operation types are supported: WriteFile, DeleteFile, RenameFile, CreateNewFile, TcpIpConnect, TcpIpAccept, RegSetValue.

FINISH | CHECK SYNTAX | CLOSE | DELETE | SAVE AS | EXPORT

Zoznámte sa s ESET riešeniami

- **Vyžiadajte si business trial licenciu u svojho ESET obchodníka alebo ESET resellera:**

- **EDTD na 3 mesiace – pre existujúcich zákazníkov s EEPS / EEPA / ESB balíkmi na ochranu 100 a viac endpointov**

- **ESA na 3 mesiace – pre existujúcich aj nových ESET zákazníkov**

- EFDE na 1 mesiac - pre existujúcich zákazníkov s EEPS / EEPA / ESB balíkmi

- EEI na 1 mesiac - pre existujúcich zákazníkov s EEPS / EEPA / ESB balíkmi na ochranu 250 a viac endpointov


Otázky?

OndrejKrajč

ESET Senior Technical Pre-Sales Representative

krajc@eset.sk

/ESET @ESET

ENJOY SAFER TECHNOLOGY™