Digital Security
Progress. Protected.

ESET PROTECT ELITE

Visaptveroša profilakse, atklāšana un reaģēšana, apvienojot uzņēmuma klases XDR un pilnīgu daudzlīmeņu aizsardzību.

Egils Rupenheits

Digital Security
Progress. Protected.

Par ESET

30+ gadu pieredze

Privāts uzņēmums
bez parādsaistībām

Ar fokusu uz
tehnoloģiju attīstību

ES uzņēmums

Mērķtiecīga un
stabila izaugsme

Uzņēmuma
dibinātāju īpašums

Stabilas vērtības

Progress.
Protected.

PROTECT ENTRY

Pārvaldības konsole	ESET PROTECT
Moderna darbstaciju aizsardzība	ESET Endpoint Security
Serveru aizsardzība	ESET Server Security

Mūsdienīga daudzslāņaina iekārtu aizsardzība uzņēmējdarbībai ar spēcīgu mašīnmācīšanos un viegli lietojamu mākoņa vai lokālā pārvaldību.

Vairāku platformu risinājums ar iekļautu servera drošību.

PROTECT ADVANCED

Pārvaldības konsole	ESET PROTECT
Moderna darbstaciju aizsardzība	ESET Endpoint Security
Serveru aizsardzība	ESET Server Security
Mākoņ-smilškaste	ESET LiveGuard Advanced
Diska šifrēšana	ESET Full Disk Encryption

Savā klasē labākā iekārtu aizsardzība pret izspiedējvīrusu un nulltās dienas apdraudējumiem, ko nodrošina jaudīgs datu drošības risinājums

PROTECT COMPLETE

Pilnīga daudzslāņu aizsardzība iekārtām, mākoņa lietojumprogrammām un e-pastam (primārajam draudu vektoram)

Pārvaldības konsole	ESET PROTECT
Moderna darbstaciju aizsardzība	ESET Endpoint Security
Serveru aizsardzība	ESET Server Security
Mākoņ-smilškaste	ESET LiveGuard Advanced
Diska šifrēšana	ESET Full Disk Encryption
E-pastu drošība	ESET Mail Security
Mākoņprogrammu aizsardzība	ESET Cloud Office Security
Ievainojamību un atjauninājumu pārvaldība	ESET Vulnerability & Patch Management

PROTECT ELITE

Viss vienā novēršana, noteikšana un reaģēšana, kas apvieno uzņēmuma līmeņa XDR ar pilnīgu daudzslāņu aizsardzību

Pārvaldības konsole	ESET PROTECT
Moderna darbstaciju aizsardzība	ESET Endpoint Security
Serveru aizsardzība	ESET Server Security
Mākoņ-smilškaste	ESET LiveGuard Advanced
Diska šifrēšana	ESET Full Disk Encryption
E-pastu drošība	ESET Mail Security
Mākoņprogrammu aizsardzība	ESET Cloud Office Security
Ievainojamību un atjauninājumu pārvaldība	ESET Vulnerability & Patch Management
EDR/XDR	ESET Inspect
Multifaktoru autentifikācija	ESET Secure Authentication

ESET PROTECT ELITE

- Aizsardzība darbstacijām un serveriem
- Pilna diska šifrēšana
- XDR - ESET INSPECT iespējas
- ESET Live Guard - mākoņ-smilškastes iespējas
- E-pastu aizsardzība
- Multi-faktoru autentifikācija
- Mākoņprogrammu aizsardzība
- Vulnerability & patch management - Ievainojamību un atjauninājumu pārvaldība

ESET ENDPOINT SECURITY

ESET SERVER SECURITY

ENDPOINT SECURITY

ESET Endpoint Security priekš Windows/macOS/Android

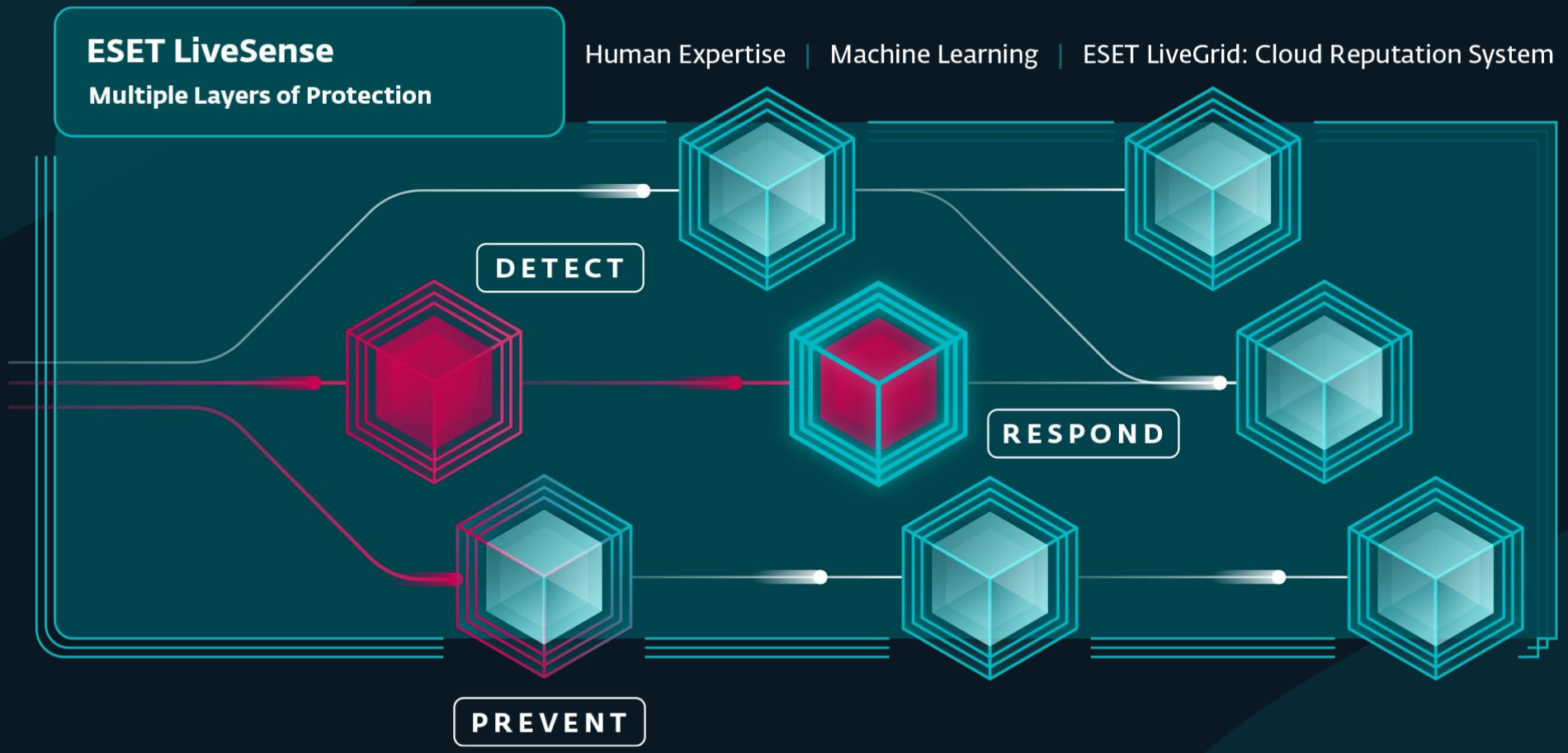
ESET Endpoint Antivirus priekš Windows/macOS/Linux

ESET Endpoint Security priekš Android

ESET MDM priekš iOS un iPadOS

ESET Server Security priekš Windows Server/Linux/Azure

EPDR – ESET PREVENT | DETECT | RESPOND



ESET FULL DISK ENCRYPTION

Datu aizsardzība jebkura lieluma uzņēmumiem

ESET FULL DISK ENCRYPTION

Galvenās funkcionalitātes

- Pre-Boot drošība
- Pilna diska šifrēšana
- Pārvaldāms, izmantojot ESET Protect
- Centralizēta paroļu politiku iestatīšana
- Attālināti bloķējiet, anulējiet vai atiestaties paroles pārvaldītajās iekārtās
- Visi produkti tiek pārvaldīti no vienas konsoles
- Identitāte un datu aizsardzība
- Dažādu OS atbalsts
- Uzstādīšana ar vienu klikšķi
- Pilnībā pārbaudīts

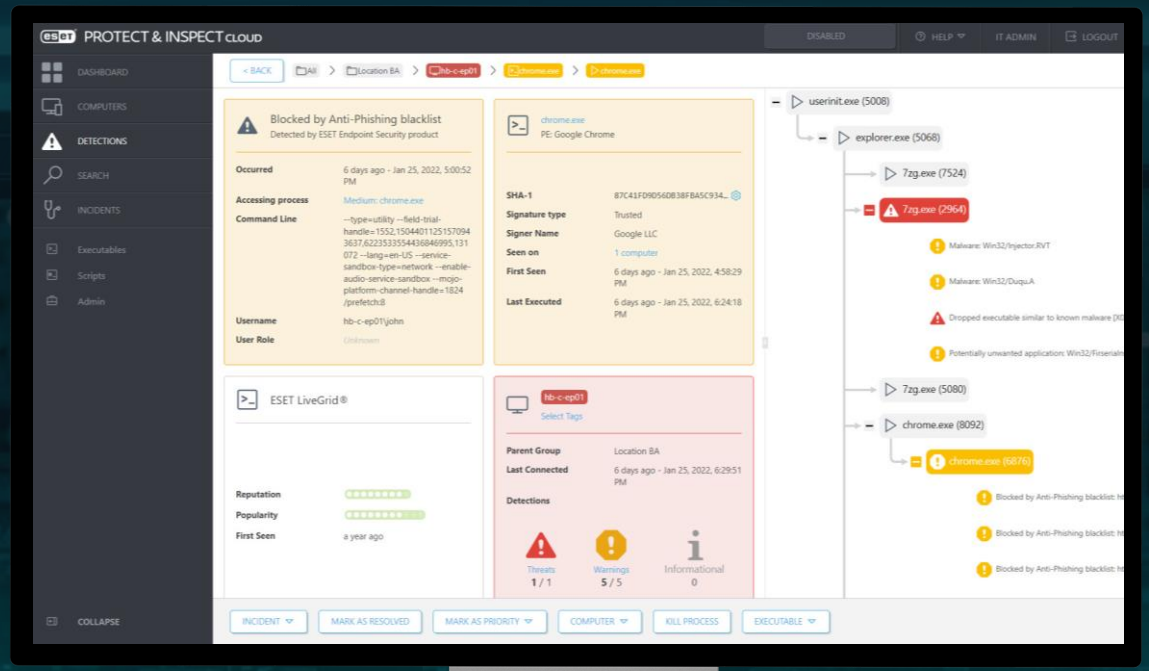
ESET INSPECT

Ļoti pielāgojama iekārtu apdraudējumu noteikšana un reakcija

ESET INSPECT

Galvenās funkcionalitātes

- Apkopo reāllaika notikumus
- Nodrošina plašu filtrēšanu un šķirošanu
- Izmanto ESET reputācijas sistēmu
- Pielāgoti paziņošanas noteikumi
- Bloķēšana un novēršana
- Paredzēts draudu medībām



ESET INSPECT

KONSTATĀCIJA

Atrodiet ļaunprātīgu anomāliju

PĀRREDZAMĪBA

Kas tiek ietekmēts?

Kad tas notika?

Kā tas notika?

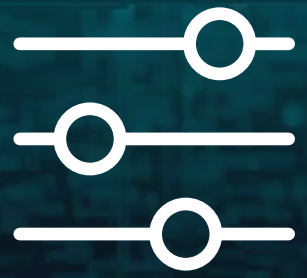
NOVĒRŠANA

Bloķējiet to

Dzēsiet to

ESET INSPECT

PĀRREDZAMĪBA



KONTROLE

Pārredzamība par to, kas notiek iekārtās

Aktīvās komponentes

Bezfailu uzbrukumi

Galvenais cēlonis

Izplatība vidē

Iespaidotie dati

Izmantotās tehnikas

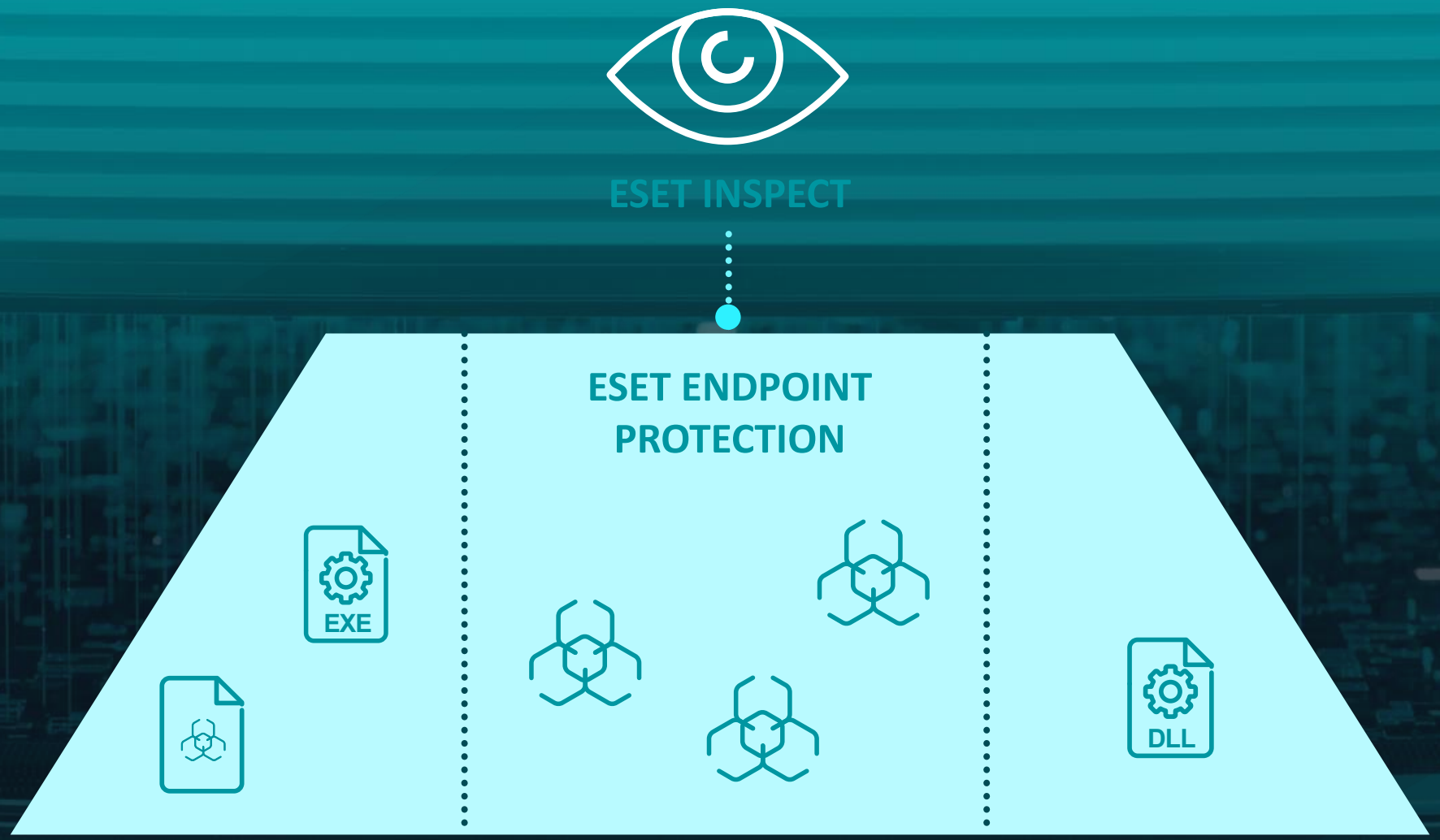
Varat kontrolēt atbildes reakciju

Bloķēt izpildi

Izolēt iekārtu

Izbeigt procesu

Attīrīt failu


ESET INSPECT
ESET ENDPOINT PROTECTION
EXE
DLL

Scenārijs 1

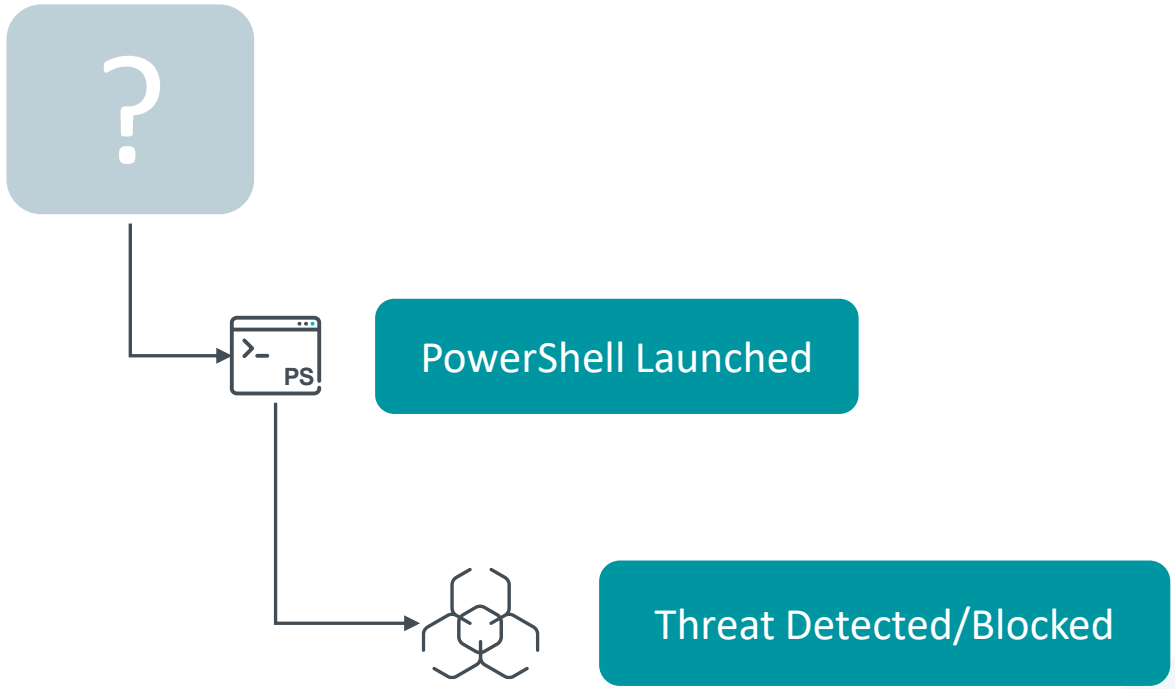
ESET Endpoint Protection aptur apdraudējumu


?
PowerShell

Bez ESET Inspect:

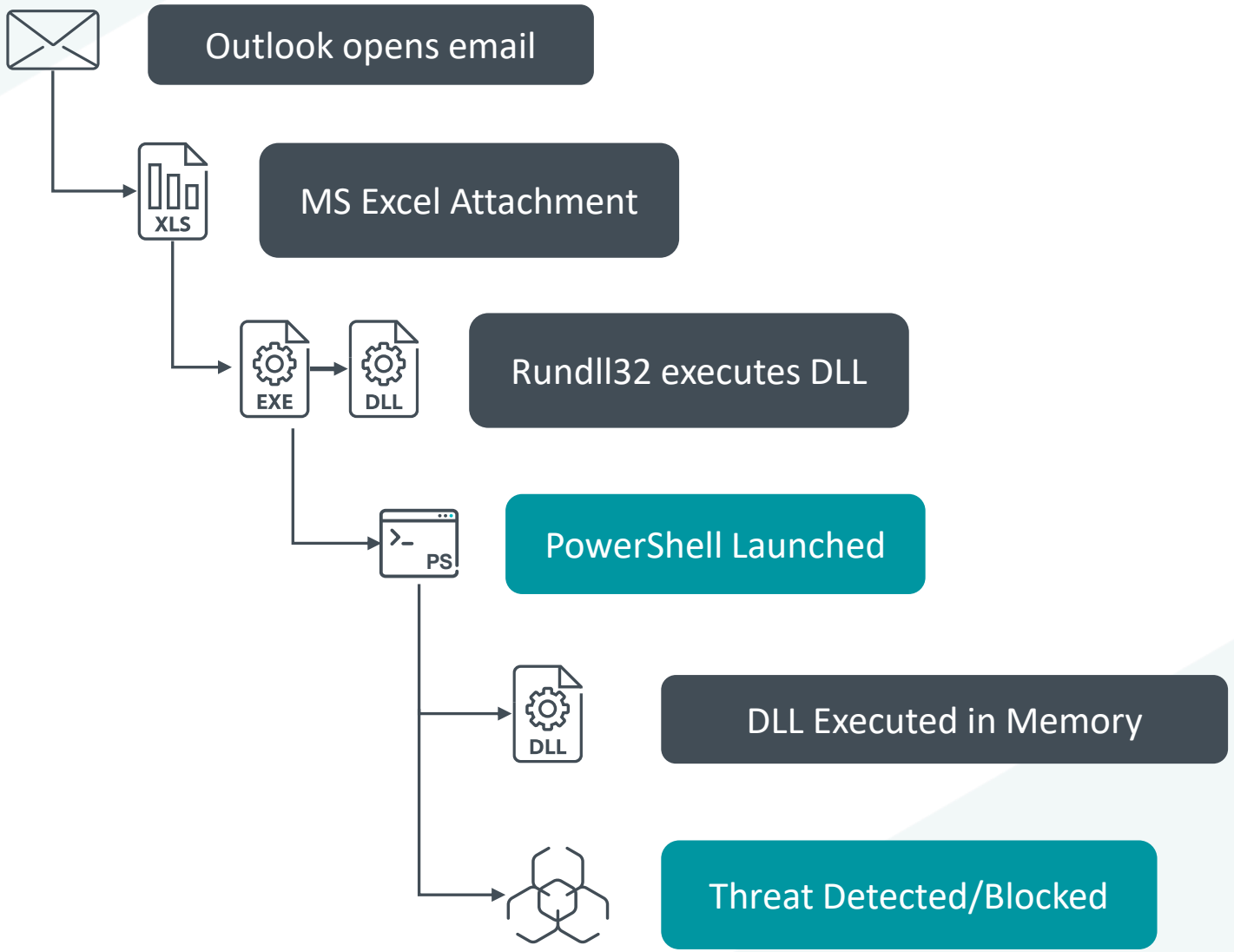
MINIMĀLA PĀRREDZAMĪBA

NENOTEIKTĪBA



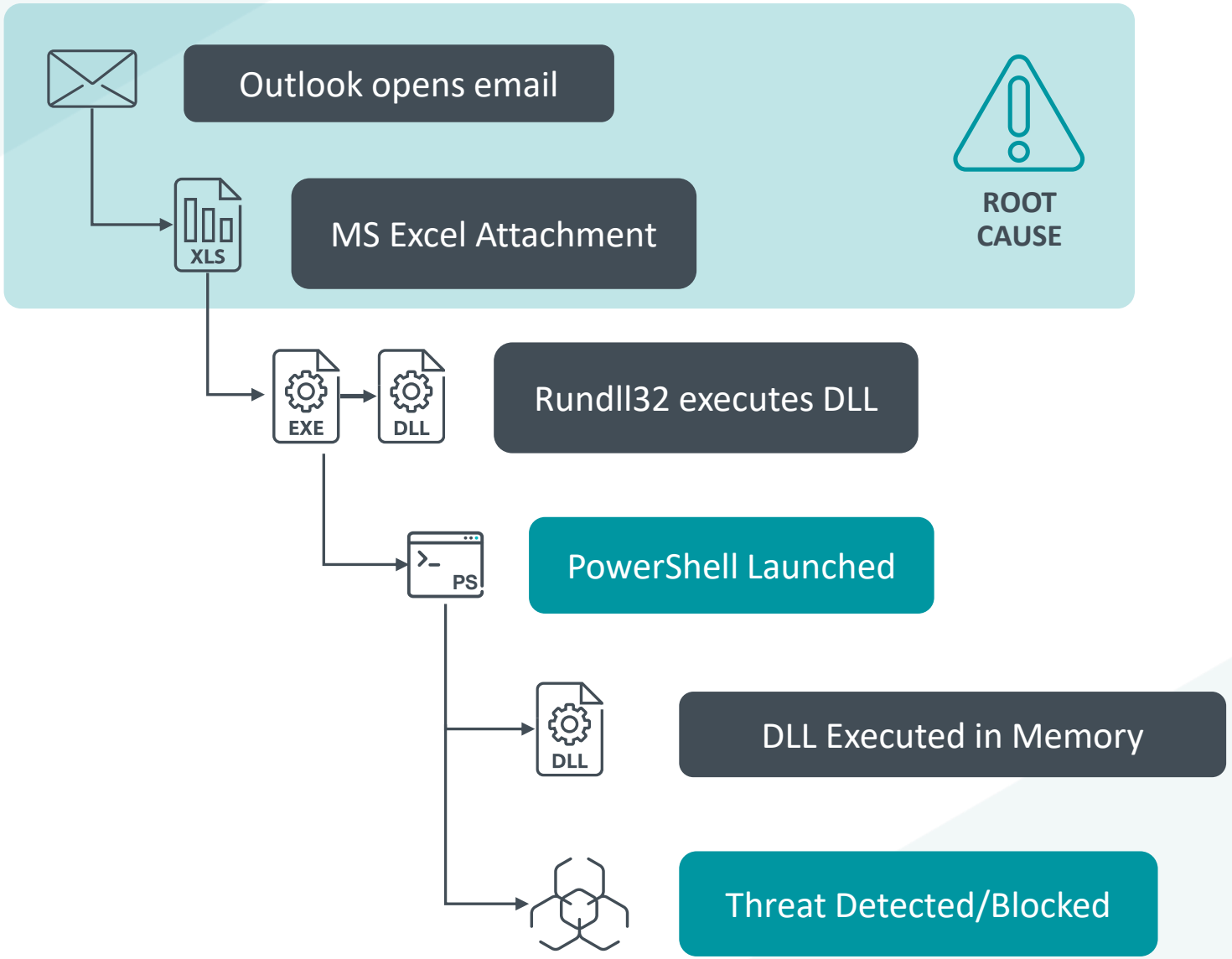
Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA



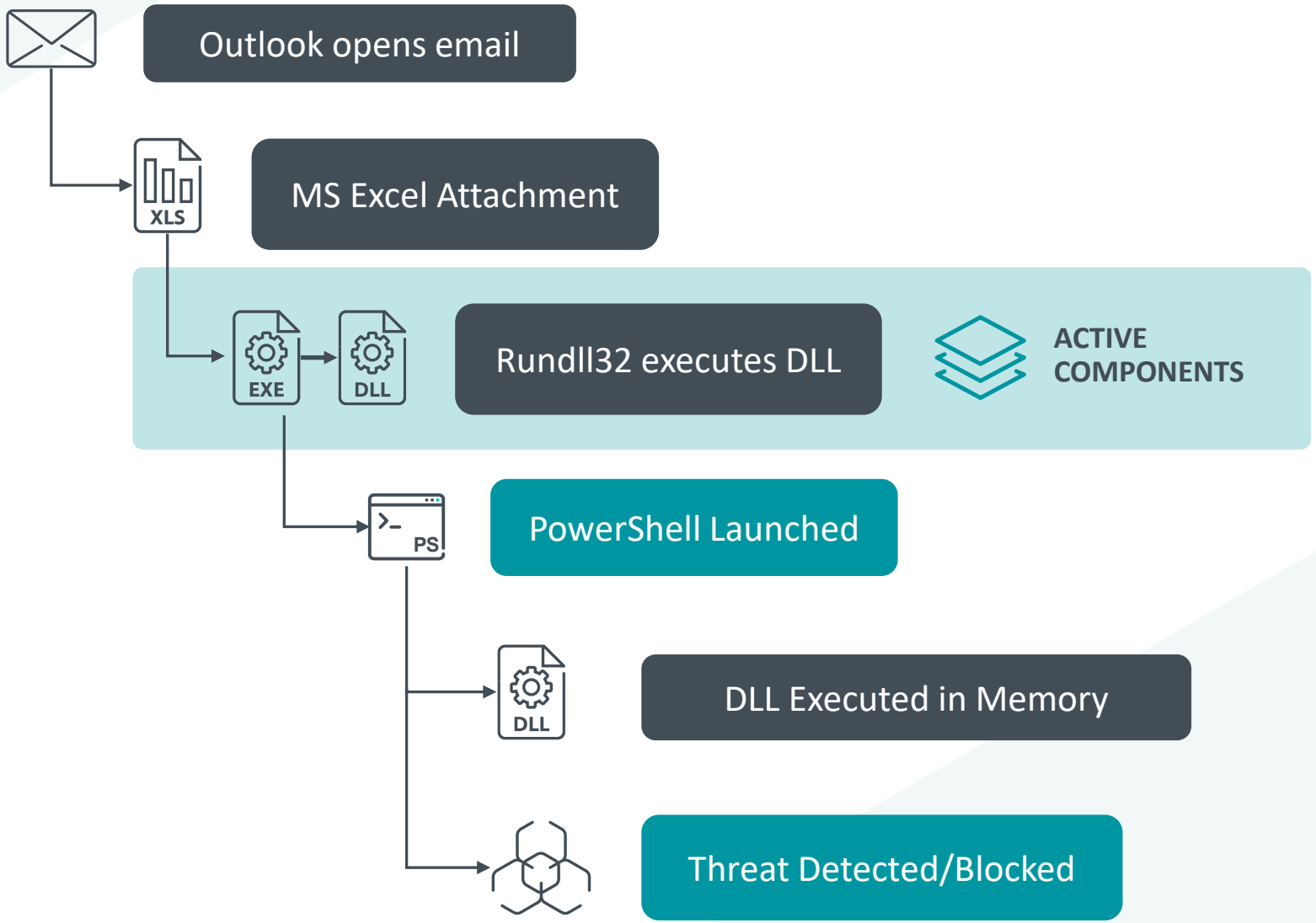
Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA



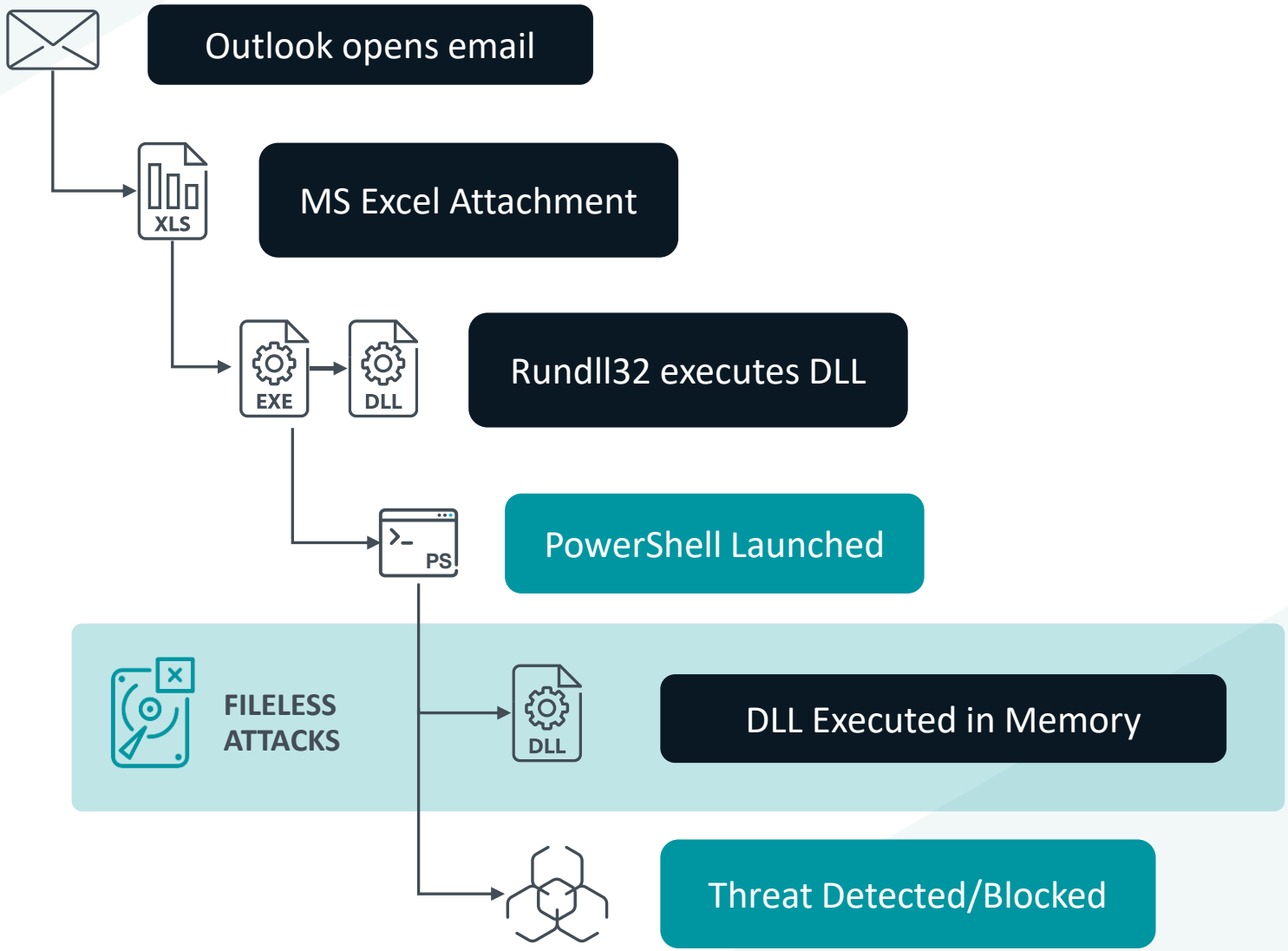
Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA



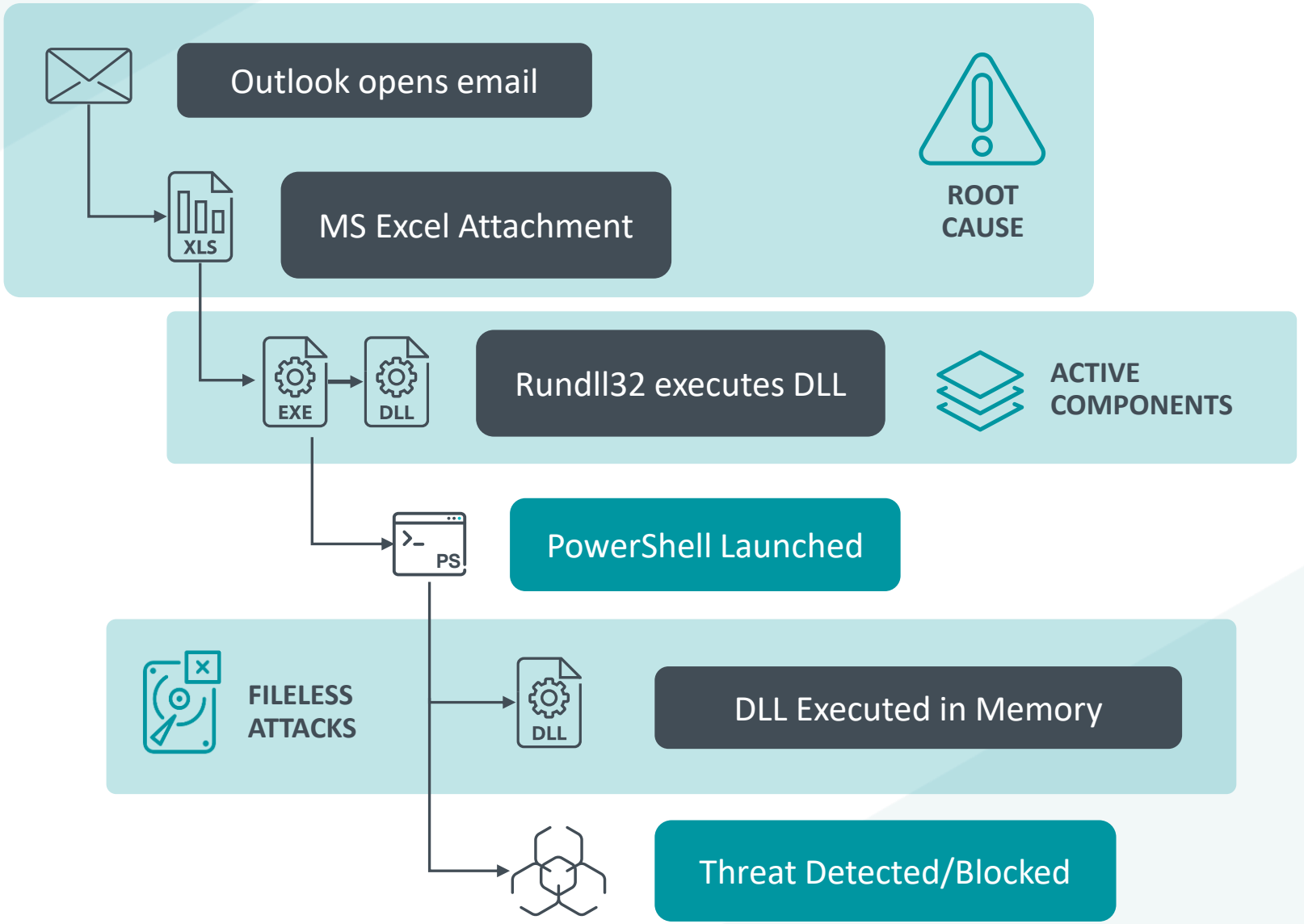
Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA



Ar ESET Inspect Jūs iegūstat:

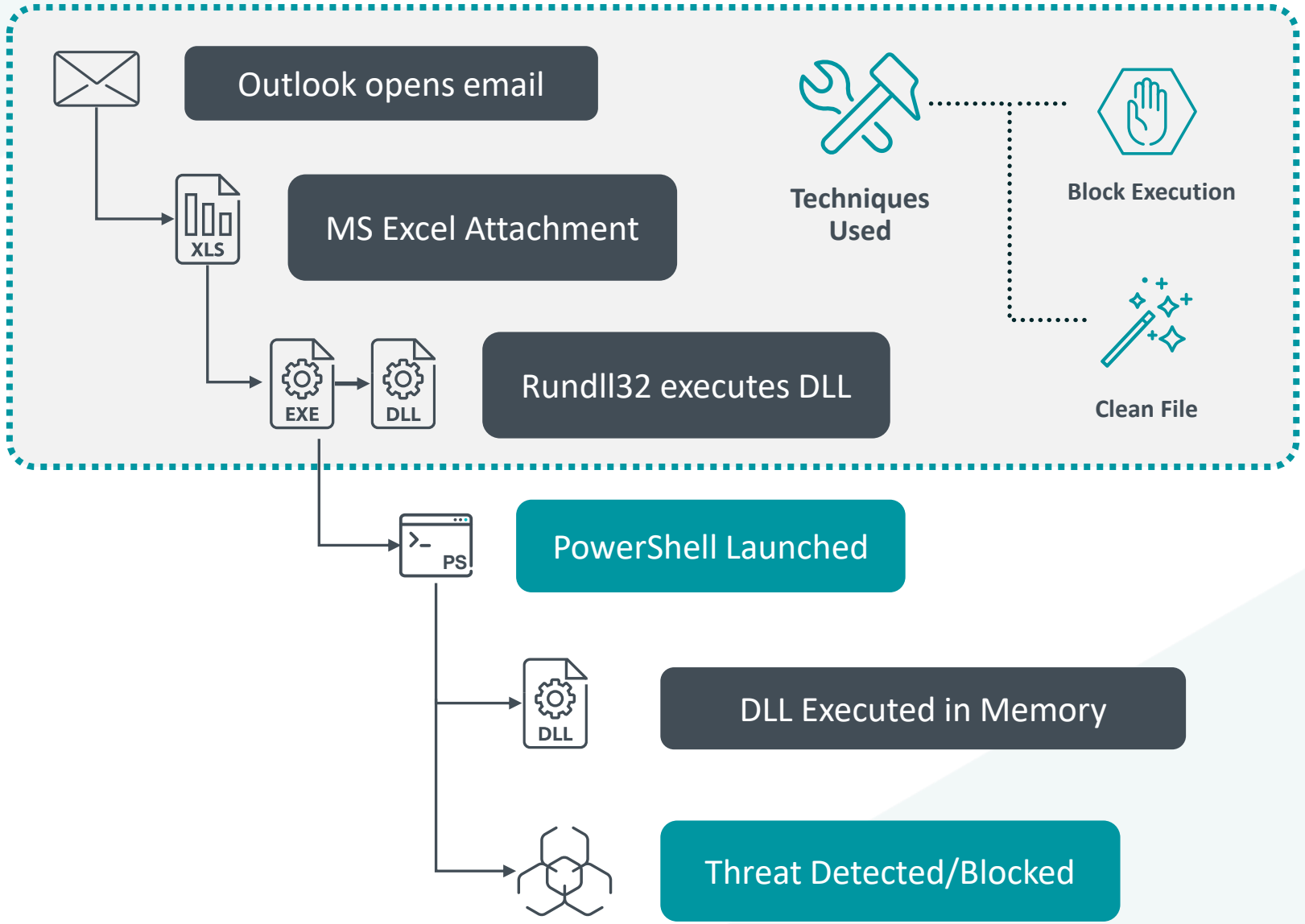
PALIELINĀTA PĀRREDZAMĪBA



Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA

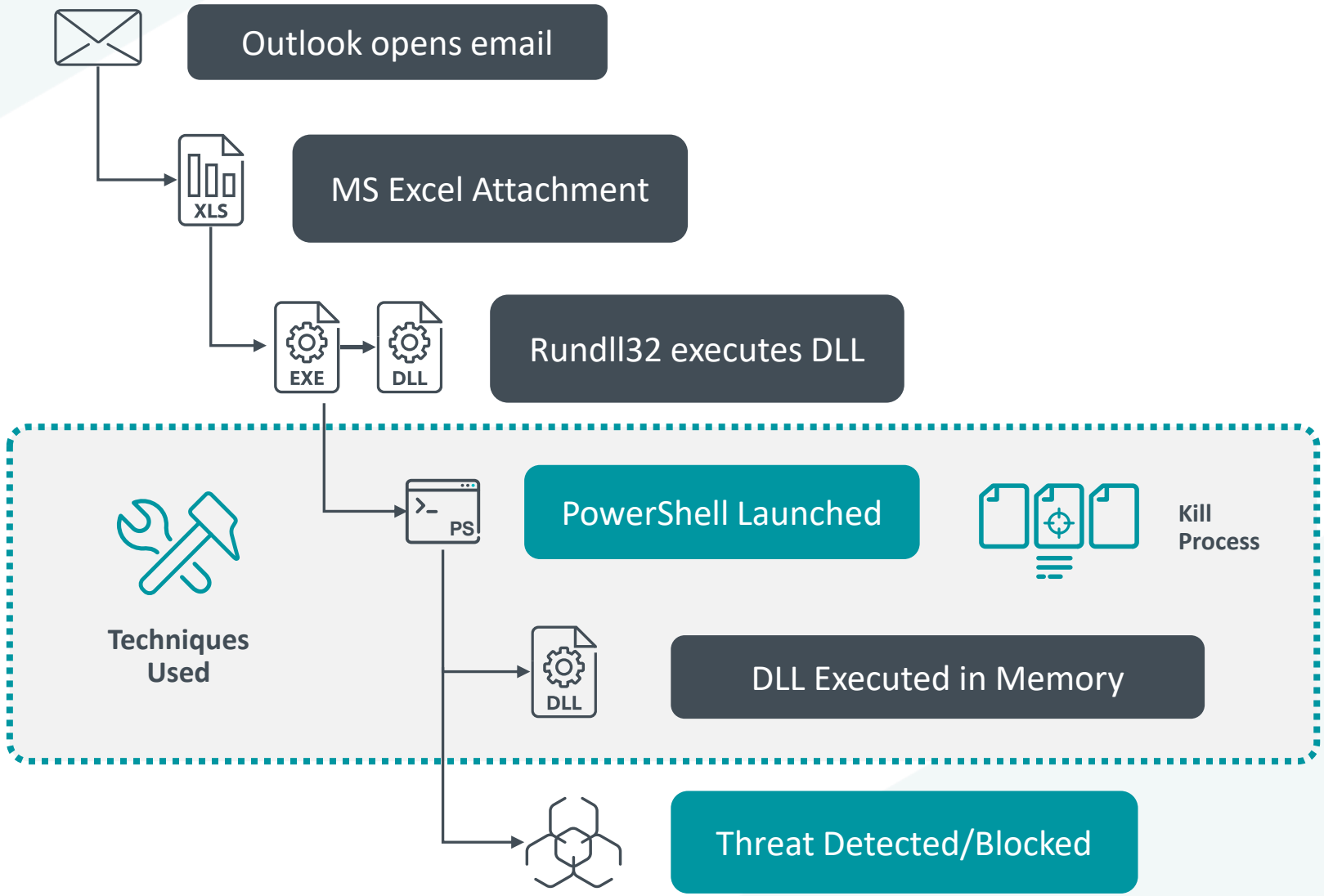
PAPILDU KONTROLE



Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA

PAPILDU KONTROLE

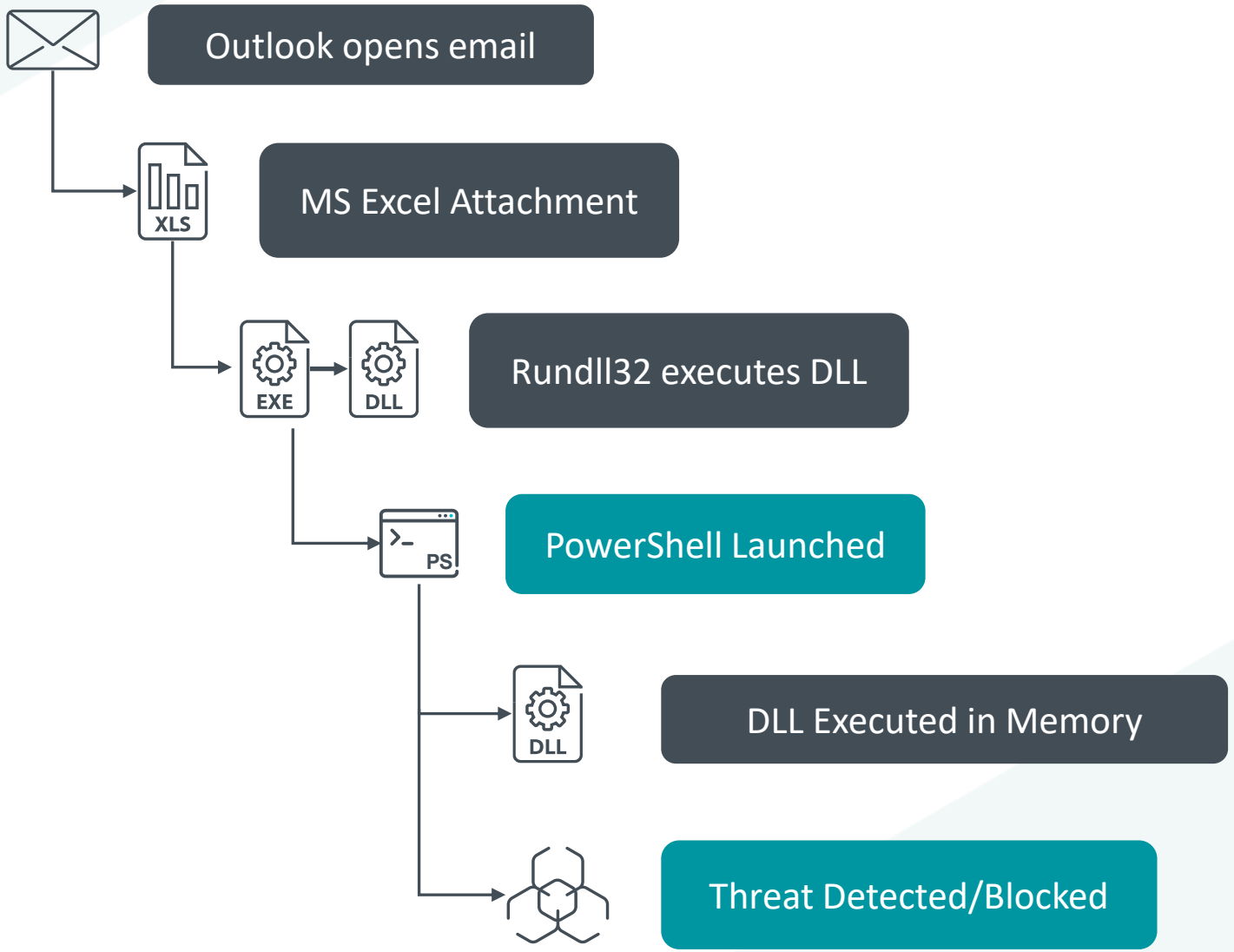


Ar ESET Inspect Jūs iegūstat:

PALIELINĀTA PĀRREDZAMĪBA

PAPILDU KONTROLE

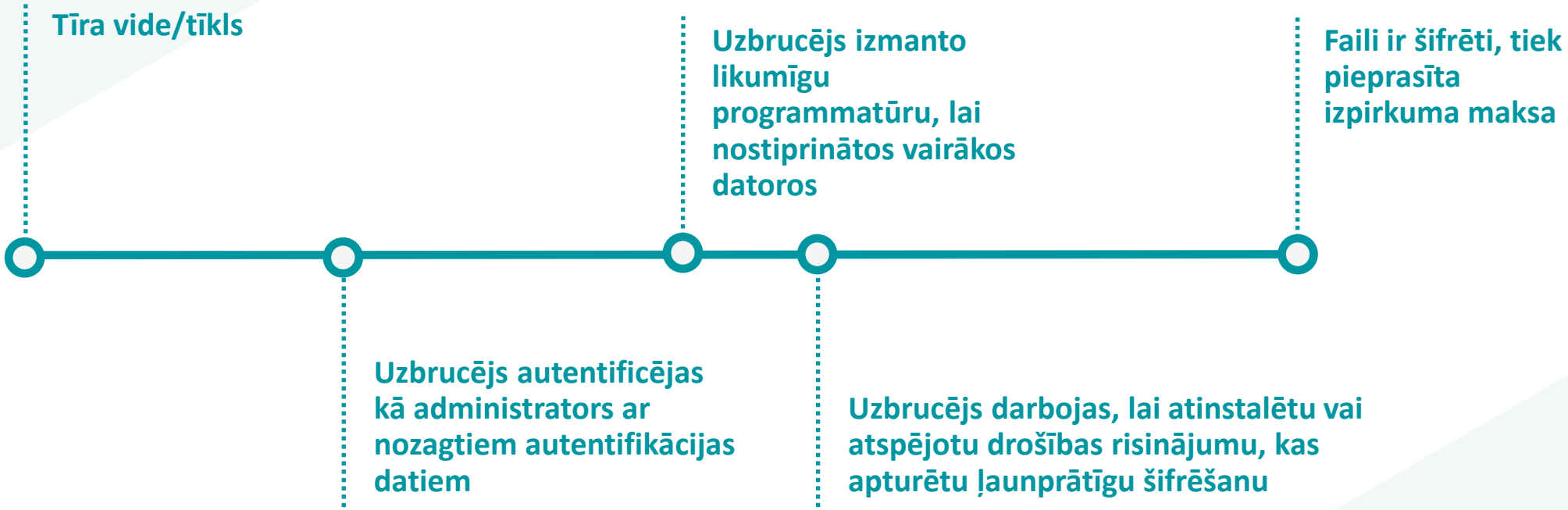
PĀRLIECĪBU PAR DROŠĪBU UN SIRDSMIERU



Scenārijs 2

Ransomware

Kā izskatās Ransomware uzbrukums?



Bez ESET Inspect:

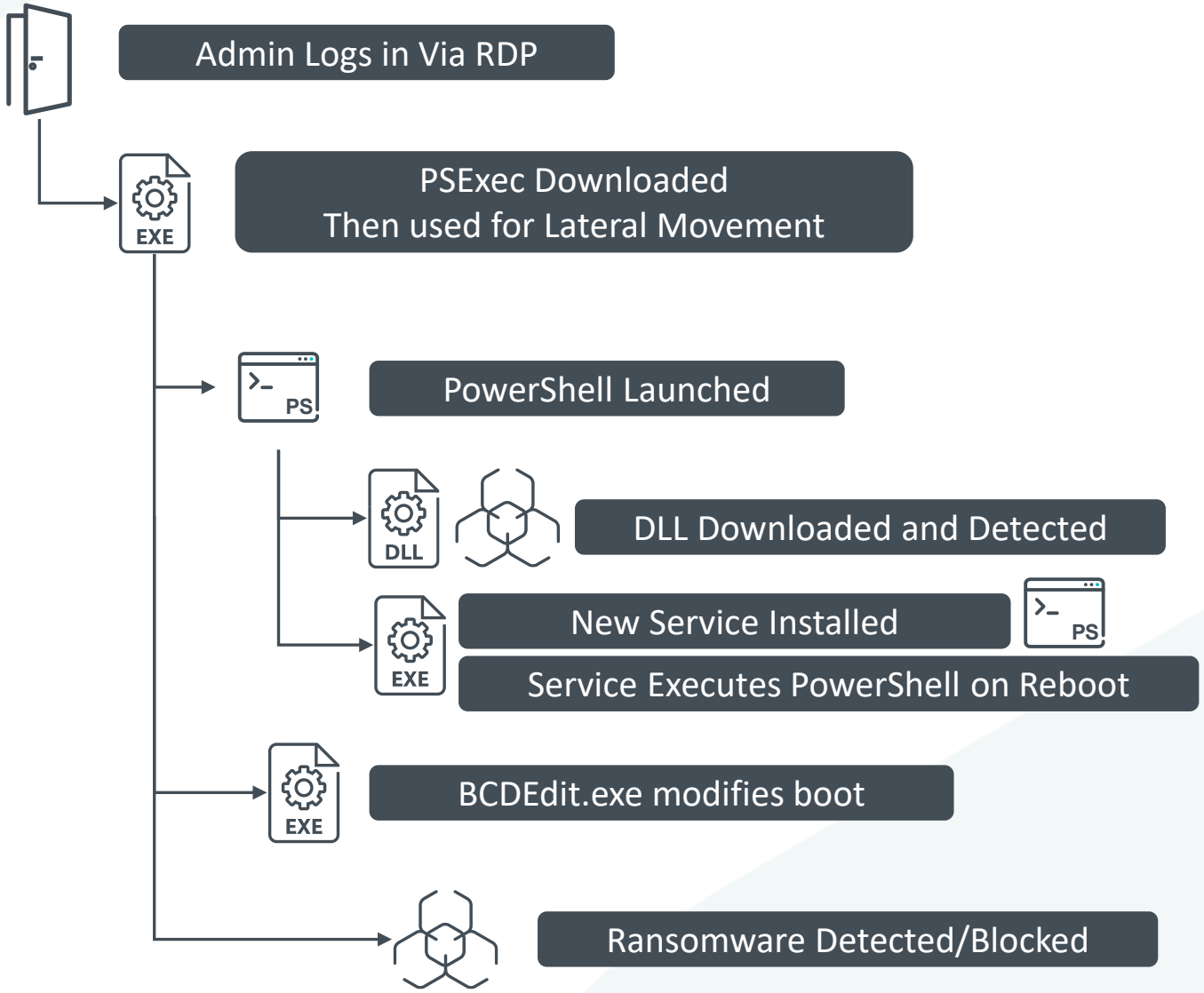
Minimāla redzamība

Nepamana leģitīmo programmu izmantošanu

Var pamanīt, ka drošība ir atspējota

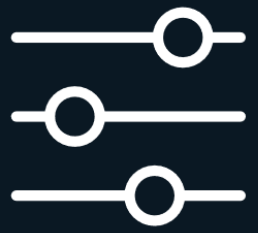
Ar ESET Inspect Jūs iegūstat:

- Paaugstināta pārredzamība
- Papildus kontroles iespējas
- Izpildiet kiberrisku apdrošināšanas prasības
- Pārliecinātību par drošību un sirdsmieru



Ar ESET Inspect Jūs iegūstat

Pārredzamību



Kontoli

Sirdsmieru

Varat kvalificēties kiberrisku apdrošināšanai

LIVEGUARD ADVANCED

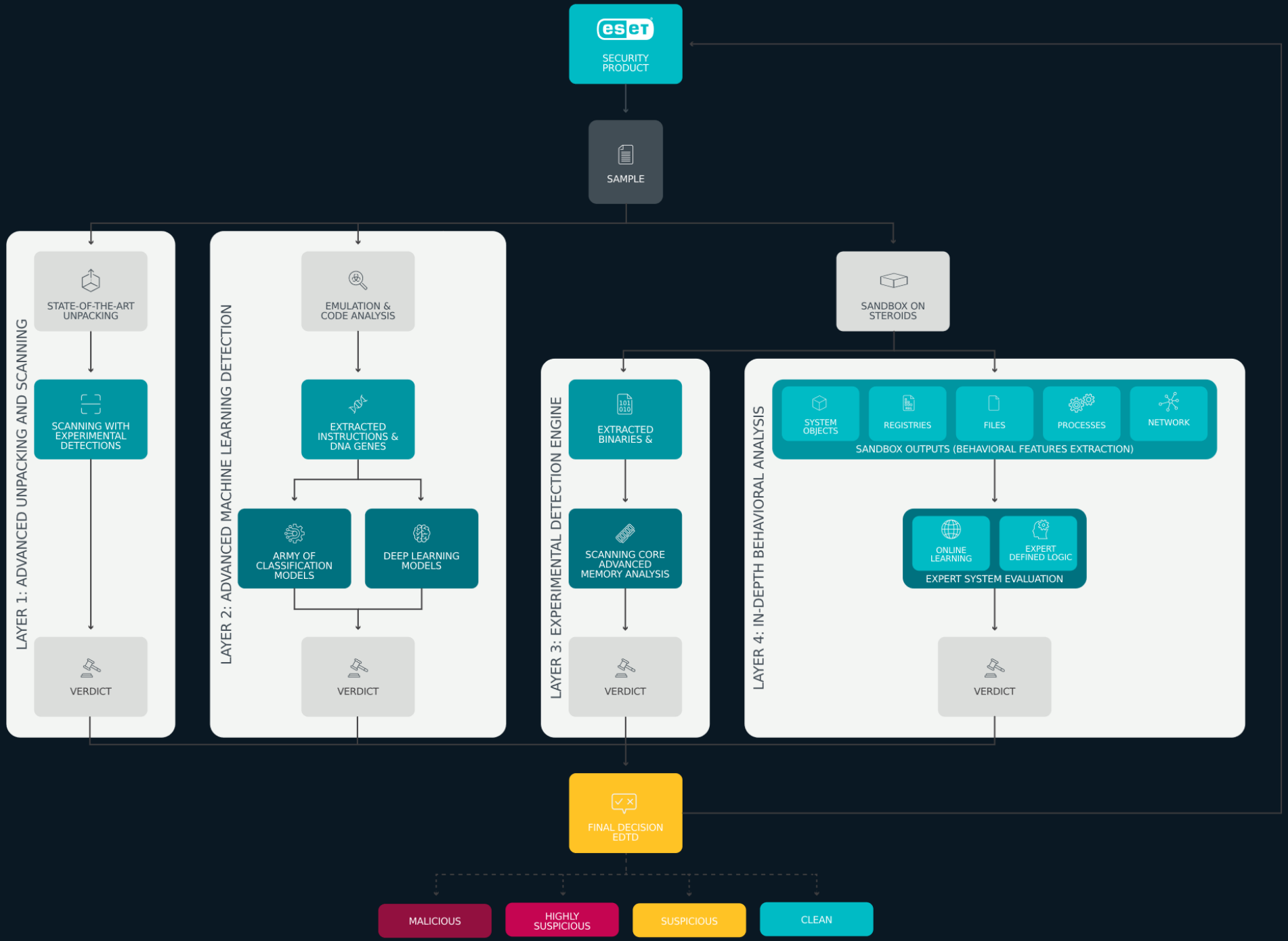
Proaktīva aizsardzība pret nulltās dienas aprdaudējumiem un iepriekš neredzētiem apdraudējumu veidiem

ESET LIVEGUARD ADVANCED

- Atklāj nulltās dienas apdraudējumus un nekad neredzētus apdraudējumus
- Uz mākoņ-smilškastēm balstīta tehnoloģija
- Uz uzvedību balstīta noteikšana

ESET LIVEGUARD ADVANCED

- Visu iesniegto paraugu detaļas redzamas ESET PROTECT pārvaldība konsolē
- 99% paraugu tiek pārbaudīti mazāk nekā 5 minūtēs
- Darbojas tieši ar ESET Endpoint Security, Mail Security un Cloud Office Security
- Ļoti detalizēti konfigurējama iekārtas politika


SECURITY PRODUCT
SAMPLE
LAYER 1: ADVANCED UNPACKING AND SCANNING
STATE-OF-THE-ART UNPACKING
SCANNING WITH EXPERIMENTAL DETECTIONS
VERDICT
LAYER 2: ADVANCED MACHINE LEARNING DETECTION
EMULATION & CODE ANALYSIS
EXTRACTED INSTRUCTIONS & DNA GENES
ARMY OF CLASSIFICATION MODELS
DEEP LEARNING MODELS
VERDICT
LAYER 3: EXPERIMENTAL DETECTION ENGINE
EXTRACTED BINARIES &
SCANNING CORE ADVANCED MEMORY ANALYSIS
VERDICT
SANDBOX ON STEROIDS
LAYER 4: IN-DEPTH BEHAVIORAL ANALYSIS
SYSTEM OBJECTS
REGISTRIES
FILES
PROCESSES
NETWORK
SANDBOX OUTPUTS (BEHAVIORAL FEATURES EXTRACTION)
ONLINE LEARNING
EXPERT DEFINED LOGIC
EXPERT SYSTEM EVALUATION
VERDICT
FINAL DECISION EDTD
MALICIOUS
HIGHLY SUSPICIOUS
SUSPICIOUS
CLEAN

ESET MAIL SECURITY

Pilnīga pasta serveru aizsardzība
E-pasts ir primārais draudu vektors

ESET MAIL SECURITY

Iekšēji izstrādāta pretsurogātpasta, pretpikšķerēšanas un paša servera aizsardzība.

Apvienojot mašīnmācīšanos, lielos datus un cilvēku zināšanas.

- Antiļaunprogrammatūra
- Antispam
- Antipikšķerēšana
- E-pasta servera aizsardzība
- Uz mašīnmācīšanos balstīta aizsardzība
- Stingra karantīnas vadība
- Custer atbalsts
- Hibrīda Office 365 skenēšana

ESET SECURE AUTHENTICATION

Daudzfaktoru autentifikācija, ko ir viegli ieviest un ērti lietot

ESET SECURE AUTHENTICATION

Galvenās funkcionalitātes

- Darbojas ar fiziskajām atslēgām (hardware tokens) un viedtālruņiem
- Nav nepieciešama īpaša aparatūra
- Tiek nodrošināts pilns API un SDK
- Atbalsta standarta (SAML2) protokolu, lai izveidotu savienojumu ar klientu sistēmām
- Attālā vadība
- Push autentifikācija
- Uzstādīšana 10 minūtēs (klienta)

61% no datu noplūdēm ir saistītas ar autentifikācijas datu noplūdi*

*Avots: Verizon 2021 Data Breach Investigation Report

ESET SECURE AUTHENTICATION

Pielietojums

- Pieteikties fiziskajā lokālajā datorā | Virtuālais dators | Attālā darbvirsma (RemoteDesktop)
- VPN aitentifikācija
- Webmail, CRM un citi pakalpojumi, kas pieejami caur pārlūkprogrammu
- Piesakieties trešās puses pakalpojumos, piemēram, Dropbox

ESET CLOUD OFFICE SECURITY

Aizsardzība Microsoft 365 lietojumprogrammām

ESET CLOUD OFFICE SECURITY

- Aizsardzība pret ļaunprātīgu programmatūru Exchange Online, OneDrive, SharePoint Online un Teams
- Aizsardzība pret surogātpastu Exchange Online
- Aizsardzība pret pikšķerēšanu Exchange Online
- ESET LiveGuard Advanced — vēl neredzētu draudu noteikšana
- Izvēršana un tūlītēja aizsardzība tikai piecās minūtēs

ESET CLOUD OFFICE SECURITY

Galvenās funkcionalitātes

- Informācijas panelis ar konstatāciju statistiku un filtrēšanu
- Exchange Online aizsardzība pret ļaunprātīgu programmatūru
- Aizsardzība pret surogātpastu Exchange Online
- Iekļauts ESET LiveGuard Advanced
- Uzstādīšana tikai 5 minūtēs
- Multitenancy iespēja ar piekļuves pārvaldību
- Audita žurnalēšana
- Aizsardzība pret pikšķerēšanu:
  - OneDrive, SharePoint Online un Teams
  - Exchange Online
- Pārvaldiet Teams un vietnes
- Visaptveroša žurnalēšana
- Politikas un automatizācija
- Karantīnas pārvaldība
- Mērogojamība

VULNERABILITY & PATCH MANAGEMENT

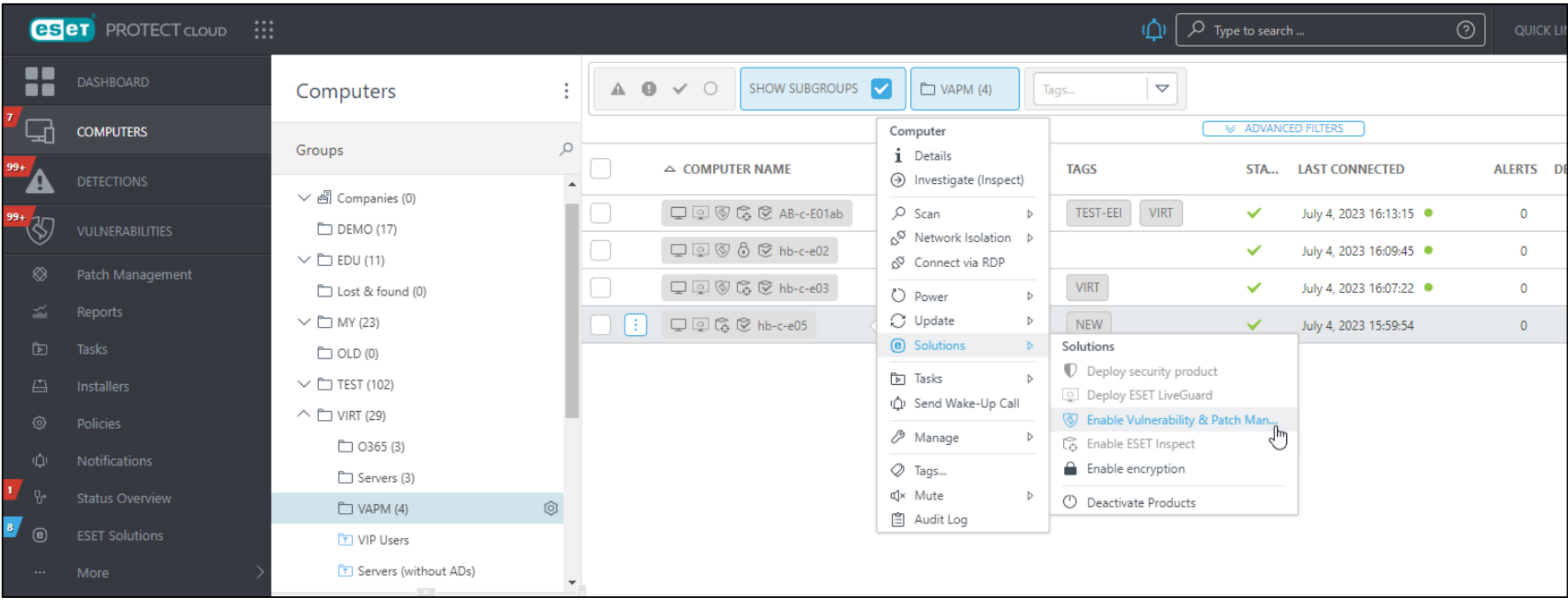
Izseko ievainojamības un nodrošina automātisku ielāpu

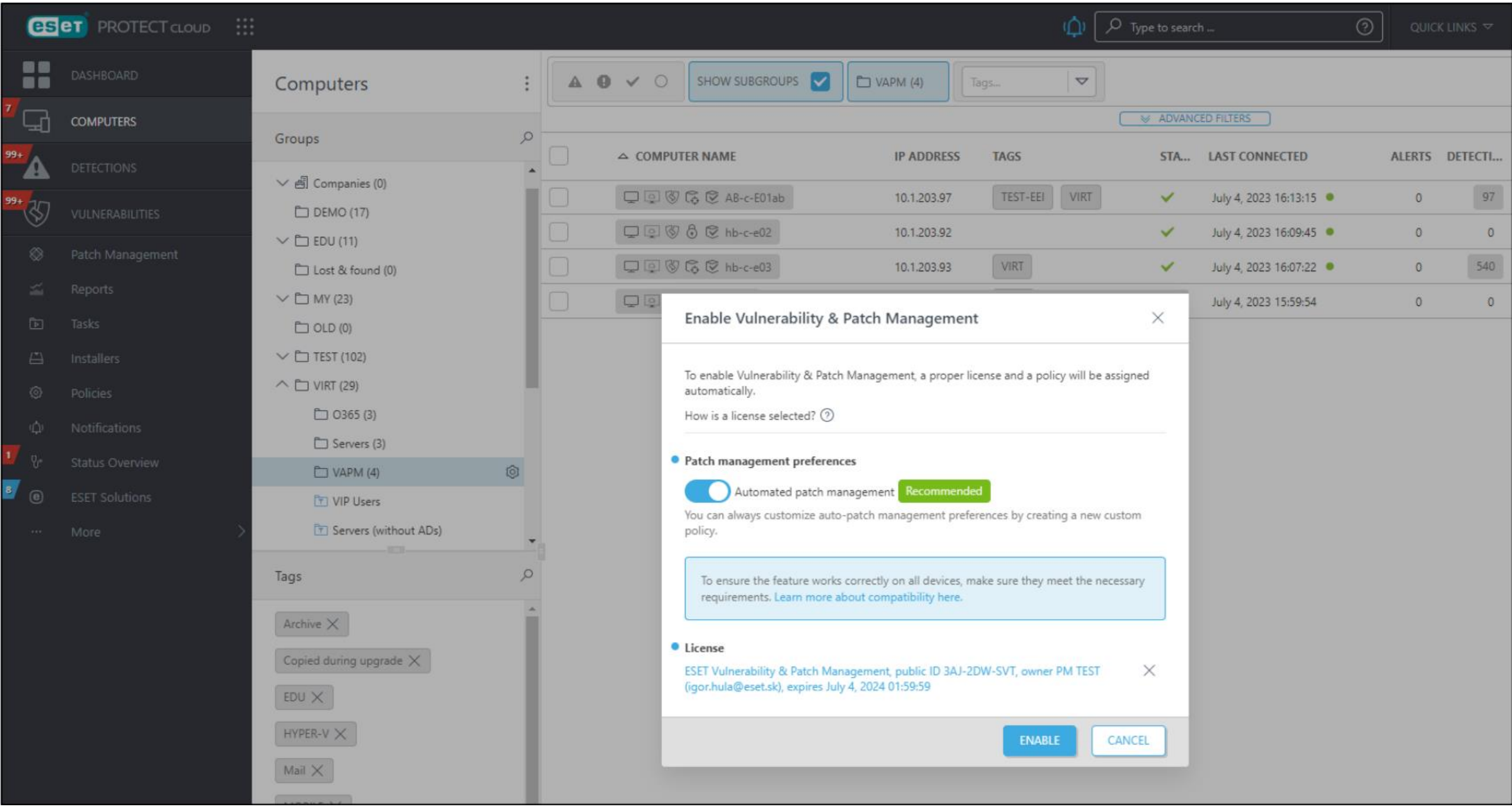
VULNERABILITY & PATCH MANAGEMENT

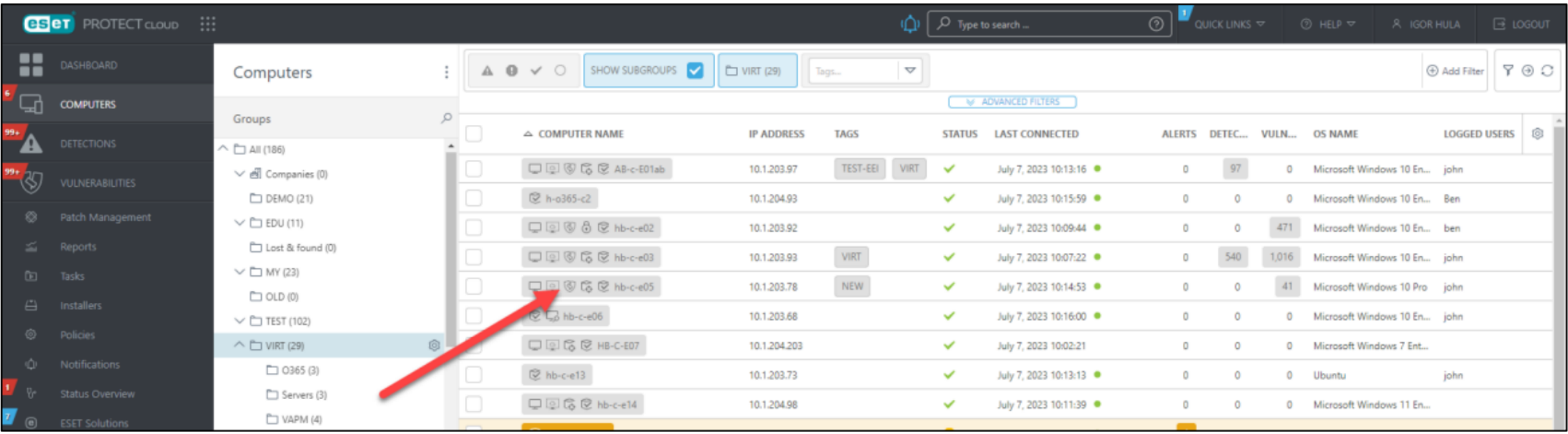
Konstatē un novērš ievainojamības visās Jūsu iekārtās

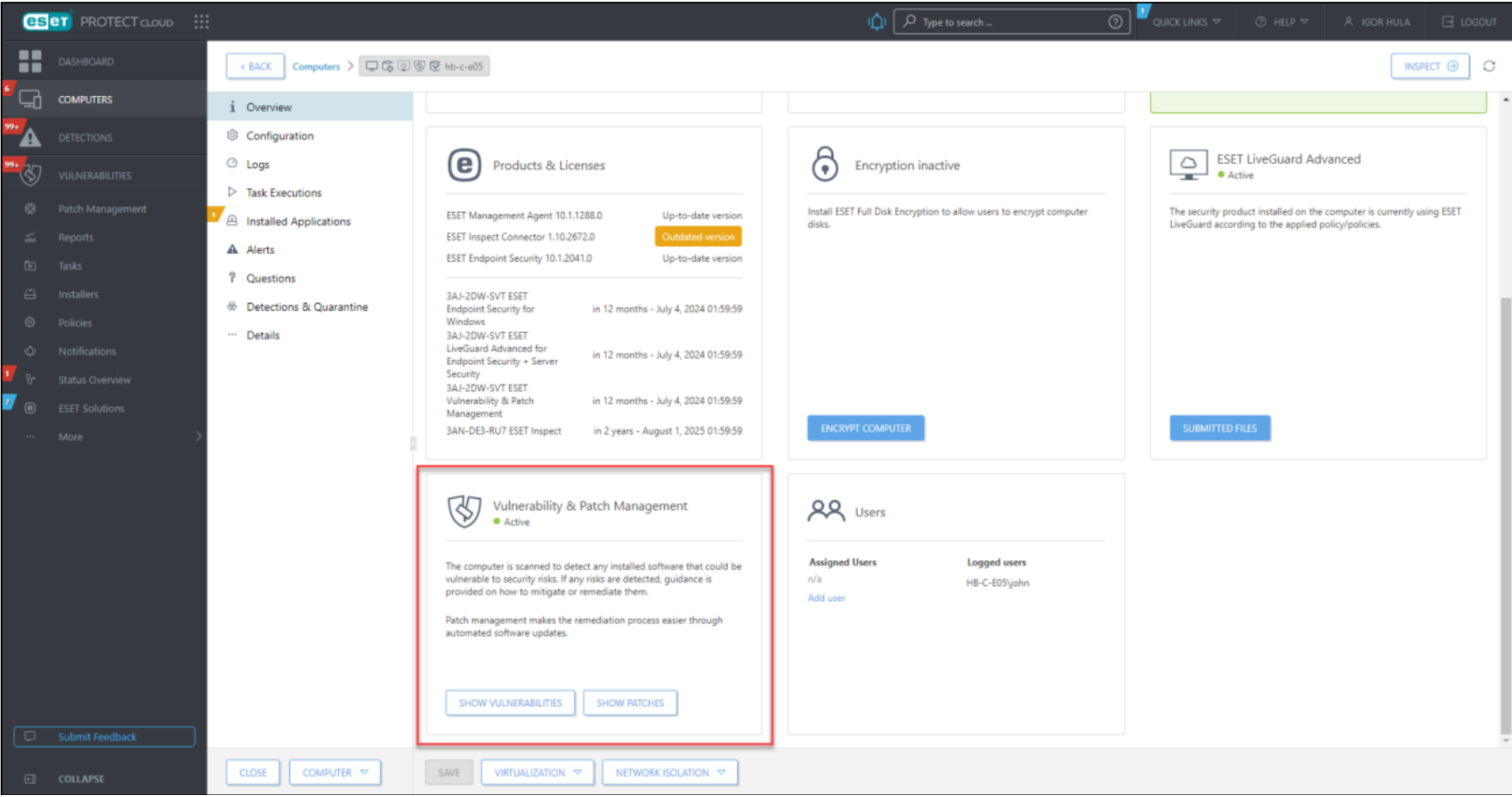
ESET ievainojamību un ielāpu pārvaldība aktīvi izseko operētājsistēmu un izplatītāko lietojumprogrammu ievainojamības un nodrošina automātisku ielāpu ielādi visos galapunktos, ko pārvalda, izmantojot mūsu vienoto platformu.

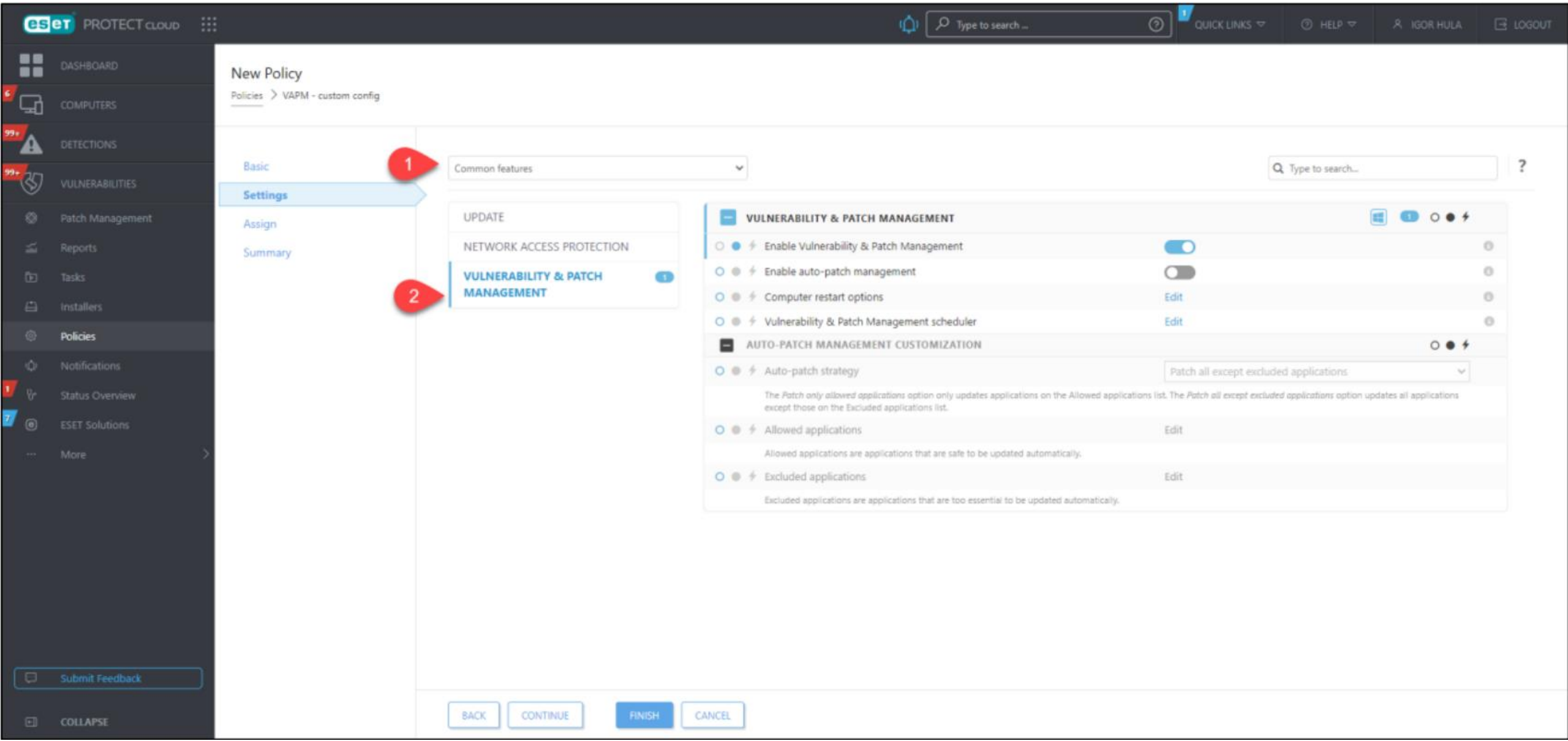
- **Pārvaldiet ielāpu centralizēti, izmantojot ESET PROTECT Cloud konsoli**
- **Automatizējiet skenēšanu, izmantojot pielāgojamus grafika iestatījumus**
- **Filtrējiet, grupējiet un kārtojiet ievainojamības, pamatojoties uz to nopietnību**
- **Izvēlieties kādu no automātiskajām un manuālajām ielāpu iespējām**
- **Pielāgojiet savas ielāpu politikas**

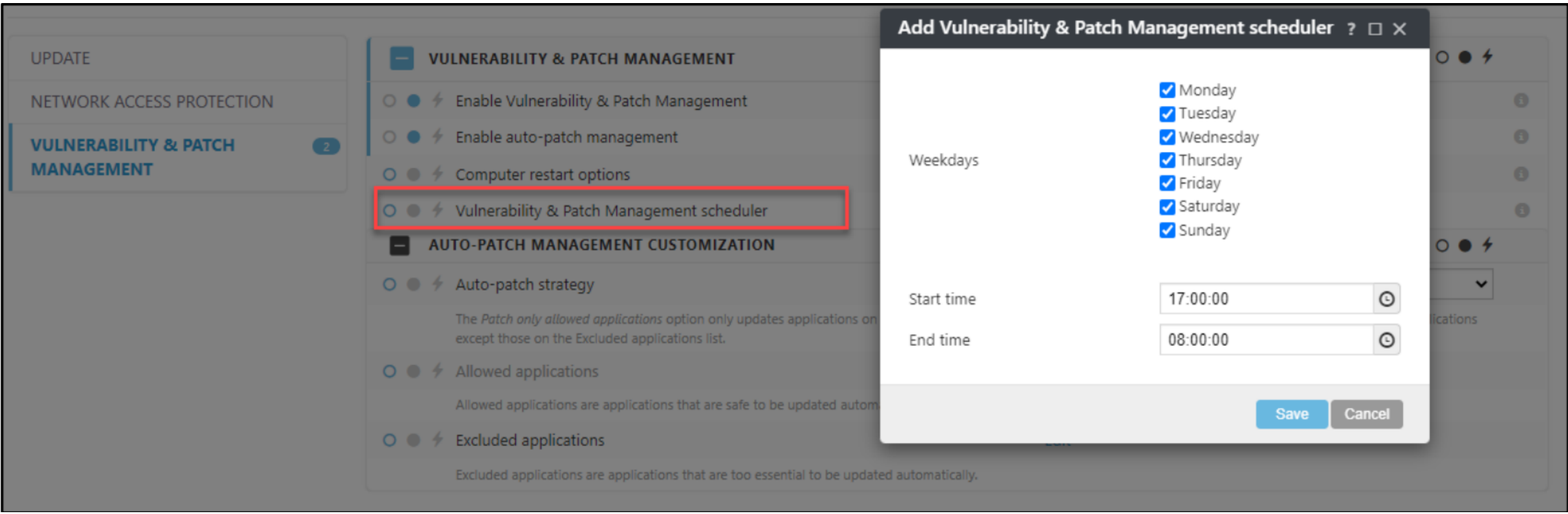

ESET PROTECT CLOUD
Type to search ...
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Computers
Groups
Companies (0)
DEMO (17)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
O365 (3)
Servers (3)
VAPM (4)
VIP Users
Servers (without ADs)
SHOW SUBGROUPS
VAPM (4)
Tags...
ADVANCED FILTERS
COMPUTER NAME
TAGS
STA...
LAST CONNECTED
ALERTS
AB-c-E01ab
TEST-EEI
VIRT
July 4, 2023 16:13:15
0
hb-c-e02
July 4, 2023 16:09:45
0
hb-c-e03
VIRT
July 4, 2023 16:07:22
0
hb-c-e05
NEW
July 4, 2023 15:59:54
0
Computer
Details
Investigate (Inspect)
Scan
Network Isolation
Connect via RDP
Power
Update
Solutions
Tasks
Send Wake-Up Call
Manage
Tags...
Mute
Audit Log
Solutions
Deploy security product
Deploy ESET LiveGuard
Enable Vulnerability & Patch Man...
Enable ESET Inspect
Enable encryption
Deactivate Products

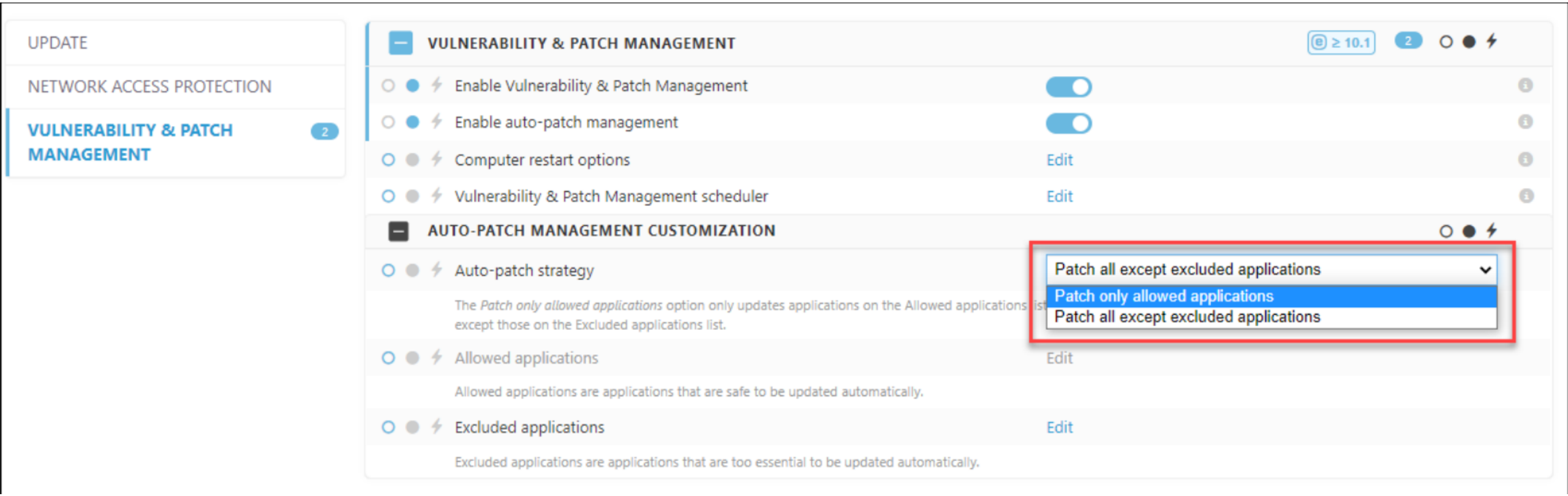

ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Computers
Groups
Companies (0)
DEMO (17)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
O365 (3)
Servers (3)
VAPM (4)
VIP Users
Servers (without ADs)
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
SHOW SUBGROUPS
VAPM (4)
Tags...
ADVANCED FILTERS
COMPUTER NAME
IP ADDRESS
TAGS
STA...
LAST CONNECTED
ALERTS
DETECTI...
AB-c-E01ab
10.1.203.97
TEST-EEI
VIRT
July 4, 2023 16:13:15
0
97
hb-c-e02
10.1.203.92
July 4, 2023 16:09:45
0
0
hb-c-e03
10.1.203.93
VIRT
July 4, 2023 16:07:22
0
540
July 4, 2023 15:59:54
0
0
Enable Vulnerability & Patch Management
To enable Vulnerability & Patch Management, a proper license and a policy will be assigned automatically.
How is a license selected?
Patch management preferences
Automated patch management
Recommended
You can always customize auto-patch management preferences by creating a new custom policy.
To ensure the feature works correctly on all devices, make sure they meet the necessary requirements. Learn more about compatibility here.
License
ESET Vulnerability & Patch Management, public ID 3AJ-2DW-SVT, owner PM TEST (igor.hula@eset.sk), expires July 4, 2024 01:59:59
ENABLE
CANCEL

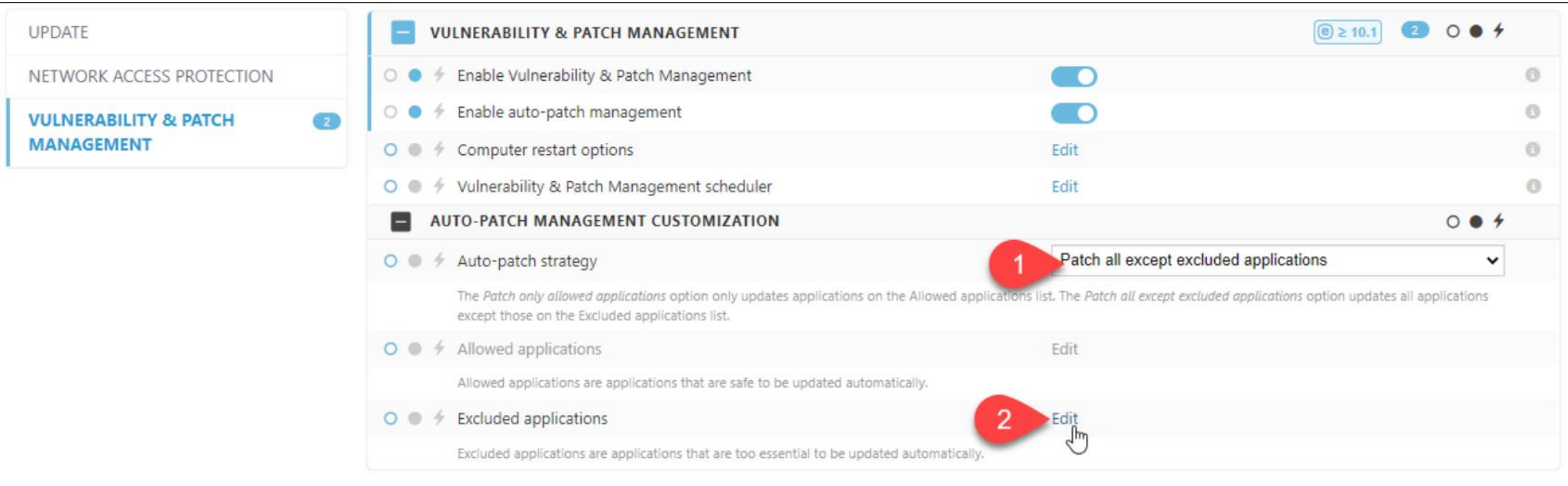

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
Computers
Groups
SHOW SUBGROUPS
VIRT (29)
Tags...
Add Filter
ADVANCED FILTERS
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
O365 (3)
Servers (3)
VAPM (4)
COMPUTER NAME
IP ADDRESS
TAGS
STATUS
LAST CONNECTED
ALERTS
DETEC...
VULN...
OS NAME
LOGGED USERS
AB-c-E01ab 10.1.203.97 TEST-EEI VIRT July 7, 2023 10:13:16 0 97 0 Microsoft Windows 10 En... john
h-o365-c2 10.1.204.93 July 7, 2023 10:15:59 0 0 0 Microsoft Windows 10 En... Ben
hb-c-e02 10.1.203.92 July 7, 2023 10:09:44 0 0 471 Microsoft Windows 10 En... ben
hb-c-e03 10.1.203.93 VIRT July 7, 2023 10:07:22 0 540 1,016 Microsoft Windows 10 En... john
hb-c-e05 10.1.203.78 NEW July 7, 2023 10:14:53 0 0 41 Microsoft Windows 10 Pro john
hb-c-e06 10.1.203.68 July 7, 2023 10:16:00 0 0 0 Microsoft Windows 10 En... john
HB-C-E07 10.1.204.203 July 7, 2023 10:02:21 0 0 0 Microsoft Windows 7 Ent...
hb-c-e13 10.1.203.73 July 7, 2023 10:13:13 0 0 0 Ubuntu john
hb-c-e14 10.1.204.98 July 7, 2023 10:11:39 0 0 0 Microsoft Windows 11 En...

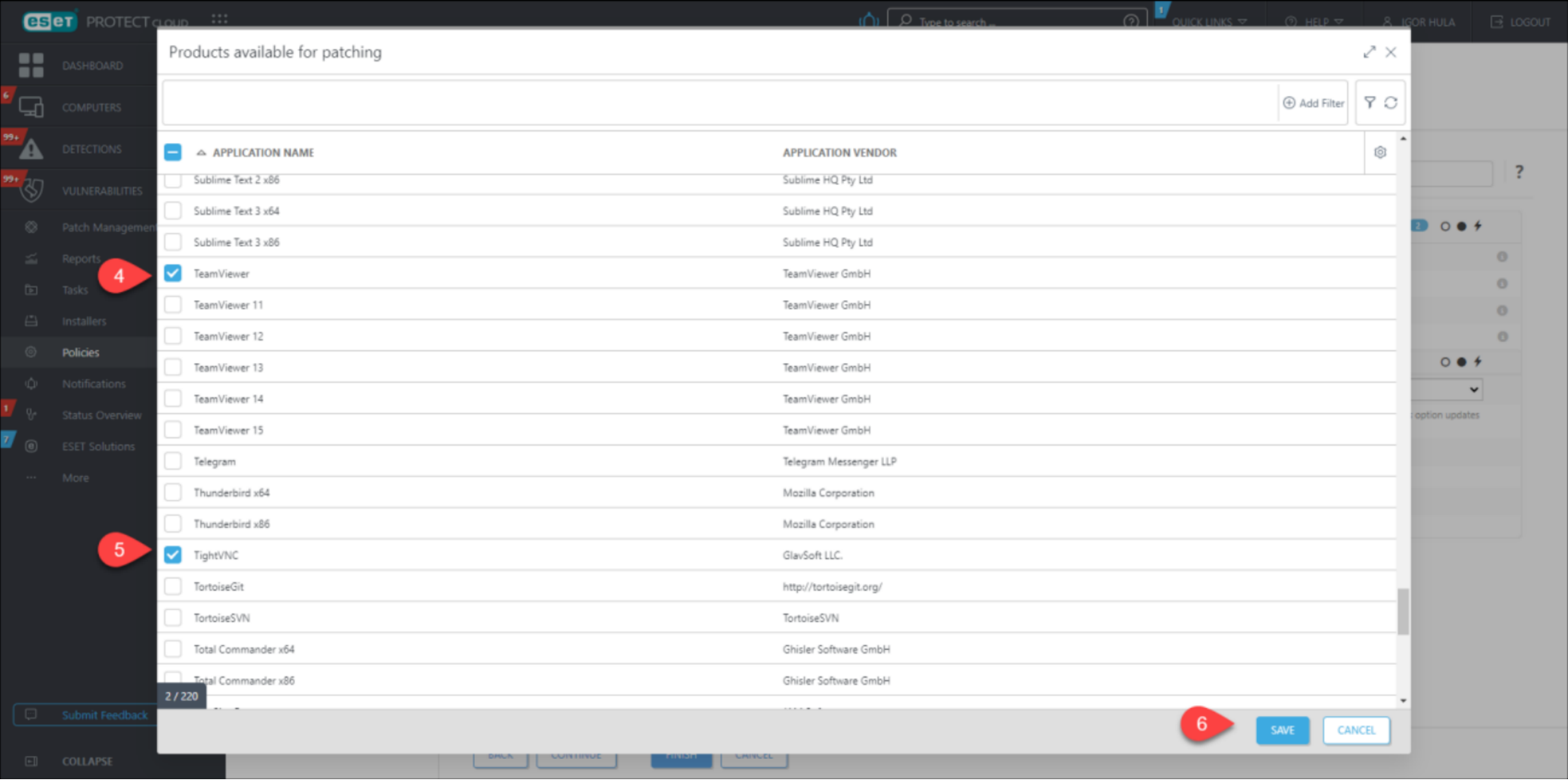

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
< BACK
Computers
hb-c-e05
INSPECT
Overview
Configuration
Logs
Task Executions
Installed Applications
Alerts
Questions
Detections & Quarantine
Details
Products & Licenses
ESET Management Agent 10.1.1288.0
Up-to-date version
ESET Inspect Connector 1.10.2672.0
Outdated version
ESET Endpoint Security 10.1.2041.0
Up-to-date version
3AJ-2DW-SVT ESET Endpoint Security for Windows
in 12 months - July 4, 2024 01:59:59
3AJ-2DW-SVT ESET LiveGuard Advanced for Endpoint Security + Server Security
in 12 months - July 4, 2024 01:59:59
3AJ-2DW-SVT ESET Vulnerability & Patch Management
in 12 months - July 4, 2024 01:59:59
3AN-DE3-RU7 ESET Inspect
in 2 years - August 1, 2025 01:59:59
Encryption inactive
Install ESET Full Disk Encryption to allow users to encrypt computer disks.
ENCRYPT COMPUTER
ESET LiveGuard Advanced
Active
The security product installed on the computer is currently using ESET LiveGuard according to the applied policy/policies.
SUBMITTED FILES
Vulnerability & Patch Management
Active
The computer is scanned to detect any installed software that could be vulnerable to security risks. If any risks are detected, guidance is provided on how to mitigate or remediate them.
Patch management makes the remediation process easier through automated software updates.
SHOW VULNERABILITIES
SHOW PATCHES
Users
Assigned Users
n/a
Add user
Logged users
HB-C-E05\john
CLOSE
COMPUTER
SAVE
VIRTUALIZATION
NETWORK ISOLATION


eset PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
New Policy
Policies > VAPM - custom config
Basic
Settings
Assign
Summary
1
Common features
Type to search...
2
UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT
VULNERABILITY & PATCH MANAGEMENT
Enable Vulnerability & Patch Management
Enable auto-patch management
Computer restart options
Edit
Vulnerability & Patch Management scheduler
Edit
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
Patch all except excluded applications
The Patch only allowed applications option only updates applications on the Allowed applications list. The Patch all except excluded applications option updates all applications except those on the Excluded applications list.
Allowed applications
Edit
Allowed applications are applications that are safe to be updated automatically.
Excluded applications
Edit
Excluded applications are applications that are too essential to be updated automatically.
BACK
CONTINUE
FINISH
CANCEL

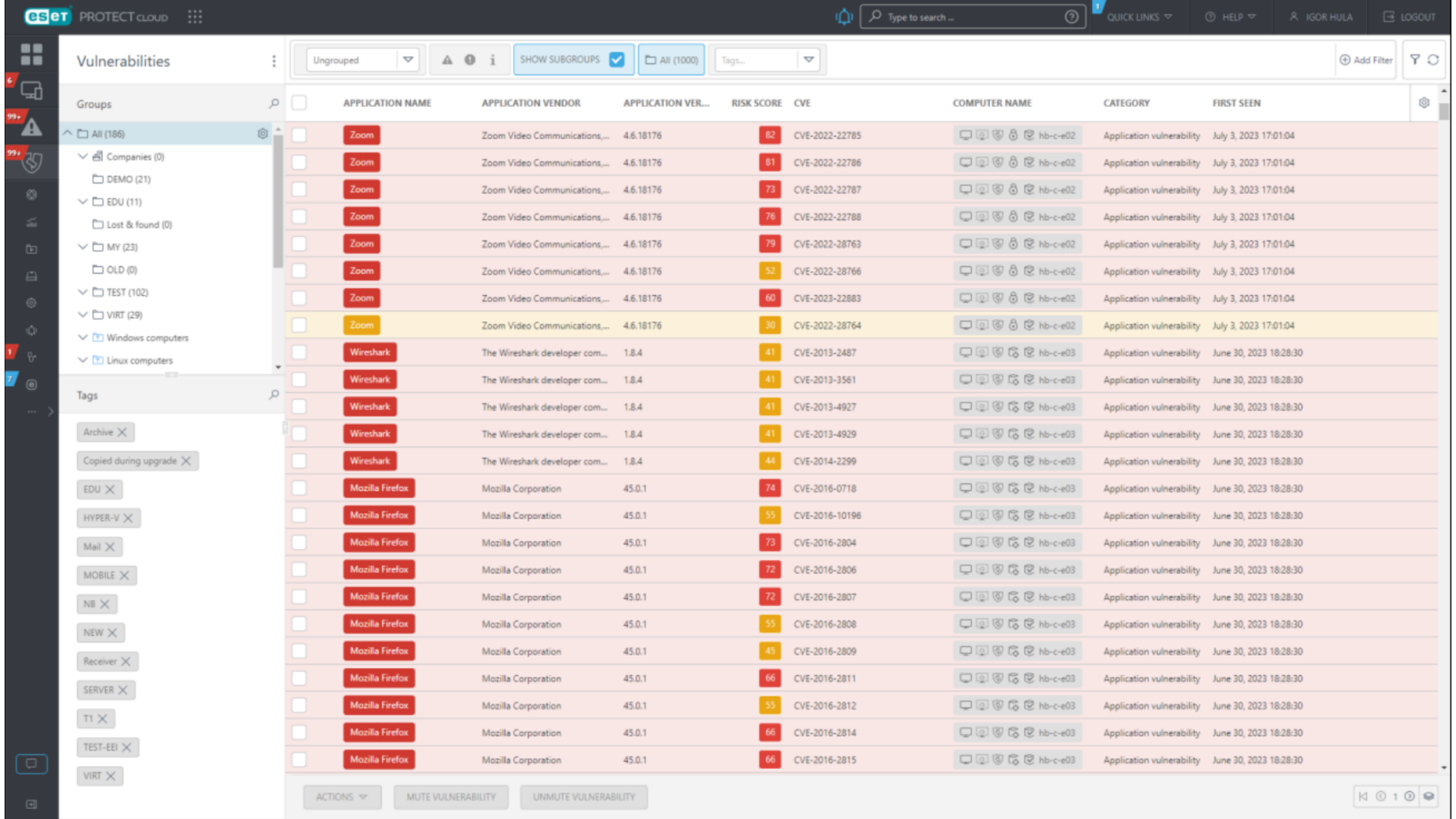

UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT
2
VULNERABILITY & PATCH MANAGEMENT
Enable Vulnerability & Patch Management
Enable auto-patch management
Computer restart options
Vulnerability & Patch Management scheduler
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
The Patch only allowed applications option only updates applications on
except those on the Excluded applications list.
Allowed applications
Allowed applications are applications that are safe to be updated autom
Excluded applications
Excluded applications are applications that are too essential to be updated automatically.
Add Vulnerability & Patch Management scheduler
Weekdays
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Start time
17:00:00
End time
08:00:00
Save
Cancel

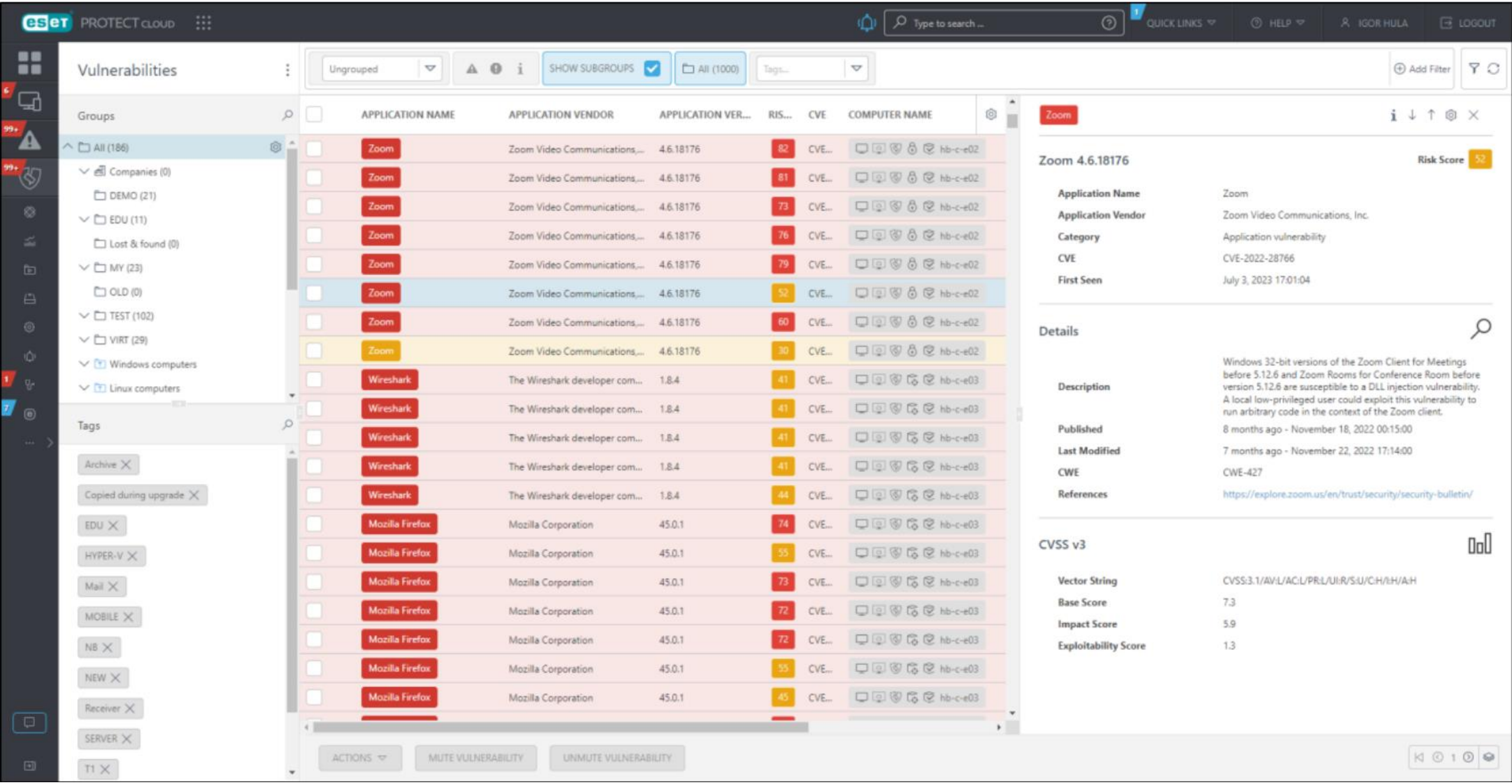

UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT 2
VULNERABILITY & PATCH MANAGEMENT
≥ 10.1
2
Enable Vulnerability & Patch Management
Enable auto-patch management
Computer restart options
Edit
Vulnerability & Patch Management scheduler
Edit
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
Patch all except excluded applications
Patch only allowed applications
Patch all except excluded applications
The Patch only allowed applications option only updates applications on the Allowed applications list
except those on the Excluded applications list.
Allowed applications
Edit
Allowed applications are applications that are safe to be updated automatically.
Excluded applications
Edit
Excluded applications are applications that are too essential to be updated automatically.

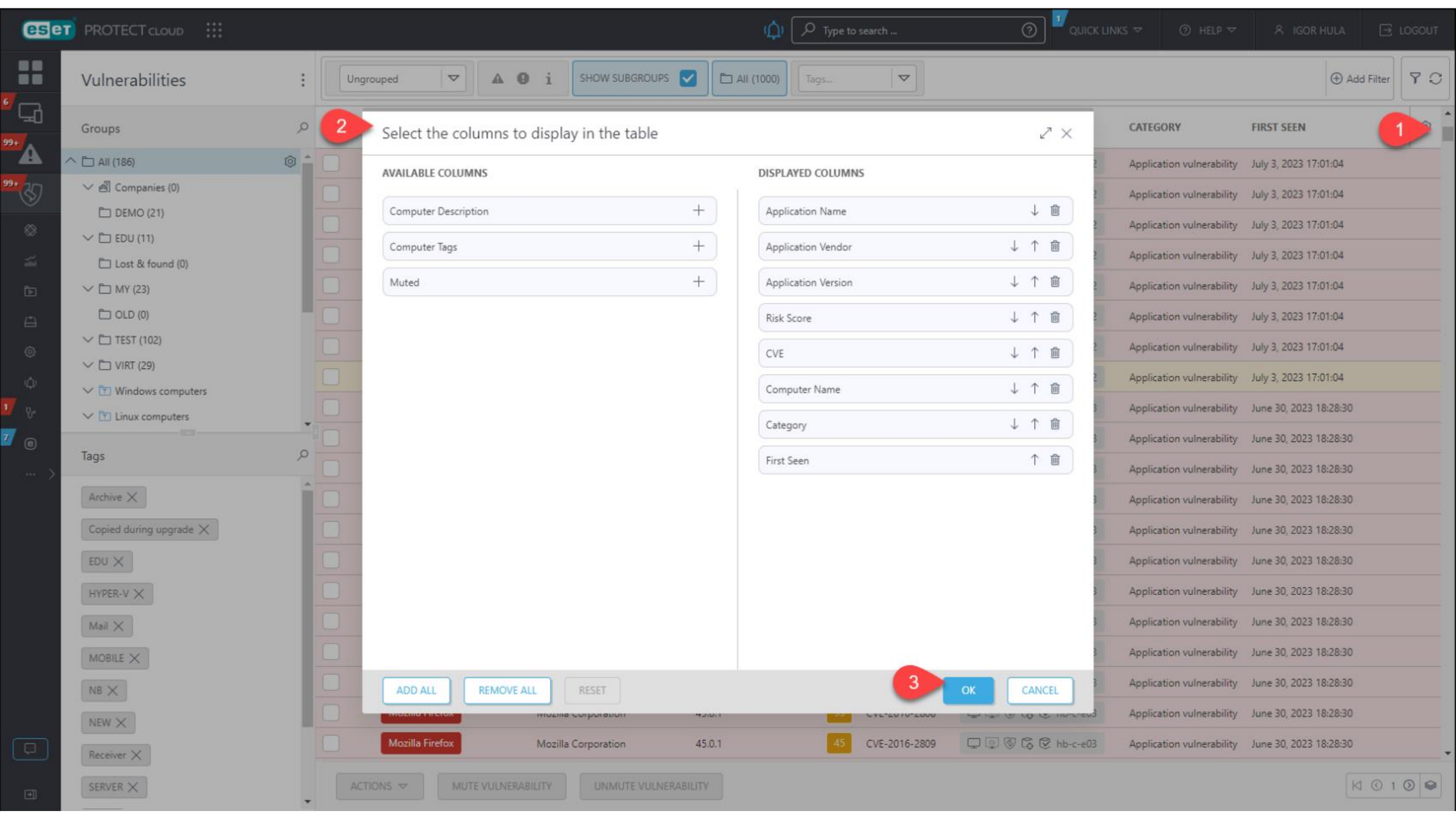

UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT 2
VULNERABILITY & PATCH MANAGEMENT
≥ 10.1
2
Enable Vulnerability & Patch Management
Enable auto-patch management
Computer restart options
Edit
Vulnerability & Patch Management scheduler
Edit
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
1
Patch all except excluded applications
The Patch only allowed applications option only updates applications on the Allowed applications list. The Patch all except excluded applications option updates all applications except those on the Excluded applications list.
Allowed applications
Edit
Allowed applications are applications that are safe to be updated automatically.
Excluded applications
2
Edit
Excluded applications are applications that are too essential to be updated automatically.

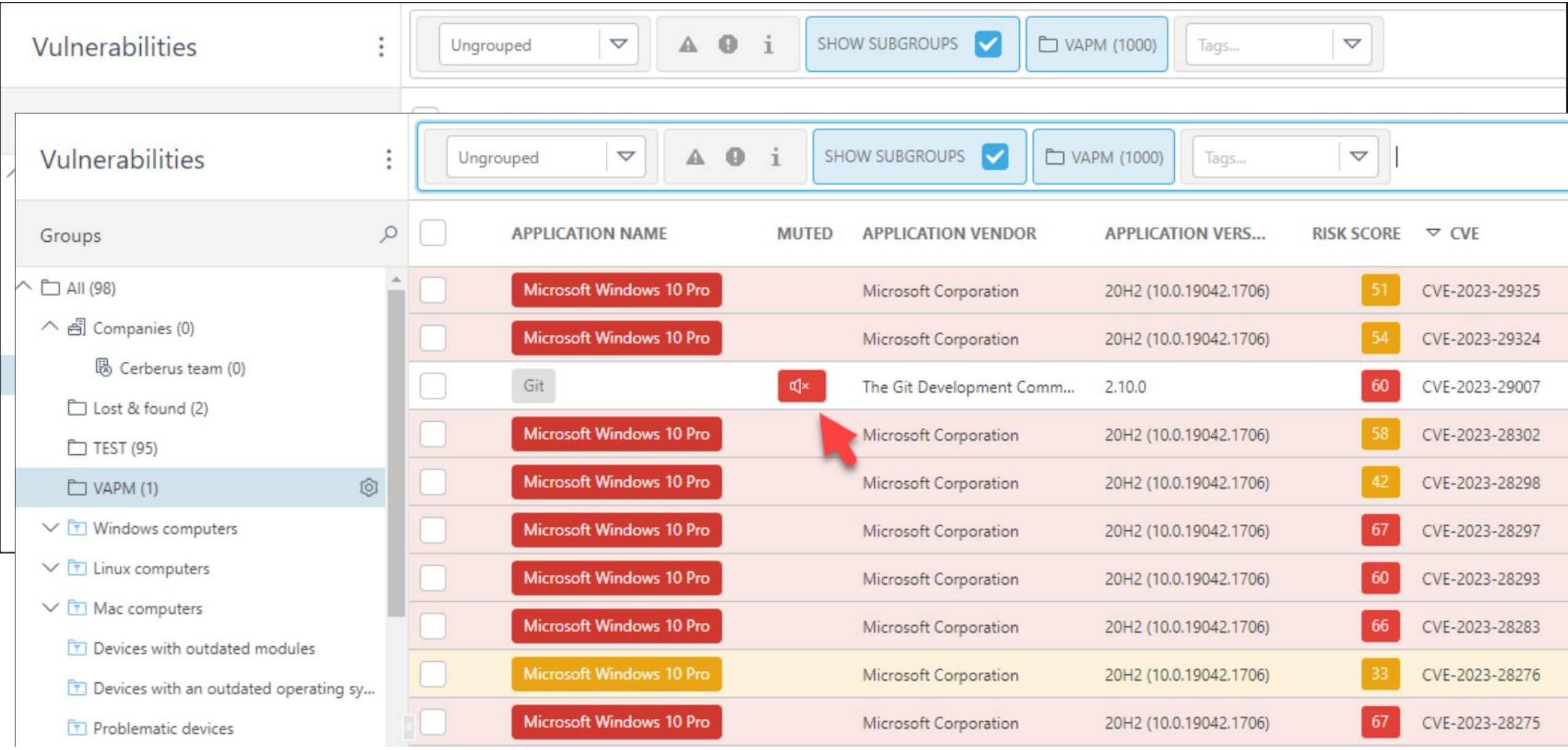


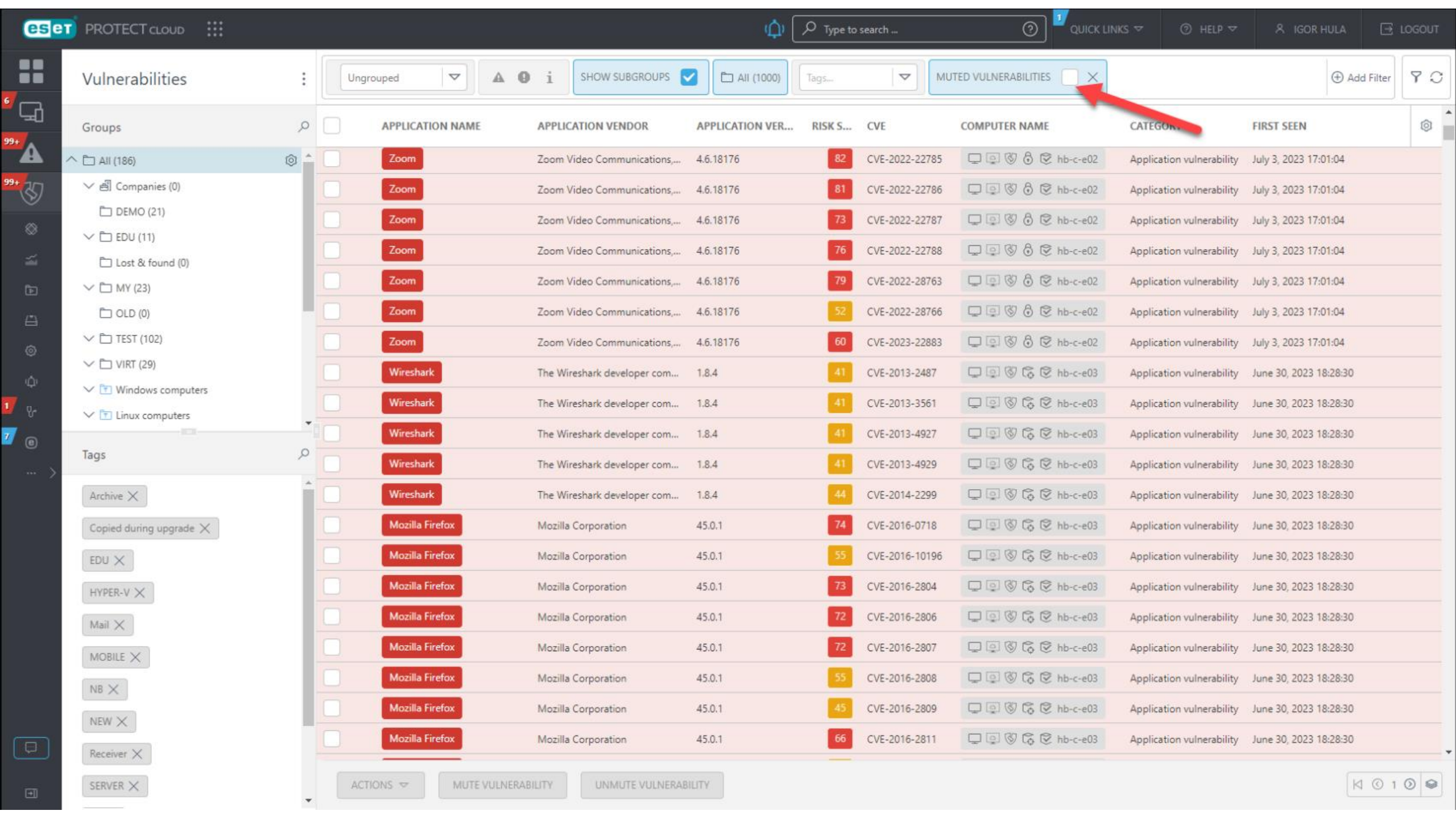
2023-09-25 - 240 programmatūras

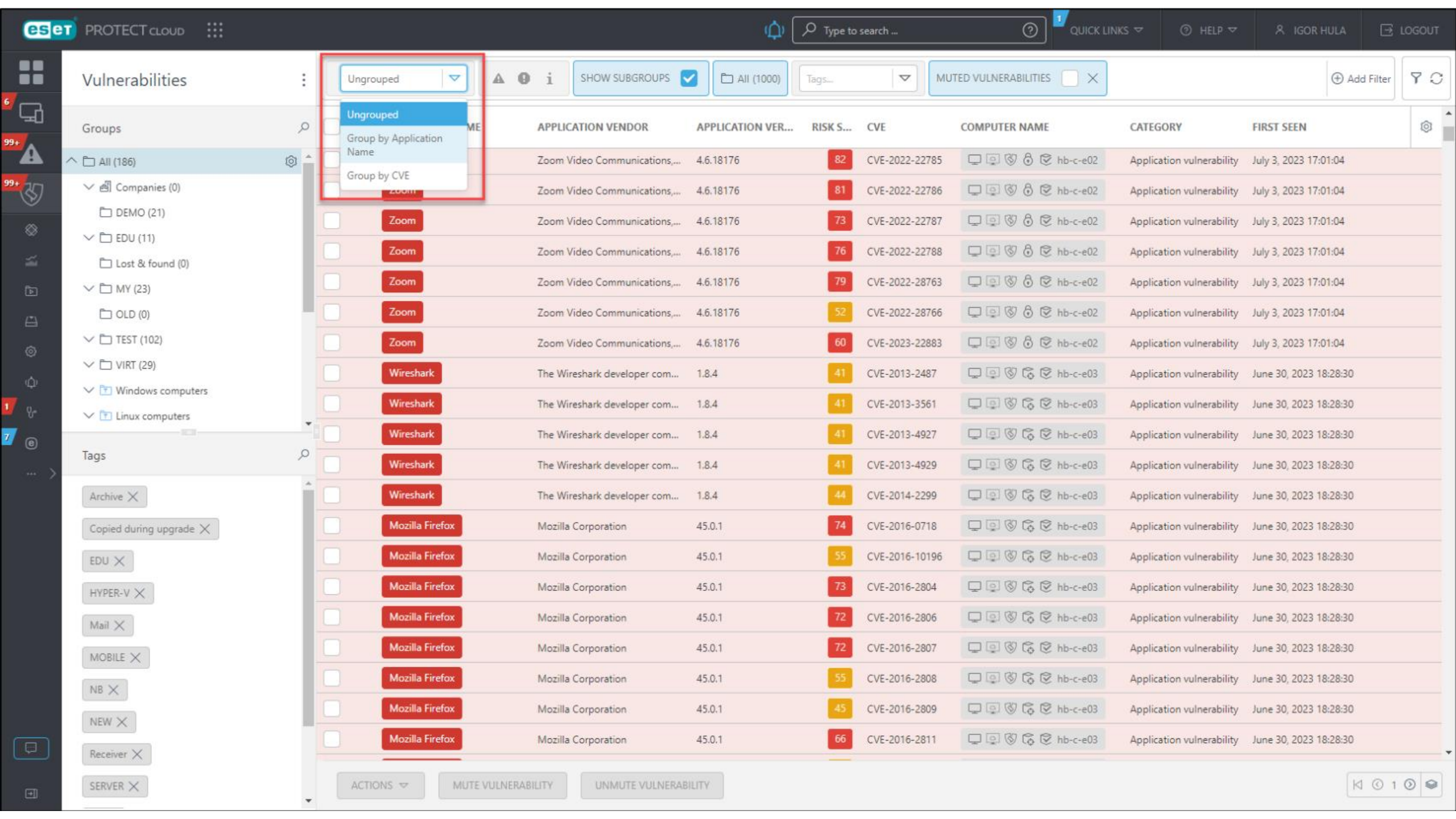

ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
Vulnerabilities
Groups
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
Windows computers
Linux computers
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
MOBILE
NB
NEW
Receiver
SERVER
T1
TEST-EEI
VIRT
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
APPLICATION NAME
APPLICATION VENDOR
APPLICATION VER...
RISK SCORE
CVE
COMPUTER NAME
CATEGORY
FIRST SEEN
Zoom Zoom Video Communications,... 4.6.18176 82 CVE-2022-22785 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 81 CVE-2022-22786 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 73 CVE-2022-22787 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 76 CVE-2022-22788 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 79 CVE-2022-28763 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 52 CVE-2022-28766 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 60 CVE-2023-22883 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 30 CVE-2022-28764 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-2487 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-3561 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-4927 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-4929 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 44 CVE-2014-2299 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 74 CVE-2016-0718 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 55 CVE-2016-10196 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 73 CVE-2016-2804 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 72 CVE-2016-2806 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 72 CVE-2016-2807 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 55 CVE-2016-2808 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 45 CVE-2016-2809 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 66 CVE-2016-2811 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 55 CVE-2016-2812 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 66 CVE-2016-2814 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 66 CVE-2016-2815 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
ACTIONS
MUTE VULNERABILITY
UNMUTE VULNERABILITY
1

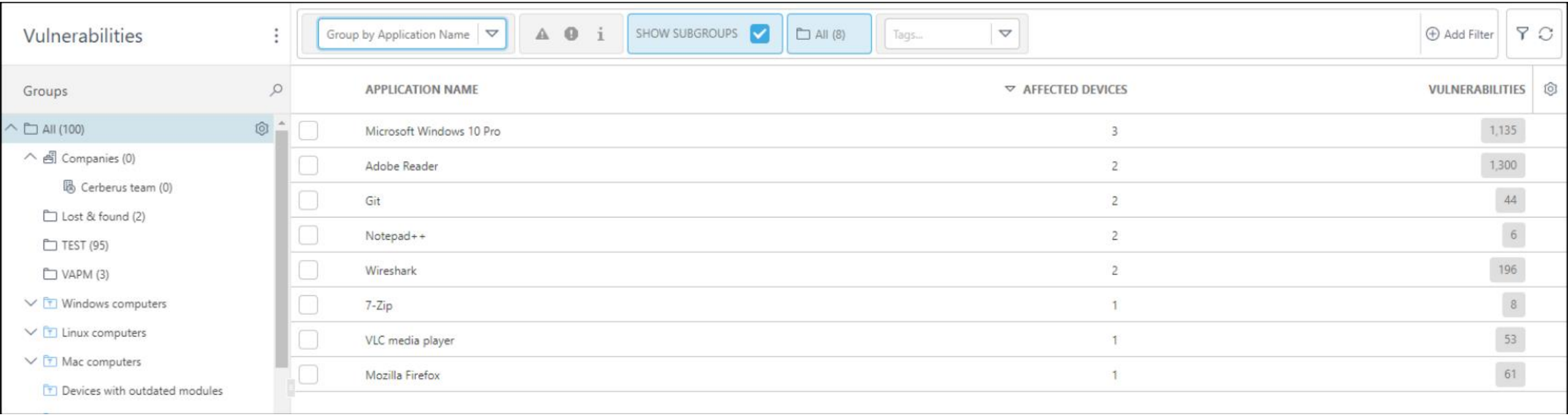

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
Windows computers
Linux computers
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
MOBILE
NB
NEW
Receiver
SERVER
T1
APPLICATION NAME
APPLICATION VENDOR
APPLICATION VER...
RIS...
CVE
COMPUTER NAME
Zoom
Zoom Video Communications,...
4.6.18176
CVE...
hb-c-e02
Wireshark
The Wireshark developer com...
1.8.4
hb-c-e03
Mozilla Firefox
Mozilla Corporation
45.0.1
ACTIONS
MUTE VULNERABILITY
UNMUTE VULNERABILITY
Zoom 4.6.18176
Risk Score
Application Name
Zoom
Application Vendor
Zoom Video Communications, Inc.
Category
Application vulnerability
CVE
CVE-2022-28766
First Seen
July 3, 2023 17:01:04
Details
Description
Windows 32-bit versions of the Zoom Client for Meetings before 5.12.6 and Zoom Rooms for Conference Room before version 5.12.6 are susceptible to a DLL injection vulnerability. A local low-privileged user could exploit this vulnerability to run arbitrary code in the context of the Zoom client.
Published
8 months ago - November 18, 2022 00:15:00
Last Modified
7 months ago - November 22, 2022 17:14:00
CWE
CWE-427
References
https://explore.zoom.us/en/trust/security/security-bulletin/
CVSS v3
Vector String
CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
Base Score
7.3
Impact Score
5.9
Exploitability Score
1.3

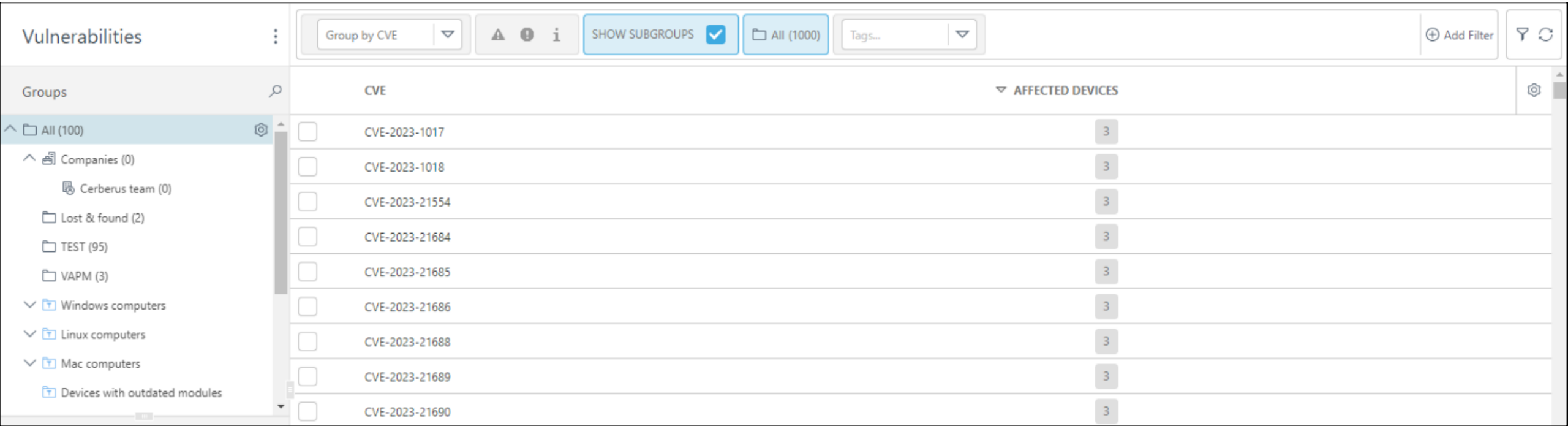

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
Windows computers
Linux computers
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
MOBILE
NB
NEW
Receiver
SERVER
CATEGORY
FIRST SEEN
Application vulnerability
July 3, 2023 17:01:04
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
CVE-2016-2809
hb-c-e03
ACTIONS
MUTE VULNERABILITY
UNMUTE VULNERABILITY
1
2
Select the columns to display in the table
AVAILABLE COLUMNS
Computer Description
Computer Tags
Muted
DISPLAYED COLUMNS
Application Name
Application Vendor
Application Version
Risk Score
CVE
Computer Name
Category
First Seen
ADD ALL
REMOVE ALL
RESET
3
OK
CANCEL

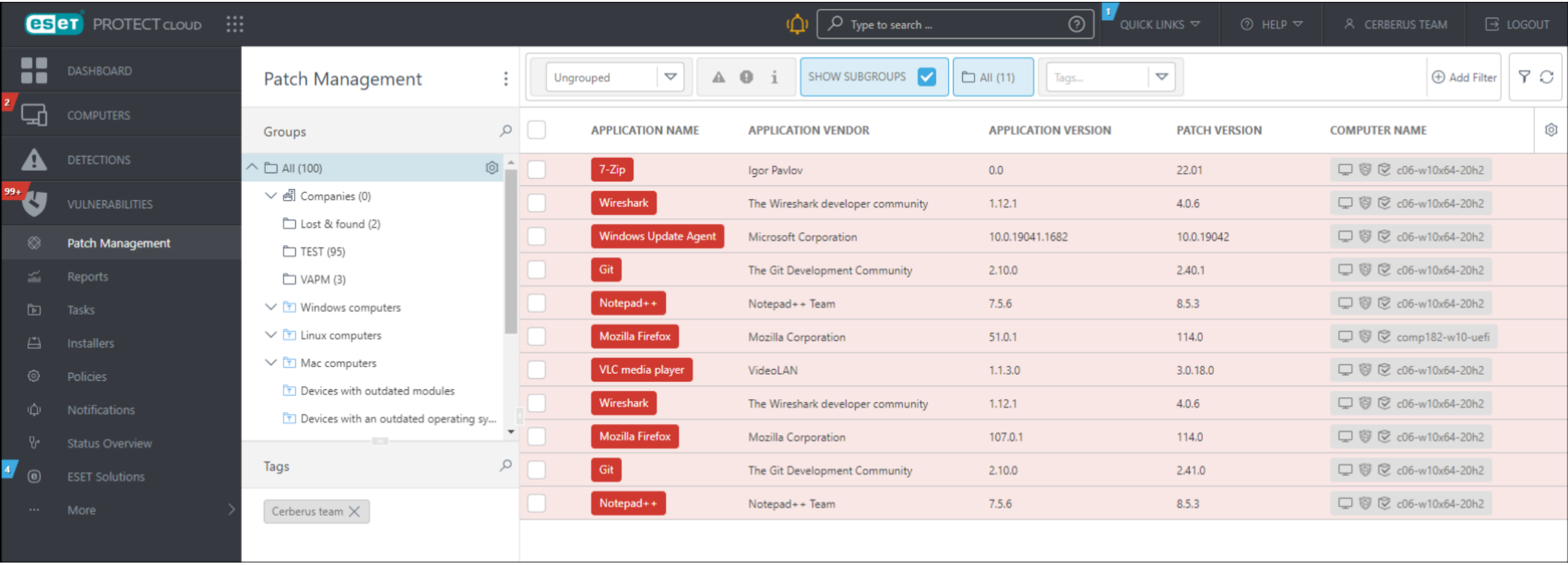

Vulnerabilities
Ungrouped
SHOW SUBGROUPS
VAPM (1000)
Tags...
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
VAPM (1000)
Tags...
Groups
All (98)
Companies (0)
Cerberus team (0)
Lost & found (2)
TEST (95)
VAPM (1)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Devices with an outdated operating sy...
Problematic devices
APPLICATION NAME
MUTED
APPLICATION VENDOR
APPLICATION VERS...
RISK SCORE
CVE
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
51
CVE-2023-29325
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
54
CVE-2023-29324
Git
The Git Development Comm...
2.10.0
60
CVE-2023-29007
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
58
CVE-2023-28302
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
42
CVE-2023-28298
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
67
CVE-2023-28297
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
60
CVE-2023-28293
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
66
CVE-2023-28283
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
33
CVE-2023-28276
Microsoft Windows 10 Pro
Microsoft Corporation
20H2 (10.0.19042.1706)
67
CVE-2023-28275

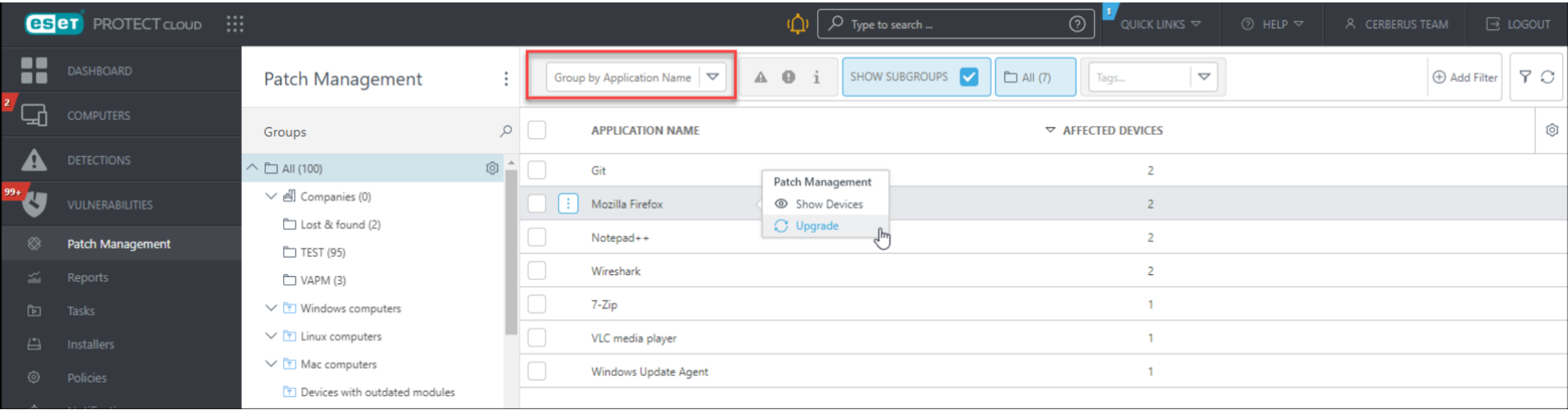

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
MUTED VULNERABILITIES
Add Filter
Groups
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
Windows computers
Linux computers
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
MOBILE
NB
NEW
Receiver
SERVER
APPLICATION NAME
APPLICATION VENDOR
APPLICATION VER...
RISK S...
CVE
COMPUTER NAME
CATEGORY
FIRST SEEN
Zoom
Zoom Video Communications,...
4.6.18176
82
CVE-2022-22785
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
81
CVE-2022-22786
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
73
CVE-2022-22787
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
76
CVE-2022-22788
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
79
CVE-2022-28763
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
52
CVE-2022-28766
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Zoom
Zoom Video Communications,...
4.6.18176
60
CVE-2023-22883
hb-c-e02
Application vulnerability
July 3, 2023 17:01:04
Wireshark
The Wireshark developer com...
1.8.4
41
CVE-2013-2487
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Wireshark
The Wireshark developer com...
1.8.4
41
CVE-2013-3561
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Wireshark
The Wireshark developer com...
1.8.4
41
CVE-2013-4927
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Wireshark
The Wireshark developer com...
1.8.4
41
CVE-2013-4929
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Wireshark
The Wireshark developer com...
1.8.4
44
CVE-2014-2299
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
74
CVE-2016-0718
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
55
CVE-2016-10196
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
73
CVE-2016-2804
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
72
CVE-2016-2806
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
72
CVE-2016-2807
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
55
CVE-2016-2808
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
45
CVE-2016-2809
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
Mozilla Firefox
Mozilla Corporation
45.0.1
66
CVE-2016-2811
hb-c-e03
Application vulnerability
June 30, 2023 18:28:30
ACTIONS
MUTE VULNERABILITY
UNMUTE VULNERABILITY
1


PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
IGOR HULA
LOGOUT
Vulnerabilities
Ungrouped
Group by Application Name
Group by CVE
SHOW SUBGROUPS
All (1000)
Tags...
MUTED VULNERABILITIES
Add Filter
Groups
All (186)
Companies (0)
DEMO (21)
EDU (11)
Lost & found (0)
MY (23)
OLD (0)
TEST (102)
VIRT (29)
Windows computers
Linux computers
Tags
Archive
Copied during upgrade
EDU
HYPER-V
Mail
MOBILE
NB
NEW
Receiver
SERVER
APPLICATION VENDOR
APPLICATION VER...
RISK S...
CVE
COMPUTER NAME
CATEGORY
FIRST SEEN
Zoom Video Communications,... 4.6.18176 82 CVE-2022-22785 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Video Communications,... 4.6.18176 81 CVE-2022-22786 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 73 CVE-2022-22787 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 76 CVE-2022-22788 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 79 CVE-2022-28763 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 52 CVE-2022-28766 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Zoom Zoom Video Communications,... 4.6.18176 60 CVE-2023-22883 hb-c-e02 Application vulnerability July 3, 2023 17:01:04
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-2487 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-3561 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-4927 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 41 CVE-2013-4929 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Wireshark The Wireshark developer com... 1.8.4 44 CVE-2014-2299 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 74 CVE-2016-0718 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 55 CVE-2016-10196 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 73 CVE-2016-2804 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 72 CVE-2016-2806 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 72 CVE-2016-2807 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 55 CVE-2016-2808 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 45 CVE-2016-2809 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
Mozilla Firefox Mozilla Corporation 45.0.1 66 CVE-2016-2811 hb-c-e03 Application vulnerability June 30, 2023 18:28:30
ACTIONS
MUTE VULNERABILITY
UNMUTE VULNERABILITY
1


Vulnerabilities
Group by Application Name
SHOW SUBGROUPS
All (8)
Tags...
Add Filter
Groups
All (100)
Companies (0)
Cerberus team (0)
Lost & found (2)
TEST (95)
VAPM (3)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
APPLICATION NAME
AFFECTED DEVICES
VULNERABILITIES
Microsoft Windows 10 Pro 3 1,135
Adobe Reader 2 1,300
Git 2 44
Notepad++ 2 6
Wireshark 2 196
7-Zip 1 8
VLC media player 1 53
Mozilla Firefox 1 61


Vulnerabilities
Group by CVE
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (100)
Companies (0)
Cerberus team (0)
Lost & found (2)
TEST (95)
VAPM (3)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
CVE
AFFECTED DEVICES
CVE-2023-1017 3
CVE-2023-1018 3
CVE-2023-21554 3
CVE-2023-21684 3
CVE-2023-21685 3
CVE-2023-21686 3
CVE-2023-21688 3
CVE-2023-21689 3
CVE-2023-21690 3


ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
CERBERUS TEAM
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Patch Management
Ungrouped
SHOW SUBGROUPS
All (11)
Tags...
Add Filter
Groups
All (100)
Companies (0)
Lost & found (2)
TEST (95)
VAPM (3)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Devices with an outdated operating sy...
Tags
Cerberus team
APPLICATION NAME
APPLICATION VENDOR
APPLICATION VERSION
PATCH VERSION
COMPUTER NAME
7-Zip
Igor Pavlov
0.0
22.01
c06-w10x64-20h2
Wireshark
The Wireshark developer community
1.12.1
4.0.6
c06-w10x64-20h2
Windows Update Agent
Microsoft Corporation
10.0.19041.1682
10.0.19042
c06-w10x64-20h2
Git
The Git Development Community
2.10.0
2.40.1
c06-w10x64-20h2
Notepad++
Notepad++ Team
7.5.6
8.5.3
c06-w10x64-20h2
Mozilla Firefox
Mozilla Corporation
51.0.1
114.0
comp182-w10-uefi
VLC media player
VideoLAN
1.1.3.0
3.0.18.0
c06-w10x64-20h2
Wireshark
The Wireshark developer community
1.12.1
4.0.6
c06-w10x64-20h2
Mozilla Firefox
Mozilla Corporation
107.0.1
114.0
c06-w10x64-20h2
Git
The Git Development Community
2.10.0
2.41.0
c06-w10x64-20h2
Notepad++
Notepad++ Team
7.5.6
8.5.3
c06-w10x64-20h2

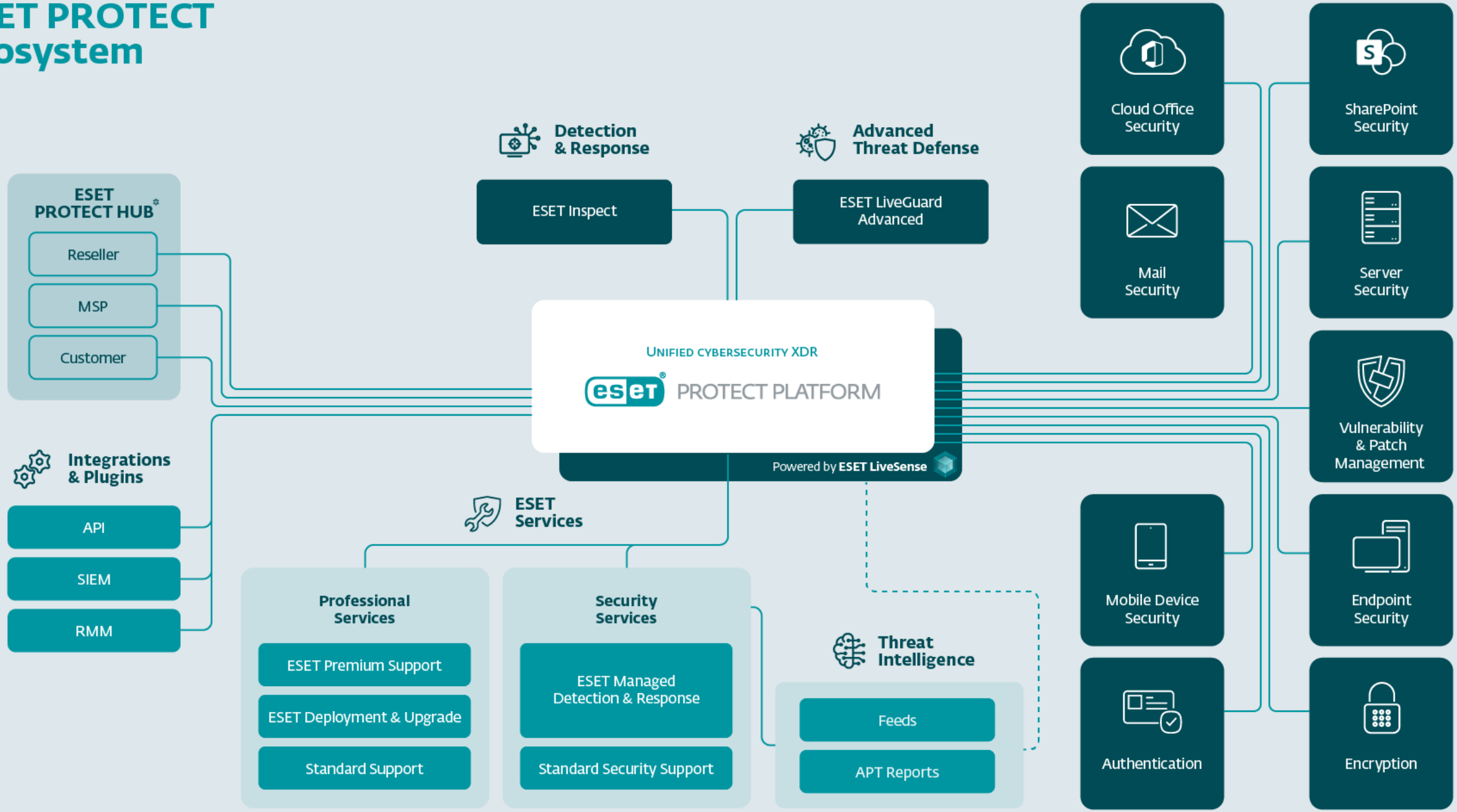

ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
CERBERUS TEAM
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Patch Management
Group by Application Name
SHOW SUBGROUPS
All (7)
Tags...
Add Filter
Groups
All (100)
Companies (0)
Lost & found (2)
TEST (95)
VAPM (3)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
APPLICATION NAME
AFFECTED DEVICES
Git 2
Mozilla Firefox 2
Notepad++ 2
Wireshark 2
7-Zip 1
VLC media player 1
Windows Update Agent 1
Patch Management
Show Devices
Upgrade

PROTECT ELITE

Viss vienā novēršana, noteikšana un reaģēšana, kas apvieno uzņēmuma līmeņa XDR ar pilnīgu daudzslāņu aizsardzību

Pārvaldības konsole	ESET PROTECT
Moderna darbstaciju aizsardzība	ESET Endpoint Security
Serveru aizsardzība	ESET Server Security
Mākoņ-smilškaste	ESET LiveGuard Advanced
Diska šifrēšana	ESET Full Disk Encryption
E-pastu drošība	ESET Mail Security
Mākoņprogrammu aizsardzība	ESET Cloud Office Security
Ievainojamību un atjauninājumu pārvaldība	ESET Vulnerability & Patch Management
EDR/XDR	ESET Inspect
Multifaktoru autentifikācija	ESET Secure Authentication

ESET PROTECT Ecosystem



* Coming H2/2023

Paldies

Egils Rupenheits

ESET Digital Security
Progress. Protected.

Technology can change the world.
Protecting technology is our world.

Digital Security
Progress. Protected.