ENJOY SAFER TECHNOLOGY™

Een niet zo’n coole presentatie over cybersecurity.

Dave Maasland
Managing Director
ESET Nederland

Dave@eset.nl

CRUNCH NETWORK

Why Breach Detection Is Your New Must-Have, Cyber Security Tool

BANEN

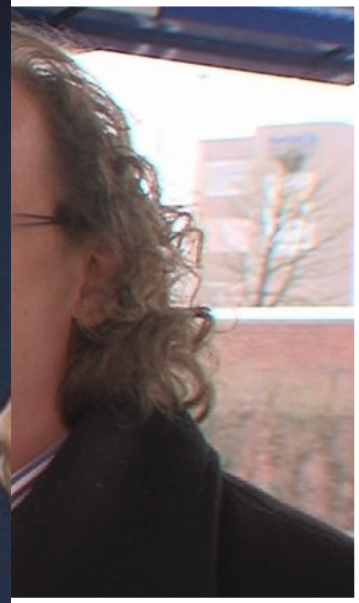
Nieuws | Cultuur & Leven

Economie

Cursisten leren bij PwC hoe zij om moeten gaan met een
te loodsen. © Raymond Rutting/de Volkskrant

Bedrijven zijn zo le

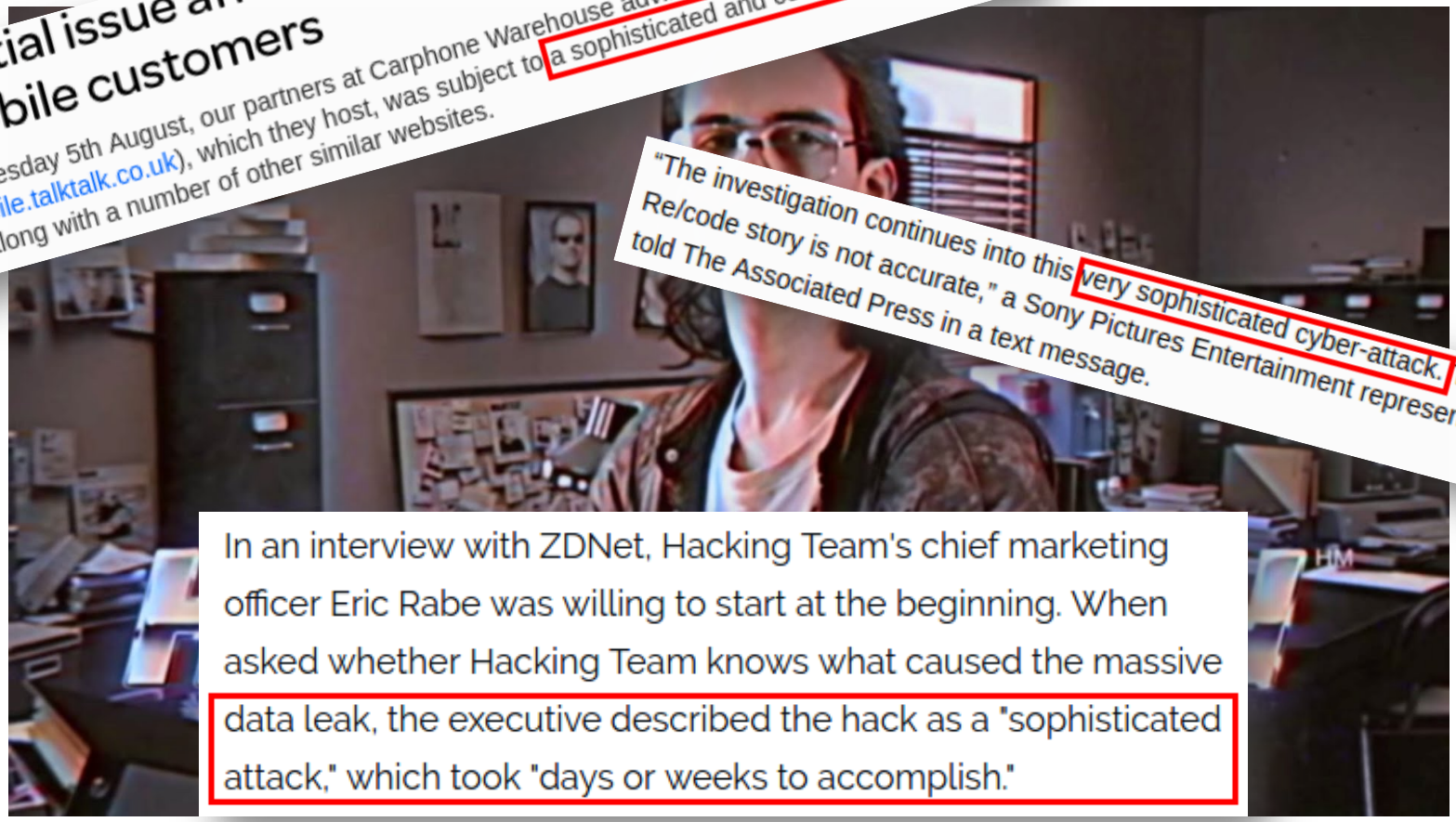
n pakken, lukt



De w derd

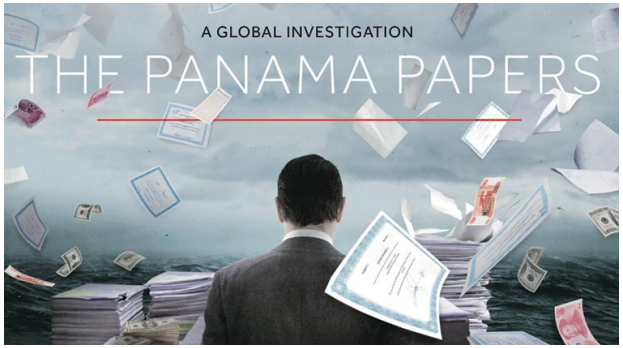
Potential issue affecting the personal information of mobile customers

On Wednesday 5th August, our partners at Carphone Warehouse advised us that our mobile sales site (mobile.talktalk.co.uk), which they host, was subject to a sophisticated and co-ordinated cyber attack, along with a number of other similar websites.



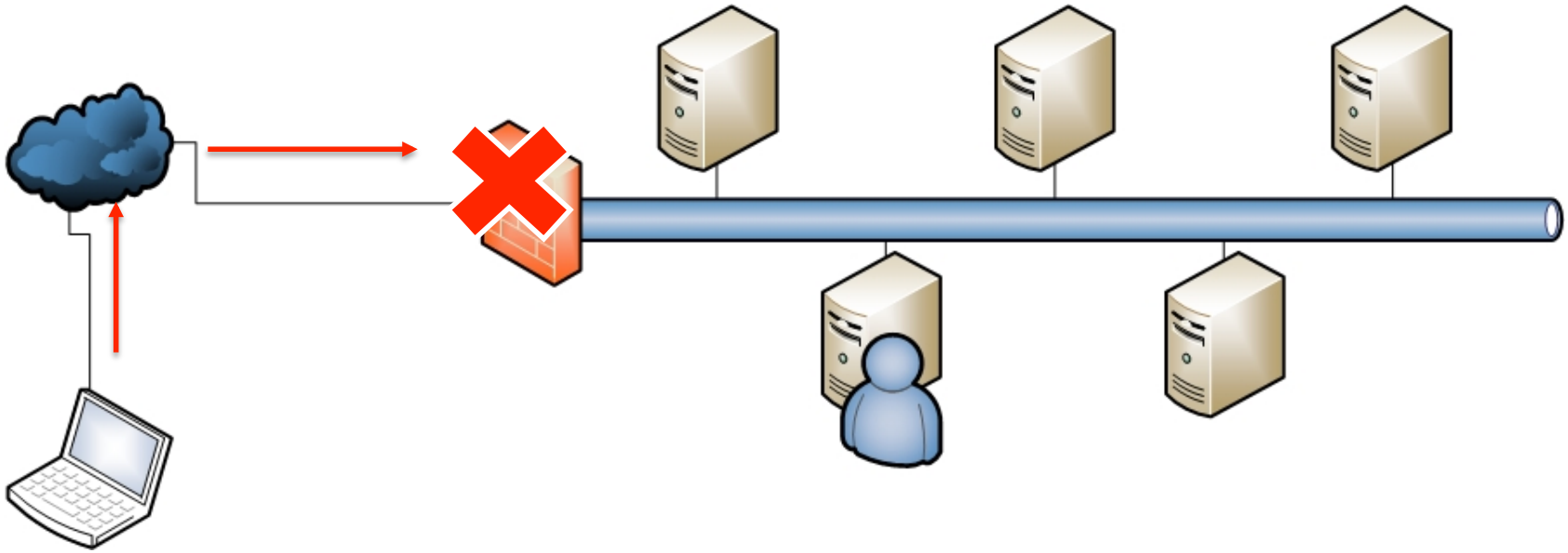
"The investigation continues into this very sophisticated cyber-attack. The Re/code story is not accurate," a Sony Pictures Entertainment representative told The Associated Press in a text message.

In an interview with ZDNet, Hacking Team's chief marketing officer Eric Rabe was willing to start at the beginning. When asked whether Hacking Team knows what caused the massive data leak, the executive described the hack as a "sophisticated attack," which took "days or weeks to accomplish."

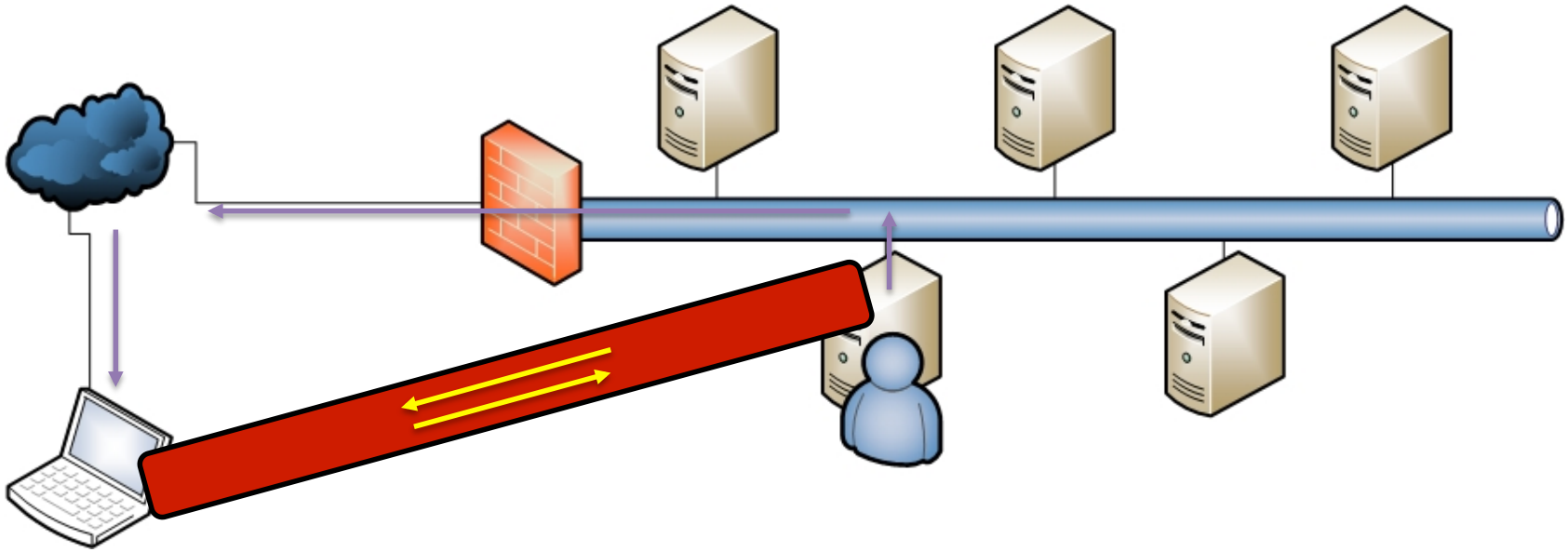


The hackers from Impact Team told Motherboard: *"We worked hard to make fully undetectable attack, then got in and found nothing to bypass….Nobody was watching. No security. Only thing was segmented network. You could use Pass1234 from the internet to VPN to root on all servers."*

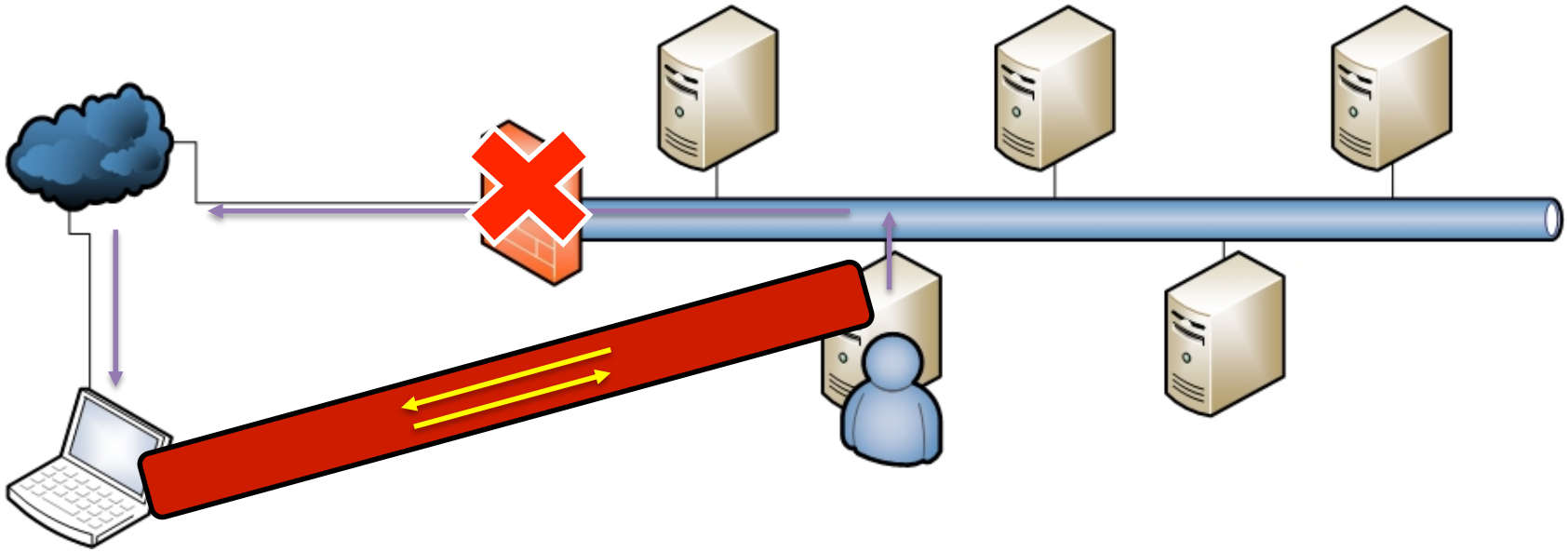
De super-geavanceerde-cyber-aanval:



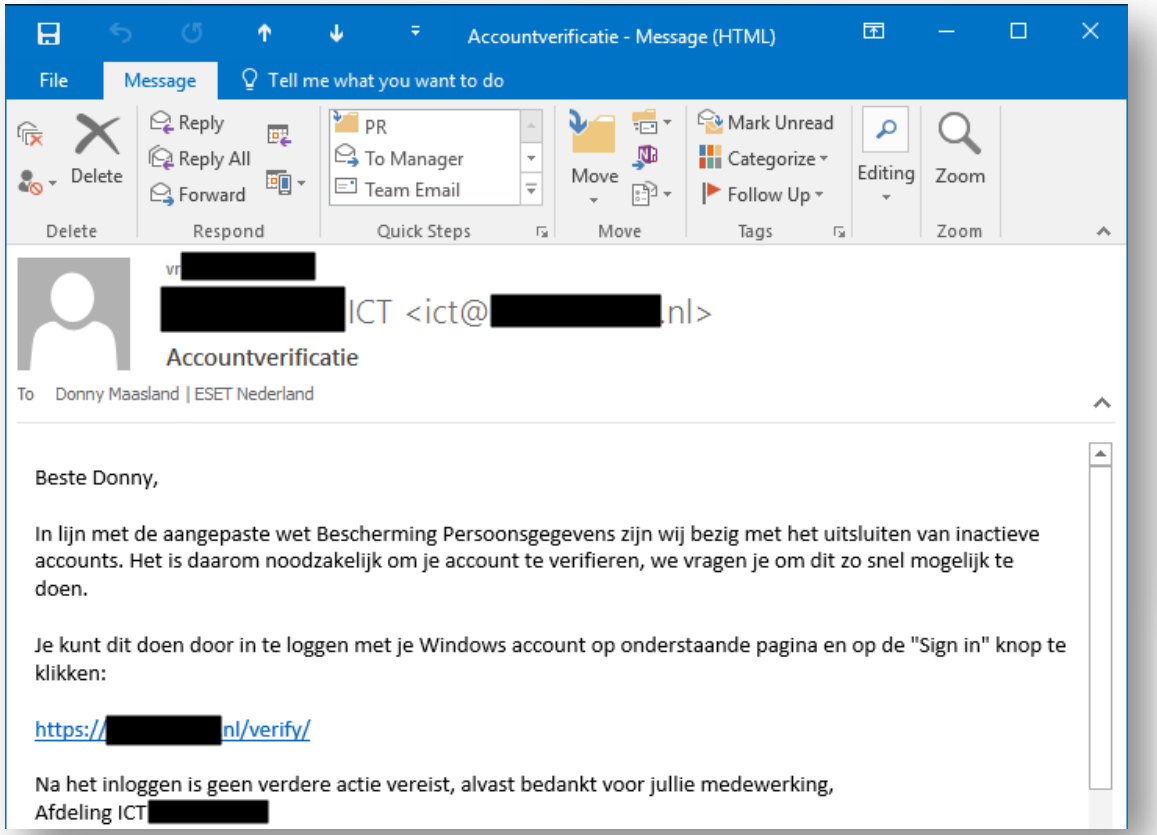
De super-geavanceerde-cyber-aanval:

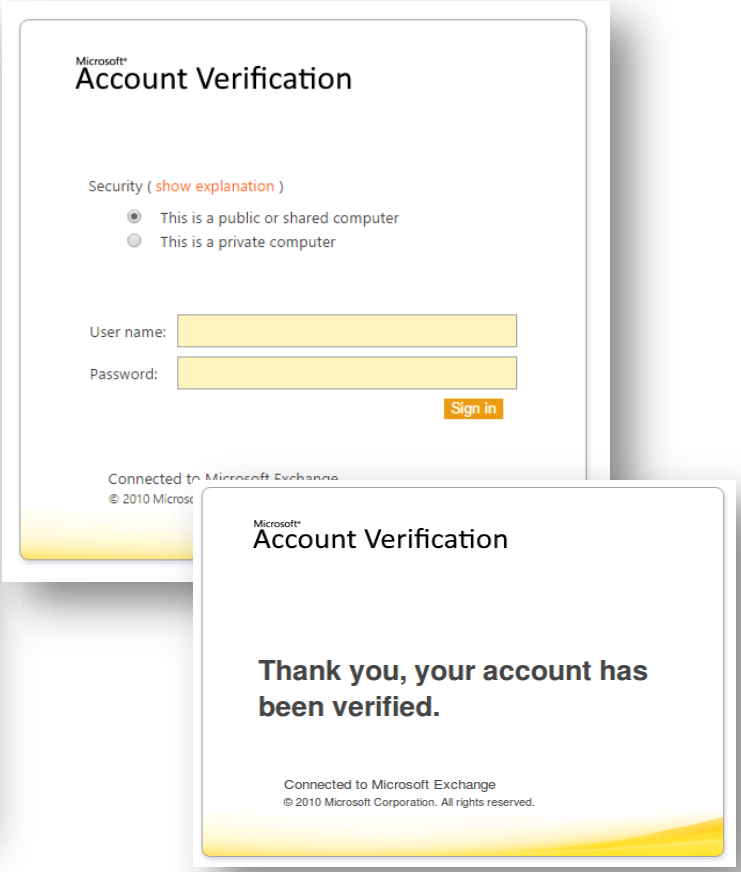


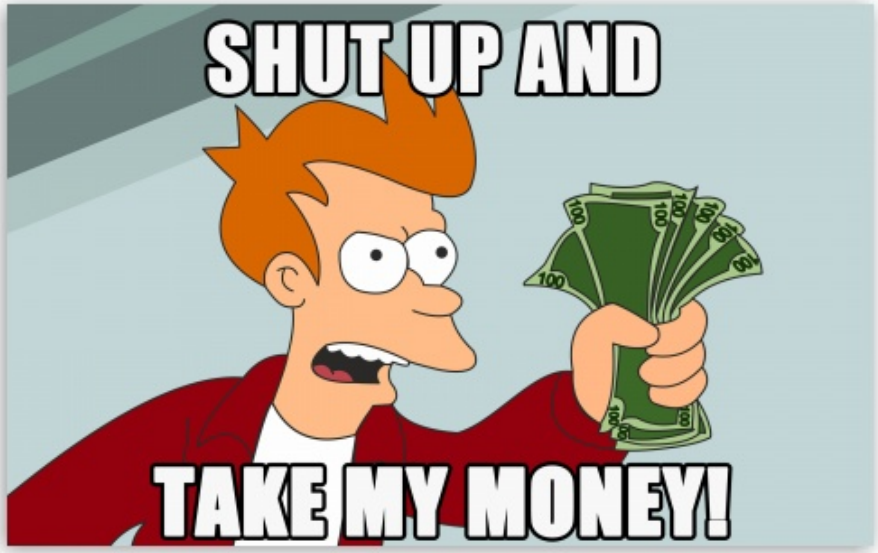
Het internet is magisch:



De super-geavanceerde-cyber-aanval:






SHUT UP AND
TAKE MY MONEY!

The cool kids table

It works:

PREVENTIE

WAT WETEN WE OVER DATALEKKEN:

1. IN 69% VAN ALLE GEVALLEN WORDT MALWARE GEBRUIKT.
2. IN 80% VAN ALLE GEVALLEN WORDT HACKING* GEBRUIKT.

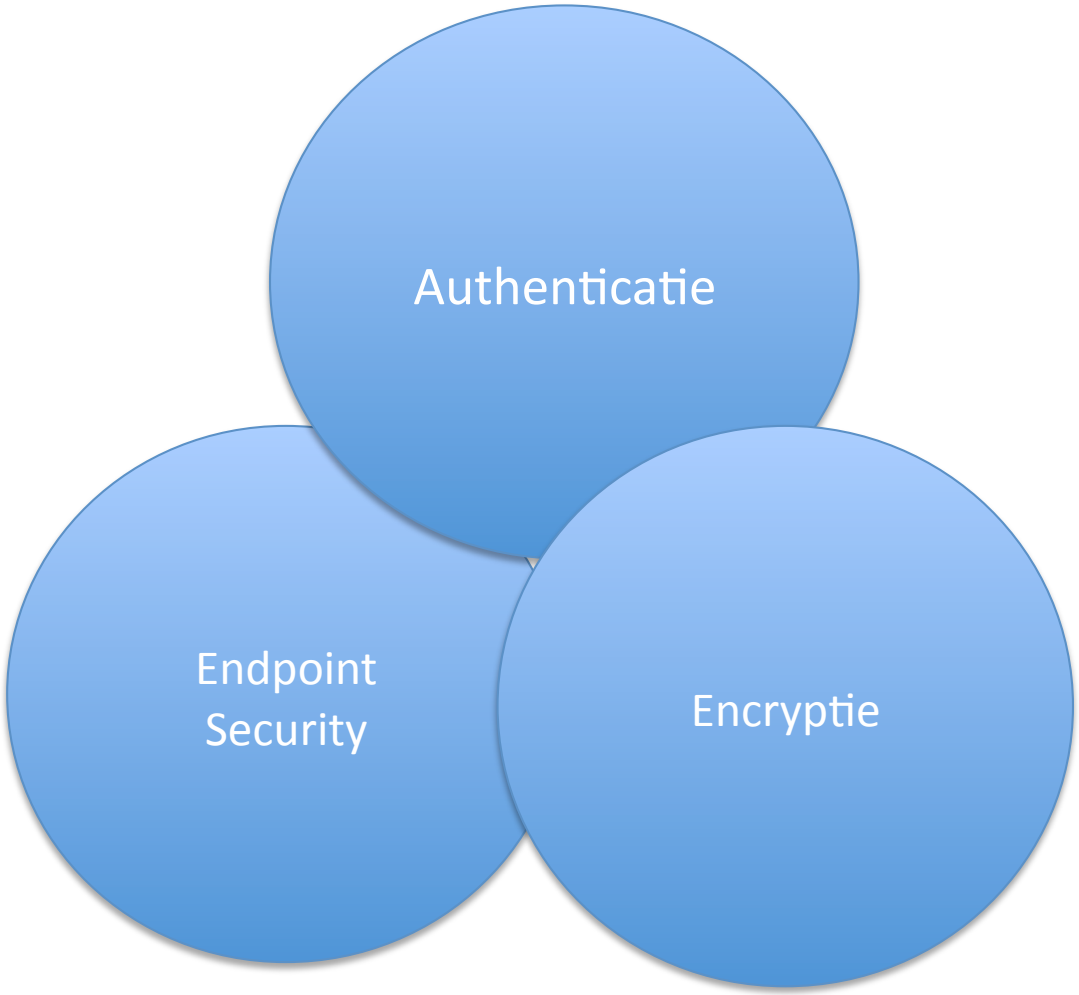
(MALWARE EN HACKING SAMEN IN 61% VAN DE GEVALLEN)

3. IN 97% VAN ALLE GEVALLEN VEROUDERDER SOFTWARE, NON-HARDENED INSTELLINGEN EN ZWAKKE WACHTWOORDEN.

In 80% van alle hacks zijn paswoorden: default, niet aanwezig, gestolen, geraden of kraakbaar.

Ponemon breach report 2015

Focus:

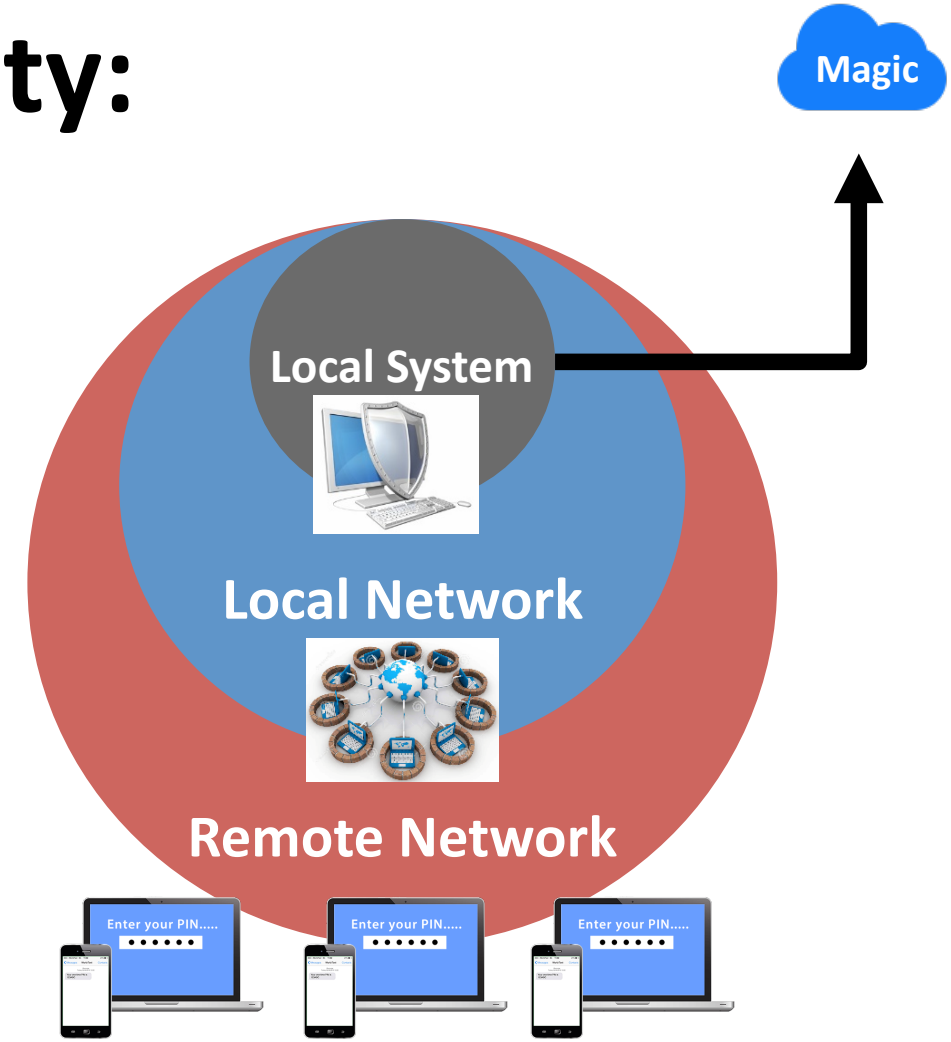


Gelaagde Security:

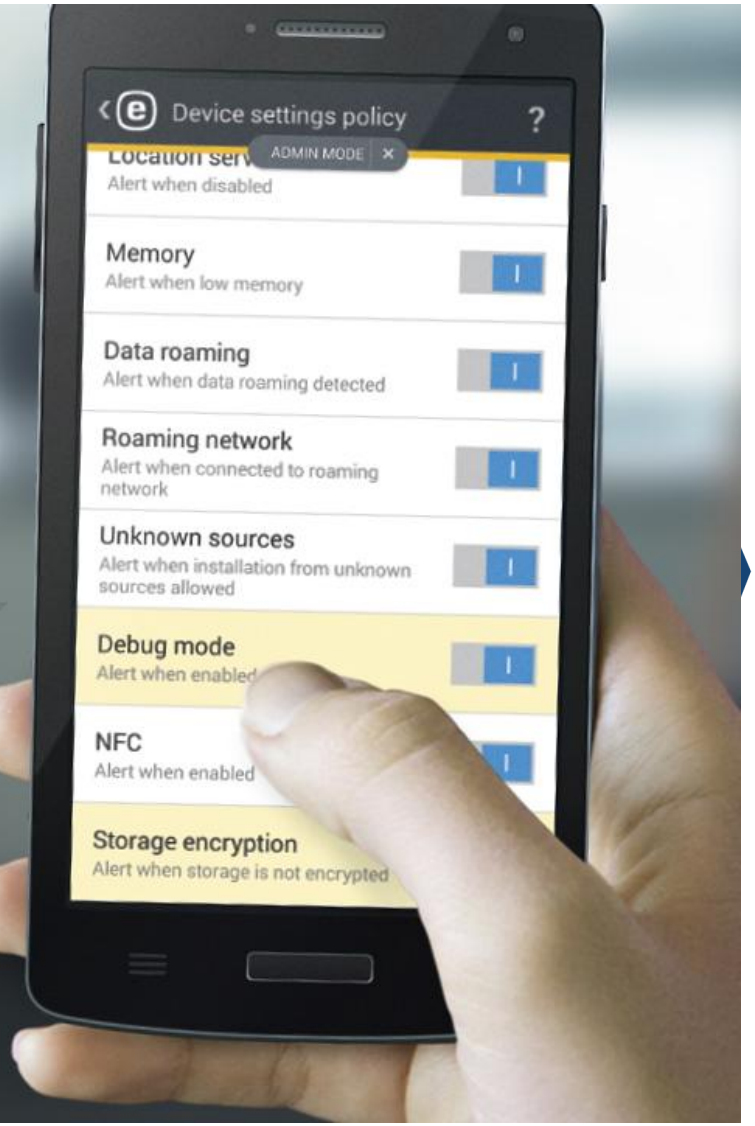
- Endpoint Security
- Mobile Security
- Encryptie

- DLP
- Server Security

- Authenticatie
- Patch Management



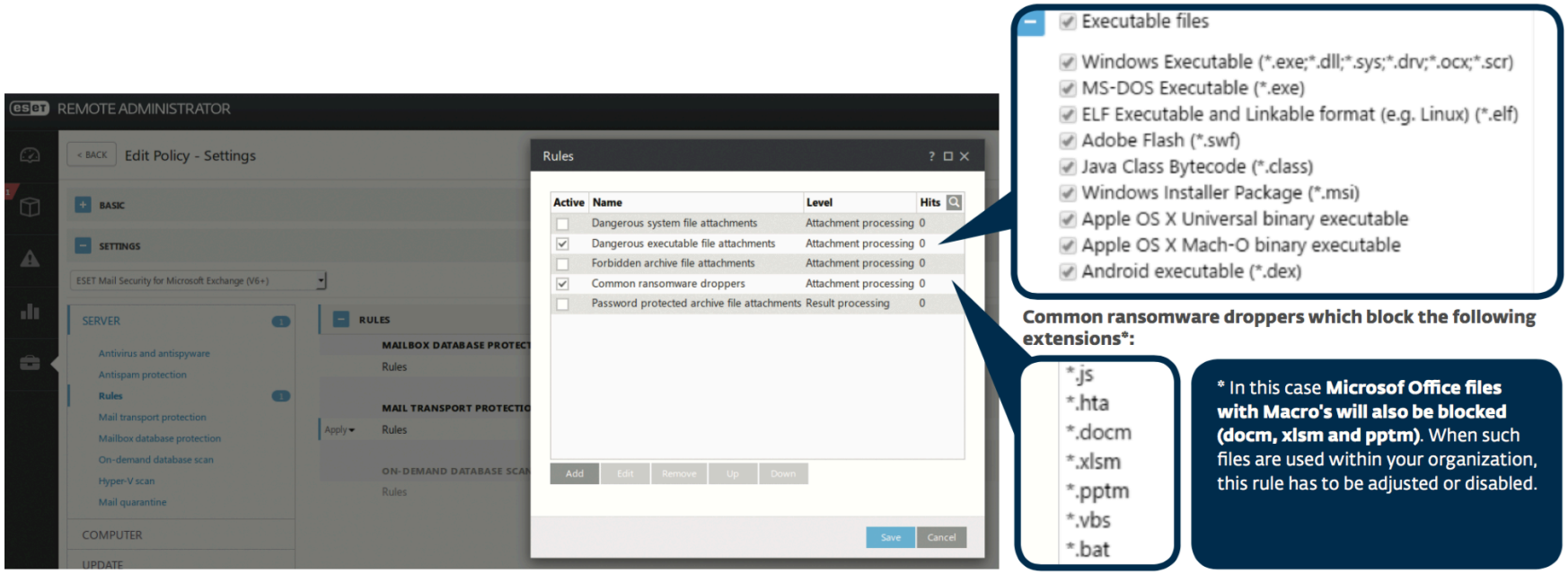
MONITOR PRE-DEFINED DEVICE SETTINGS FOR COMPLIANCY



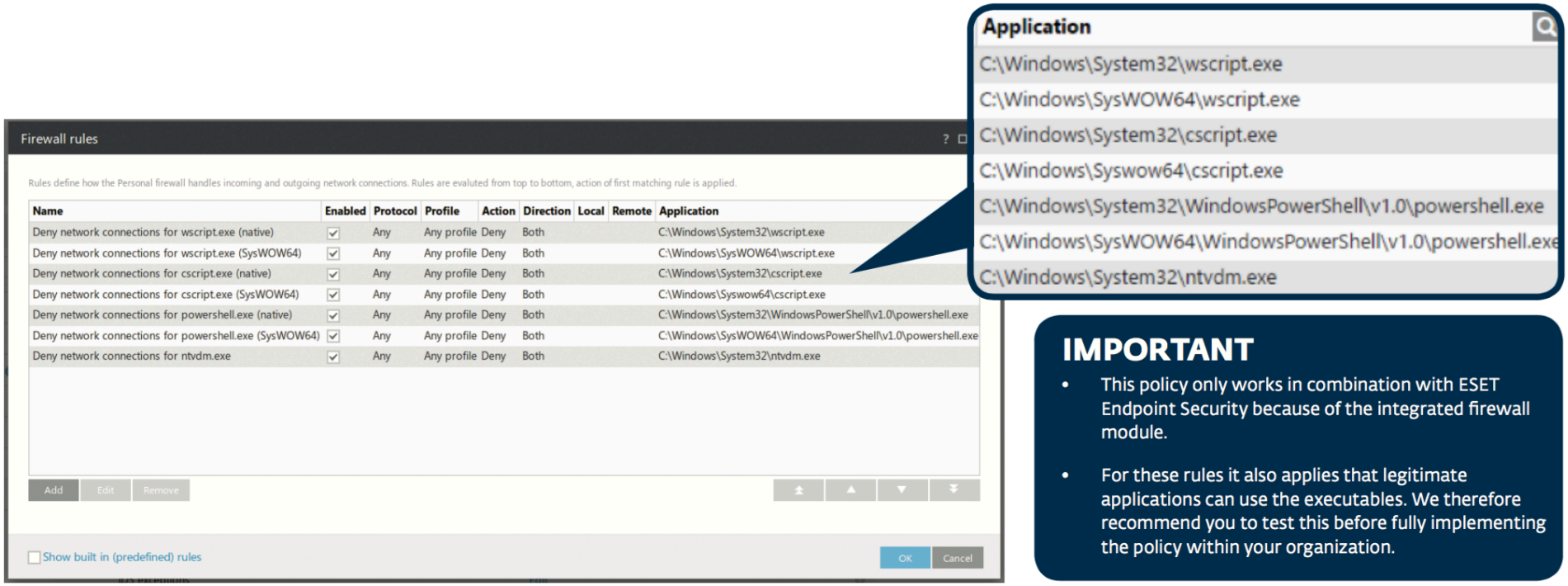
ENDPOINT SECURITY
FOR ANDROID

ENJOY SAFER TECHNOLOGY™

Antispam:


REMOTE ADMINISTRATOR
< BACK
Edit Policy - Settings
BASIC
SETTINGS
ESET Mail Security for Microsoft Exchange (V6+)
SERVER
Antivirus and antispyware
Antispam protection
Rules
Mail transport protection
Mailbox database protection
On-demand database scan
Hyper-V scan
Mail quarantine
COMPUTER
UPDATE
RULES
MAILBOX DATABASE PROTECT
Rules
MAIL TRANSPORT PROTECTIO
Rules
ON-DEMAND DATABASE SCAN
Rules
Apply
Rules
Active
Name
Level
Hits
Dangerous system file attachments
Attachment processing
0
Dangerous executable file attachments
Attachment processing
0
Forbidden archive file attachments
Attachment processing
0
Common ransomware droppers
Attachment processing
0
Password protected archive file attachments
Result processing
0
Add
Edit
Remove
Up
Down
Save
Cancel
Executable files
Windows Executable (*.exe;*.dll;*.sys;*.drv;*.ocx;*.scr)
MS-DOS Executable (*.exe)
ELF Executable and Linkable format (e.g. Linux) (*.elf)
Adobe Flash (*.swf)
Java Class Bytecode (*.class)
Windows Installer Package (*.msi)
Apple OS X Universal binary executable
Apple OS X Mach-O binary executable
Android executable (*.dex)
Common ransomware droppers which block the following extensions*:
*.js
*.hta
*.docm
*.xlsm
*.pptm
*.vbs
*.bat
* In this case Microsof Office files with Macro's will also be blocked (docm, xlsm and pptm). When such files are used within your organization, this rule has to be adjusted or disabled.

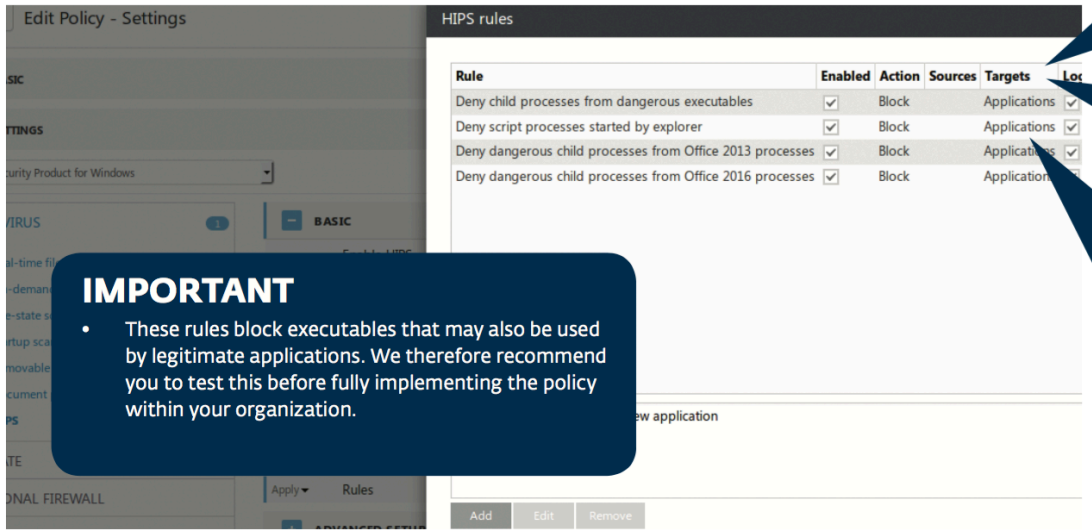
Firewall:



IMPORTANT

- This policy only works in combination with ESET Endpoint Security because of the integrated firewall module.
- For these rules it also applies that legitimate applications can use the executables. We therefore recommend you to test this before fully implementing the policy within your organization.

HIPS:



IMPORTANT

- These rules block executables that may also be used by legitimate applications. We therefore recommend you to test this before fully implementing the policy within your organization.

Deny child process from dangerous executables.

Application
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\Syswow64\cscript.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\ntvdm.exe

Deny script processes started by explorer

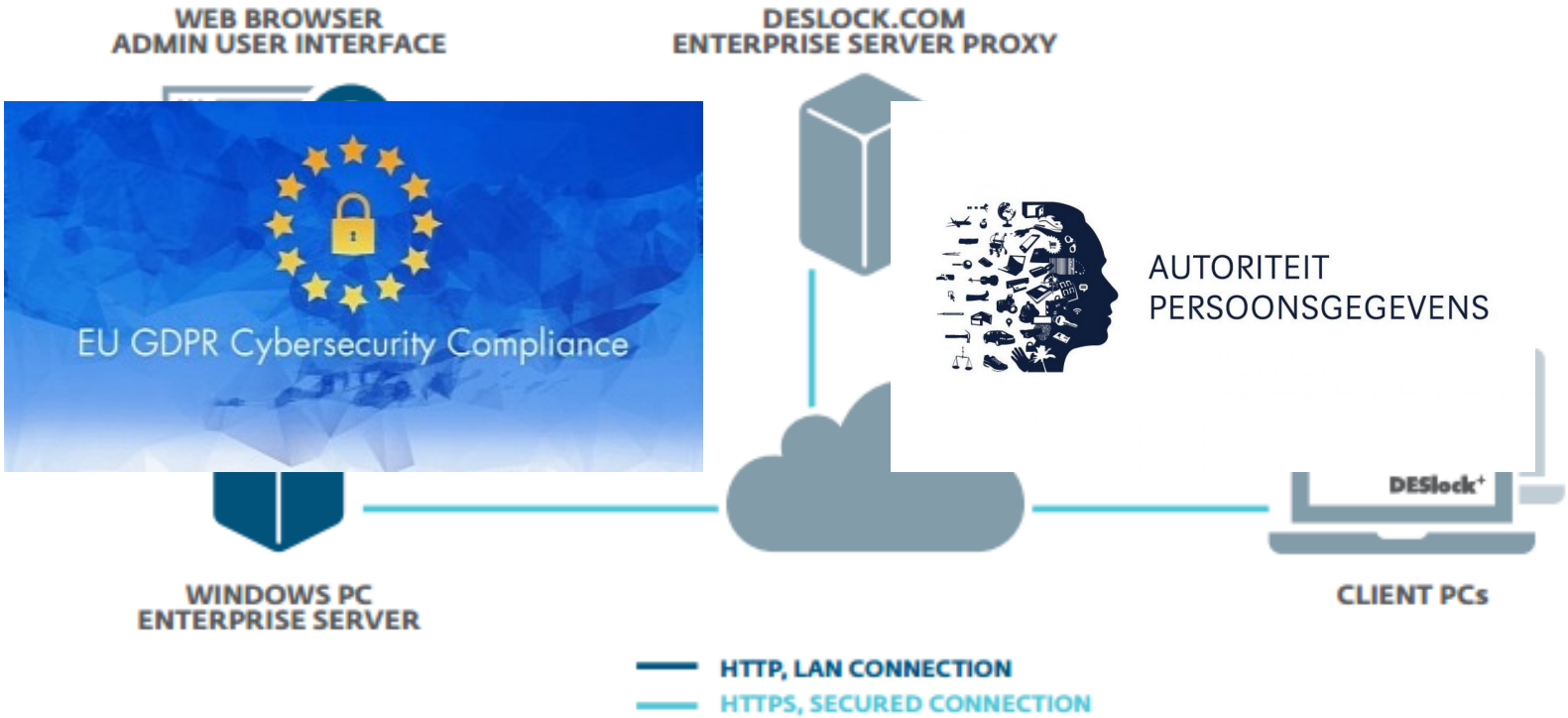
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe

Deny Dangerous child processes from Office 201x

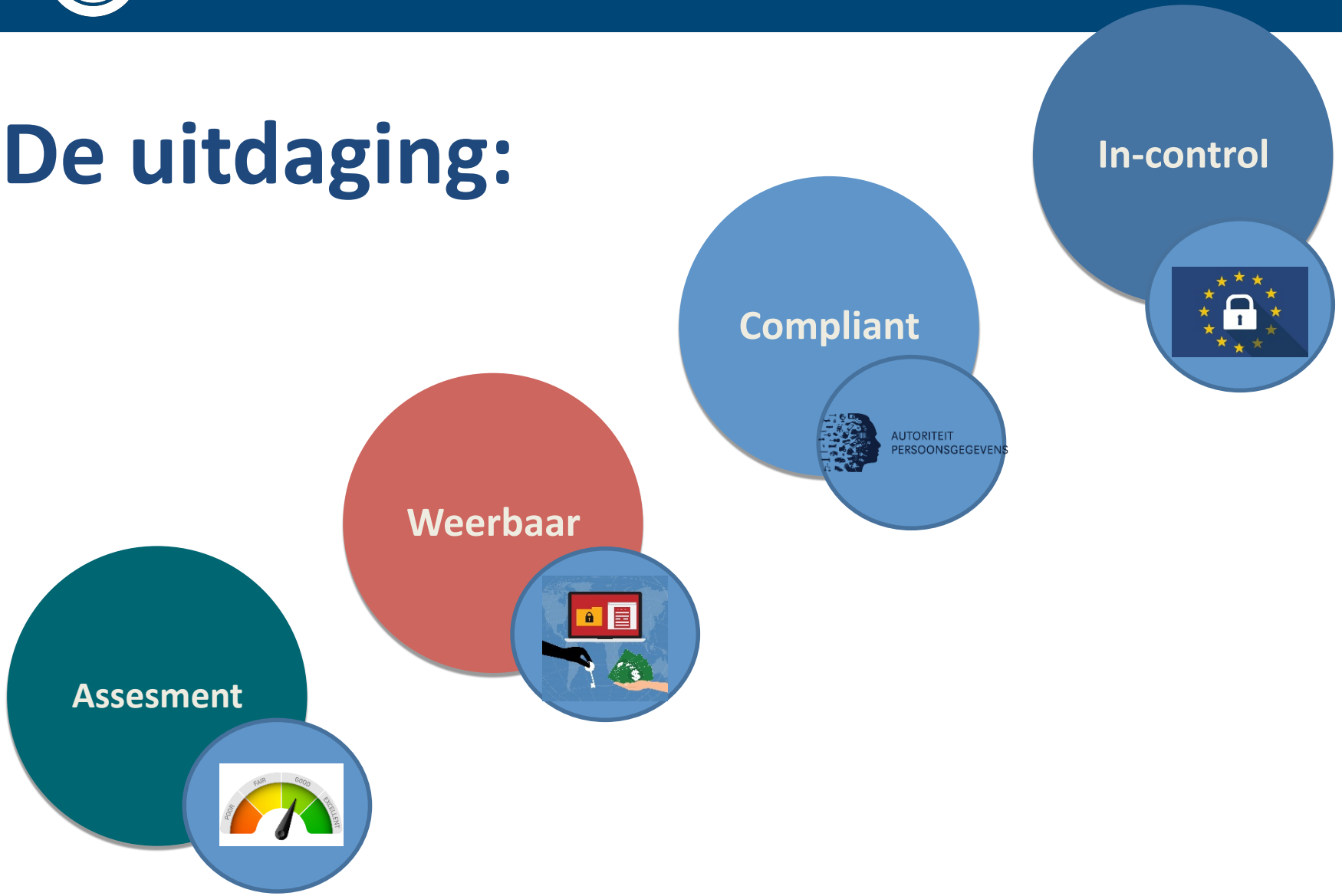
C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\ntvdm.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

2-Factor Authentication

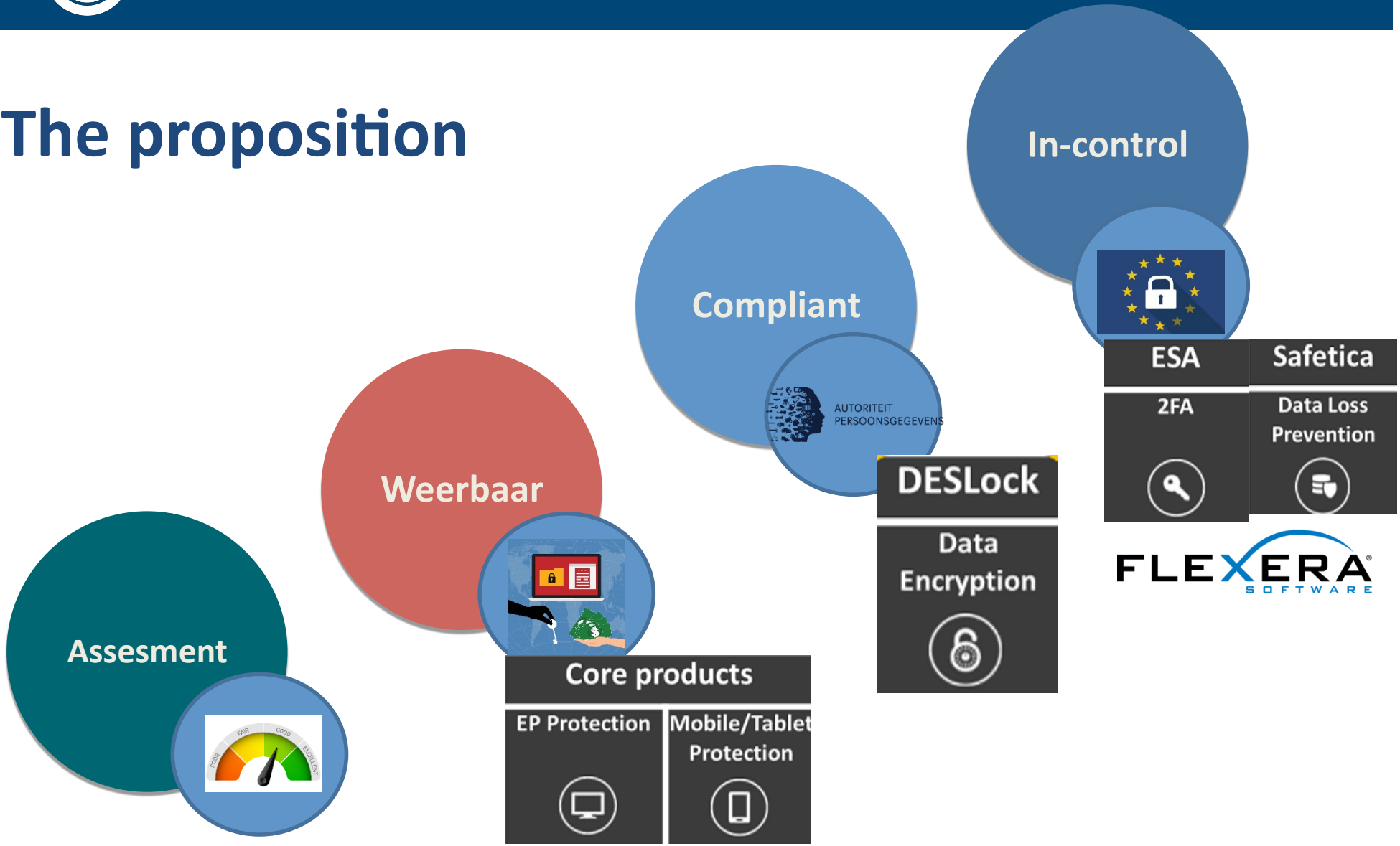
Encryption


WEB BROWSER
ADMIN USER INTERFACE
DESLOCK.COM
ENTERPRISE SERVER PROXY
EU GDPR Cybersecurity Compliance
AUTORITEIT
PERSOONSGEGEVENS
DESlock+
WINDOWS PC
ENTERPRISE SERVER
CLIENT PCs
HTTP, LAN CONNECTION
HTTPS, SECURED CONNECTION

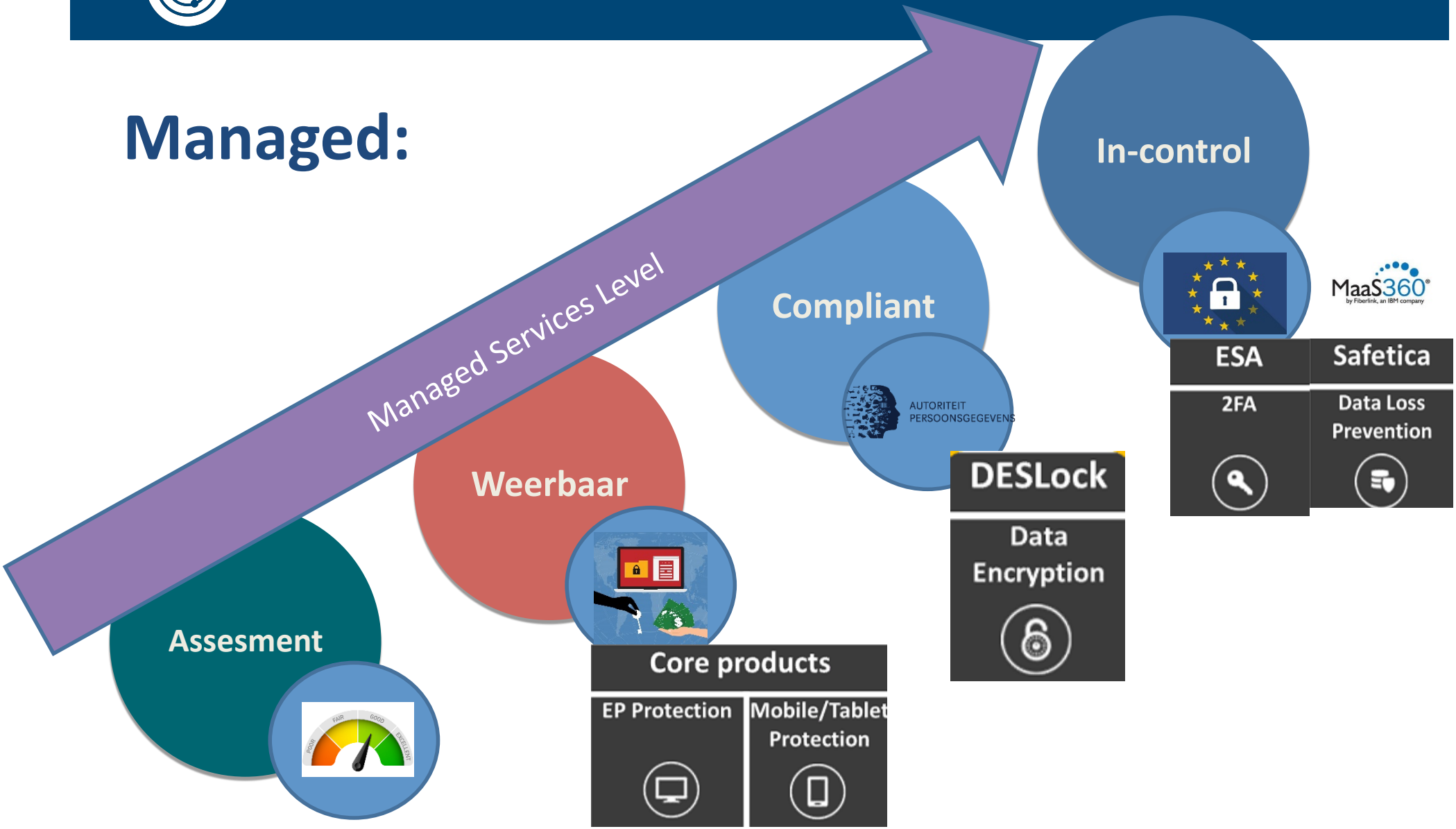
De uitdaging:



The proposition



Managed:


Managed Services Level
Assesment
Weerbaar
Compliant
In-control
Core products
EP Protection
Mobile/Tablet Protection
AUTORITEIT PERSOONSGEGEVENS
DESLock
Data Encryption
MaaS360
ESA
Safetica
2FA
Data Loss Prevention

ENJOY SAFER TECHNOLOGY™

Thank You

www.WeLiveSecurity.com
Dave@eset.nl