

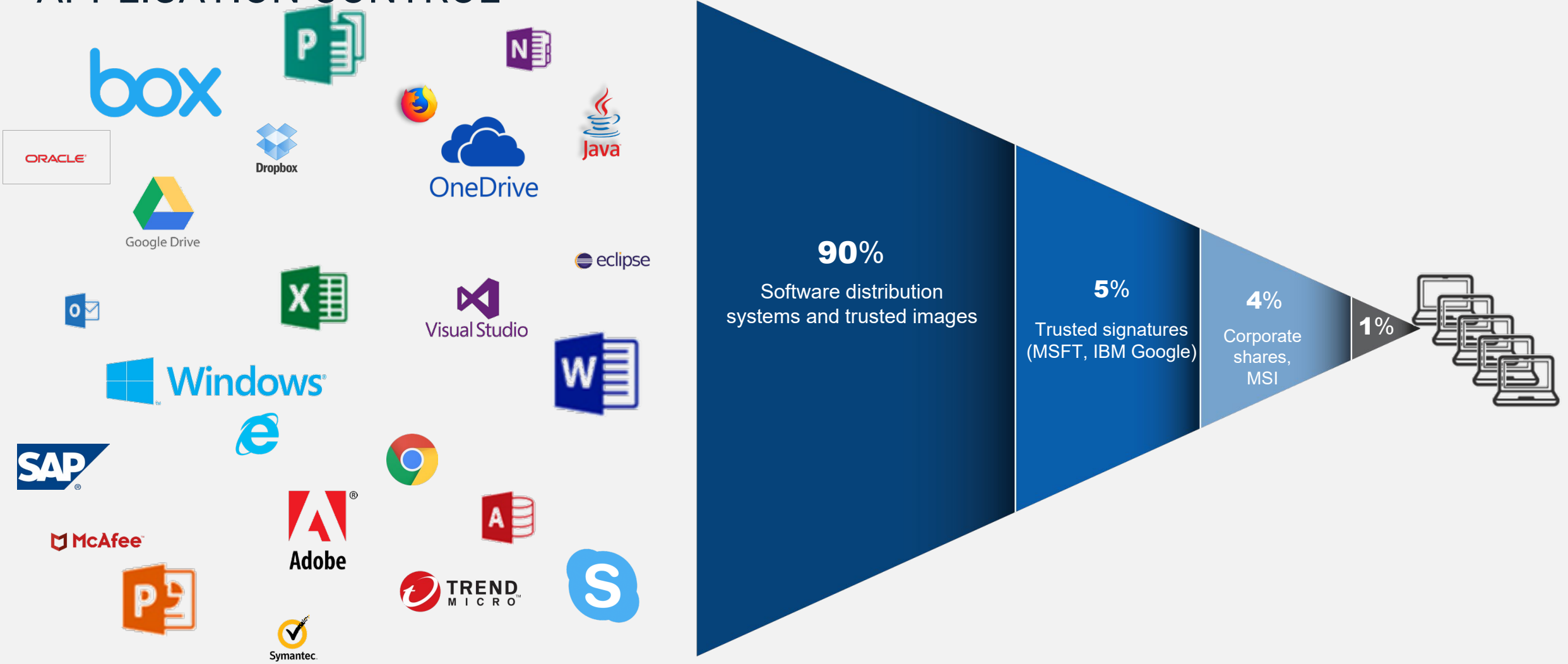


ATTACK + DEFEND

LAB 3 – TRUSTED PUBLISHERS

Setting up policies for Least Privilege

TRUSTED SOURCES REMOVES THE BARRIERS TO APPLICATION CONTROL



CyberArk automates policy creation for over 99% of application and system software

Detecting Internet Applications.

- Go back to Policies...Default Policies and set Control unhandled applications downloaded from the internet. To Detect. Click Edit policy settings.
- Under options, make sure all three check boxes are checked. Click save and confirm the policy changes.
- Refresh the EPM policy on the agent.

Detect privileged unhandled applications Off On

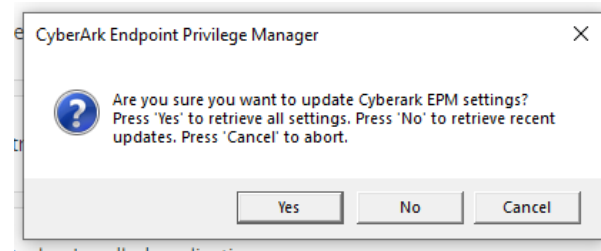
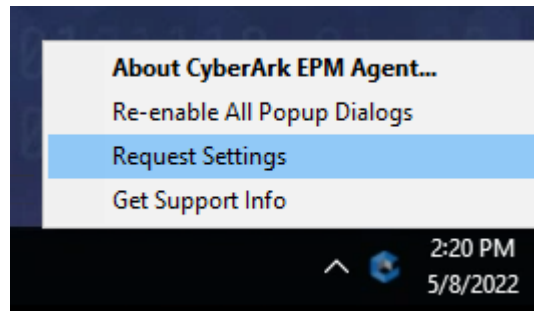
Protect against ransomware (Windows Only) Off Detect Restrict

Control unhandled applications downloaded from the internet (Windows Only) Off Detect Restrict Block Edit

Control unhandled applications Off Detect Restrict

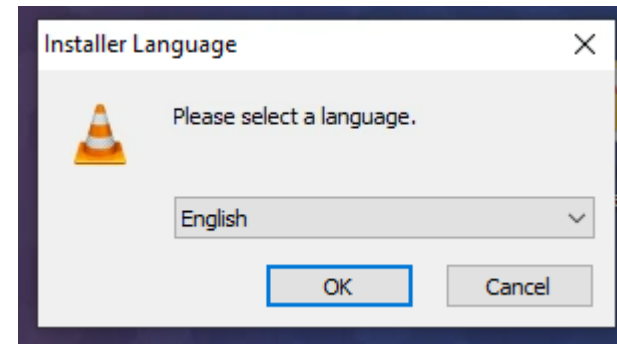
Options

- Detect installation of unhandled applications downloaded from the internet ⓘ
 - Detect launch of unhandled applications downloaded from the internet ⓘ
- Notify end users when an unhandled application is launched
- Off Preview
- Detect access to the sensitive resources by unhandled applications downloaded from the internet ⓘ
 - Internet
 - Intranet
 - Network shares
 - Memory of other processes



Executing Code

- From the 'Lab 3 – Trusted Publishers' folder, click the vlc-3.0.10-win64.exe shortcut and note how it is also runs. Immediately close the installer.
- From the 'Lab 3 – Trusted Publishers' folder, click the Download vlc-3.0.09-win64.exe shortcut
- Run vlc-3.0.09.exe and observe the result.



Configure trusted source policy

- Go to Events Management (beta)
- Find vlc-3.0.10-win64.exe
- Click ... and select Trust by publisher's signature. Click Yes to confirm.

Events Management (beta)

Updated at: 11:26 AM

Filters

Event

Find event by filename, checksum, publisher or threat protection policy

Event type: All Platform: All By administrator

1 of 1 results

May 09 Today

11:07:25 AM Block vlc-3.0.10-win64.exe Signed by VideoLAN

7 1 1

Trust by publisher's signature

- Apply recommendation (planned)
- Trust by publisher's signature
- Allow normal running and do not report
- Block and do not report
- Add to custom policy (planned)
- Create new custom policy (planned)
- Copy application details (planned)
- Delete event

Trust by publisher's signature?

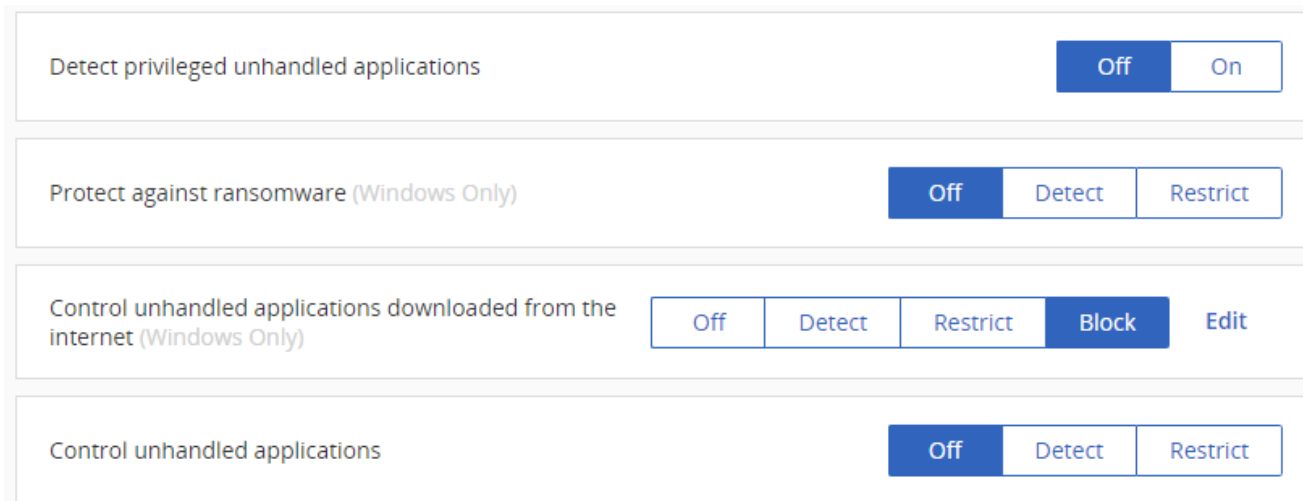
Add the "VideoLAN" signature to the "Trusted Sources" group of publishers for Windows.

Application files signed with this signature are elevated if necessary, including their child processes and applications installed by them.

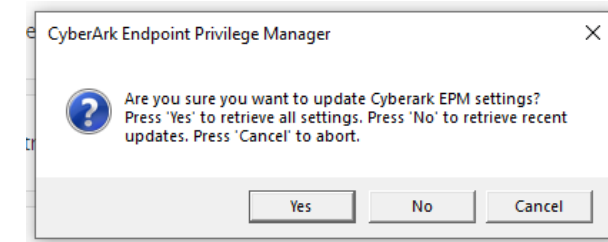
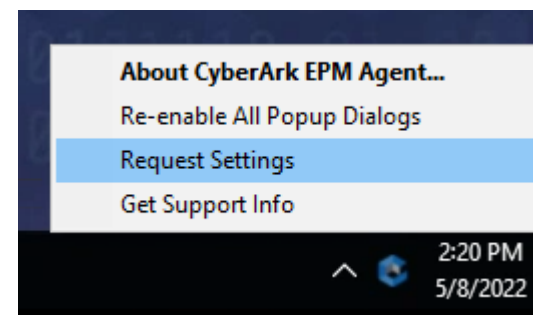
To edit this policy after it has been created, look for "VideoLAN" on the "Policies > Application Groups" pane.

Locking it down.

- Go back to Policies...Default Policies. Set 'Control unhandled applications downloaded from the internet' back to Block. Click Yes to confirm.



- Refresh EPM Agent Policy.



Executing 7zip Installer

- Navigate to 'Lab 4 – Trusted Sources'.
- Examine the two files and their properties.
- Run vlc-3.0.09-win64.exe and observe the result.
- Run vlc-3.0.10-win64.exe and observe the result.

