MC2MC

A practical guide to Application Control for business

Speakers

Kim Oppalfens

Founder, AppControl.AI

✉ Kim.oppalfens@oscc.be

@thewmiguy

Tom degreef

Founder, AppControl.AI

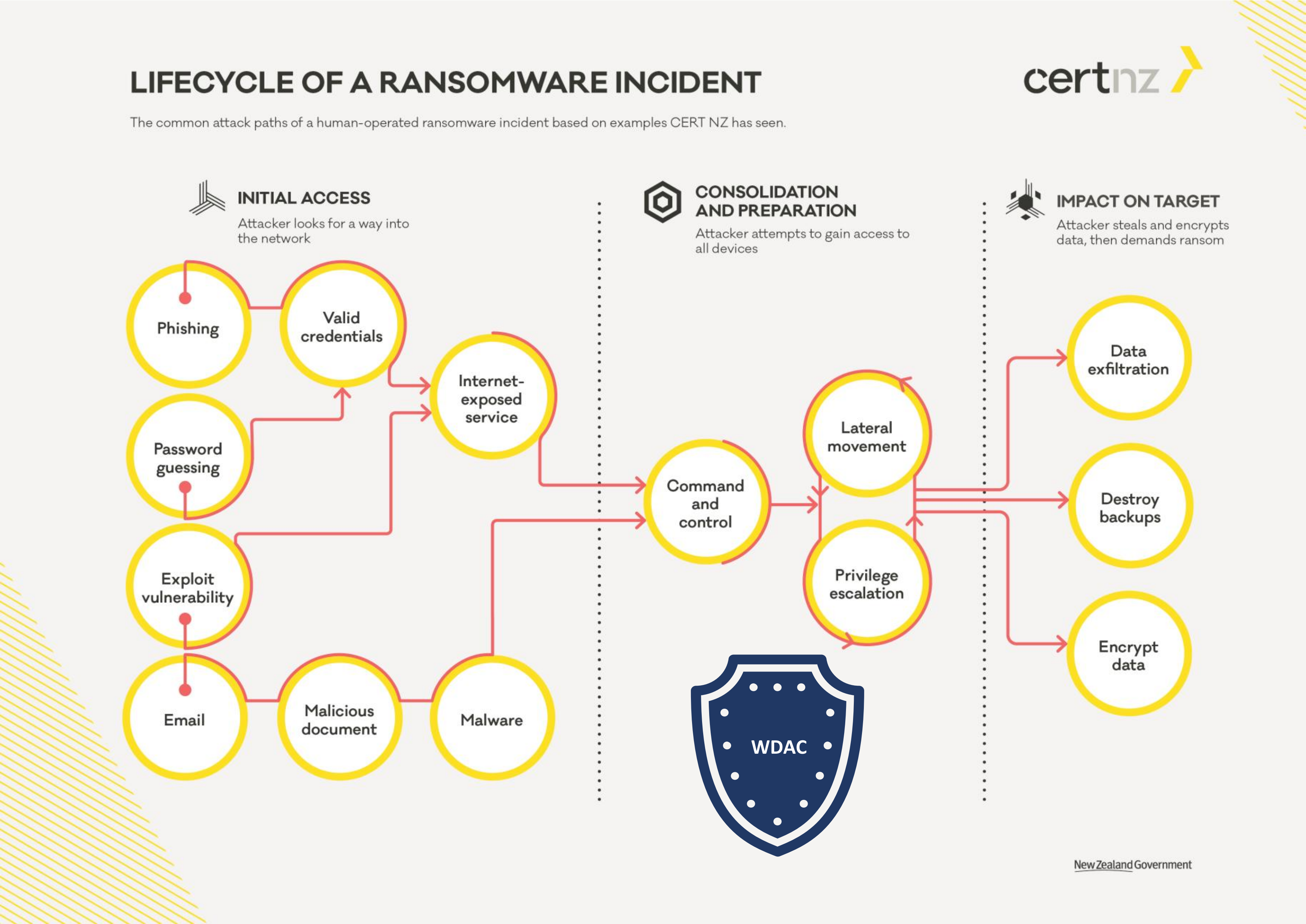
@tomdegreef

1-2-3; 2-3; 1-3; 2-3

Welcome

- Benefits
- The different starting Policies
- A word on Policy Types
- Intune as a Managed Installer & The ISG
- The path rules
- Handling Packaged Apps
- SecurityCatalogs
- AppControl.AI
- Training

Benefits


LIFECYCLE OF A RANSOMWARE INCIDENT
certnz
The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.
INITIAL ACCESS
Attacker looks for a way into the network
CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices
IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom
Phishing
Valid credentials
Password guessing
Internet-exposed service
Exploit vulnerability
Email
Malicious document
Malware
Command and control
Lateral movement
Privilege escalation
Data exfiltration
Destroy backups
Encrypt data
WDAC
New Zealand Government

The different starting policies

- Corporate Base policy
  - Supplemental Corporate signing policy
  - Supplemental Packaged apps also known as store apps policy
  - Optional: Supplemental Pathrule policy
  - Optional: Supplemental Publisher policy
  - Optional: Supplemental Self-updating app policies*
- Security catalogs for applications
- Recommended block rule Base policy

The Policy Options
Getting started edition

⚠

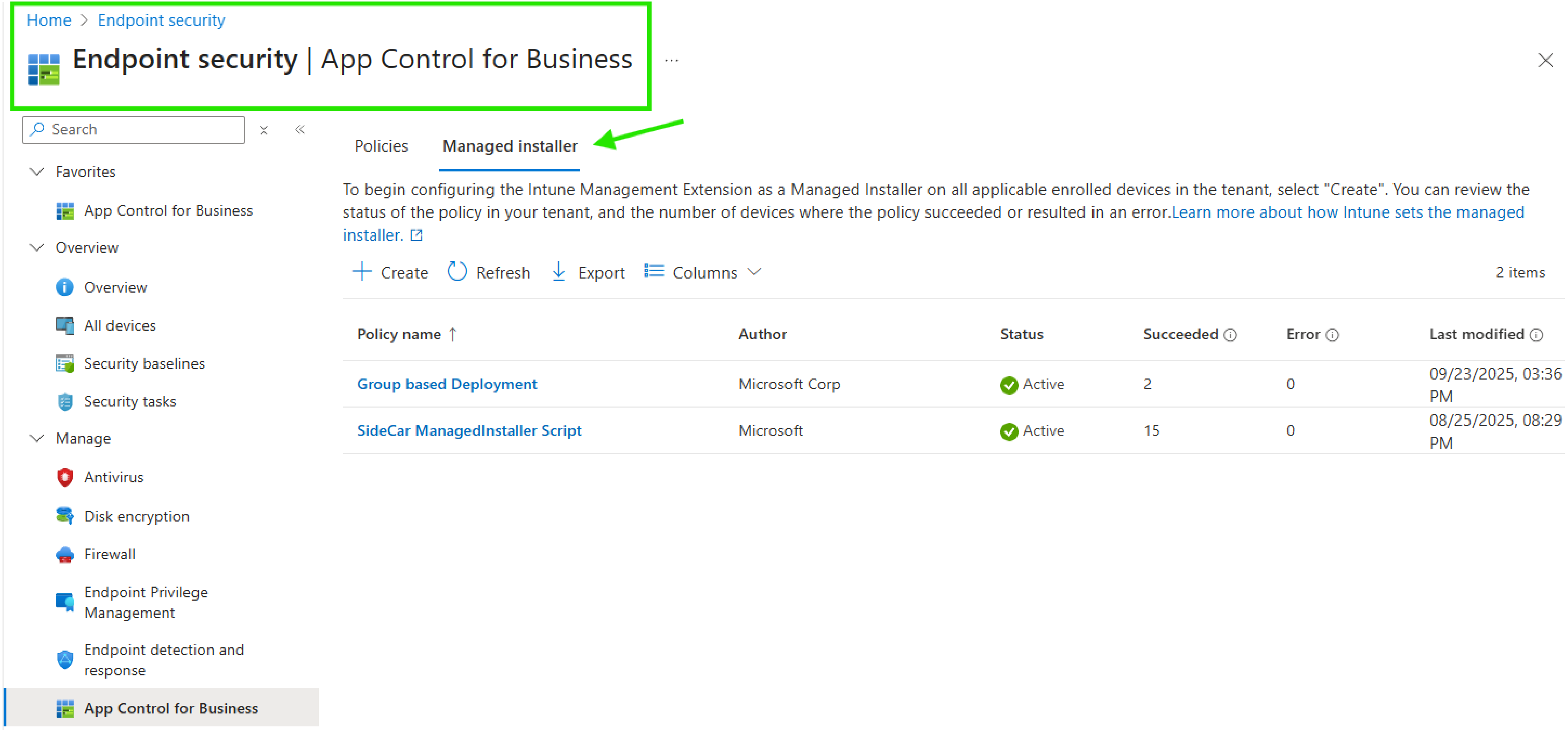
Use the same Policy options across your base policies

- 0 - Enabled:UMCI
- 3 - Enabled:Audit Mode
- **4 – Prevent “Flighted” builds (EG: Windows insider)**
- 6 - Enabled:Unsigned System Integrity Policy
- 9 - Enabled:Advanced Boot Options Menu
- **12 – Required: Enforce Store Applications**
- **13 – Managed installer**
- 16 - Enabled:Update Policy No Reboot
- 17 – Enabled: Allow supplemental policies

Managed Installer

- Allow applications to run when installed by your Systems Management Solution* (*assuming they were installed after the managed installer was defined.)
- Limitations
  - Modifying files trusted based on Managed Installer extended attributes invalidates the trust
    - EG: Self-updating apps become untrusted after an update
  - Broken Process Trees
    - Windows Installer Custom Actions (WIX)

Enabling the Managed Installer



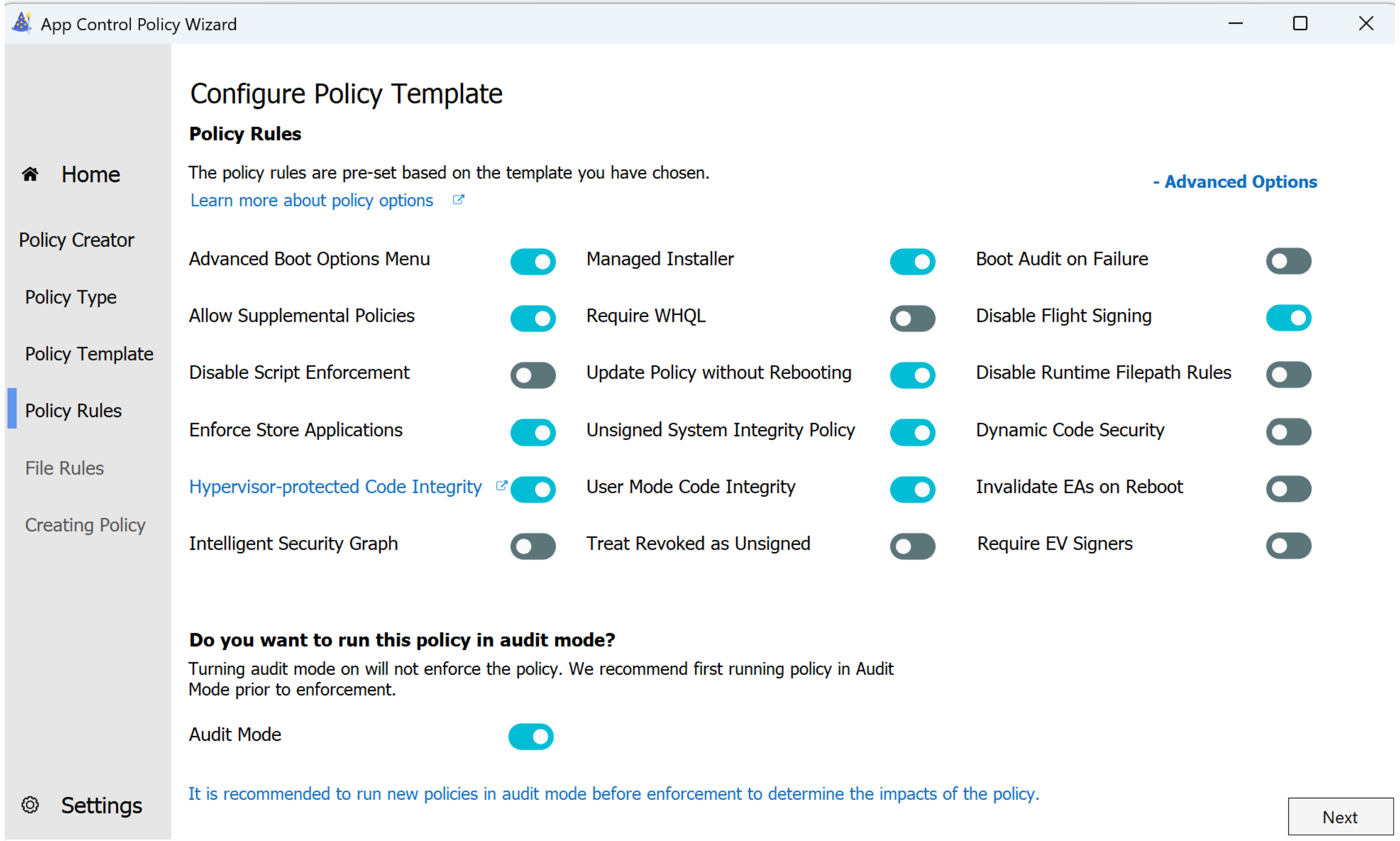
To begin configuring the Intune Management Extension as a Managed Installer on all applicable enrolled devices in the tenant, select "Create". You can review the status of the policy in your tenant, and the number of devices where the policy succeeded or resulted in an error.Learn more about how Intune sets the managed installer.

Policy name ↑	Author	Status	Succeeded ⓘ	Error ⓘ	Last modified ⓘ
Group based Deployment	Microsoft Corp	✓ Active	2	0	09/23/2025, 03:36 PM
SideCar ManagedInstaller Script	Microsoft	✓ Active	15	0	08/25/2025, 08:29 PM

Intelligent Security Graph

- Authorize Reputable Apps
- Geared towards organizations without Centralized software distribution capabilities
- Reputable != excluded from Malicious use
- Challenges
  - Python
  - Teamviewer
  - PSTools
  - Putty

Demo: Create the Corporate Base policy



Configure Policy Template

Policy Rules

The policy rules are pre-set based on the template you have chosen.
Learn more about policy options

Advanced Boot Options Menu	●	Managed Installer	●	Boot Audit on Failure	○
Allow Supplemental Policies	●	Require WHQL	○	Disable Flight Signing	●
Disable Script Enforcement	○	Update Policy without Rebooting	●	Disable Runtime Filepath Rules	○
Enforce Store Applications	●	Unsigned System Integrity Policy	●	Dynamic Code Security	○
Hypervisor-protected Code Integrity	●	User Mode Code Integrity	●	Invalidate EAs on Reboot	○
Intelligent Security Graph	○	Treat Revoked as Unsigned	○	Require EV Signers	○

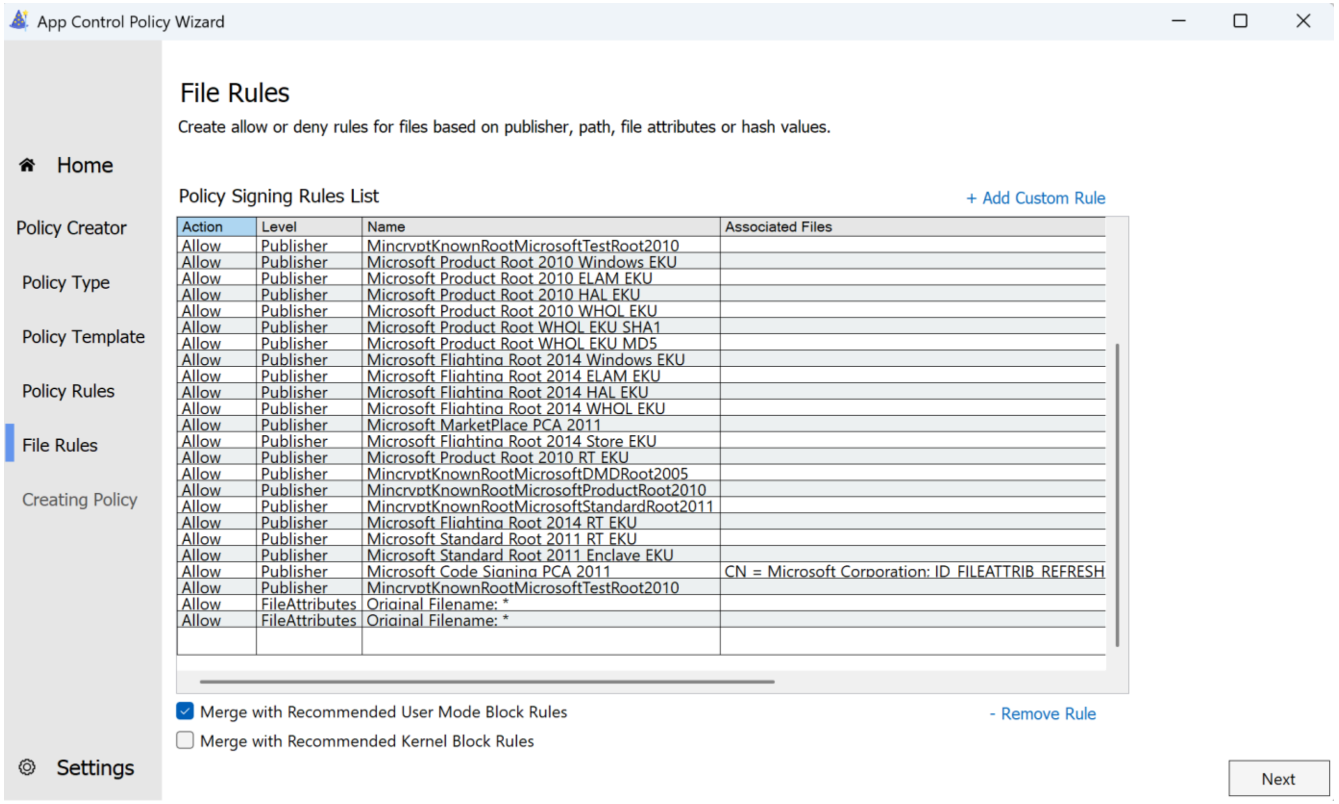
Do you want to run this policy in audit mode?

Turning audit mode on will not enforce the policy. We recommend first running policy in Audit Mode prior to enforcement.

Audit Mode ●

It is recommended to run new policies in audit mode before enforcement to determine the impacts of the policy.

Demo: Create the base recommended block rules policy



App Control Policy Wizard

File Rules

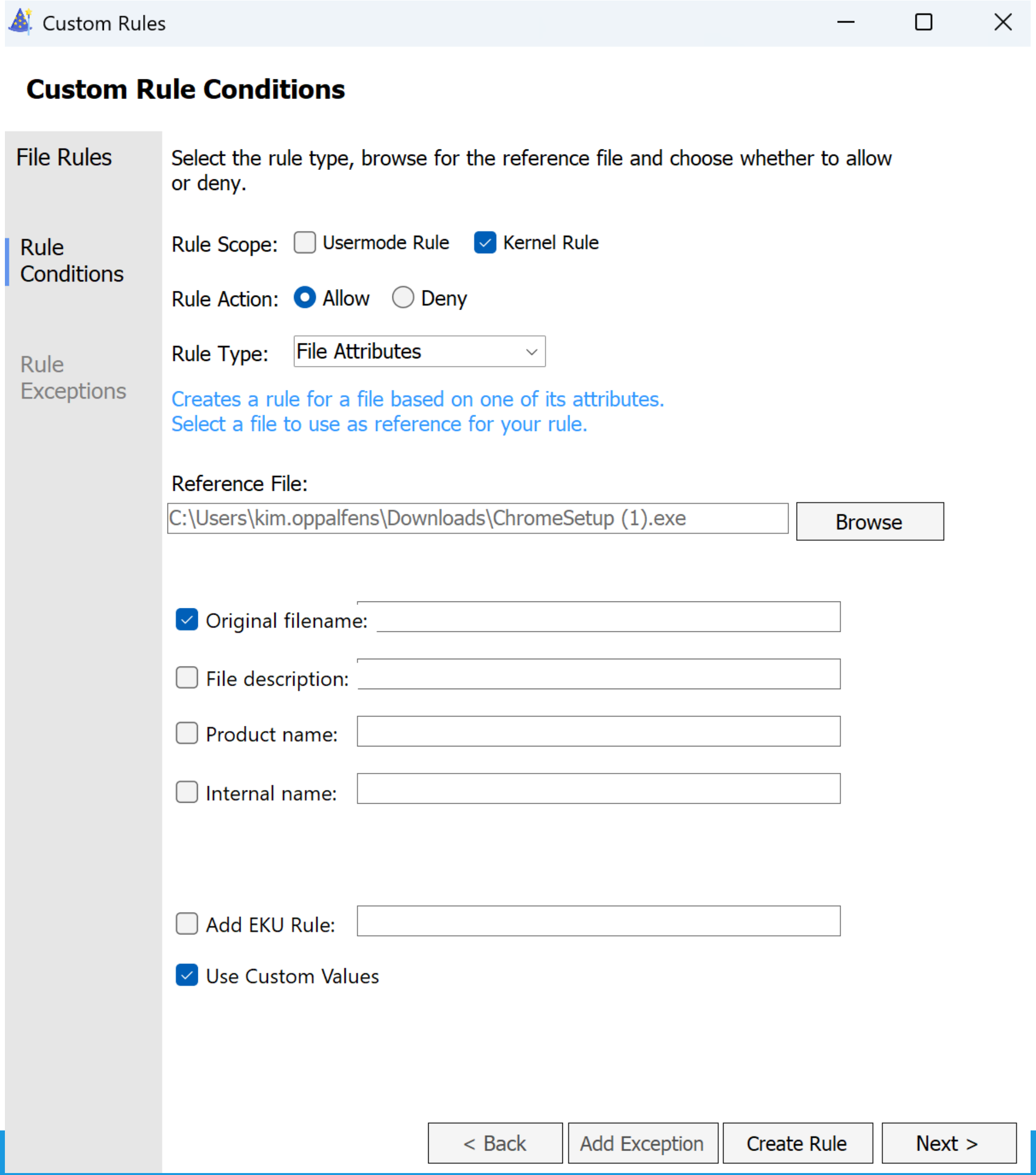
Create allow or deny rules for files based on publisher, path, file attributes or hash values.

Policy Signing Rules List

Action	Level	Name	Associated Files
Allow	Publisher	MincryptKnownRootMicrosoftTestRoot2010	
Allow	Publisher	Microsoft Product Root 2010 Windows EKU	
Allow	Publisher	Microsoft Product Root 2010 ELAM EKU	
Allow	Publisher	Microsoft Product Root 2010 HAL EKU	
Allow	Publisher	Microsoft Product Root 2010 WHQL EKU	
Allow	Publisher	Microsoft Product Root WHQL EKU SHA1	
Allow	Publisher	Microsoft Product Root WHQL EKU MD5	
Allow	Publisher	Microsoft Flighting Root 2014 Windows EKU	
Allow	Publisher	Microsoft Flighting Root 2014 ELAM EKU	
Allow	Publisher	Microsoft Flighting Root 2014 HAL EKU	
Allow	Publisher	Microsoft Flighting Root 2014 WHQL EKU	
Allow	Publisher	Microsoft MarketPlace PCA 2011	
Allow	Publisher	Microsoft Flighting Root 2014 Store EKU	
Allow	Publisher	Microsoft Product Root 2010 RT EKU	
Allow	Publisher	MincryptKnownRootMicrosoftDMDRoot2005	
Allow	Publisher	MincryptKnownRootMicrosoftProductRoot2010	
Allow	Publisher	MincryptKnownRootMicrosoftStandardRoot2011	
Allow	Publisher	Microsoft Flighting Root 2014 RT EKU	
Allow	Publisher	Microsoft Standard Root 2011 RT EKU	
Allow	Publisher	Microsoft Standard Root 2011 Enclave EKU	
Allow	Publisher	Microsoft Code Signing PCA 2011	CN = Microsoft Corporation; ID_FILEATTRIB_REFRESH
Allow	Publisher	MincryptKnownRootMicrosoftTestRoot2010	
Allow	FileAttributes	Original Filename: *	
Allow	FileAttributes	Original Filename: *	

☑ Merge with Recommended User Mode Block Rules

□ Merge with Recommended Kernel Block Rules



Custom Rules

Custom Rule Conditions

Select the rule type, browse for the reference file and choose whether to allow or deny.

Rule Scope: □ Usermode Rule ☑ Kernel Rule

Rule Action: ● Allow ○ Deny

Rule Type: File Attributes

Creates a rule for a file based on one of its attributes. Select a file to use as reference for your rule.

Reference File: C:\Users\kim.oppalfens\Downloads\ChromeSetup (1).exe

☑ Original filename:

□ File description:

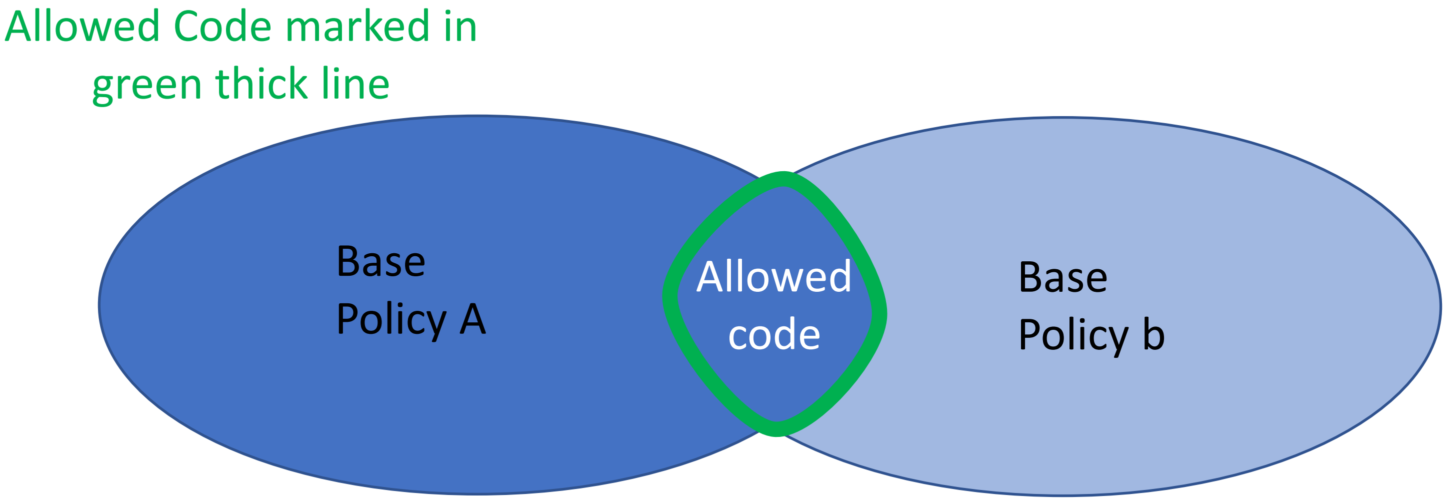
□ Product name:

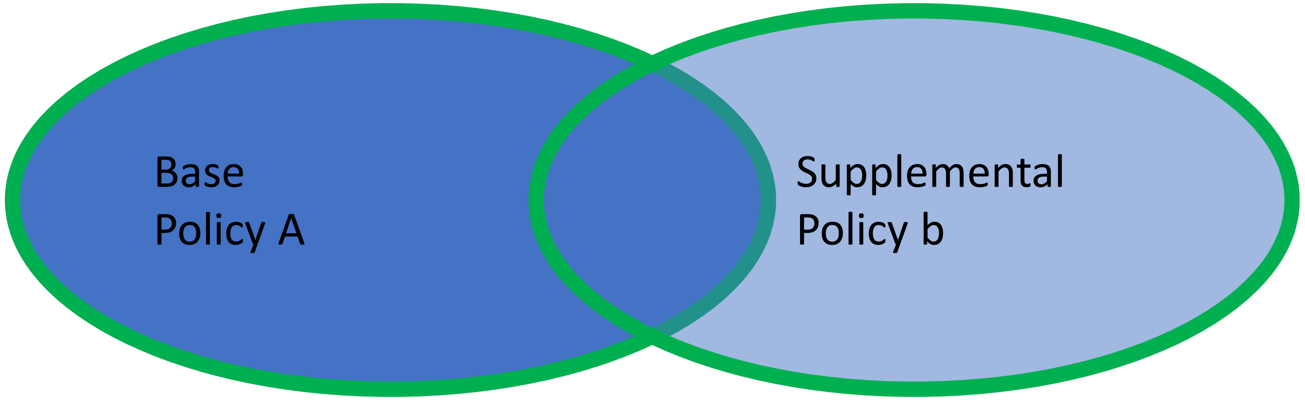
□ Internal name:

□ Add EKU Rule:

☑ Use Custom Values

A word on policy types





Supplemenal policies can only expand the trust scope so Deny rules can't be in Supplemental policies

Supplemental Corporate signing policy

```
$cert = New-SelfSignedCertificate -Type CodeSigningCert -Subject
'Application control signing cert' -CertStoreLocation Cert:\CurrentUser\my
```

```
Export-Certificate -Cert $cert -filepath appcontrolcert.cer
```

Create supplemental policy by browsing to .Cer file

Demo: Create the supplemental Corporate Signing Policy

Handling Packaged Apps

- Default Application Control policy trusts all store apps
  - Based on Enhanced Key Usage property on store signing cert that is part of the Default policy
- Create Package Family name based roles to effectively manage store apps
- Challenges
  - Python, PSTools, Teamviewer, yet again
  - Electron Apps bypass as discovered by the IBM Red team

Demo: Create the supplemental PFN based packaged app policy

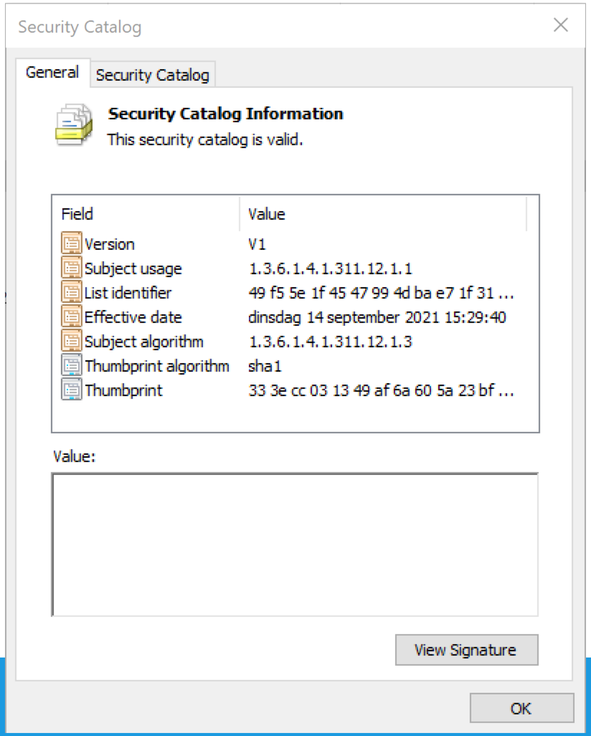
The Path rules

- No Windows* Path Rule needed
  - OS Binaries are trusted by the Default policy and digitally signing
    - Applies to Classic Teams, Intune, Defender for Endpoint Agent, Onedrive & Edge too
- C:\Windows\Assembly\*
  - Dotnet Native images (Performance penalty + Log Pollution)
- C:\Windows\Installer\*
  - Increase managed installer success for MSI Custom actions
- Program files* & Program files (x86)*

Demo: Create the path rules supplemental policy

Windows Security catalog basics

- .cat files, Introduced 2 decades ago with Windows 2000
- Enforcement started in Windows XP
  - Driver signing is Kernel Mode Code Integrity
- Windows Defender Application Control adds User mode Code Integrity

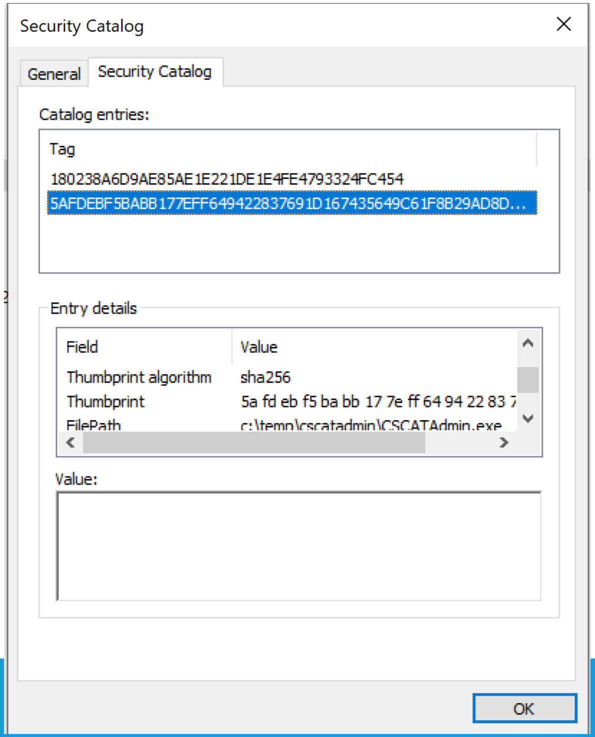


Security Catalog Information

This security catalog is valid.

Field	Value
Version	V1
Subject usage	1.3.6.1.4.1.311.12.1.1
List identifier	49 f5 5e 1f 45 47 99 4d ba e7 1f 31 ...
Effective date	dinsdag 14 september 2021 15:29:40
Subject algorithm	1.3.6.1.4.1.311.12.1.3
Thumbprint algorithm	sha1
Thumbprint	33 3e cc 03 13 49 af 6a 60 5a 23 bf ...

Value:



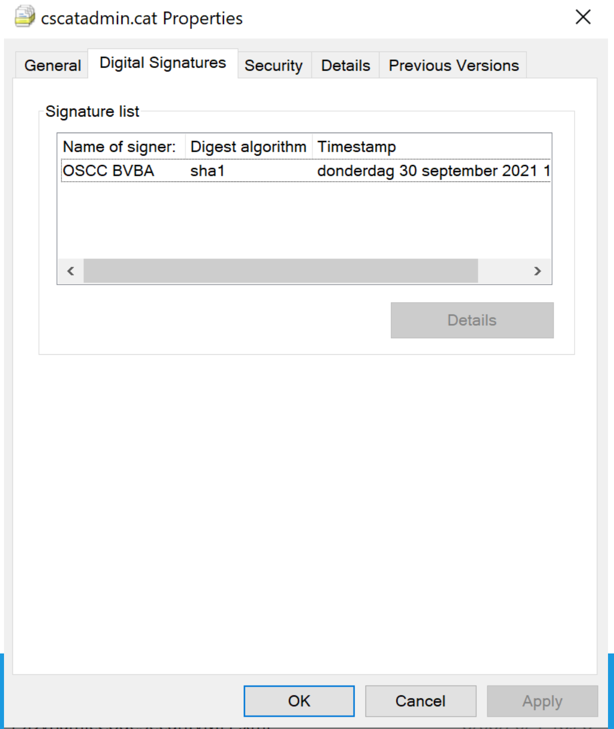
Catalog entries:

Tag
180238A6D9AE85AE1E221DE1E4FE4793324FC454
5AFDEBF5BABB177EFF649422837691D167435649C61F8B29AD8D...

Entry details

Field	Value
Thumbprint algorithm	sha256
Thumbprint	5a fd eb f5 ba bb 17 7e ff 64 94 22 83 7
FilePath	c:\temp\cscatadmin\CSCATAdmin.exe

Value:



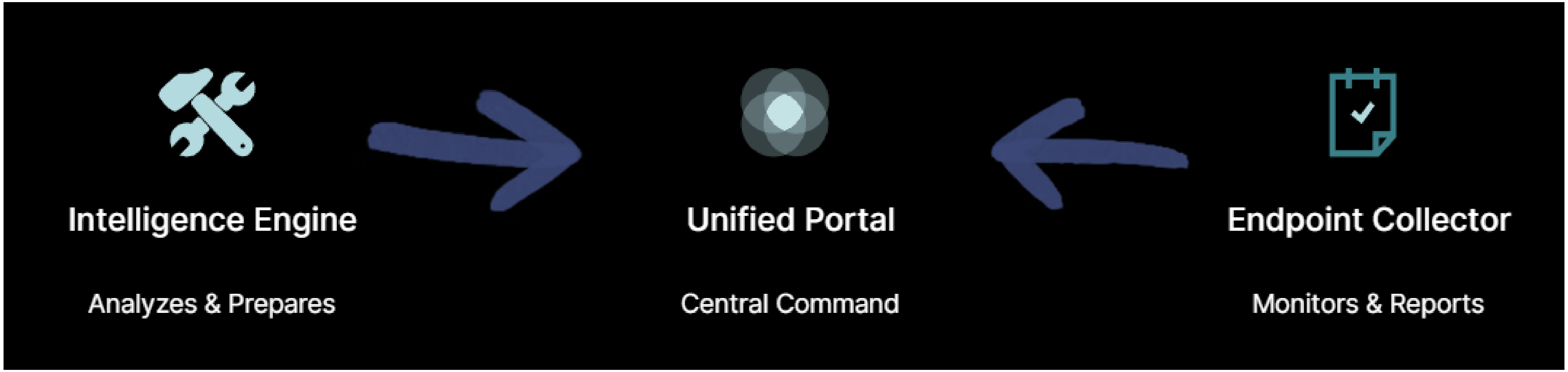
Signature list

Name of signer:	Digest algorithm	Timestamp
OSCC BVBA	sha1	donderdag 30 september 2021 1

Catalog use cases

- Catalogs can make apps trusted without modifying your CodeIntegrity policy!
- Catalogs are great for
  - Unsigned binaries
  - Non-Greenfield scenarios / Managed Installer backlog
  - ConfigMgr Tasksequence installed applications
  - Quick go-to market applications
    - Repeatable procedure
  - Tight / manageable control
  - Application Control automation

WWW.AppControl.AI



Intelligence Engine

Analyzes & Prepares

Unified Portal

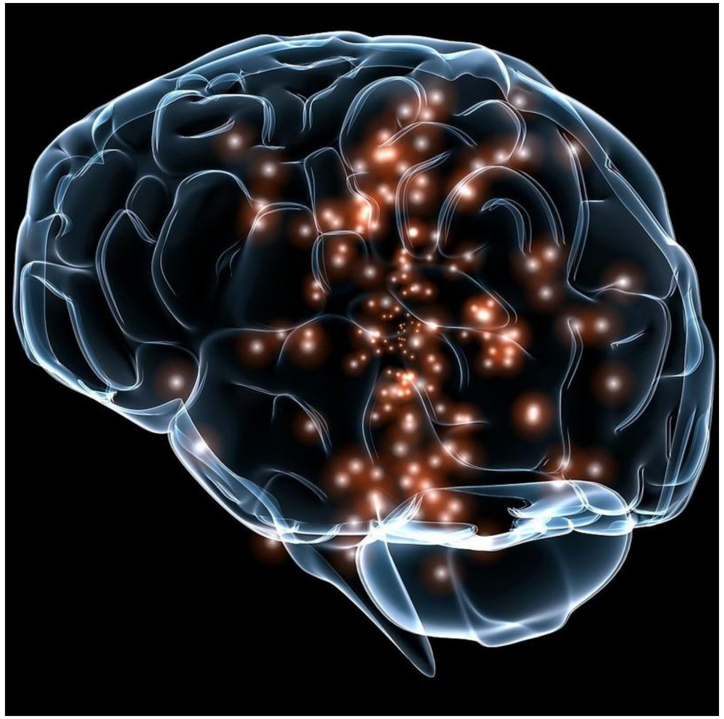
Central Command

Endpoint Collector

Monitors & Reports

AppControl for Business - Masterclass

- Dinsdag 12 Mei 2026 – 16:00-19:30
- Donderdag 14 Mei 2026 – 16:00-19:30
- Dinsdag 19 Mei 2026 – 16:00-19:30
- Donderdag 21 Mei 2026 – 16:00-19:30
- Dinsdag 26 Mei 2026 – 16:00-19:30



academy.viamonstra.com

We would love to hear your feedback!

Session feedback available in home feed of the app after the session

run events

Thank You!

MC^2