

정책 : 정책 생성

개요

Carbon Black App Control 정책 생성에 대한 가이드 문서입니다.

기능 소개

1. Policies

1.1 정책 생성

- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > [Add Policy] 버튼 클릭하여 정책 생성

Add Policy

Policy Name:

Description:

Mode:

☒ Visibility ☐ Control ☐ Disabled

Initial Settings:

Template Policy ▼

Options:

☐ Automatically Upgrade Agents ☒ Track File Changes
☐ Load Agent in Safe Mode ☐ Suppress Logo In Notifier

Total Computers:

0

Connected Computers:

0

Save & Exit

Save

Cancel

- 조직별 정책 및 목적별 정책을 생성하여 사용

- Policy Name : 정책 이름
- Description : 정책 설명
- Mode : 서버와 컴퓨터가 통신하는 상태 혹은 통신하지 않는 상태에 대해 동작할 모드 설정
 - Visibility : 파일 활동 및 이벤트 추적하기 위한 모드 (파일 실행/쓰기/금지 영향 없음) - 보안 기능을 인한 동작 방해 없음
 - Control : 파일 실행에 대한 제어 및 단계 설정
 - High (Block Unapproved) : 승인되지 않은 파일 실행 차단 및 이벤트 추적
 - Medium (Prompt Unapproved) : 승인되지 않은 파일 실행 차단 및 사용자가 파일 실행 여부 선택 가능
 - Low (Monitor Unapproved) : 승인되지 않은 파일 실행 허용 및 이벤트 추적
 - Disabled : 파일 활동에 대한 추적 중단 - 에이전트 제거 시 사용
- Initial Settings : 템플릿으로 사용할 정책 선택
- Options
 - Automatically Upgrade Agents : 에이전트에 대한 자동 업그레이드
 - Track File Changes : 파일 추가/삭제/변경 추적
 - Load Agent in Safe Mode (기본값) : 안전 모드에서 에이전트 로드
 - Suppress Logo in Notifier : 에이전트 알림이 발생할 경우 로고를 표시하지 않음
- Total Computer : 정책에 연결된 총 컴퓨터 개수
- Connected Computer : 정책에 연결된 컴퓨터 중, 서버와 연결된 컴퓨터 개수

1.2 정책 구성

📄 정책 별 상세 가이드 : <https://bs.etever.s.tech/books/carbon-black-app-control-handbook/page/3def1>

- [App Control] 웹 콘솔 접속 > [Policies] 메뉴 선택 > '정책'의  (View Details) 버튼 클릭

Advanced	File Rules	Custom Rules	Memory Rules	Registry Rules	Publisher Rules	Rapid Configs	Computers	Device Control Settings
Name			Status	Notifiers				
Block unanalyzed scripts and executables			Active	<default>: Block unanalyzed scripts and executables				
Block unapproved scripts			Active	<default>: Block unapproved scripts				
Block unapproved executables			Active	<default>: Block unapproved executables				
Block banned file names			Active	<default>: Block banned file names				
Block banned file hashes			Active	<default>: Block banned file hashes				
Block executables run from a network drive			Off	<default>: Block executables run from a network drive				
Block files with banned publishers or certificates			Active	<default>: Block files with banned publishers or certificates				
Enforce memory rules			Active	<default>: Enforce memory rules				
Enforce registry rules			Active	<default>: Enforce registry rules				
Enforce custom (file and path) rules			Active	<default>: Enforce custom (file and path) rules				
Enforce tamper protection			Active	<default>: Enforce tamper protection				
Terminate processes with banned images			Report Only	<default>: Terminate processes with banned images				
			<input checked="" type="checkbox"/>	Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High				

- Advanced : 개별적으로 등록되는 타 정책과 달리 전체 범위에서의 특정 동작에 대한 파일/스크립트 허용 및 차단
 - Active : 활성화
 - Off : 비활성화
 - Report Only : 정책 테스트 - 파일 차단에 대한 로그 기록

Advanced

File Rules

Custom Rules

Memory Rules

Registry Rules

Publisher Rules

Rapid Configs

Computers

Device Control Settings

Show Filters

Show Columns

Export to CSV

Refresh Table

☒ Show Rules That Apply To All Policies








Search:

Enter File Hash, Name

☐ Automatically apply

Showing 25 out of 240 item(s)

Showing 1 out of 1 group(s)

Type	Name	File Hash	Source Name	Date Modified	Is Global	
Type: Approval		240 item(s)				
	Approval	B9CustomAction.dll	d7103f91ecf520dfcf600c6bc24b1139d663be69f4a8a3376369b19ab374bce	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	ParityAgentDB.dll	ec337f688a2045bf7210183493618c39662b20d38777547487d5e8bfe26325b3	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	cb7zip.dll	96b0ddd51e2027b56ea499a4cd178246d9f3859bd252afd2dd04206702aa69b0	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	Crawler.exe	cc85f2e65b0d1add8ebafa31558e62bcaa37745addc68a6e8f7b9f31753ec601	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	DasCLI.exe	6581d9cc447c4dfe954e9b2cd674db89003d0f6914db0d3de7a5e5ebd5a52a86	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	dbghelp.dll	1e3770a286d59b0a300535ff0c47696353c6549ea668aba1d81ee798e0ebd373	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes
	Approval	ipworks8.dll	3d66133777b880f7ef677c414627482b99de340987402507cd27d308890eca0b	Carbon Black Installation	Feb 18 2024 04:42:19 PM	Yes

- File Rules : 엔드포인트 설치 시 검출된 파일 또는 사용자가 등록한 개별 파일 해시 값을 통한 파일 승인 및 차단
 - Approval : 파일 실행 허용
 - Ban : 파일 실행 차단
 - Ban (Monitor) : 파일 실행에 대한 이벤트 발생

Advanced	File Rules	Custom Rules	Memory Rules	Registry Rules	Publisher Rules	Rapid Configs	Computers	Device Control Settings
rch: <input type="text" value="Enter Name, Path, Process"/> <input type="checkbox"/> Automatically apply Showing 43 out of 43 item(s)								
Rank	Status	Platform	Rule Type	Name	Action			
1	Enabled	Windows	Expert	Tag process as msisxex identified by yara	Tag Target			
2	Enabled	Windows	Performance Optimization	Ignore system log files	Ignore			
5	Enabled	Windows	Expert	Examine powershell script contents	Tag Target			
6	Enabled	Windows	Expert	Block powershell scripts that execute memory	Block, Finish Rule Group			
8	Enabled	Windows	Expert	Do not treat these processes as .NET applications	Remove Process Tags			
9	Enabled	Windows	Expert	Report read-only memory map operations on unapproved executables by .NET applications	Report, Query Reputation			
12	Enabled	Windows	Expert	Deny read-only memory map operations on banned executables by .NET applications	Block			

- Custom Rules : 사용자가 소프트웨어 프로세스 행위에 대한 작업 규칙

Advanced	File Rules	Custom Rules	Memory Rules	Registry Rules	Publisher Rules	Rapid Configs	Computers	Device Control Settings				
<div>Show Filters ▶ Show Columns ▶ Export to CSV Refresh Table</div> <div><input type="checkbox"/> Show Disabled Rules <input type="checkbox"/> Show Rules That Apply To All Policies</div> <div>Search: <input type="text" value="Enter Name, Path, Process"/> <input type="checkbox"/> Automatically apply Showing 0 out of 0 item(s)</div>												
Rank ▲	Status	Platform	Name	Action	Operation	Permissions	Path	Process	User or Group	Date Modified	Last Modified By	Policy
No data found.												
Showing 00s												
Showing all data												

- Memory Rules : 사용자나 프로세스가 특정 프로세스의 메모리에 접근하거나 변경하는 등의 행위 허용 및 차단

Advanced

File Rules

Custom Rules

Memory Rules

Registry Rules

Publisher Rules

Rapid Configs

Computers

Device Control Settings

Show Filters

Show Columns

Export to CSV

Refresh Table

☒

Show Disabled Rules

☒

Show Rules That Apply To All Policies

Search:

Enter Name, Path, Process

☐ Automatically apply

Showing 7 out of 7 item(s)

Rank	Status	Platform	Name	Action	Operation	Path	
	1	Disabled	Windows	Case Sensitivity: Block Registry Modifications	Block, Finish Rule Group	Create Key, Rename Key, Delete Key,...	HKLM\SYSTEM*co
	2	Disabled	Windows	[Sample] Block Suspicious System Changes	Block, Finish Rule Group	Create Key, Rename Key, Delete Key,...	HKLM\software\mic
	3	Disabled	Windows	[Sample] Prompt on Suspicious changes to Startup Files	Prompt, Finish Rule Group	Create Key, Rename Key, Delete Key,...	*\software\microso
	4	Disabled	Windows	[Sample] Report Typical Changes to Startup Files	Report	Create Key, Rename Key, Delete Key,...	*\software\microso

- Registry Rules : Windows OS에서 특정 레지스트리를 변경하는 행위 허용 및 차단

Advanced

File Rules

Custom Rules

Memory Rules

Registry Rules

Publisher Rules

Rapid Configs

Computers

Device Control Settings

Filters

Add filter

Apply

Cancel

Reset

Search:

Enter Name





☐ Automatically apply

Showing 28 out of 28 item(s)

Showing 2 out of 2 group(s)

Name	State	Date Approved or Banned	Approved or Banned By	First Seen Date	Trust	Acknowledged
State: Unapproved 25 item(s)						
Microsoft Windows	Unapproved			Feb 18 2024 04:56:17 PM	Not trusted (Unknown)	No
Microsoft Windows Publisher	Unapproved			Feb 18 2024 04:56:19 PM	Not trusted (Unknown)	No
Microsoft Windows Hardware Abstraction Layer Publisher	Unapproved			Feb 18 2024 04:56:28 PM	Not trusted (Unknown)	No
Microsoft Windows Hardware Compatibility Publisher	Unapproved			Feb 18 2024 04:56:32 PM	Not trusted (Unknown)	No
VMware Inc.	Unapproved			Feb 18 2024 04:57:52 PM	Not trusted (Unknown)	No

- Publisher Rules : Windows 및 MAC 에서 사용되는 소프트웨어 인증서에 대한 승인 및 미승인 규칙 정의하여 파일 허용 및 차단

Advanced	File Rules	Custom Rules	Memory Rules	Registry Rules	Publisher Rules	Rapid Configs	Computers	Device Control Settings		
Name ▲		Description				Enabled	Configured	Platform	Modified By	Policy
	Browser Protection	Reports or prevents potentially malicious behavior related to browsers. This includes execution of files downloaded by browsers, modification of the hosts file, and modification of browser related registry entries. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.				No	No	Windows	System	All Current and Future Policies
	Carbon Black App Control Server Tamper Protection	Provides protection against tampering with the Carbon Black App Control Server. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.				No	Yes	Windows	System	All Current and Future Policies
	Carbon Black EDR Tamper Protection	Prevents tampering with Carbon Black EDR. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.				No	Yes	Windows	System	All Current and Future Policies
	Cryptomining Protection	Reports or prevents potentially malicious behavior related to file based cryptomining attacks. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.				No	No	Windows	System	All Current and Future Policies

- Rapid Configs : 세부적인 정책을 적용하기 전, 신속하게 엔드포인트 보호 환경을 정의하기 위한 정책 적용

AdvancedFile RulesCustom RulesMemory RulesRegistry RulesPublisher RulesRapid ConfigsComputersDevice Control Settings

Show Filters ▶ | Show Columns ▶ | Export to CSV | Refresh Table

Search: ☐ Automatically apply Showing 1 out of 1 item(s)

Computer Name	Connected	Policy Status	Upgrade Status	IP Address
ETVS\SEUNGMIN-WINDOW	<div></div>	Up to date	Up to date	10.6.71.15

Showing 1 out of 1 itemShowing all data

- Computers : 정책이 적용된 엔드포인트 목록 확인

AdvancedFile RulesCustom RulesMemory RulesRegistry RulesPublisher RulesRapid ConfigsComputersDevice Control Settings

Name	Status	Notifiers
Block writes to unapproved removable devices	<div>Off</div>	<div><default>: Block writes to unapproved removable devices</div> Add Edit
Block writes to banned removable devices	<div>Active</div>	<div><default>: Block writes to banned removable devices</div> Add Edit
Report reads from unapproved removable devices	<div>Off</div>	<div><none></div>
Report reads from banned removable devices	<div>Off</div>	<div><none></div>
Block executions from unapproved removable devices	<div>Off</div>	<div><default>: Block executions from unapproved removable devices</div> Add Edit
Block executions from banned removable devices	<div>Active</div>	<div><default>: Block executions from banned removable devices</div> Add Edit

- Device Control Settings : 금지 및 미승인된 이동식 장치에 대한 실행 및 쓰기 행위에 대한 허용 및 차단

↻ 버전 #8

★ 생성 16 2월 2024 09:55:07

✎ 수정 18 4월 2025 17:06:16