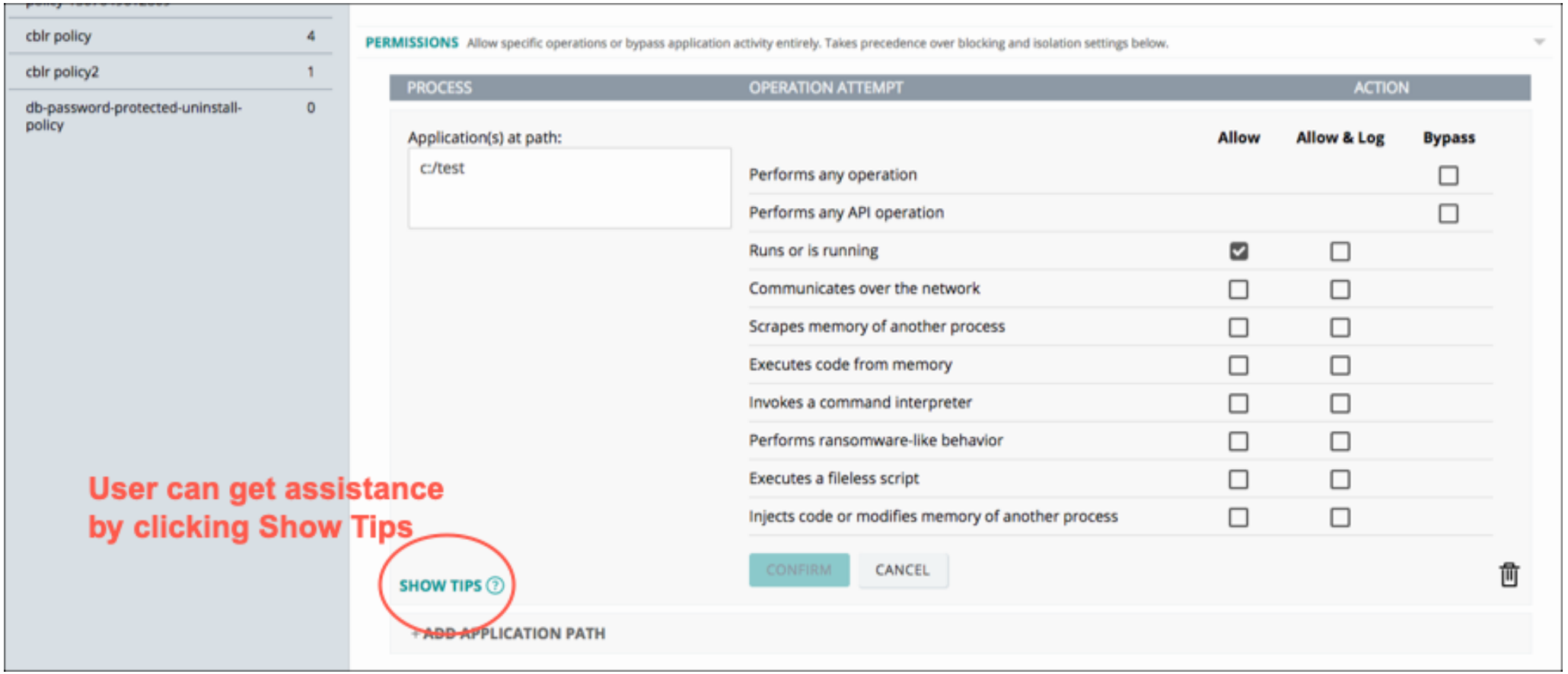
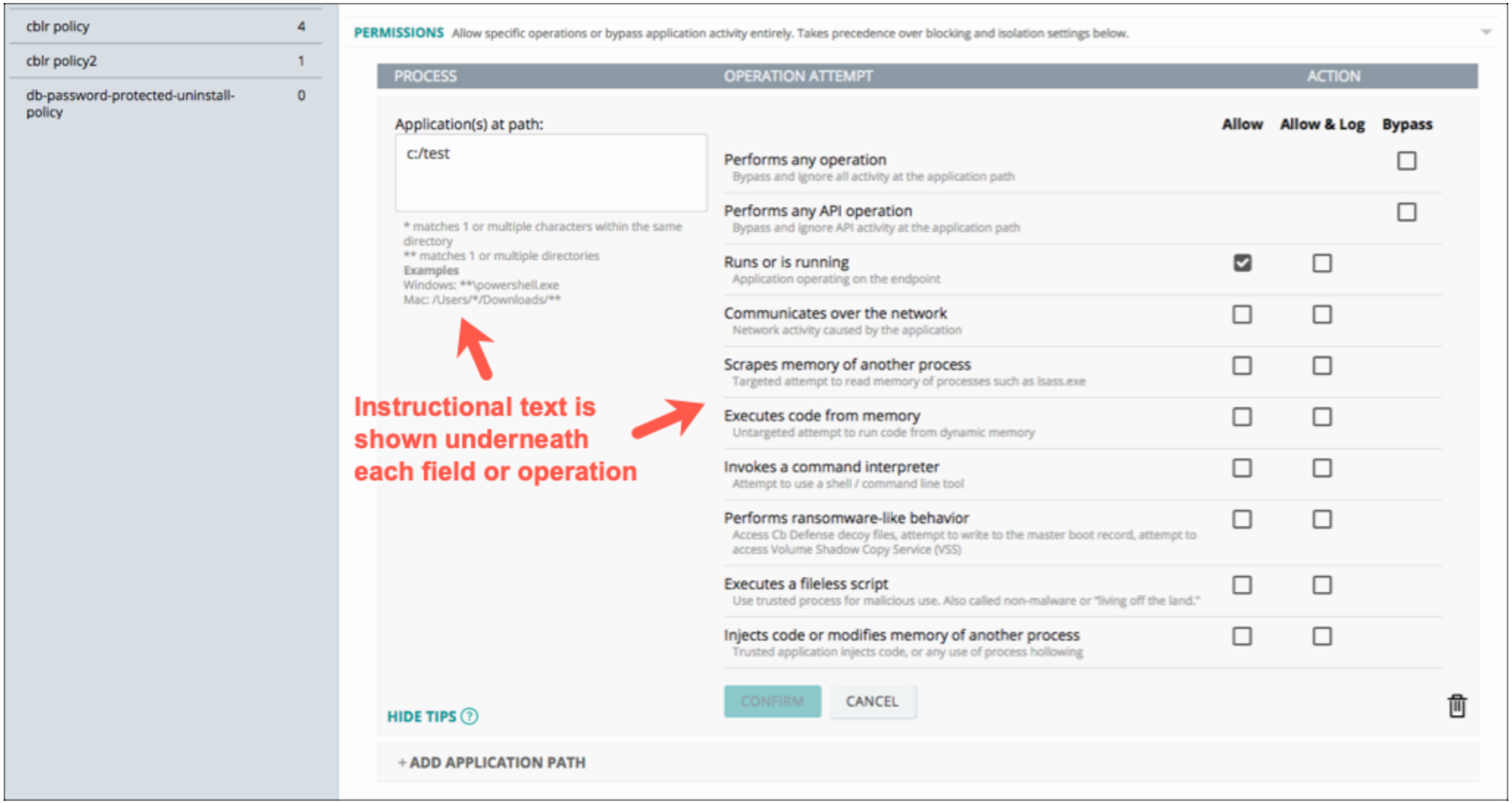
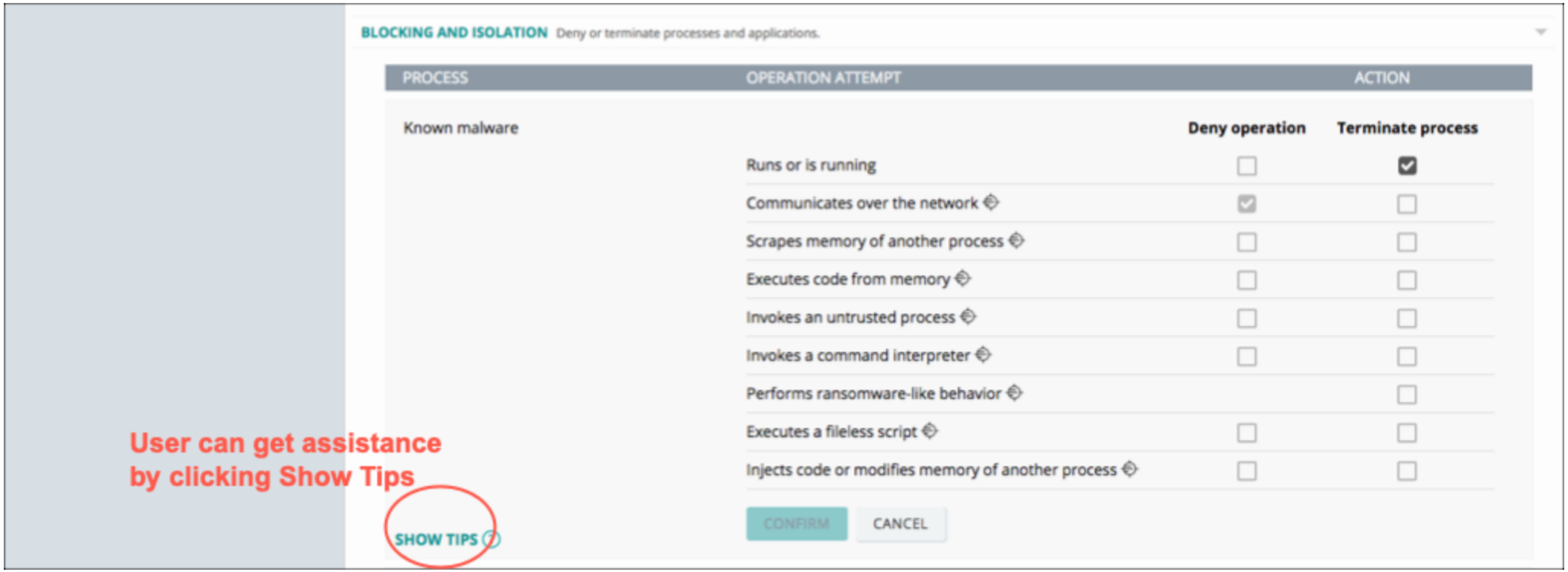
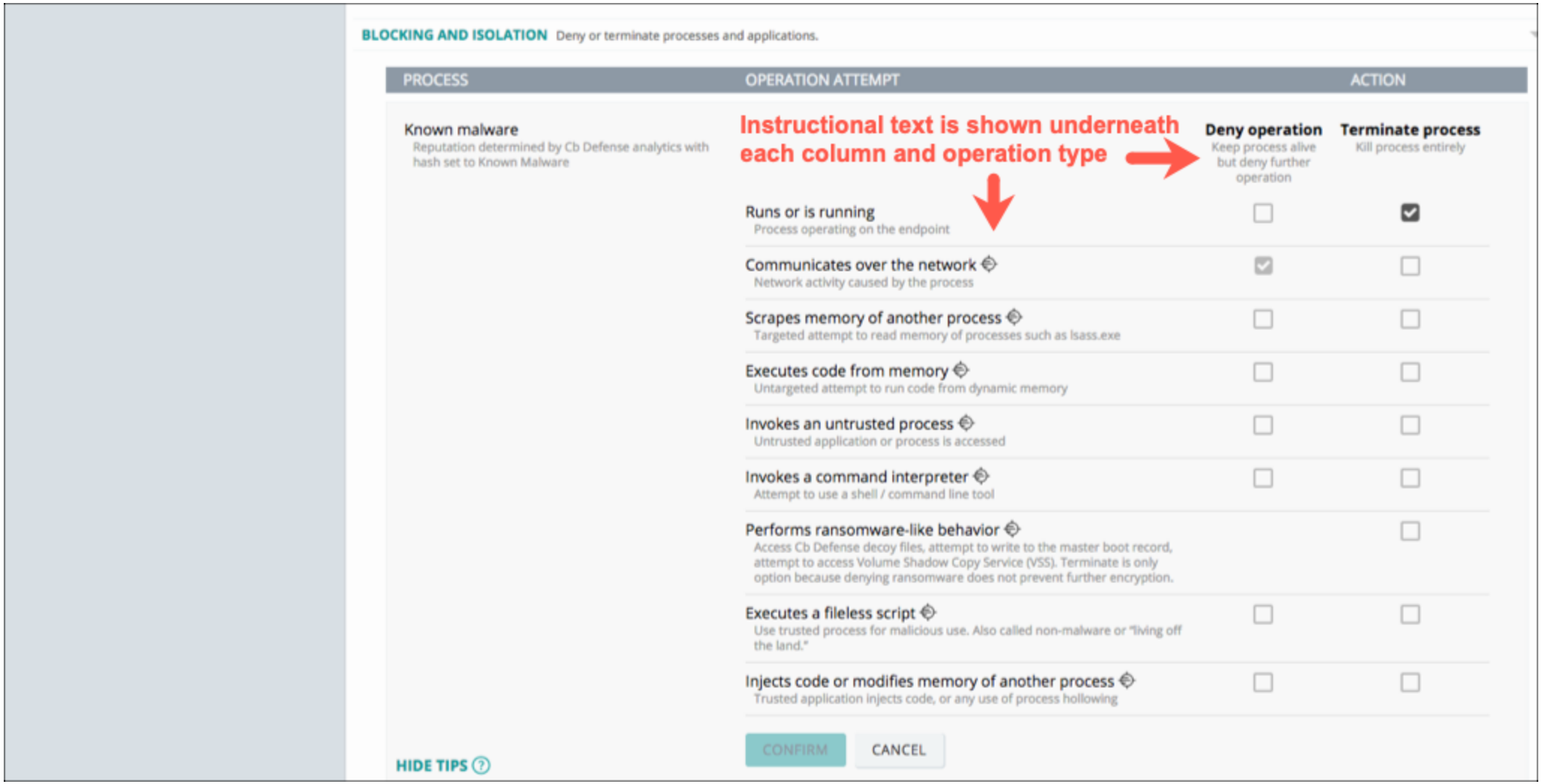

cblr policy 4
cblr policy2 1
db-password-protected-uninstall-policy 0
PERMISSIONS Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.
PROCESS
OPERATION ATTEMPT
ACTION
Application(s) at path:
c:/test
Allow
Allow & Log
Bypass
Performs any operation
Performs any API operation
Runs or is running
Communicates over the network
Scrapes memory of another process
Executes code from memory
Invokes a command interpreter
Performs ransomware-like behavior
Executes a fileless script
Injects code or modifies memory of another process
CONFIRM
CANCEL
SHOW TIPS
+ ADD APPLICATION PATH
User can get assistance
by clicking Show Tips


cblr policy 4
cblr policy2 1
db-password-protected-uninstall-policy 0
PERMISSIONS Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.
PROCESS
OPERATION ATTEMPT
ACTION
Application(s) at path:
c:/test
* matches 1 or multiple characters within the same directory
** matches 1 or multiple directories
Examples
Windows: **\powershell.exe
Mac: /Users/*/Downloads/**
Instructional text is shown underneath each field or operation
Allow
Allow & Log
Bypass
Performs any operation
Bypass and ignore all activity at the application path
Performs any API operation
Bypass and ignore API activity at the application path
Runs or is running
Application operating on the endpoint
Communicates over the network
Network activity caused by the application
Scrapes memory of another process
Targeted attempt to read memory of processes such as lsass.exe
Executes code from memory
Untargeted attempt to run code from dynamic memory
Invokes a command interpreter
Attempt to use a shell / command line tool
Performs ransomware-like behavior
Access Cb Defense decoy files, attempt to write to the master boot record, attempt to access Volume Shadow Copy Service (VSS)
Executes a fileless script
Use trusted process for malicious use. Also called non-malware or "living off the land."
Injects code or modifies memory of another process
Trusted application injects code, or any use of process hollowing
CONFIRM
CANCEL
HIDE TIPS
+ ADD APPLICATION PATH


BLOCKING AND ISOLATION Deny or terminate processes and applications.
PROCESS
OPERATION ATTEMPT
ACTION
Known malware
Deny operation
Terminate process
Runs or is running
Communicates over the network
Scrapes memory of another process
Executes code from memory
Invokes an untrusted process
Invokes a command interpreter
Performs ransomware-like behavior
Executes a fileless script
Injects code or modifies memory of another process
CONFIRM
CANCEL
SHOW TIPS
User can get assistance
by clicking Show Tips


BLOCKING AND ISOLATION Deny or terminate processes and applications.
PROCESS
OPERATION ATTEMPT
ACTION
Known malware
Reputation determined by Cb Defense analytics with hash set to Known Malware
Instructional text is shown underneath each column and operation type
Deny operation
Keep process alive but deny further operation
Terminate process
Kill process entirely
Runs or is running
Process operating on the endpoint
Communicates over the network
Network activity caused by the process
Scrapes memory of another process
Targeted attempt to read memory of processes such as lsass.exe
Executes code from memory
Untargeted attempt to run code from dynamic memory
Invokes an untrusted process
Untrusted application or process is accessed
Invokes a command interpreter
Attempt to use a shell / command line tool
Performs ransomware-like behavior
Access Cb Defense decoy files, attempt to write to the master boot record, attempt to access Volume Shadow Copy Service (VSS). Terminate is only option because denying ransomware does not prevent further encryption.
Executes a fileless script
Use trusted process for malicious use. Also called non-malware or "living off the land."
Injects code or modifies memory of another process
Trusted application injects code, or any use of process hollowing
CONFIRM
CANCEL
HIDE TIPS