DriveLock Application Behavior Control: Application control with even greater security

In this digital era, data protection and security are becoming increasingly important issues for companies. While Application Control is one of the most effective cyber attacks and data breaches prevention technologies, Application Behavior Control takes this protection to an even higher security level.

The number of cyber attacks is continually growing. Attackers are becoming more inventive. In 2019, there were over 1 billion different malware and ransomware variants with devastating consequences.

Application Control combined with Application Behavior Control - the most effective protection against any kind of malware.

Application Control with predictive whitelisting enables administrators to control the execution of any application against a list of approved programs. In "traditional" type of attacks, external malware is primarily installed or executed on the target system. However, attackers use approved administration or system tools, which already exist on the target system, to initiate an attack with fileless malware such as "living off the land" method. In short, even whitelisted applications can pose a potential threat if they are not restricted in their behaviour and permissions.

Built on DriveLock Application Control, **Application Behavior Control provides additional security by modifying software permissions** to manage its behavior. This solution also provides enhanced anti-malware capabilities and offer better prevention against the possible circumvention of the application whitelist. Legitimate whitelisted programs can be restricted to a minimum of required actions and permissions to ensure that only authorised software and scripts are executed, or that they are allowed to start other processes as required. Application Behavior Control also manages access permissions to scripting tools like MS PowerShell, VBS, Python and the command line.

Advantages of Application Behavior Control

- + ADVANCED ANTI-MALWARE CAPABILITIES
- + PREVENT BYPASSING OF APPLICATION WHITELIST
- + NO ENTRY POINT FOR ATTACKERS
- + MINIMAL ADMINISTRATIVE EFFORT
- + CENTRALISED MANAGEMENT
- + SELF-SERVICE CAPABILITY FOR TRUSTED END USERS
- + CLOUD AND ON PREMISE SOLUTION
- + COMPLIANCE WITH LEGAL REQUIREMENTS

Cyber Threats - Status Quo

- + DIGITALISATION BLURS OUT COMPANIES' BORDERS
- + MORE THAN 50% OF COMPANIES WORLDWIDE HAVE BEEN THE TARGET OF A CYBER ATTACK
- + FILE-BASED OR FILELESS ATTACKS USING SCRIPTS, MACROS OR MS OFFICE
- + CONSEQUENTIAL LOSS DUE TO AN ATTACK: € 3.9 MILLION

DriveLock

Advantages of Application Behavior Control

- **Prevent whitelisted applications from starting further applications (including processes or scripts) which could pose potential threats to the system.**
- **Specify which type of access a particular application is allowed (e.g. read/write access to files or access to the registry).**
- **Provide better protection against fileless attacks and block the invocation of certain subordinate processes.**

Reduced effort through automatic learning and application categories

To simplify administration and ease pressure on IT departments, the correct application behaviour can be learnt automatically. An application is observed over a certain period of time and its behaviour is either adopted as part of central policies or specified for a computer as with a local whitelist. The application may then only perform the learnt operations.
"Application Collections" are collections of applications that belong together thematically. They may contain applications of the same type, e.g. browsers or e-mail clients.
Instead of creating individual rules for each application, one single rule for an entire category of applications can be created to reduce and simplify your rule set.

Important Use Cases/Scenarios

- **Launching the PowerShell:** You want to prevent your browser from launching PowerShell, and therefore malware, from possibly getting onto your computers.
  Solution: Create a rule that prohibits the browser and any processes it launches from launching PowerShell.
- **Email client and browser are only allowed to perform authorised actions,** such as writing to specific directories or launching legitimate applications.
- **Loading a DLL:** Dynamic Link Libraries (DLLs) are set up to be loaded from specific directories only, for example, to prevent Windows Media Player from loading DLLs from network drives.
- **Script execution:** You want to prevent browsers from running VB scripts.
- **Reading from a specific directory:** You want to ensure that only a specific application has read access only to a specific directory. This prevents the possibility of a malicious software, through a security breach in the browser, to gain read access to another directory which may have your bank data. This can be achieved with application permissions.

Other Advantages

+ AUTOMATIC LEARNING OF APPLICATION BEHAVIOR CREATES LOCAL RULES AND MINIMISES ADMINISTRATIVE OVERHEADS.
+ TEMPORARY MONITORING OF APPLICATIONS HELPS ADMINISTRATORS TO SET RESTRICTIONS ON APPLICATION USE QUICKER AND IN A MORE TARGETED MANNER.
+ QUICKLY CREATE APPLICATION RULES FOR A WHOLE APPLICATION CATEGORY

DriveLock - Features

+ SELF-LEARNING APPLICATION BEHAVIOUR
+ TARGETED BLOCKING OF SUB-PROCESSES
+ RESTRICTION OF LEGITIMATE APPLICATIONS TO REQUIRED ACTIONS AND PERMISSIONS
+ ACCESS CONTROL OF APPLICATIONS ON THE FILE SYSTEM AND REGISTRY
+ REGULATION OF AUTHORISATION HIERARCHIES
+ CENTRALISED DASHBOARD

DriveLock: Expert in IT and data security for more than 20 years

The German company **DriveLock SE** was founded in 1999 and is now one of the leading international specialists for cloud-based endpoint and data security. The solutions include measures for a prevention, as well as for the detection and containment of attackers in the system.

DriveLock is Made in Germany, with development and technical support from Germany.

DriveLock SE • Germany • France • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com