DriveLock Application Control: Effective protection against malware

In the course of digitalisation, the issues of data protection and security within companies are becoming increasingly important. The demands on today's IT security solutions are increasing. We are committed to protecting your data, devices and systems.

The number of Cyber Attacks is continuously increasing. Attackers are becoming more and more targeted and tricky. In 2019 alone, there were over 1 billion different malware and ransomware variants, with devastating consequences. Traditional attack types primarily involve installing or running external malware on the target system. In addition, with file-less malware, attackers abuse administration & system tools that are already present on the target system.

Application Whitelisting - the most effective protection against all types of malware. How does the DriveLock solution work?

Antivirus software only detects known malware. But malware sometimes disguises itself, or it is unknown to an antivirus solution at the time of an attack.

Intelligent application control allows administrators to control the execution of any application. Different rules or policies determine which applications are allowed run, and which are blocked.

The flexibility to combine blacklist & whitelist rules makes application control both easy to use and a powerful tool for the protection. With DriveLock you get the best of both rule types.

Centralized Rules
Self-Service
Predictive Whitelisting

With application whitelisting, you can create a list of trusted entities (applications, software libraries, scripts) that are allowed to access a system or network and block everything else. The configuration is managed centrally and can be assigned to specific end devices, groups or groups of people.

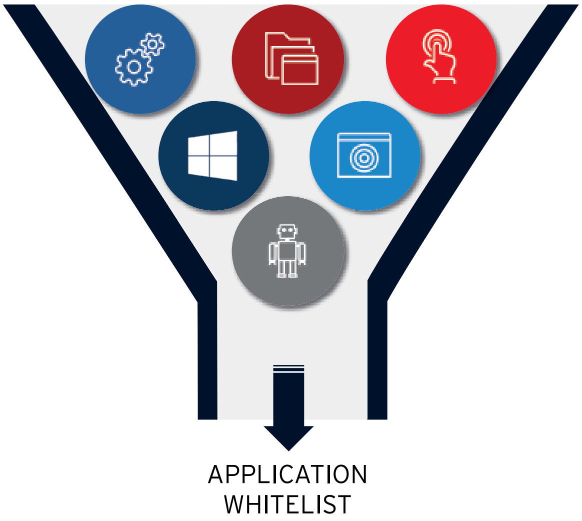
Advantages of application control

- ✚ PROTECTION AGAINST MALWARE & RANSOMWARE
- ✚ MINIMAL ADMINISTRATIVE EFFORT
- ✚ AUTOMATIC LEARNING OF WHITELISTS
- ✚ SELF-SERVICE FOR END USERS
- ✚ COMPLIANCE WITH LEGAL REQUIREMENTS
- ✚ SECURE PROTECTION FOR OLDER SYSTEMS
- ✚ CENTRALIZED MANAGEMENT

Cyber Threats - Status Quo

- ✚ DIGITIZATION MAKES COMPANY BORDERS DISAPPEAR
- ✚ MORE THAN 50% OF ALL COMPANIES ARE THE TARGET OF AN ATTACK
- ✚ Ø CONSEQUENTIAL COSTS OF AN ATTACK: 3.9 MILLION €
- ✚ TOO LITTLE SKILLED PERSONNEL
- ✚ INSIDER ACTIONS OR EXTERNAL ATTACKS

Maintenance of the whitelist



Predictive Whitelisting

Algorithmic-based, automatic approval based on the manufacturer certificates

Central Rules

Specification of central rules using different rule types

Operating System

Automatic approval of system components and Windows updates

Temporary Unlock

Manual software installation with activated learning mode

Trusted Sources

Sources like “Admin shares" or the local cache of the software distribution agent

Trusted Processes

Automatic software and patch installation

APPLICATION WHITELIST

Advantages of the DriveLock Application Control through intelligent whitelisting

The approach using static blacklists or whitelists only works to a limited extent in the rapidly changing threat situation and often requires a disproportionate maintenance effort. "Predictive" whitelisting reduces the maintenance overhead.

At the time of a DriveLock installation, the system is "sealed". As of now, there are only defined and configured ways in which changes to the whitelist are self-learning. The automated learning of the whitelist always ensures the security standard by preventing the implementation and execution of unknown applications.

Safe and productive

For unknown applications, DriveLock provides several ways for users to be notified and take control. Depending on the security settings, users are only informed, or they can determine themselves how the system should behave. This gives IT departments the opportunity to hand over responsibility to the end users. The IT managers then check which applications have been installed and started through self-approval from a central point.

Test in simulation mode

Before you start blocking applications, you can use the simulation mode to pre-test your rules and determine which applications will be blocked. During the simulation, DriveLock generates event messages for started or blocked applications according to your rules. However, the execution itself is not prevented thereby. This mode is ideal for a step-by-step introduction into production environments.

Rule Types

- MANUFACTURER CERTIFICATES
- FILE-OWNER
- APPLICATION-HASH VALUES
- TRUSTED SOURCES
- RULES FOR OS COMPONENTS, UPDATES, .NET FRAMEWORK ETC.
- WHITELIST AND BLACKLIST OF ANY SCRIPTS AND MSI PACKAGES
- APPROVAL BY USER

DriveLock - Features

- SIMULATION MODE
- AUDIT ONLY DETECTS POTENTIAL VERSIONS
- WHITELIST / BLACKLIST / OR COMBINATION
- DLL AND SCRIPT CONTROL
- CUSTOMIZED USER NOTIFICATIONS
- CENTRALIZED DASHBOARD

DriveLock: Expert for 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.