DriveLock
securing your digital tomorrow

DriveLock Application Control

Whitepaper

Content

Effective protection for your company

In times of digital transformation, your success depends on how you can reliably protect people, businesses and services from cyber-attacks and the loss of valuable data.

Application control is an essential part of endpoint security, and a challenge where security policies on the one hand and user requirements in an office environment on the other hand usually do not harmonise. Some IT departments completely block endpoint devices from installing new software, updates, etc. to avoid licensing and compliance conflicts and for security reasons. This can be very annoying for users, as uncritical but useful tools may not be installed, and thus hinder efficient work. In addition, numerous requests for the installation of certain applications can quickly lead to an overload of the IT support. The same applies in the industrial environment for time-critical updates. Complete blocking is therefore inefficient in many cases and appropriate flexible procedures with an exception handling mechanism need to be found.

The threat landscape

What are the current and very acute challenges we are all facing? Let us first take a look at the current threat situation.

- Many companies complain that they do **not** have enough **qualified personnel** to operate a sufficient security strategy. IT departments are overwhelmed or do not have the necessary skills.
- Many violations are either the direct result of **insider actions** (malicious or unintentional) or of **external attackers** using compromised user data or negligent user interactions to gain access to the company.
- Digitisation and digital transformation have caused the original **boundaries of the company to disappear**. Users and services connect from virtually anywhere. A digital company lives wherever customers, employees and partners connect and interact with data and services.
- New legal **regulations** such as the GDPR increase the pressure to act.

And it does not just affect the big companies. Hospitals are being targeted, just like industrial plants and other sectors. The consequences of business interruptions cause monetary damage and companies suffer from the lost reputation.

Surveys have shown that more than 50 % of ALL companies have been the target of an attack, medium-sized companies are particularly affected.

Let's take a look at the approach of the attackers and the different attack vectors

- The number of attacks is continuously increasing. And attackers are becoming more and more targeted, demanding and tricky.
- For example, they specifically exploit the human factor by designing phishing mails as deceptively real emails, but also by using malware or the principle of social engineering.
- USB sticks and removable storage devices are still one of the most common sources of malware infections.
- In 2019 alone, there were more than 1 billion different malware and ransomware, some with devastating consequences for industry and public institutions. Infected sysems are often completely encrypted, and entire networks are significantly disrupted.
- "LotL" methods, also known as "file-less malware", differ from "traditional" types of attack. Primarily no external malware is installed on the target system. Instead, attackers use administration or system tools that already exist on the target system to initiate an attack, i. e. scripts or software macros such as Powershell or MS-Office.
- In the case of an APT (advanced persistent threat), attackers proceed in a very targeted manner and may invest a lot of effort to penetrate further into the victim's local IT infrastructure after the initial intrusion into a computer.

Therefore, it is important to stop "break-ins" or at least limit the business impact of the theft of sensitive data. This is exactly our goal: We can protect your data, devices, and systems! To this end, we rely on technologies and solutions based on the Zero Trust model.

Costs for companies

In addition to the threat situation, the question arises as to the costs for companies that are subject to an attack or data breach. Cybercrime is a lucrative business, with relatively low risks compared to other forms of crime. The Ponemon Institute has prepared a management report. In 2019, the average time for a detection and containment of an infringement was 279 days. The faster a data security breach can be detected and contained after a cyber-attack, the lower the cost. The average total cost of a „Data Breach" worldwide is US$ 3.9 million, in APAC 2.6 US$ million. Unintentional data breaches due to human error and system failures are still the cause of nearly half (49 percent) of the data breaches examined in the report. Human misconduct is often through „unintentional insiders" who are compromised by phishing attacks or whose devices can be infected or lost/stolen.

$3.9 M ($4.8M Germany)
Average total cost of data breaches

279 Days
Time to identify and contain a breach
(MTTD 206, MTTR 73)

+27 % ($4.45M vs. $3.5M)
Breaches caused by a malicious attack were more costly than breaches caused by human error

51 %
Malicious attacks were the most common and most expensive root cause of breaches

Application Whitelisting - the most effective protection against all types of file-based malware

We need a holistic and multi-layered protection. Fundamentally, a firewall and antivirus software are not problematic, but they are only part of the whole and needs more security checks. The problem with antivirus software is that only known malware is detected. But malware disguises itself or is not yet known to the AV at the time of an attack. AV also does not protect against zero-day exploits and LotL attacks.

The standard application control enables administrators to control the execution of any application on computers. Different rules or strategies can be used to determine which applications are executed and which are blocked. This release or lock can be defined using various criteria and rule types:

- Application hash databases
- Manufacturer Certificate Rules (Digital Signature e.g. Microsoft Windows)
- File Owner Rules (NTFS permissions)
- Hash rules (Application Hash Database)
- Trusted Updater Rules
- File name and path rules (e.g. .exe/.dll/.msi)
- Special rules (allow all OS components, updates, .net framework etc.)
- User Approval/Local Authority (Privilege elevation)
- Predictive Whitelisting (more on this below)

The flexibility to combine both blacklist and whitelist rules makes application control both easy to use and powerful as a security tool.

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. It is based on a „Zero Trust" principle, which essentially denies everything and only allows what is necessary. Given the fact that blacklists are limited to known patterns (documented malware, etc.) and that malware variants constantly bypass behavioural or signature-based detection modes, many people believe that whitelisting is the more sensible approach to information security. From a security point of view, it makes more sense to first ban everything across the board and then allow specific applications and scripts. If only approved software is allowed to run, the chances of malware taking over the system are minimised.

DriveLock lets you take advantage of the best of both worlds - blacklisting and whitelisting. On the one hand, you will only approve the software, software libraries and scripts that are needed for productive work. On the other hand, you can blacklist built-in tools that are abused by offenders or restrict their use to certain administrative users. The configuration for Application Control is managed centrally in DriveLock policies and can be assigned to all computers or only to certain groups, or it can be restricted to groups of people. You are always in control.

Operating Modes

The application control can be operated in different modes.

- **Audit only - Before a rollout, the AC can be operated in an audit-only mode. Here, only applications which actually started are logged. No restriction is made.**
- **Simulation mode - If white or blacklists exist, the application controller is only simulated. All messages and events appear, but the execution of an application is not prevented. This is for a better evaluation, and administrators can get better familiarised with the rule code before arming it.**
- **Whitelist/Blacklist/or combination of both.**
- **DLL control - Not only for executable files, but also for program files.**
- **Script control - it is also possible to define rules for scripts and other files and file types.**

Prioritisation of rules

When we are in a mode, there must also be a prioritisation of rules. In a whitelist mode, a blacklist rule always takes precedence. This must be the case, because if, for example, a path rule says that everything is allowed under C:\Windows, then there must be the possibility to explicitly forbid certain files or subfolders. In blacklist mode this works exactly the other way round. In addition, all rules in the policies also follow a prioritised order, so that the specifications can be precisely mapped in the enterprise environment.

Application Control with intelligent whitelisting

Application Control plays a decisive role in the security strategy. The conventional approach with static blacklists or whitelists only works to a limited extent in the rapidly changing situation and administrators often complain about the disproportionate maintenance effort. In contrast, DriveLock's „predictive" whitelisting keeps the effort of whitelist maintenance to a minimum and ensures security standards by automating whitelist learning, preventing the implementation and execution of unknown applications. This prevents cyber-attacks caused by any type of file-based and file-less malware, including ransomware or APTs. To minimise the administrative effort, it is possible to approve all existing applications. For this purpose, the „local" whitelist must be activated. You can limit the learning process to certain directories if you wish. The DriveLock Operations Center provides an overview and thus control over the latest additions to the local whitelist at any time.

Integrate your software deployment agent with DriveLock Application

To simplify the application control, it is possible to integrate software distribution systems, patch management systems, and stand-alone updaters with the DriveLock application control. The agent or updater is defined as a trusted process. This means that the agent or updater can start software setups that are not on the whitelist. Files written by these setups during installation are automatically added to the local whitelist. This simplifies the maintenance of the whitelist considerably. The combination of trusted process and automatic learning allows the software deployment agent to launch previously unknown applications, such as software setups. Anything written by this or other child processes during installation will automatically be added to the local whitelist.

File repositories can be classified as trustworthy

To further simplify the application control, central or local file repositories can be classified as trusted. This can be a share where the IT department stores trusted software or a local folder, such as a software distribution agent's cache. Previously unknown software setups that are called from such a trusted source can be started in this way. All files written to the hard disk by this process or a subordinate process are automatically added to the local whitelist without any administrator intervention. Administrators can set additional permissions or restrictions. It also makes sense to limit permissions to a trusted user or user group, such as members of the IT department or an administrator group. Tasks can be divided between the central IT and responsible end users. End users can be asked for approval on the computer before a process is executed. This prevents software from being inadvertently added to the whitelist.

This response stores the local whitelist for the current user session. This will last until the user logs off or the client is restarted. This combination of a centralised IT department and the involvement of end users relieves the burden for the IT on the one hand and increases user productivity without major restrictions on the other.

Temporary unlocking of a computer with learning enabled for manual software installations

Not all software is installed via software distribution. For manual software installations, DriveLock Application Control provides the ability to temporarily unlock a computer and put the DriveLock agent into a learning mode. Define which users or user groups can use the self-service functions. It is also possible to have the learned files checked in advance before they are added to the whitelist at the end of the temporary unlock. This is a very simple way to maintain the whitelist. This does not result in any significant additional expenditure for IT administration.

All relevant changes made to the system within this „unlock" time are automatically added to the local whitelist.

Control for scripts and script interpreters

Support for scripts in addition to application whitelisting enables organisations to achieve a high level of security. DriveLock offers a holistic approach and full configurability.
You can run script files using a hash value, digital signature, path, or as the file owner. The scripts and their interpreters can be extended at any time. White and blacklists can also be used for scripts, and not just for applications and DLLs.

Application control additionally reduces the attack surface

In the application permissions, you can configure what permitted applications are allowed to do, i. e. which permissions the applications are given, in which directories applications are allowed to write or which processes they are allowed to start. He control over the execution of subordinate application processes reduces your attack surface. Creating malicious child processes is a common malware strategy. Malware that misuses MS Office as an attack vector often runs VBA macros and exploits code to download and attempt to run additional payloads. However, some legitimate industry applications can also create subprocesses for good purposes, such as creating a command prompt or using PowerShell to configure registry settings.

Control over the process chain
Attackers often use native programs to compromise an endpoint device. DriveLock provides you with full control to prevent such access.

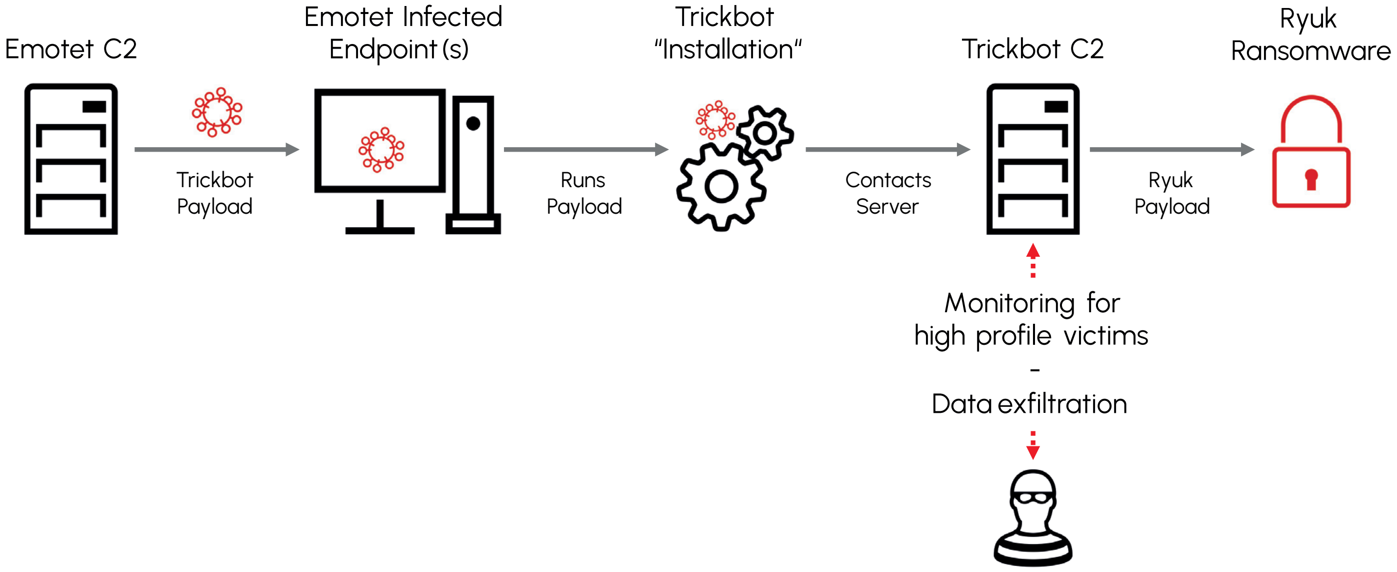
Protection of files, folders and the registry
Access to specific files, folders and registry keys can be restricted or logged. This protects the file and system integrity.

Skripts and interpreters under control
Skripts and Interpretes can be defined generically, Thus, the solution can be extended at any time. If required, scripts can be released via whitelisting.

A closer look at Emotet & LockBit

Despite the dismantling of Emotet's infrastructure in 2021, similar approaches of targeted attacks (Advanced Persistent Threads) can still be expected. Originally **Emotet** was a banking Trojan. Emotet can now also be used as a "downloader" or „dropper", whose primary function is to infect the victim's system unnoticed and to reload further malicious software in a modular fashion. This is done by means of e-mails with a Word file attached or a link which, when clicked, establishes a connection to the Internet. This will attempt to download a file in the Word format. By opening the document and activating the macro function, the code embedded in the document leads to the execution of a command line code (Powershell) and the download of the actual Emotet malware for installation on the target system. The computer is then under the control of the perpetrators. Even in its basic version, the Emotet malware can execute some criminal activities without additional modules: Downloader, Espionage, Keylogger, DDoS, Ryuk, Dridex, Trickbot, UmbreCrypt. Due to constant modification, the malicious programs are usually initially not detected by common virus protection programs. According to the BSI once infected systems are to be regarded as completely compromised, they must be rebuilt.

The example of Emotet shows the extent to which the application areas of a particular malware can vary over time.



One of the latest threats is called LockBit Ransomware. This Trojan is able to block all data on a compromised system very quickly and to extort ransom money. The starting point is usually an e-mail that encourages you to execute an attachment. However, this is usually a macro file that infects the target system when executed. The attackers try to hide their activities by making them look like normal, automated administrative tasks and using legitimate tools. For camouflage, PowerShell files are renamed, for example. In addition, the built-in anti-malware protection is modified so that it can no longer function.

A further characteristic is that the camouflaged tools automatically search for specific business applications, such as tax or accounting software, that are vital for smaller companies in their daily business. Then the actual LockBit attack is started: This renames files to the file extension .abcd and locks them. After the encryption process, a ransom note „Restore-My-Files.txt" is stored in each affected folder. It prompts to make payment of a ransom, preferably in Bitcoin.

Application authorisations control the application behaviour

The purpose of application permissions is to provide enhanced anti-malware capabilities and better prevention against possible application whitelist bypassing. They offer better protection against the already mentioned „fileless" (LotL) attacks. These rules can also block the call of certain subordinate processes. They can further restrict legitimate programs (which are on the whitelist) to actually required actions and permissions, making it even more difficult for attackers. This ensures that only authorised software and scripts are executed. They also control access to scripting tools like MS PowerShell, VBS, Python and the command line.

The application authorisations offer the following advantages:

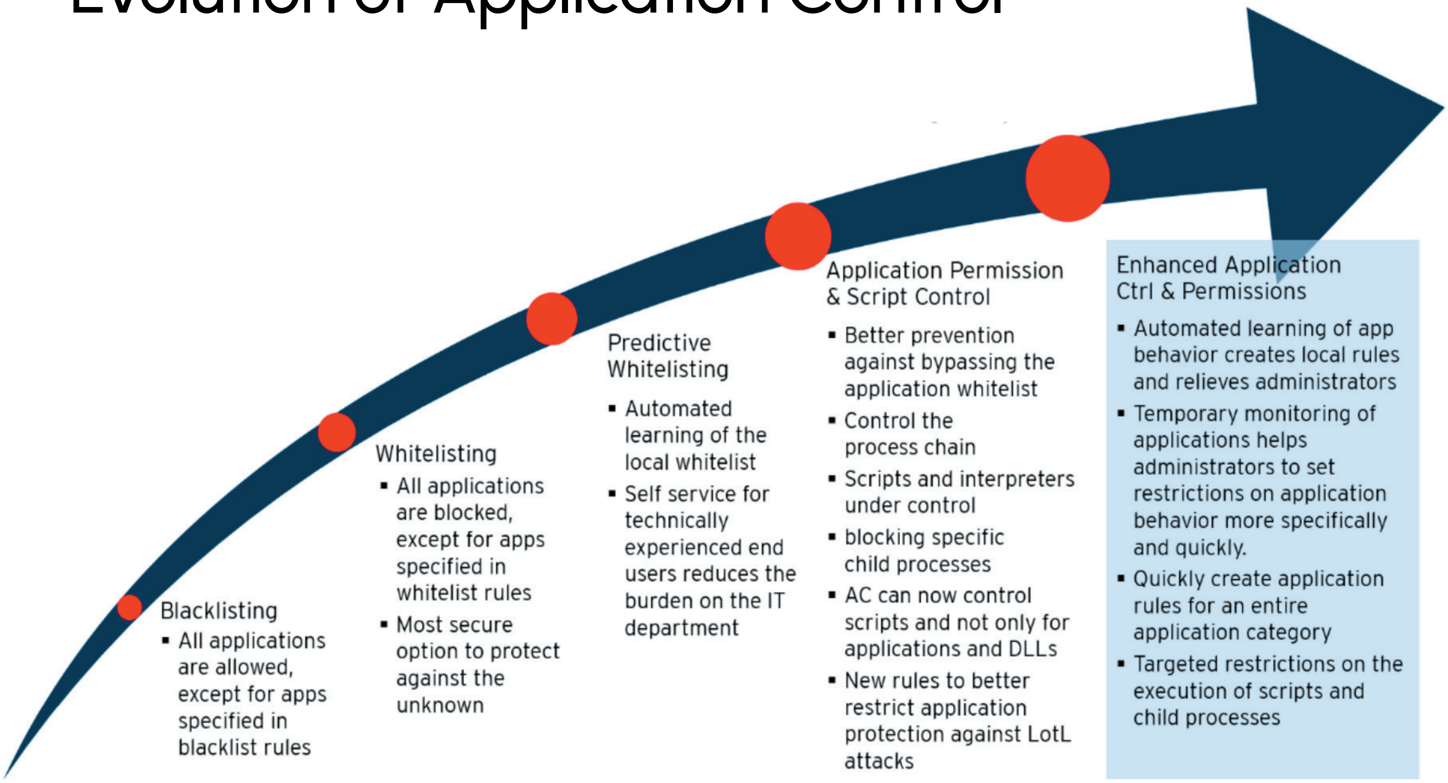
- They prevent another application (or process, script) from being started from a permitted application that could pose a potential threat to the system.
- They define what type of access is allowed to a specific application (e.g. read or write access to files or access to the registry).

The following functions, among others, are available for this purpose:

- You can specify the action to be taken if access is made by a specific application (e.g. the application is blocked or not).
- You can determine whether an application authorisation should be inherited by subordinate processes.
- Various file and directory filters can be specified.
- Script types can be specified that may be used when executing scripts.
- It can be defined which application is allowed to read or write to the registry.
- A set of rules in which order application authorisations are processed.
- The combination of rules: e.g. a rule that allows the browser to start Windows Media Player (high priority) and another rule that forbids the browser to start other programs (low priority).
- Inheritance of file permissions to called processes that start other processes or scripts. This prevents permissions from being circumvented by starting other processes.

To greatly simplify administration and to relieve the burden on IT departments, the correct application behaviour can be learned automatically. For this purpose, applications are observed over a certain period of time and this behaviour is either adopted as central policies or noted for the computer as with a local whitelist. After that, the application may only perform operations that have been successfully learned.

Evolution of Application Control



Blacklisting

- All applications are allowed, except for apps specified in blacklist rules

Whitelisting

- All applications are blocked, except for apps specified in whitelist rules
- Most secure option to protect against the unknown

Predictive Whitelisting

- Automated learning of the local whitelist
- Self service for technically experienced end users reduces the burden on the IT department

Application Permission & Script Control

- Better prevention against bypassing the application whitelist
- Control the process chain
- Scripts and interpreters under control
- blocking specific child processes
- AC can now control scripts and not only for applications and DLLs
- New rules to better restrict application protection against LotL attacks

Enhanced Application Ctrl & Permissions

- Automated learning of app behavior creates local rules and relieves administrators
- Temporary monitoring of applications helps administrators to set restrictions on application behavior more specifically and quickly.
- Quickly create application rules for an entire application category
- Targeted restrictions on the execution of scripts and child processes

Use cases

In addition to the Emotet scenario described above, there are a number of general use cases that illustrate how application control and permissions work.

1

Preventing the PowerShell from starting - scenario:
You want to prevent PowerShell from starting when you use a browser, and you want to prevent malware from being installed on your computers. Because you want to prevent the browser from calling up Powershell.exe from the command line (cmd.exe) (this is a child process), blocking call-ups to child processes can be inherited.

2

Restricting the loading of a DLL - Scenario:
You want to specify that DLLs may only be loaded from certain directories. In this specific case, Windows Media Player should be prevented from loading DLLs from network drives.

3

Script execution - scenario:
You want to prevent VB scripts (*.vbs) from being executed by browsers.

4

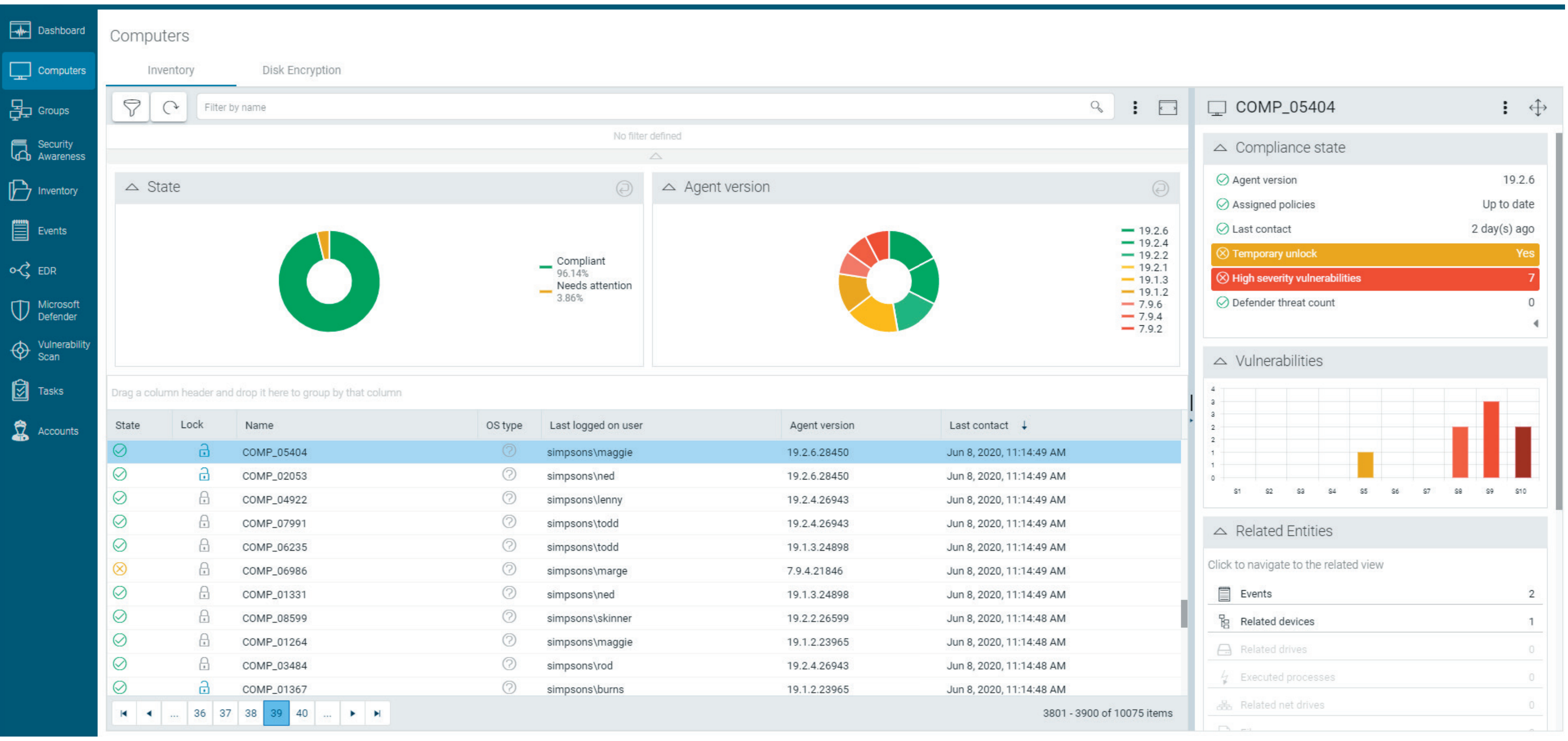
Reading of a specific directory - scenario:
You want to ensure that only a specific application has read access to a specific directory, and no other application should have read access to this directory. Due to a security gap in the browser, it is possible that malicious software could gain read access to this directory and thus read your bank data. This must be prevented. You create two application authorisations: With the first one you allow (=not block) the software access to the directory. For the second, you specify the placeholder * as the executing application so that no other application can access (=block) the specified directory. With regard to priorities, „Do not block before blocking" applies.

More visibility within the company

The DriveLock Operations Center - DOC for short - is a modern web console for management and visualisation. The dashboards provide all the information for administrators, help desk, and IT staff. It simplifies and optimises the necessary management tasks in daily operations. The DOC is available for both our DriveLock Managed Services and on-premise customers.

For application control, the console provides a comprehensive dashboard as well as an overview that gives administrators a clear visibility into the enterprise environment:

- **all computers that have application control enabled**
- **status of learning behaviour, applications in the whitelist, and what was the trigger for their inclusion**
- **blocked applications per computer and which ones were blocked in total**



State	Lock	Name	OS type	Last logged on user	Agent version	Last contact ↓
✓		COMP_05404	?	simpsons\maggie	19.2.6.28450	Jun 8, 2020, 11:14:49 AM
✓		COMP_02053	?	simpsons\ned	19.2.6.28450	Jun 8, 2020, 11:14:49 AM
✓		COMP_04922	?	simpsons\lenny	19.2.4.26943	Jun 8, 2020, 11:14:49 AM
✓		COMP_07991	?	simpsons\todd	19.2.4.26943	Jun 8, 2020, 11:14:49 AM
✓		COMP_06235	?	simpsons\todd	19.1.3.24898	Jun 8, 2020, 11:14:49 AM
⊗		COMP_06986	?	simpsons\marge	7.9.4.21846	Jun 8, 2020, 11:14:49 AM
✓		COMP_01331	?	simpsons\ned	19.1.3.24898	Jun 8, 2020, 11:14:49 AM
✓		COMP_08599	?	simpsons\skinner	19.2.2.26599	Jun 8, 2020, 11:14:48 AM
✓		COMP_01264	?	simpsons\maggie	19.1.2.23965	Jun 8, 2020, 11:14:48 AM
✓		COMP_03484	?	simpsons\rod	19.2.4.26943	Jun 8, 2020, 11:14:48 AM
✓		COMP_01367	?	simpsons\burns	19.1.2.23965	Jun 8, 2020, 11:14:48 AM

3801 - 3900 of 10075 items

COMP_05404

Compliance state

✓ Agent version	19.2.6
✓ Assigned policies	Up to date
✓ Last contact	2 day(s) ago
⊗ Temporary unlock	Yes
⊗ High severity vulnerabilities	7
✓ Defender threat count	0

Vulnerabilities

Related Entities

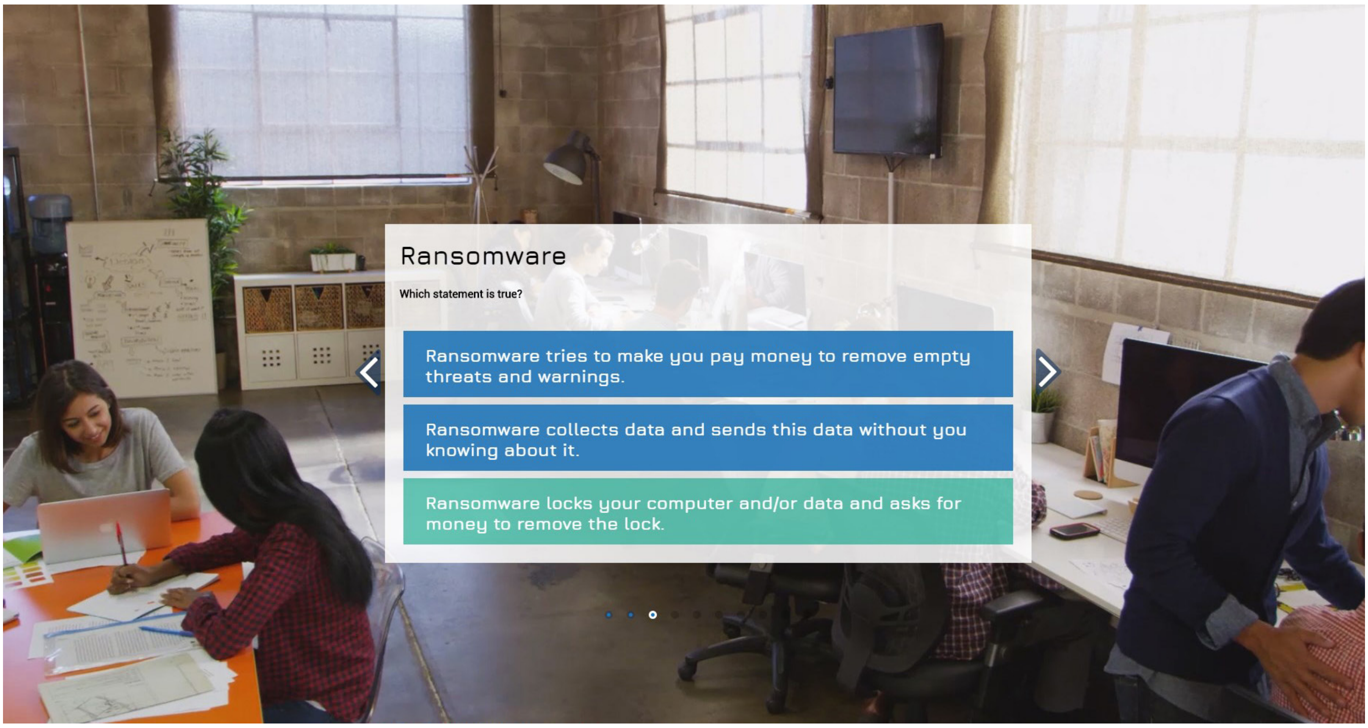
Click to navigate to the related view

Events	2
Related devices	1
Related drives	0
Executed processes	0
Related net drives	0

Reduce the potential for human error

People are often described as the weakest link in the security chain. People are cleverly deceived or manipulated, for example, to smuggle malware into company networks. This danger can be significantly reduced by targeted training measures for the employees. Such „awareness" training is effective and sustainable if it is conducted in direct temporal relation to a security-related activity. Employees can receive targeted information about the correct behaviour and necessary security measures when performing certain activities, such as inserting a USB stick or starting an application (security awareness campaigns). When users try to install an application or open attachments, try to install software on the system, these actions are blocked by the Application Control. This is exactly the right time to inform users about the risks generally associated with these activities, and to make recommendations on how to avoid such activities in the future. Through this temporal connection, the illustrated regulations will remain anchored more sustainably in people's minds. This is much more effective than security training, which must be taken during onboarding or at regular intervals (online or onsite). This means that security training is no longer perceived as unnecessary, disruptive, or annoying by the employees.

With DriveLock Security Education, your employees will become an additional firewall to protect against cyber-attacks.



Ransomware

Which statement is true?

Ransomware tries to make you pay money to remove empty threats and warnings.

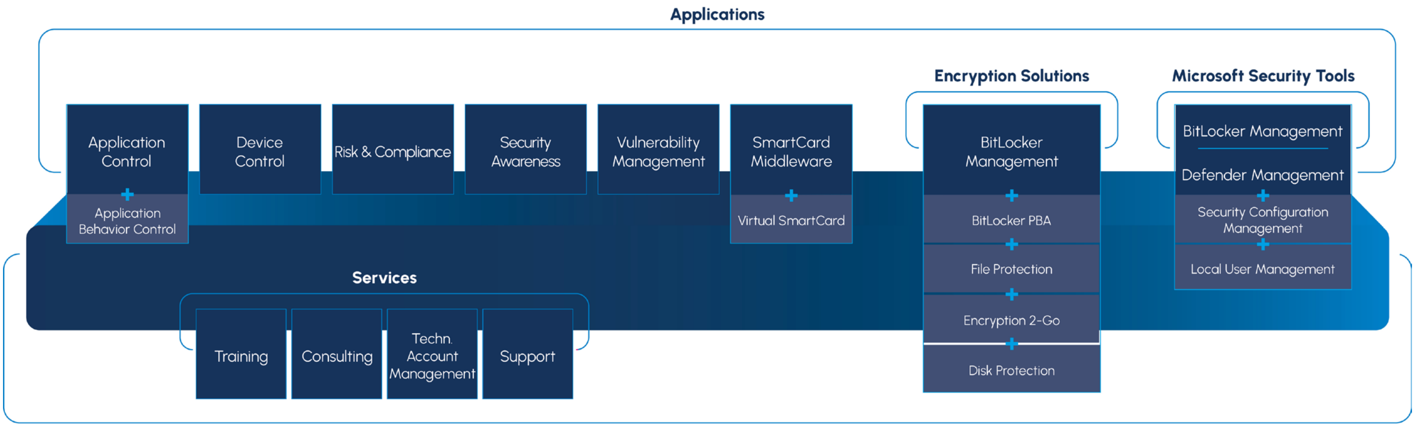
Ransomware collects data and sends this data without you knowing about it.

Ransomware locks your computer and/or data and asks for money to remove the lock.

More effective security with Zero Trust

Finally, the DriveLock Zero Trust platform comes into play. The basic idea behind Zero Trust is: A digital company has no boundaries. Now more important than ever: Employees work from home, sometimes with private computers, also with the use of mobile devices, etc. It is therefore important to establish a holistic cyber security protection for a more effective security both inside and outside the company. That is why DriveLock brings Zero Trust to the endpoint - the device you work with. DriveLock Zero Trust combines the elements of Data Protection, Endpoint Protection, Endpoint Detection & Response, and Identity & Access Management.

> **In the past, it was sufficient to maximise protection against external attacks. And that was almost the only critical security check. Today we assume that we are compromised anytime and anywhere.**



DriveLock Zero Trust Platform

DriveLock
securing your digital tomorrow

Conclusion

The demands on today's IT security solutions have increased significantly. In the course of digitalisation, issues of data protection and security within companies are becoming increasingly important. In addition, there is a growing demand for software solutions that allow the new laws and guidelines to be implemented simply and effectively.

The DriveLock solution helps companies protect their data and comply with regulatory requirements. The solution includes preventive measures to avert attacks, and thus prevent systems from becoming infected. DriveLock's Zero Trust solution platform is constantly evolving to ensure the security of sensitive data.

DriveLock is a leading international specialist for IT and data security and has been developing security software exclusively in Germany since 1999. DriveLock solutions stand for best possible endpoint protection „Made in Germany" without a backdoor.

Everything from a single source:

DriveLock offers its Endpoint Protection Solutions as a building block of a Zero Trust platform to achieve a holistic security strategy.

Contact us!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com