DriveLock Native Security Management:

Convenient and centralised management of Microsoft security functions

Microsoft BitLocker hard disk encryption, Defender Antivirus, Firewall Management and the local Security Settings in the operating system are part of a set of native security solutions that Microsoft makes available to its customers. For many companies, they are an integral part of their IT security concept. DriveLock simplifies the management of the native security solutions, adds important functions and creates real added value for more effective cyber security.

Major operating system vendors such as Microsoft have continually expanded their built-in security features. The security functions referred to as "native security" or "OS security" include security controls for data security/hard disk encryption, antivirus protection, protection against zero day exploits and firewall management. They can be managed from the operating system interface. Depending on the scope of the licence, the solutions are included with the purchase of the operating system. IT managers no longer have to rely on a multitude of solutions.

In the increasingly professional world of cyberattacks, the native security offerings not only cover important basic functions for IT security, but also generate valuable data. When processed by a professional tool, you gain additional behaviour-based protection and thus more security. This is where DriveLock comes in.

DriveLock Native Security Management

DriveLock optimises the management of native security functions and simplifies the setup of central security policies. This allows native solutions to cope with the complexity of large organisations with thousands of workstations, permissions and profiles.

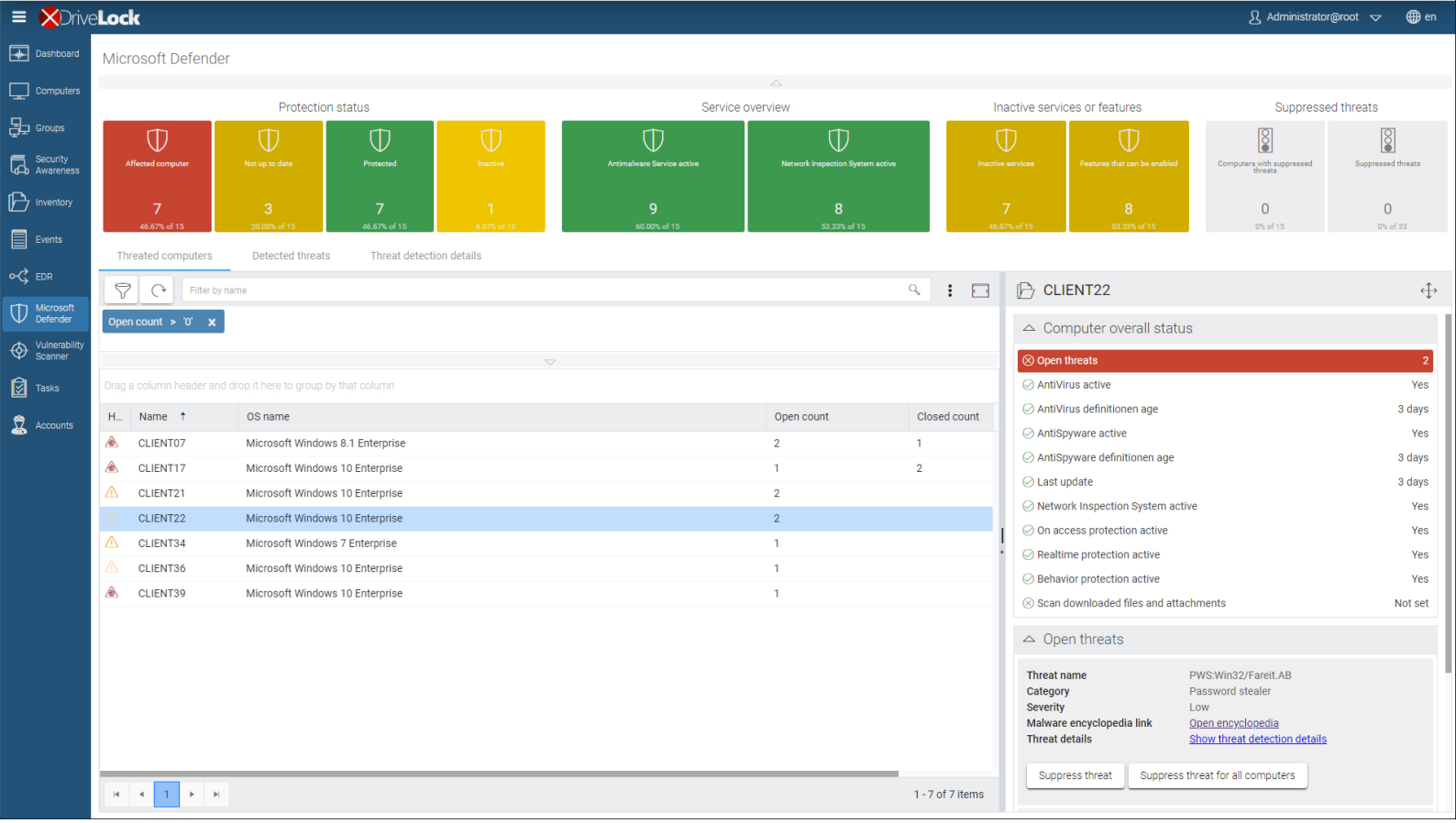
DriveLock also extends the range of functions with important features, such as Microsoft BitLocker hard disk encryption with powerful pre-boot authentication (PBA).

Advantages of DriveLock Native Security Management

- SAVES RESOURCES AND AVOIDS INCOMPATIBILITIES
- SIMPLIFIES THE CONFIGURATION OF THE MOST IMPORTANT PROTECTIVE MEASURES ANCHORED IN THE OPERATING SYSTEM FROM A CENTRAL LOCATION
- PROVIDES A HOLISTIC VIEW OF THE CURRENT LEVEL OF SECURITY ACROSS ALL PROTECTION LAYERS
- ENRICHES BEHAVIORAL ANALYSIS WITH EVENT DATA COLLECTED BY THE OPERATING SYSTEM AND COMPLETES THE COMPLIANCE OVERVIEW
- ENHANCES THE SECURITY FEATURES OFFERED BY OPERATING SYSTEM MANUFACTURERS
- ENABLES NATIVE SECURITY TO BE APPLIED AND CONTROLLED INDEPENDENTLY OF THE OS VENDORS' RESPECTIVE INFRASTRUCTURES, WHILE STILL ADAPTING INDIVIDUALLY TO THE HYBRID CUSTOMER INFRASTRUCTURE

Cyber threats - Status Quo

- 50% OF COMPANIES WORLDWIDE ARE THE TARGET OF AN ATTACK
- AVERAGE TOTAL COST OF A DATA BREACH WAS $4.24(USD) MILLION WORLDWIDE IN 2021



Additionally, native security functions generate useful information for behavioural analysis. This allows DriveLock to supplement and process its solution with security log data from the operating system. By analysing the runtime activities of applications and devices, DriveLock provides behavioural protection and can potentially detect and respond to attacks in progress.

With the Native Security Management Module, DriveLock offers centralised management via a single interface and enables IT departments to work comfortably.

Get more out of Native Security with DriveLock!

Advantage of DriveLock Native Security - Single Agent

DriveLock not only manages and monitors the Microsoft security functions centrally in a management console, but with Drivelock you only need **a single agent on the endpoint** which saves resources and avoids incompatibilities.

DriveLock enables integrated management of all modules both locally installed ("on premise") and as a managed service from the cloud.

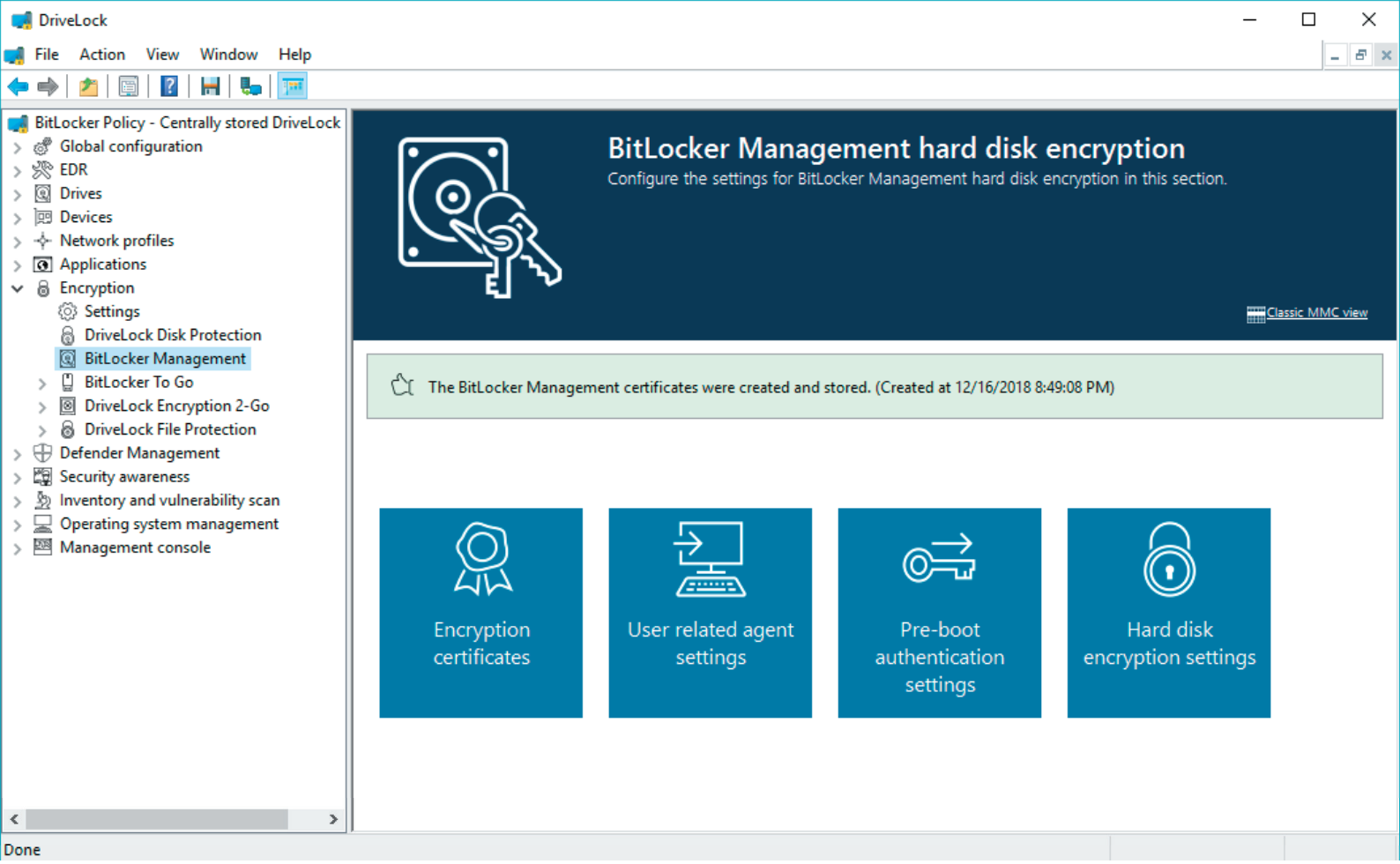
The Components of DriveLock Native Security Management

Microsoft Defender Antivirus Management

The real-time protection integrated in Windows 10, Microsoft Defender Antivirus, makes an important contribution to the detection and elimination of malware and unwanted programs. But antivirus software is only one component in a complete security solution. DriveLock makes the most of scan results, integrating Microsoft Defender Antivirus management into its Zero Trust Platform and enabling shared, convenient and centralised management along with DriveLock's prevention and detection tools. These are DriveLock Application Control, Device Control and Endpoint Detection & Response (EDR).

Advantages of DriveLock Defender Antivirus Management

- + MANAGES ALL MS DEFENDER AV SETTINGS WITHIN A DRIVELOCK POLICY CENTRALLY, EASILY AND QUICKLY WITHOUT GROUP POLICIES
- + ENABLES MANAGEMENT WITHOUT MICROSOFT INTUNE OR SCCM
- + GRANTS INSIGHT INTO THE CURRENT SECURITY SITUATION AT ANY TIME
- + VISUALISES THE CLASSIFICATION OF DETECTED MALWARE AND SHOWS STATUS CHANGES AND THREAT LEVELS OVER TIME
- + USES SCAN RESULTS FOR DRIVELOCK FUNCTIONS SUCH AS APPLICATION AND DEVICE CONTROL AND EDR
- + INTEGRATES WITH DRIVELOCK DEVICE CONTROL, SCANS EXTERNAL MEDIA PRIOR TO RELEASE AND USE
- + DRIVELOCK EDR USES THE SCAN RESULTS AS A BASIS FOR DETECTION RULES, TRIGGERS ALERTS AND TAKES RESPONSIVE ACTION.



Microsoft BitLocker Management

Hard disk encryption is an effective measure for data protection and maintaining the confidentiality of information. It is an effective prevention against data loss, manipulation or theft and is recommended by the and is recommended by national information security authorities for desktop clients and notebooks. Microsoft provides BitLocker hard disk encryption free of charge for many versions of Windows.

But with increasing regulatory requirements, this is often not enough on its own. DriveLock BitLocker Management manages your existing BitLocker installation and extends it with important functions such as one-time recovery or a central configuration of BitLocker Disk Encryption independent of Active Directory (AD). With DriveLock BitLocker Management you reduce the administration effort by a central management of all settings.

Advantages of DriveLock BitLocker Management

- ENABLES CENTRAL CONFIGURATION AND COMPANY-WIDE IMPLEMENTATION OF ENCRYPTION POLICIES
- REDUCES THE ADMINISTRATION EFFORT
- INCLUDES A COMPLIANCE DASHBOARD
- ENABLES CENTRALISED CONFIGURATION INDEPENDENT OF ACTIVE DIRECTORY
- PROVIDES SECURE ONE-TIME RECOVERY WITH AUTOMATIC KEY EXCHANGE
- OFFERS A POWERFUL PRE-BOOT AUTHENTICATION: DRIVELOCK PBA FOR BITLOCKER. THIS ENABLES, AMONG OTHER THINGS, FURTHER AUTHENTICATION METHODS AND EMERGENCY LOGON

Simplified Firewall Rule Management

Microsoft Firewall aims to be at the forefront of closing primary gateways for criminals, including enabling or disabling port shares. DriveLock gives you even more control over the management of Microsoft Defender firewall rules. With DriveLock policies, you can easily control incoming and outgoing connections. In addition, the firewall rules can be linked to criteria such as time, network connection, computer or user in the DriveLock Policy.

Local Users & Groups Management

In particular, the local accounts and groups predefined in the operating system are the target of attackers. The purpose of this integration in DriveLock is to protect against so-called "privilege escalation" attacks that attempt to access or take over existing accounts with administrative rights. You can additionally protect these accounts with DriveLock. Both the password of the administrator account and its name can be randomly assigned on a daily basis.

Manage your local users and groups with DriveLock. Each local account on a single computer can be created, updated or deleted. Password settings are also possible. The DriveLock Agent stores each password securely encrypted, so working with a „run as" command line is still possible. Based on rules, settings can be changed automatically when a user moves from the home office to the corporate network and vice versa.

Advantages of DriveLock Firewall Management

- + MANAGES ALL LOCAL WINDOWS FIREWALL SETTINGS SIMPLY AND CENTRALLY
- + TAKES ADVANTAGE OF DRIVELOCK POLICIES TO RESPOND FLEXIBLY TO COMPANY-SPECIFIC SECURITY REQUIREMENTS
- + DRIVELOCK RULES ALLOW YOU TO DYNAMICALLY ADJUST FIREWALL SETTINGS ON THE FLY BASED ON CURRENT USERS, GROUPS, COMPUTERS OR TIME.

Advantages of DriveLock Local Users & Groups Management

- + THIS VERY EFFECTIVE METHOD SECURES YOUR WORKPLACE EVEN BETTER.
- + PROTECTS AGAINST "PRIVILEGE ESCALATION"
- + CENTRAL MANAGEMENT OF ALL LOCAL ACCOUNTS AND GROUPS ON EACH COMPUTER
- + AUTOMATIC ACTIVATION OR DEACTIVATION OF ACCOUNTS ON THE OPERATING SYSTEM
- + RANDOM PASSWORD CHANGE OF ACCOUNTS
- + "RUN AS" COMMAND LINE IN AN EVEN MORE SECURE AND CONVENIENT WAY
- + AUTOMATIC CHANGE OF SETTINGS DEPENDING ON WHETHER YOU ARE ON THE LAN OR AT HOME

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 • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com