DriveLock
securing your digital tomorrow

DriveLock Native Security Management Get the Most Out of Microsoft Security Features* with DriveLock

eBook

* BitLocker, Defender Antivirus, Firewall Management, Local Users & Groups Management

DriveLock
securing your digital tomorrow

Contents

DriveLock
securing your digital tomorrow

1. From Native Security to Comprehensive IT Security with DriveLock: A Small Step for You, a Big One for Your Endpoint Security!

BitLocker hard disk encryption, Defender antivirus 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, these are an integral part of their IT security concept: each solution creates an extra hurdle that attackers have to overcome. The goal is to make the work of cyber criminals as difficult as possible.

With the increase in security tools, the complexity for administrators and information security officers has also grown. Security policies, profiles and authorisations need to be managed effectively. In other words: the more tools, and end devices and users there are, the more complex it will become.

With the motto "IT security made easy", we, as endpoint security specialists, set ourselves the goal of getting more out of native security solutions. DriveLock optimises its administration and enables the setting up of central security policies. In this way, the solutions also meet the complexity of large companies with thousands of workstations, authorisations and profiles. Administrators manage the security functions **centrally in a management console with a single agent**.

However, DriveLock not only optimises the management of the native security solutions, but also complements them with important functions and creates real added value by combining the data collected from the operating systems using DriveLock - resulting in added security.

DriveLock gives your Microsoft Security Tools a full boost!
Test DriveLock free of charge and without obligation at
https://www.drivelock.com/drivelock-managed-security-services-free-trial

2. Why We Can Get Even More Out of Operating System Tool

What is Native Security?

The major operating system vendors such as Microsoft have continuously improved their inbuilt security features. The security functions referred to as "Native Security" or "Native 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. This, of course, frees decision-makers from having to purchase a multitude of solutions and has the advantage that these solutions are included with the purchase of the operating system. Many corporate IT security professionals are planning to increase the use of native security tools as part of their IT security strategy.

We Mine Your Data Treasures and Enrich Native Security Functions

Native security offerings cover important basic IT security functions and provide valuable data in the increasingly professional world of cyberattacks. Threat intelligence solutions, such as the DriveLock Zero Trust Platform, further process the security log data collected by the operating system. They extend the native IT protection functions with behavior-based protection, in particular by analysing the runtime activities of applications and devices, and thus provides greater levels of security.

The DriveLock Zero Trust Platform, together with the data collected from native security controls, further protects your environment from cyber-attacks and alerts you to potential attacks that are currently in progress. Accordingly, DriveLock advantageously complements its own functionality with that of Native Security to provide optimal protection. With the Native Security Management Module, DriveLock provides centralised management through a single interface, enabling IT departments to work more comfortably. **Give Native Security an added boost!**

DriveLock
securing your digital tomorrow

3. DriveLock Strengthens Native Security Functionalities

DriveLock makes the most of native and proprietary security features. DriveLock bundles the respective strengths of native security controls and supports them ideally in interaction. In addition, DriveLock significantly improves the protection level of endpoints through its integrated security functions, such as **device control, application white-listing or EDR**.

The advantages of DriveLock Native Security Management:

- DriveLock simplifies the configuration of the most important protective measures anchored in the operating system from a central location.
- DriveLock provides a holistic view of the current security level across all protections.
- DriveLock enriches the behavioral analysis with event data collected by the operating system and completes the compliance overview.
- DriveLock enriches the security features offered by operating system manufacturers.
- DriveLock enables the application and control of native security independent of the respective infrastructure of the OS manufacturers and yet adapts individually to the hybrid customer infrastructure with different end devices

With Drivelock, you only need a single agent at the endpoint:
You manage and monitor the Microsoft security functions **centrally from one management console.**
This saves resources and avoids incompatibilities.

DriveLock enables integrated management of native security both **on premise** and **in the cloud**.

4. The Modules of DriveLock Native Security Management

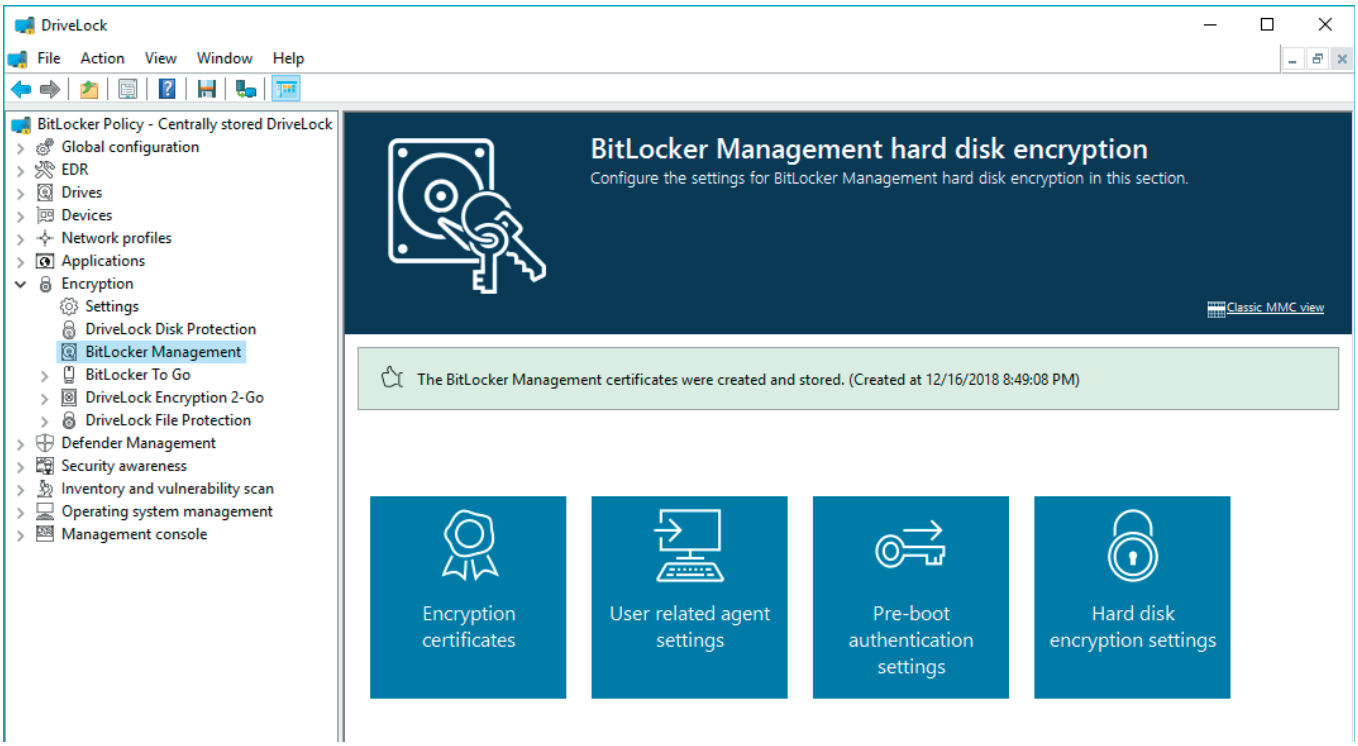
4.1 BitLocker Management

Hard disk encryption is an effective measure for data protection and maintaining the confidentiality of information. It is the simplest prevention against data loss, manipulation or theft and is recommended by regulatory authorities, especially for desktop clients and notebooks. Microsoft provides BitLocker hard disk encryption free of charge for many versions of Windows. But with increasing regulatory requirements, it is often not sufficient by itself.

DriveLock BitLocker Management manages your existing BitLocker installation and extends it with important functions. This way, you reduce the administration effort by centrally managing all settings.

The advantages of DriveLock BitLocker Management:

- enables central configuration and company-wide implementation of encryption policies
- reduces administration effort
- encludes 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



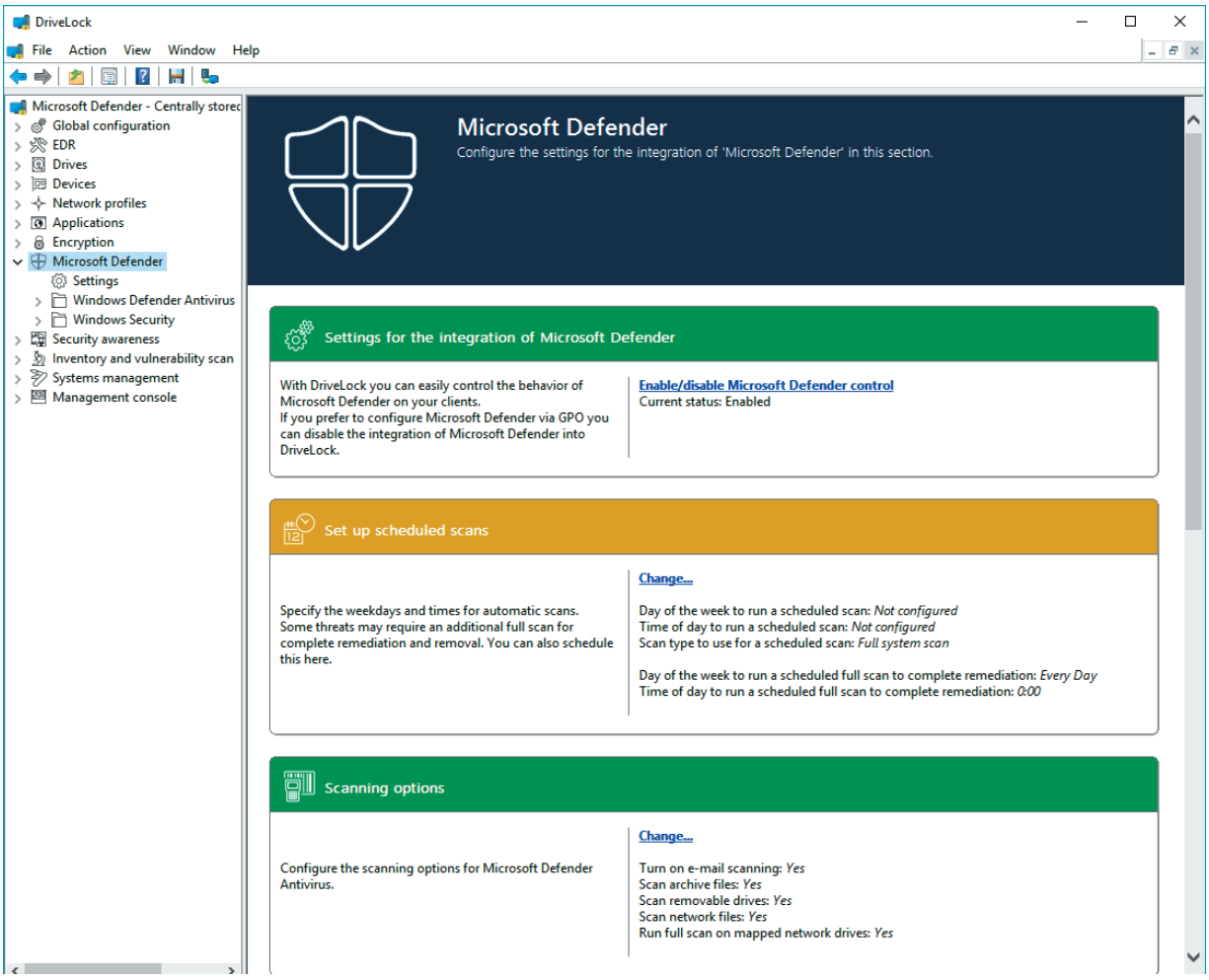
4.2 Defender Antivirus Management

The real-time protection Microsoft Defender Antivirus preinstalled on Windows 10 makes an important contribution to the detection and elimination of malware and unwanted programs. But virus scanning is only one component in a complete security solution.

DriveLock integrates the management of Microsoft Defender Antivirus into its Zero Trust Platform and enables a common, convenient central management of the DriveLock prevention tools **Application Control**, **Device Control** and **EDR** (Endpoint Detection & Response) with Microsoft Defender Antivirus.

The advantages of DriveLock Defender Antivirus Management:

- entral policy-driven configuration
- scans externally connected drives for threats before unlocking them
- grovides insight into the current security situation at any time
- visualises the classification of detected malware
- shows status changes and threat levels over time
- reuse of scan results and use for other DriveLock functions such as EDR



4.3 Firewall 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 even user in the DriveLock Policy.

The advantages of DriveLock Firewall Management:

- manages all 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.

4.4 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 is to protect against so-called "privilege escalation" attacks, which attempt to access or take over existing accounts with administrative rights. You can additionally protect these accounts with DriveLock by, for example, randomly changing the password of the "Administrator" account or even the name on a daily basis.

The advantages of DriveLock Local Users & Groups Management:

- effective protection against "privilege escalation"
- central management of all local accounts and groups on each endpoint
- 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
- automated change of settings depending on whether you are on the LAN or at home

5. Conclusion: DriveLock and Native Security - A Perfect Combination

Native and DriveLock services are compatible with each other. With DriveLock, we create added value for our users by offering all services from a single user interface, using a single agent.

DriveLock's mission is to protect corporate data, devices and systems. To achieve this, we rely on technologies and solutions based on the Zero Trust model. DriveLock brings Zero Trust to endpoints. The fully integrated Zero Trust Platform supports multiple operating systems and endpoints and is offered as both an on-premise solution and a cloud managed security service.

The DriveLock Zero Trust Platform combines the elements of:

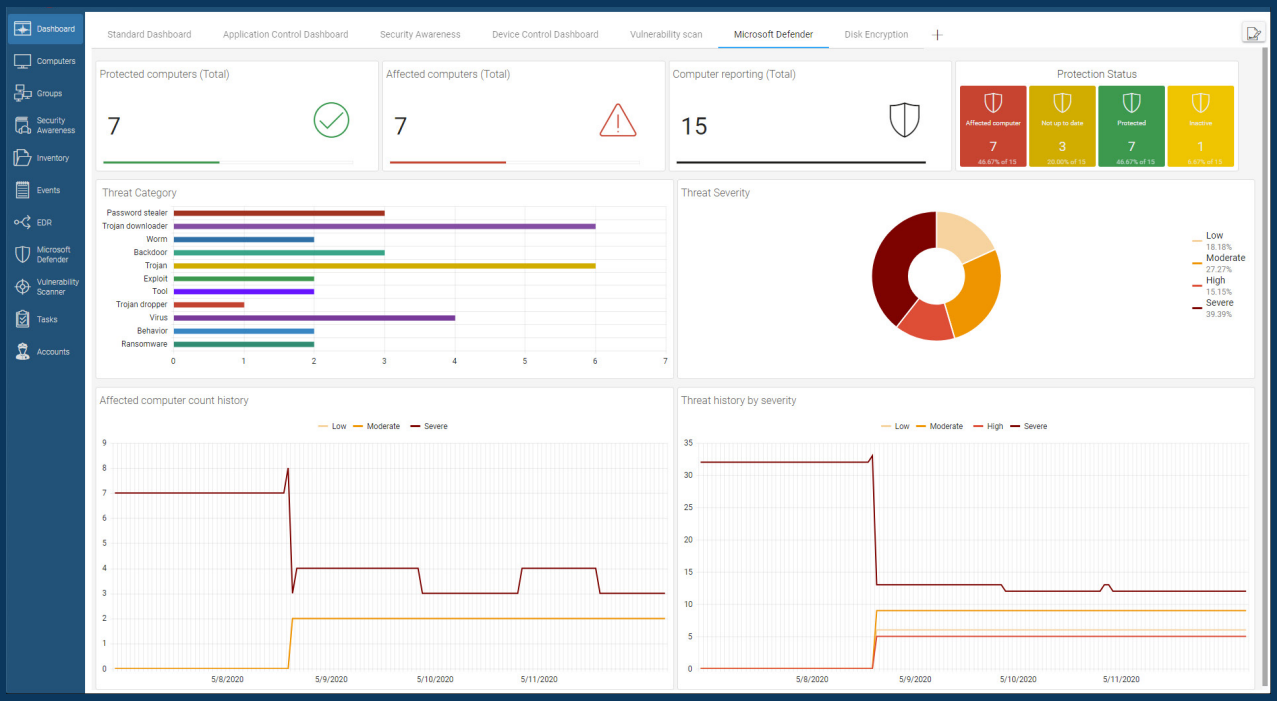
- Data Protection
- Endpoint Protection
- Endpoint Detection & Response and
- Identity & Access Management

We offer holistic protection by means of various modules, including:

- Hard disk or removable media encryption to protect data from stolen or lost laptops and removable media
- Application control to protect against Zero Day attacks and fileless "living off the land" attacks
- Device con trol offers protection against malware and thus also against data theft.
- Security awareness training strengthens your human firewall and integrates users into the security strategy
- Integrated BitLocker & Defender Management - Integrated management of native Microsoft OS security (Bitlocker + PBA, MS Defender and MS Firewall, Privilege Escalation Prevention)
- Integrated EDR solution aligned with the MITRE ATT&CK® framework

Furthermore, DriveLock also offers:

- Uniform interface for configuring all protective functions/modules/protective measures - DriveLock Management Console (DMC)



- Web-based and customisable interface with extensive evaluation and analysis options - DriveLock Operations Center (DOC)

We support multiple environments, including both fat clients and virtual environments.

Contact us!

DriveLock SE

+49 (89) 546 36 49-0

info@drivelock.com

www.drivelock.com