Management of Microsoft Defender Antivirus

More than just a Microsoft antivirus scanner configuration

convenient - integrative - holistically secure

- Centralised configuration for all prevention tools via the DriveLock management console eliminates the need for additional management solutions such as Microsoft Intune or SCCM.
- Defender settings can be tailored to the security features of DriveLock application control.
- All Defender AV settings can be easily and quickly configured within a DriveLock policy, without having to distribute individual group policies.
- Via the DriveLock management console the use of external drives can be linked to the result of a Defender AV scan.
- Threats from AV scans can trigger alerts in the DriveLock Endpoint Detection & Response (EDR) solution, which will then trigger automated processes in response (launch of an information campaign, execution of scripts, etc.).
- The defender's view in the DriveLock Operations Centre meet legal obligation requirements and enables compliance reporting.

Management of Microsoft Defender Antivirus

Pre-installed in Windows 10, **Microsoft Defender Antivirus** is real-time antivirus protection developed by Microsoft to detect and remove malware and other potentially unwanted programs.

DriveLock **integrates** the Microsoft Defender Antivirus management into its Zero Trust platform and enables shared centralised management of DriveLock prevention tools - **application control, interface control, and EDR - with the Microsoft antivirus scanner.**

This allows DriveLock customers to further minimise the risk of losing data due to malware, spyware, or ransomware and manage everything from a centralised platform within DriveLock.

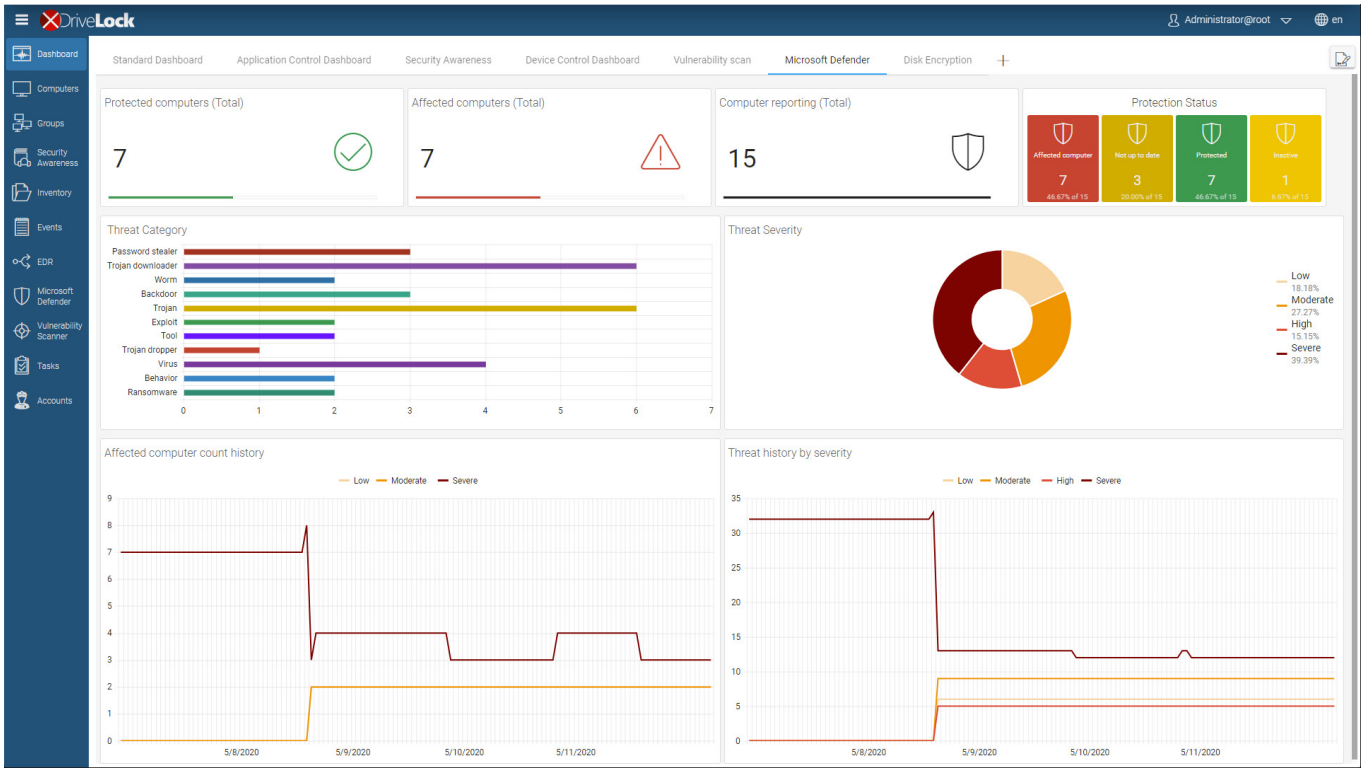
The DriveLock Management Console can be used to configure the following Windows Defender client settings using DriveLock policies:

- **Scan settings for file accesses and response options if malware is found**
- **Enable rules for file checks or processes**
- **Regular scan checks with the date, time, frequency and type of response**
- **Use of the virus scanner when connecting external drives and automatic blocking of access if malware is detected**
- **Overview of the nature and content of end-user notifications**

DriveLock EDR functions enable additional responsiveness through an integration with Microsoft Defender Antivirus. When malware is detected, **automatic processes can be enabled to** which effectively prevent further propagation, such as shutting down or isolating computers on the network.

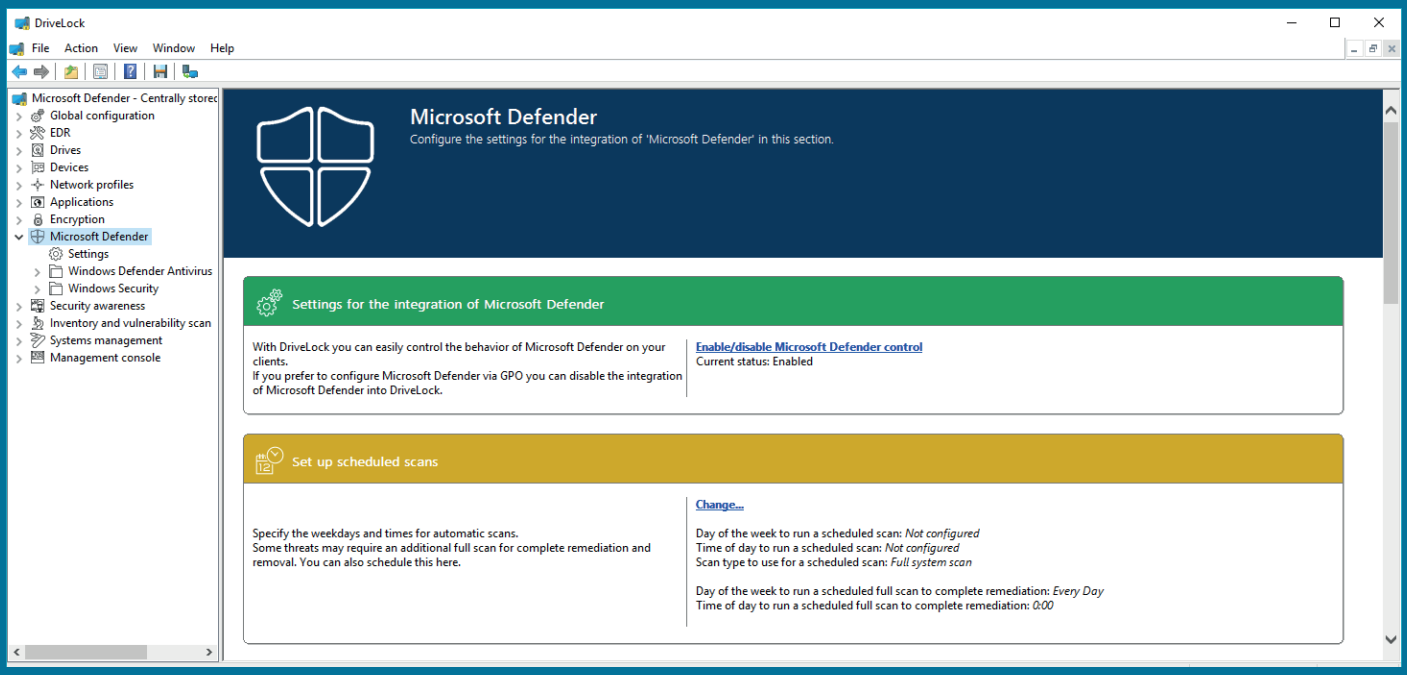
The state-of-the-art **DriveLock Operations Centre** with its own anti-virus dashboard provides a quick overview of the current protection level allows administrators not only to perform a detailed analysis of individual systems but also to perform additional activities in the event of security incidents, such as starting a complete scan, a computer or manually updating threat definitions.

An overview of detected threats, Defender security audit results, and the health of DriveLock protected computers helps managers assess and demonstrate the effectiveness of their compliance and protection measures.



Advantages of the DriveLock Microsoft Defender Management at a glance

- The configuration of DriveLock and Microsoft Defender Antivirus security settings through a single policy
- Management of the system environment using dashboards and modular overview graphics via the central and web-based DriveLock Operations Centre
- Simple configuration options



- Automatic response to detected threats, such as blocking user access or applying tighter security settings

Holistic security from a single source:
DriveLock offers Defender Antivirus Management as a building block of its Zero Trust platform to implement a comprehensive security strategy.

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