

DriveLock Antivirus combines an award-winning antivirus engine with the DriveLock Management Console for easy central management. The engine has a long, proven track record of blocking virtually any type of malware, including worms, spyware and Trojan horses.

DriveLock⁷
Intelligent Data Protection



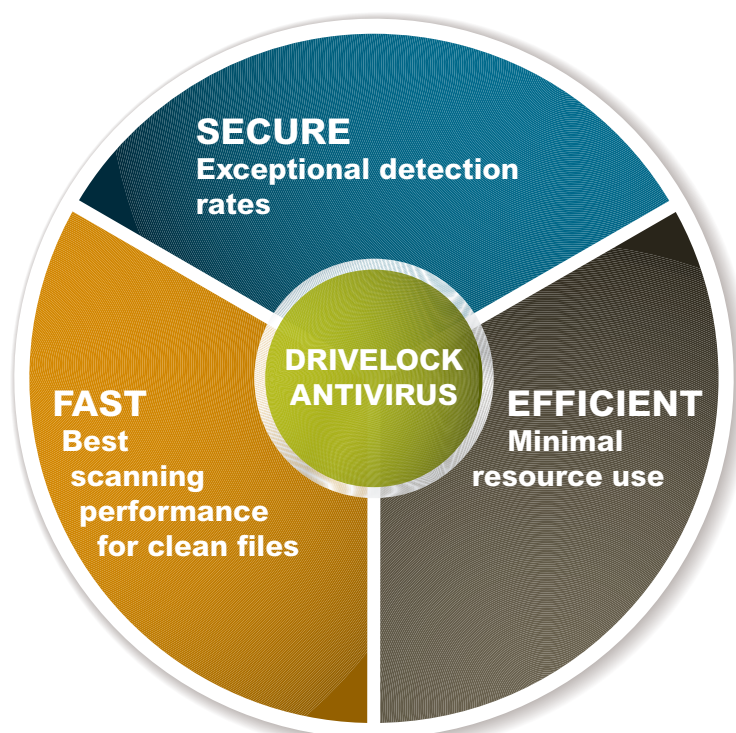
DriveLock Antivirus

Threats from viruses, spyware, Trojan horse programs and other malicious software are constantly increasing at an alarming rate. Globalization of business, which is accelerated by the Internet, creates new demands for IT infrastructures. Creating new malware is easier than ever and commercialization of malware is the latest trend. There is also an increase in the use of malware for industrial espionage, and even small and medium-sized businesses can become targets. A layered approach to protecting crucial company data is a core component of any successful security strategy that can protect against these threats. The antivirus component in DriveLock Endpoint Shield can be an important part of such a strategy by protecting desktop computers, laptops and servers from current threats.

DriveLock Antivirus monitors all data transfers on local hard disks and external media in realtime to proactively prevent the spread of viruses. In addition, DriveLock Antivirus can perform on-demand scans of all drives, external media or specific folders. Such scans can be performed on a schedule, when media is inserted or started manually by a user or administrator.

Fast – Efficient – Secure

Because the vast majority of files that are scanned by an anti-virus engine contain no malware, good scanning performance for “clean” files is one of the most important aspects of an engine. The average scanning speed of DriveLock Antivirus is over 7 MB/s. This lightning-fast performance ensures that scanning



of uninfected systems is completed quickly with minimal impact on users. **DriveLock** Antivirus also has only a minimal impact on system resources. During normal operations, realtime protection uses only 1 – 2 MB of RAM. This means that computer startup times are not impacted, there's no need to buy more RAM and the lifespan of existing hardware is extended.

In test results by AV-TEST, the Antivirus engine that is integrated into **DriveLock** consistently ranks among the top 5. In May 2011 the detection rate was 99.99%. **DriveLock** also contains a protection mechanism to protect the Endpoint Shield files and services against malicious tampering. The seamless integration with **DriveLock's** port control and application control creates intelligent, comprehensive endpoint protection that can protect endpoints even against previously unknown malware and zero day attacks. For example, **DriveLock** can block access to a flash drive until a malware scan has completed and determined that the device contains no threat.

DriveLock's antivirus engine is based on a modular framework. Specialized threat protection modules are designed to scan specific objects, such as PDF files, or to detect certain virus types, such as polymorphic viruses. This modular architecture is much more flexible than more traditional monolithic engines. It's easy to add or extend specific modules to, provide protection against new threats much more quickly and without having to update the entire engine.

Central Management and Extensive Reporting

DriveLock Antivirus is a core component of **DriveLock** Endpoint Shield. All configuration is done using the **DriveLock** Management Console. Because **DriveLock** completely integrates all endpoint security components, administrative efforts are minimized. In addition, a single maintenance contract, a single point of contact for support and competitive pricing can result in significant savings. To protect endpoints, an administrator creates central security rules that control all antivirus activities, including signature updates, scheduled scans and quarantine. Because of **DriveLock's** flexibility, it's easy to assign specific policies to selected groups or computers. For example, you can perform more frequent and thorough scans on laptops that are not currently connected to the company network. **DriveLock** can immediately and automatically

alert an administrator when a problem or infection occurs. To facilitate migration from another product, **DriveLock** can even automatically uninstall other antivirus software that may already be installed. To help with the automated deployment of malware patterns, **DriveLock** can distinguish between the production network and a staging environment. If there is ever any need to roll back to a previous **DriveLock** pattern version, this can also be accomplished quickly and easily.

The **DriveLock** Control Center provides extensive functionality for reporting and forensics while being easy to use. You can quickly view all endpoints on which malware was detected and view quarantined files on all client computers. You can also view important malware statistics and create detailed reports. The **DriveLock** Control Center also includes sophisticated forensics functionality that lets you investigate security incidents. For example, you can find out which flash drive was the source of a virus infection and where in your network this drive was used. Reporting and forensics can even include computers that are only sporadically connected to the company network.

Technical Data – System Requirements

Operating system:

Windows XP, Windows Vista, Windows 7, Windows 2003, Windows 2008 – 32-bit und 64-bit versions.

Signatures:

Incremental signature updates are only 150 KB to 300 KB. A complete pattern update, which is performed during installation, is about 28 MB. Signatures are distributed automatically. An Internet connection is required for a server running the **DriveLock** Enterprise Service.