**DriveLock Antivirus integriert eine seit fast 20 Jahren erprobte Antivirus-Engine in das zentrale DriveLock-Management. Diese mehrfach ausgezeichnete Engine blockiert jegliche Art von Malware inklusive Würmern, Spyware und Trojanern und wird von namhaften und weltweit bekannten Herstellern eingesetzt.**

DriveLock 7
Daten intelligent schützen

# DriveLock Antivirus

Weltweit steigt die Bedrohung durch Viren, Spyware, Trojaner und andere Schadsoftware in erschreckender Art und Weise an. Die durch das Internet beschleunigte Globalisierung stellt neue Anforderungen an die Sicherheit unserer IT-Systeme. Die Erstellung neuer Schadsoftware ist fast schon zum Kinderspiel geworden und wird in einem beträchtlichen Umfang kommerziell genutzt. Doch auch die Bedrohung durch Wirtschaftsspionage darf nicht unterschätzt werden, auch als kleines oder mittelständisches Unternehmen. Eine intelligente, mehrstufige Sicherheitsstrategie zum Schutz wichtiger Unternehmensdaten ist zu einem essentiellen Erfolgsfaktor geworden. Als Bestandteil von **DriveLock** schützt das Antivirus-Modul Ihre Desktops, Laptops und Server vor diesen Bedrohungen.

**DriveLock** Antivirus scannt in Echtzeit alle Dateibewegungen auf der lokalen Festplatte oder externen Speichermedien und verhindert so proaktiv die Verbreitung von Viren und Trojanern.

Zusätzlich scannt **DriveLock** Antivirus automatisch beim Verbinden externer Datenträger oder nach einem festgelegten Zeitplan ausgewählte Verzeichnisse, externe Laufwerke oder die gesamte Festplatte. Dieser On-Demand-Scan kann sowohl vom Administrator vorgegeben als auch vom Benutzer gestartet werden.

## Schnell – effizient – sicher

Der größte Teil der durch eine Antiviren-Engine überprüften Dateien enthält keine Schadsoftware. Somit ist eine hohe Performance bei "sauberen" Dateien eine der wichtigsten Eigenschaften, die eine Engine besitzen muss. Die durchschnittliche Scangeschwindigkeit von **DriveLock** Antivirus liegt bei mehr als 7 MB / Sekunde. So kann die **DriveLock**-Antiviren-Engine insbesondere bei der Geschwindigkeit ihre überragende Performance voll ausspielen. Ihr Vorteil: Der Nutzer erfährt in seiner Arbeit keinerlei Beeinträchtigung.

Einmalig ist der niedrige Ressourcenverbrauch von **DriveLock** Antivirus: Im laufenden Betrieb werden lediglich 1 – 2 MB RAM für den Echtzeitschutz beansprucht. Ihr Vorteil: Keine verlängerte Startzeit des Rechners, kein zusätzlicher Speicherbedarf, keine neue Hardware.

Laut aktuellen Ergebnissen aus dem Jahr 2011 (AV-TEST) erreicht die in **DriveLock** integrierte Antivirus-Engine jedes Mal einen der Top-Fünf-Plätze, im Mai 2011 sogar mit einer Erkennungsrate von 99,99%. Durch die eingebauten Selbstschutzmechanismen werden die **DriveLock**-Dateien und -Dienste geschützt, um nicht durch böswillige Angriffe deaktiviert werden zu können. Die nahtlose Integration in die **DriveLock**-Schnittstellenkontrolle und das reibungslose Zusammenspiel mit der **DriveLock**-Applikationskontrolle ermöglicht einen intelligenten Rundumschutz, der Ihre Systeme auch vor Zero-Hour-Angriffen und unentdeckter Schadsoftware zuverlässig schützt. So kann z. B. ein USB-Stick erst dann freigegeben werden, wenn er auf Schadsoftware gescannt wurde und keine Schadsoftware enthält. Ihr Vorteil: Optimaler, proaktiver Schutz, auch bei unbekannter Schadsoftware, schnelle Reaktion auf neue Bedrohungen.

Die Antivirus-Engine in **DriveLock** besteht aus einem modularen Framework. Die einzelnen Threat-Protection-Module wurden konzipiert, um spezifische Objekte (z. B. PDF-Dateien) zu prüfen oder nach bestimmten Virustypen (z. B. polymorphe Viren) zu suchen. Diese modulare Architektur ist den üblicherweise verwendeten monolithischen Antiviren-Engines gegenüber wesentlich flexibler und ihnen deutlich überlegen. Neue Module können schnell hinzugefügt oder einzelne Module leicht erweitert werden. Ihr Vorteil: Auch in Zukunft ein schnellerer Schutz vor neuen Bedrohungen.

## Zentrales Management und umfangreiches Reporting

**DriveLock** Antivirus ist ein fester Bestandteil von **DriveLock** EndpointShield. Die Konfiguration erfolgt zentral über die **DriveLock**-Management-Konsole. Durch die vollständige Integration sinkt der Administrationsaufwand für Endpoint Security deutlich; ein einheitlicher Wartungsvertrag, der zentrale Ansprechpartner bei Supportfällen und oft auch eine Reduzierung der Lizenzkosten bieten deutliches Einsparpotenzial. Der Administrator erstellt Sicherheitsrichtlinien, um alle Antivirus-relevanten Aktivitäten wie z. B. Signaturupdates, geplante Scans und die Quarantäne zu steuern. Dabei kann er auch die bereits bekannte und erprobte Flexibilität von **DriveLock** verwenden, um für unterschiedliche Gruppen oder Computer speziell angepasste Richtlinien zu definieren (z. B. eine häufigere und intensivere Überprüfung von Laptops, die sich aktuell nicht im Unternehmensnetzwerk befinden). Über Unregelmäßigkeiten oder Infektionen wird der Administrator sofort automatisch (z. B. per E-Mail) informiert. Um die Migration zu vereinfachen, bietet **DriveLock** bei der Installation die Möglichkeit, die bestehende Antivirus-Software automatisch zu entfernen. Bei der automatisierten Aktualisierung von Antiviren-Patterns kann zwischen einer Test- und einer Produktionsumgebung unterschieden werden (Staging). Auch ein Rollback auf eine vorherige Pattern-Version erfolgt ggf. schnell und ohne großen Aufwand.

Das **DriveLock** Control Center bietet eine umfangreiche und doch benutzerfreundliche Möglichkeit für Reporting und Forensik. Auf Knopfdruck wird erkannt, welche Endgeräte Schadsoftware enthalten und von zentraler Stelle kann auf die Quarantäne jedes Endgeräts zugegriffen werden. Zudem stehen zahlreiche Übersichtsgrafiken zur Verfügung.

Mit der Forensik kann jeder Sicherheitsvorfall blitzschnell analysiert werden. Auch nachträglich, um beispielsweise den USB-Stick zu ermitteln, der eine Schadsoftware ins System brachte. Dabei ist es für Reporting und Forensik nicht relevant, ob sich der betreffende Rechner momentan im Netzwerk befindet oder nicht.

### Technische Daten – Systemanforderungen

**Betriebssysteme:** Windows XP, Windows Vista, Windows 7, Windows 2003, Windows 2008 – jeweils 32-Bit und 64-Bit

**Signaturen:** Die inkrementellen Signaturupdates sind nur zwischen 150 KB und 300 KB groß.

Ein vollständiges Pattern wird bei der Erstinstallation geladen und ist etwa 28 MB groß. Signatur-Verteilung automatisch, Internetverbindung (für **DriveLock** Enterprise Service) notwendig.

**Support:** Lokal durch einen zertifizierten Partner vor Ort. Zusätzlich gibt es weitere Supportmöglichkeiten einschließlich Herstellersupport in deutscher Sprache.