DriveLock lässt sich leicht in Ihre bestehende Netzwerkstruktur integrieren. So sichern Sie Ihr Netzwerk und schützen alle vertraulichen Daten mit minimalem Aufwand an Zeit, Kosten und Personal.

DriveLock 7
Daten intelligent schützen

DriveLock gibt Ihnen die absolute Kontrolle darüber, wer was an welchem Computer anschließen darf und welche Programme darauf laufen. Mit der Verschlüsselung bleiben die Daten auch dann vertraulich, wenn ein Laptop oder ein Speichermedium verloren geht. Antivirus sorgt für umfassenden Schutz vor Viren, Trojanern und Malware. Alle Komponenten werden zentral gesteuert und übersichtlich ausgewertet.

Intelligenter Datenschutz leichtgemacht

Antivirus

Der perfekte Virenschutz mit **DriveLock** wird über die zentrale Konsole gesteuert. Neueste Methoden in den Antiviren- und Anti-Spy-Technologien (Heuristik und verhaltensbasierte Erkennung) sind ebenso selbstverständlich wie der proaktive Schutz vor sich selbst verändernden Schadprogrammen (polymorphe Malware) im Internet.

Kontrolle mobiler Datenträger

Unbeschränkter Gebrauch von USB-Sticks und anderen mobilen Datenträgern führt oft genug zu Datenverlust oder -diebstahl. **DriveLock** ermöglicht eine fein abgestimmte Kontrolle darüber, wer solche Datenträger benutzen kann und welche Daten übertragen werden dürfen.

Verschlüsselung von Daten

Die Verwendung von USB-Sticks und anderen mobilen Devices lässt sich kaum verhindern. Somit besteht die Gefahr, dass diese Datenträger verlorengehen – mit den darauf gespeicherten Daten. **DriveLock** verschlüsselt diese Daten automatisch und nachvollziehbar. Auch ist es möglich, verschlüsselte CDs oder DVDs zu erstellen. Der Passwort-Schutz ermöglicht einen sicheren Zugang auch auf Computern ohne **DriveLock**-Software. So kann der Datenträger an sich verlorengehen, aber keinesfalls die Daten selbst.

Full Disk Encryption

Durch die Verschlüsselung kompletter Laufwerke werden alle Ihre Daten auf allen Laptops und Desktops geschützt, einschließlich aller Daten auf der Systempartition. Durch die Pre-Boot Authentification mit Single-Sign-on ist gewährleistet, dass keinerlei Aufwand für den Anwender und den User Help Desk entsteht.

Auditing

Beim Auditing werden alle Dateibewegungen rechtssicher protokolliert: Welche Daten werden wann von wem gelesen oder geschrieben bzw. wohin kopiert? Nutzen Sie im Ernstfall die erweiterten Möglichkeiten der Datenforensik wie beispielsweise das detaillierte Drill-Down Reporting, um Datenlecks oder andere Sicherheitsrisiken zu erkennen.

Intuitive, effiziente Administration

DriveLock ist perfekt in Ihre Umgebung mit Microsoft Active Directory integriert und benötigt kein zusätzliches Management-GUI. Sicherheitsrichtlinien werden über Active-Directory-Gruppenrichtlinien verteilt. Der Schulungsaufwand für Administratoren entfällt.

Sicherheits-Policies

Fertige Sicherheits-Policies gewährleisten das Versprechen „Sicher in 4 Stunden“. Gleichzeitig haben Sie die Möglichkeit, benutzerspezifische Sicherheitsrichtlinien umzusetzen und das Sicherheitsbewusstsein der Anwender zu steigern.

Asset-Management

Für Unternehmen ist die integrierte Hard- und Software-Inventarisierung ideal: Schnell und einfach kann die Einhaltung der Compliance-Regeln dokumentiert und die Anzahl der notwendigen Lizenzen geprüft werden. Das gibt Sicherheit und spart unnötige Kosten. Auf Knopfdruck haben Sie den aktuellen Stand der Software- und Patchverteilung sowie die komplette Hardware Ihres gesamten Netzwerks aufgelistet.

Netzwerkprofile

Netzwerkprofile kontrollieren automatisch z. B. welche Anwendungen im Firmennetzwerk oder im Hotel erlaubt sind oder ob unverschlüsselte Datenübertragung zulässig ist.

Schutz von Datenträgern und Festplatten

- Sperrt dynamisch und konfigurierbar den Zugriff auf Wechseldatenträger (USB-Festplatten, CD-ROM, USB Memory Sticks, Floppy etc.)
- Sperrt Gerätetypen wie iPhone, Scanner, Kameras, Netzwerkadapter, Palms, Smartphones, Modems, Gamecontroler und vieles mehr
- Sperrt Ports wie: USB, 1394/FireWire, Bluetooth, Infrarot, PCMCIA seriell (COM) und parallel (LPT)
- Granulare Kontrolle der iPhone-Datensynchronisierung (z. B. nur Kontakte)
- Konfigurierbare Whitelist-Regeln erlauben den Zugriff auf Laufwerkstypen oder Modelle
- Ermöglicht die Freigabe von Speichermedien über die Seriennummer
- Freischaltung für Benutzer oder ganze Gruppen möglich
- Arbeitet perfekt über das Active Directory und die Gruppenrichtlinien
- Unterstützt Novell eDirectory und ZENworks
- Dynamische Anwendung der Regeln für eingeloggte User
- Der Dateifilter kontrolliert das Kopieren von Daten anhand von Dokument- oder Dateitypen
- Auditing protokolliert Daten, die auf oder von Datenträgern oder Netzwerklaufwerken übertragen oder gelesen werden
- Separate Schreib- und Leseberechtigungen für Wechseldatenträger
- Zugangsregeln für Laufwerke in Abhängigkeit von Größe oder Verschlüsselungsstatus des Laufwerks
- Hoch granulares Reglementieren auf Basis von Gerät, Netzwerkverbindung, Tageszeit etc.

Encryption 2-Go

- Verschlüsselt Daten auf mobilen Datenträgern oder Festplatten
- Automatische und nachvollziehbare Verschlüsselung beim Kopieren von Daten auf mobile Datenträger
- Erzwungene Verschlüsselung
- Zugriff auf verschlüsselte Datenträger auch auf Computern ohne **DriveLock** möglich
- Einfache und intuitive Benutzerführung
- Assistent zur Erstellung von verschlüsselten CDs und DVDs
- Absicherung durch Recovery-Funktionen bei vergessenen Passwörtern, auch offline
- Verschlüsselungsalgorithmen FIPS 140-2-konform
- Disaster Recovery ohne komplette Entschlüsselung möglich

Full Disk Encryption

- Bewährte Technologie durch sektorenweise Verschlüsselung für alle Festplatten inkl. temporärer und Indizierungsdateien
- Verschlüsselungsalgorithmen mit FIPS 140-2-Zertifizierung
- Pre-Boot Authentification zur Verhinderung eines unerlaubten Zugriffs auf alle Teile des Laufwerks
- Automatisierte Installation und zentrale Steuerung
- Wirkungsvolle Möglichkeiten zur Wiederherstellung des Passworts und Notfall-Login

Applikationskontrolle

- Legt fest, welche Programme ein Benutzer starten kann
- Blacklists verhindern das Starten unerlaubter Programme
- Whitelists stellen sicher, dass der Benutzer nur freigegebene Applikationen startet
- Schützt vor Sicherheitslücken (Zero-Day-Exploits) und bisher unbekannten Viren und Trojanern, die von der AV-Software nicht erfasst werden können
- Mustervorgaben für eine einfache Installation
- Komplette Registrierung aller Benutzeraktivitäten
- Vielfältige Regeltypen ermöglichen die Konfiguration innerhalb weniger Minuten

Antivirus-Schutz

- Höchste Erkennungsrate inklusive Zero-Hour Erkennung
- Schützt vor Malware jeden Typs, auch vor Würmern, Trojanern und Spyware
- Mehrschichtige Erkennung mithilfe von Heuristiken, verhaltensbasierten Mustern und Signaturen
- Niedrigster Ressourcenverbrauch
- Mehrstufige Sicherheitsrichtlinien, auch in Abhängigkeit der aktiven Netzwerk-Verbindung
- Vollständig integriert, keine zusätzlichen Dienste oder Softwareverteilung notwendig

Auditing

- Protokolliert die komplette Nutzung von Datenträgern und Applikationen
- **DriveLock** Control Center: eine zentrale Konsole für alle Ereignisse und Einstellungen
- Umfassende Berichte über alle Endpoint-Aktivitäten
- Vielfältige Benachrichtigungsmöglichkeiten für aktuelle **DriveLock**-Ereignisse
- Shadowing legt Kopien von Dateien an, die gelesen oder geschrieben werden
- Weitreichende Möglichkeiten für datenforensische Arbeiten und Ermittlungen

Administration

- Einstellung und Konfiguration erfolgt ausschließlich mit dem Microsoft Management Console (MMC) Snap-in
- Der Device Scanner erstellt eine Liste aller Geräte, die jemals mit dem Netz verbunden waren
- Einfache Installation und Roll-out auf Clients können über vorhandene Verteilungsprozesse erfolgen
- Zentrale Konfiguration über das Active Directory und die Gruppenrichtlinien, Novell eDirectory und ZENworks, Konfigurationsdateien oder **DriveLock**-Datenbank
- Temporäre Freischaltung für Online- oder Offline-Clients
- Fernabfrage von angeschlossenen Datenträgern
- Schnelle Erstellung von Richtlinien durch Templates
- Anpassbare Benachrichtigungseinstellungen mit HTML-Text
- Multilingual User Interface (MUI)
- Schutz gegen Manipulation und Deinstallation
- Automatische Erkennung von Agenten und DES im Netzwerk
- Statistische Auswertungen und Übersicht-Dashboards
- Security-Awareness-Kampagnen

Network Profiles

- Automatische Identifizierung verbundener Netzwerke
- Sperrt Netzwerkadapter bei Verbindung mit unerlaubten Netzwerken
- Passt Computereinstellungen oder Antivirus-Sicherheitsrichtlinien automatisch an das aktuelle Netzwerk an
- Sperrt Datenträger und Applikationen basierend auf dem aktuellen Netzwerk

Terminal Server Support

- Schnittstellen- und Applikationskontrolle für Windows- und Citrix-Terminal-Server
- Überwachung von Datenträgen und Verschlüsselung für Thin Clients

Systemvoraussetzungen

- Windows XP oder höher (inkl. Windows 7) oder Windows Server 2003 oder höher inkl. 64-Bit-Versionen
- Active Directory empfohlen für die zentrale Konfiguration

CenterTools