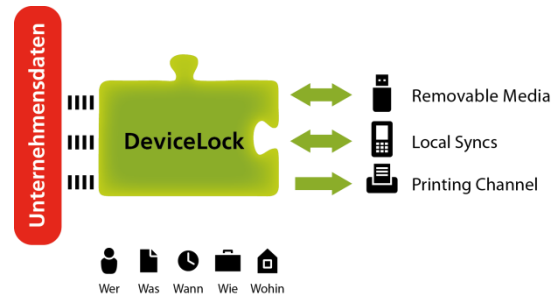


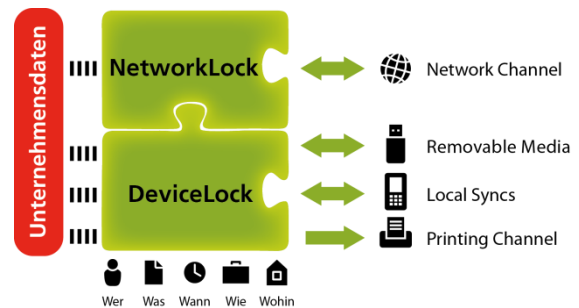
### Kontextkontrolle aller lokalen Schnittstellen/Geräte

- Kontrolle lokaler Ports (Windows und Mac OS X)
- Daten- und Gerätekontrolle in Terminalsitzungen
- Kontrolle der Zwischenablage
- Dateitypenfilterung (binär)
- Druckerkontrolle inkl. virtuelle Drucker (pdf)
- Smartphone-Synchronisationskontrolle
- Whitelist für USB und CD-/DVD-Medien
- Anti-Keylogger
- Verschlüsselungs-Integration
- DL-Administratorrechte (Dienst + Server)
- AD-Integration (GP-MMC + Template)
- Zentrale Managementkonsole
- White- und Blacklisting für CAWR
- Live Monitoring
- Flexible Verteilungsstrategien des Service
- Online/Offline Richtlinien
- Temporary Whitelist und Offline-Import der Settings
- Multilingual User interface



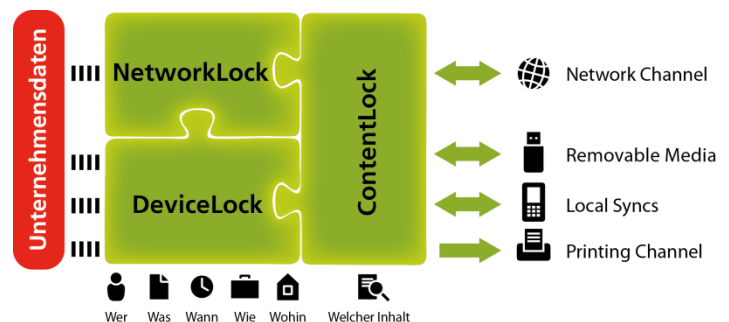
### Kontextkontrolle der Web- und Netzwerkkommunikation

- Netzwerkprotokollkontrolle (FTP, FTP über SSL, HTTP(S), MAPI, SMB, SMTP)
- Kontrolle von Cloud-Diensten (File Sharing)
- Webmail-, Messenger- und Skype-Kontrolle
- Kontrolle sozialer Netzwerke
- Erzwingung einer sicheren Übertragung
- Whitelists für alle Kontrollmöglichkeiten
- Online/Offline Richtlinien



### Kontrolle aller Inhalte auf binärer Ebene

- Inhaltskontrolle für Gerätezugriffe (120+ Dateiformate und 40 Archive)
- Inhaltskontrolle für Webzugriffe (mit NL)
- Schlagwortkatalog (branchenspezifisch)
- Kontrollregeln mit RegExp definierbar (reguläre Ausdrücke und/oder Schlagwörter)
- Vordefinierte Schablonen für RegExp
- Dokumentenfilterung anhand von Dateiattributen
- Online/Offline Richtlinien
- Volltextsuche inkl. Wortstammfilterung und OCR



### Informationsmanagement

- Zentrale Datenbank für Auditing/Shadowing
- Echtzeit Alarme, zentrale Protokollierung und Alarme für alle virtuellen DLP-Szenarien
- Richtlinienbasierte Auditierung der Zugriffe (Geräte, Protokolle und Inhalte)
- Schattenkopien von Schreibzugriffen (Dateien, Druck, Inhalt, etc.) in Abhängigkeit von Richtlinien (Inhalt, Dateityp etc.)
- Grafisches Reporting

## DeviceLock DLP Suite Überblick

### ▶ Unterstützte Betriebssysteme:

- Windows NT4 bis 8/8.1 bzw. Server 2012/2012 R2
- Mac OS X 10.6.8/10.7/10.8/10.9 (32/64-bit)

### ▶ Unterstützte Gerätetypen:

- Diskettenlaufwerke
- CD-ROMs/DVDs/BDs
- Alle Wechseldatenträger
- Festplatten
- Bandlaufwerke
- WLAN-Adapter
- Bluetooth Adapter
- Apple, BlackBerry, Windows Mobile, Palm OS
- Drucker (lokal, im Netzwerk, virtuell)

### ▶ Abgesicherte Schnittstellen:

- USB
- FireWire
- Infrarot
- Serial und parallel

### ▶ Unterstützte Netzwerkkommunikation:

- Cloud-Dienste: Google Drive, Dropbox, OneDrive, iFolder, RapidShare, Amazon S3, Yandex.Disk
- Web Mail: Outlook.com, Gmail, Yahoo!Mail, AOL Mail, GMX.de, Web.de, Yandex Mail, Yahoo
- Soziale Netzwerke: Disqus, Google+, XING.com, Studivz.de, MeinVZ.de, Facebook, Twitter, LiveInternet, LiveJournal, LinkedIn, MySpace, Tumblr, Vkontakte
- Messenger: Skype, ICQ/AOL, Windows Messenger, Jabber, IRC, Yahoo! Messenger
- Internet-Protokolle: FTP, FTP über SSL, HTTP/HTTPS, SMTP und SMTP über SSL
- Weitere Protokolle: MAPI und SMB

### ▶ Unterstützte Datentypen:

- Mehr als 5.300 Datentypen
- Datensynchronisations-Objekte: Microsoft ActiveSync®, Palm® HotSync, iTunes®
- Bilder mit als Grafik enthaltenem Text (eingebettete MS Office /PDF Dokumente, separate Grafikdateien)

### ▶ Analyisierte Dateiformate:

- 120+ Dateiformate u.a. Microsoft Office, Adobe PDF, OpenOffice, Lotus 1-2-3, WordPerfect, WordStar, Quattro Pro, E-Mail Verzeichnisse und Archive, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP, etc.

### ▶ Content Filtering Technologien:

- Schlagwort-Übereinstimmung inklusive OCR
- Reguläre Ausdrücke (advanced Regular Expressions), num. Konditionierung und boolesche Operatoren
- Vorlagen zur Erkennung von allgemeinen Datenmustern, sensitiven Schlüsselwörtern, Dateitypen etc.
- Branchenspezifische Schlüsselwörter-Verzeichnisse
- Dokumenten-/Datenobjekteigenschaften (Name, Größe, Passwortschutz, Textinhalt, Datum/Zeit, etc.)

### ▶ Virtuelle DLP für BYOD:

- DeviceLock Data Leak Prevention für Virtualisierungstechnologien (Microsoft RDS, Citrix XenApp, Citrix XenDesktop, VMware View)
- Kontext- und Inhaltskontrolle für Datentransfers und weitergeleitete Peripheriegeräte (Laufwerke, Drucker, Zwischenablage) zwischen zentral gehosteten virtuellen Desktops/Anwendungen und entfernten Terminals.
- Datenspiegelung für alle Datentransfers auf BYOD-Geräte über die weitergeleitete Zwischenablage und auf virtuelle Desktops über weitergeleitete Speichergeräte.
- Umfassender Schutz für alle BYOD-Geräte, unabhängig von der BYOD-Plattform.

### ▶ Kontrolle der Zwischenablage:

- Copy+Paste-Operation zwischen verschiedenen Applikationen
- Individuelle Kontrolle einzelner Datentypen: Dateitypen, textuelle Daten, Bilder, Audio, Sonstige
- Screenshot Aktionen (Funktion "Bildschirm drucken" und auch für Applikationen von Drittanbietern)

### ▶ Integration von Verschlüsselungssystemen:

- Windows BitLocker To Go
- PGP® Whole Disk Encryption
- TrueCrypt®
- Lexar® Media SAFE S1100 & S3000 Series
- SafeDisk®
- SecurStar® DriveCrypt® (DCPPE)
- Sophos SafeGuard Easy
- Mac OS X File Vault