DeviceLock®

Proactive Endpoint Security

Warum Sie eine Endpoint DLP Suite einsetzen sollten

Firewalls, komplexe Passwörter und Verschlüsselungslösungen schützen die Daten innerhalb Ihres Netzwerks. Dennoch sind Sie nicht sicher vor Datenverlust. Benutzer kopieren – bewusst oder unbewusst – vertrauliche Informationen von Ihren PCs oder Macs auf USB-Sticks, Smartphones, Kameras, PDAs, DVD/CDROMs oder andere tragbare Speichergeräte. Datenlecks können auch aus Benutzer-E-Mails, Instant Messages, Web-Formularen, Austausch in sozialen Netzwerken, File-Sharing Cloud Diensten oder Telnet-Sitzungen entstehen. Kabellose Schnittstellen wie Bluetooth oder WLAN und die zunehmende Nutzung von privaten mobilen Endgeräten (BYOD = Bring your own Device) erweitern die Möglichkeiten des Datenaustauschs, aber auch die Gefahr von ungewolltem Datenabfluss. Ebenso können Endpunkt PCs mit bösartiger Malware oder Keyloggern infiziert werden, die Tastatureingaben abgreifen und die gestohlenen Daten über SMTP oder FTP-Kanäle in kriminelle Hände senden. Die DeviceLock® Endpoint DLP Suite setzt für den Kontext und Inhalt von Datentransfers Datenschutzrichtlinien durch, um derartige Datenlecks zu verhindern.

Die virtuelle DLP (Data Leak Prevention) von DeviceLock erweitert diesen Schutz auf eine Vielzahl von Technologien zur Virtualisierung von Desktops und Anwendungen für sitzungsbasierte, übertragene und lokale virtuelle Maschinen sowie für BYOD-Geräte.

EINE ENDPOINT DLP SUITE.

ZUM SCHUTZ VERTRAULICHER DATEN.

IHRER DATEN.

DeviceLock
Proactive Endpoint Security

DeviceLock® Kontext und Inhalt

Die DeviceLock® Endpoint DLP umfasst die Kontrolle lokaler Schnittstellen und der Web- und Netzwerkkommunikation, ein Event-Logging und die Datenspiegelung für alle überwachten Datenkanäle. Der Content-Filter prüft und bewertet ergänzend zum Kontext den Inhalt der Datenbewegungen.

Kontexterkennung bedeutet, dass der Datenfluss in Abhängigkeit festgelegter Kriterien blockiert oder erlaubt wird: WER hat welche DATEI oder welchen DATEITYP (Was) über welches INTERFACE/GERÄT/PROTOKOLL (Wie) mit welchem ZIEL (Wohin) und mit welchem INHALT (Kontext) zu welchem ZEITPUNKT (Wann) bewegt?

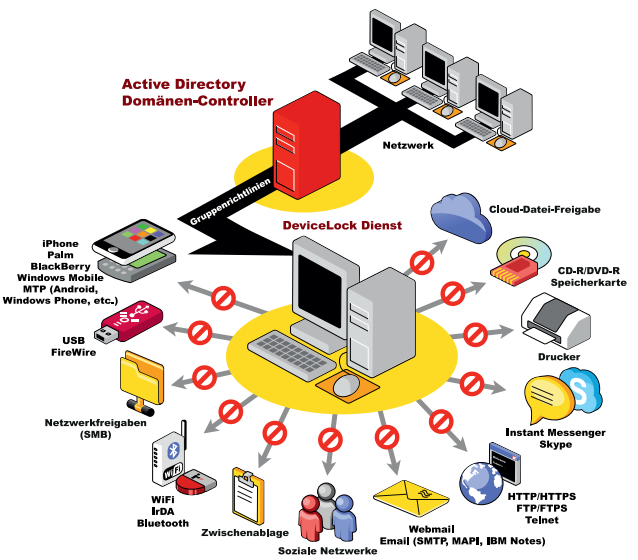
Wege des potenziellen Datenverlusts werden granular kontrolliert, auch innerhalb von Terminal-Sessions auf Thin-Clients. Klar definierte Regeln garantieren risikofreie Datentransfers und setzen individuelle Sicherheitsrichtlinien im Hinblick auf den Kontext um. In Abhängigkeit ihrer Position erhalten Benutzer verschiedene Rechte für das Übermitteln, Empfangen und Speichern von Daten. Dadurch gehen sie ungehindert ihren Aufgaben nach, ohne der Gefahr unberechtigter Datenoperationen ausgesetzt zu sein.

Die Methoden der Inhaltsanalyse fangen unerwünschte Inhalte ab. Neben binärer Inhaltsanalyse zur Bestimmung des Dateityps und der Auswertung von Dokumenteneigenschaften wird sensibler (Text-) Inhalt mit Hilfe von einer Vielzahl von unterschiedlichen Kriterien erkannt. Die entsprechende Datenbewegung wird in Abhängigkeit der Berechtigungen eines Benutzers zugelassen oder verhindert. Unterschiedliche Vorlagen (reguläre Ausdrücke (RegExp), Schlagwortverzeichnisse, etc.) sind bereits hinterlegt und können beliebig erweitert werden.

Die inhaltliche Analyse und Filterung kontrolliert den Datenaustausch mit Wechseldatenträgern, PnP-Geräten und über Netzwerk-/Webverbindungen. Letztere umfassen SMB Festplattenfreigaben, E-Mails, Internet-Zugriff, Cloud File Sharing Dienste, Soziale Netzwerke, Instant Messenger, wie z.B. Skype, sowie Netzwerkfreigaben und Telnet. Analysiert werden über 100 textbasierte Dateiformate und Datenobjekte (E-Mails, Instant Messages, Webformulare, Einträge in sozialen Netzwerken).

DeviceLock bietet einfache und transparente Werkzeuge für ein umfassendes DLP-Management und wendet zentral definierte DLP-Richtlinien an. Für die flexible Konfiguration der verteilten physischen sowie virtuellen Endpoint-Agenten nutzen Administratoren die Microsoft Windows Active Directory Gruppenrichtlinienobjekte (GPOs) und/oder die DeviceLock-Konsolen. Die DeviceLock Web-Konsole ermöglicht die Steuerung der DeviceLock-Komponenten über jeden Webbrowser. Mit DeviceLock kann der erfolgte und/oder unterbundene Datentransfer von Benutzern auf Peripheriegeräte, über lokale Schnittstellen und über Netzwerk-/Webverbindungen zentral gesteuert, protokolliert, gespiegelt, analysiert und mit einer Alarmierung verbunden werden. Zusätzlich werden Hardware-Keylogger erkannt und ihre Benutzung blockiert, um ein Ausspähen von Passwörtern und anderen proprietären Daten zu verhindern.

Die DeviceLock Endpoint DLP Suite reduziert das Risiko eines Datenverlusts durch feingliedrige Kontext-Kontrollen gefährdeter Endpunkt-Kanäle und Inhaltsfilterung von Dateien und anderen Datenobjekten. Gleichzeitig übernimmt sie die Rolle eines Werkzeugs zur Durchsetzung interner Sicherheitsrichtlinien und stellt die Einhaltung gesetzlicher Vorgaben nach dem Bundesdatenschutzgesetz (BDSG), dem Sarbanes-Oxley- Act (EURO/SOX) und den ISO/BSI-Normen sicher.



Unternehmen können mit der DeviceLock® Endpoint DLP Suite zentral eine unbegrenzte Anzahl Workstations schützen.

DeviceLock® Funktionsüberblick

Durch granulare Endpoint-Kontext-Kontrollen lokaler Datenkanäle an Mitarbeiter-PCs gepaart mit einer Inhaltsfilterung reduziert die DeviceLock Endpoint DLP Suite das Risiko vorsätzlicher oder fahrlässiger Datenverluste.

Bis zu fünf Funktionsbereiche bieten Ihnen den höchstmöglichen Schutz Ihrer IT-Umgebung bei geringem Investitionsbedarf. Die DeviceLock Endpoint DLP Suite ist entsprechend Ihren Anforderungen und Kapazitäten skalierbar und in Unternehmen jeder Größenordnung einsetzbar.

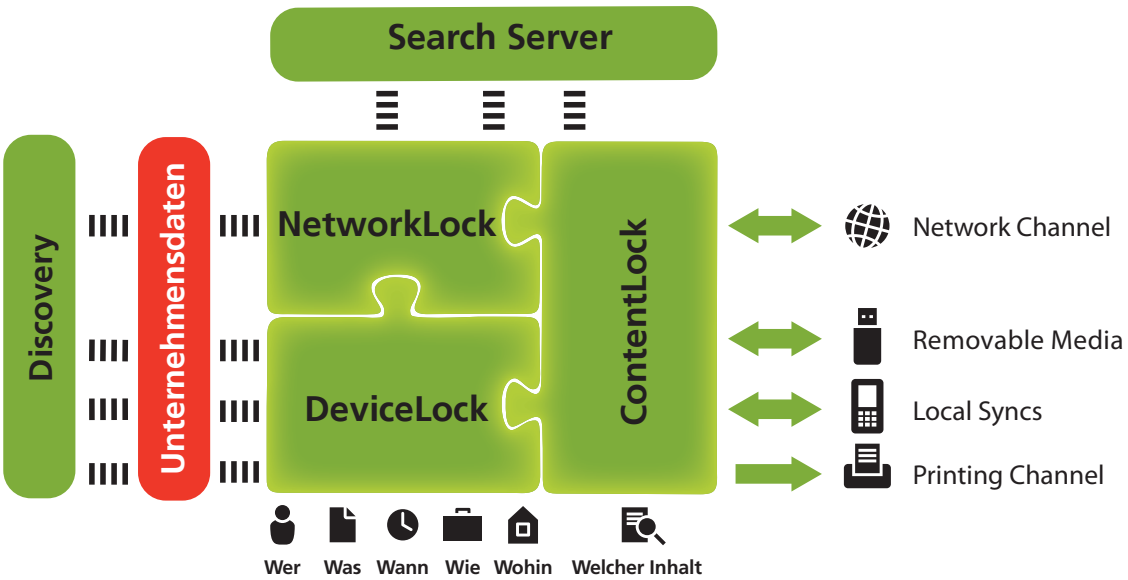
Die Kontextkontrolle lokaler Schnittstellen inklusive Event-Logging, Datenspiegelung und Alarmierung erfolgt durch DeviceLock. Diese umfasst zusätzlich Gerätetypen wie Wechseldatenträger, verbundene Smartphones/PDAs/ MTP-fähige Geräte (Android, Windows Phone, etc.), optische Laufwerke, Drucker, verbundene Laufwerke in Desktop- oder Applikations-Sitzungen und die Zwischenablage. Weiterhin umfasst DeviceLock die zentralen Management- und Administrationskomponenten.

Durch NetworkLock wird die Kontextkontrolle auf die Web- und Netzwerkkommunikation ausgedehnt. Die verwendeten Protokolle und Anwendungen werden portunabhängig erfasst und wahlweise gesteuert. Zusätzlich können sämtliche Vorgänge zentral protokolliert oder gespiegelt werden.

Als vollwertiger Inhaltsfilter ermöglicht ContentLock die Protokollierung und Filterung von Daten, die auf oder von Wechseldatenträger/n und PnP-Geräte/n kopiert werden. Damit wird sichergestellt, dass nur die zuvor geprüften Daten mit für den Benutzer freigegebenen Informationen ihre Ziele erreichen. Ergänzend werden innerhalb der Netzwerk-/Webkommunikation verschiedene Dateiobjekte analysiert und gesteuert. Dazu zählen unter anderem die von NetworkLock bereitgestellten Informationen. Über die Content-Filtering-Technologien können Echtzeit-Alarme generiert werden, die per E-Mail (SMTP) oder über ein Netzwerk (SNMP) versendet werden.

Die Volltextsuche in der zentralen Dateispiegelungs-/Protokolldatenbank ermöglicht der DeviceLock Search Server. Sie erhalten eine präzise, einfach zu handhabende und effiziente Unterstützung in den arbeitsintensiven Prozessen der Informationssicherheitsprüfungen, Untersuchung von Vorfällen und der Dateiforensik.

Um proaktiv Datenverluste zu verhindern und Compliance mit regulatorischen und unternehmerischen Datensicherheitsrichtlinien zu erreichen, benutzen Sie DeviceLock Discovery, das sich mit den „ruhenden Daten" befasst. DeviceLock Discovery scannt automatisch Daten auf Netzwerkfreigaben, Speichersystemen und Windows-basierten Computern innerhalb und außerhalb des Unternehmensnetzwerks, sucht Dokumente mit sensiblen Inhalten und bietet Optionen, um diese durch Korrekturmaßnahmen zu schützen. Wahlweise können Incident-Management-Verfahren eingeleitet werden, indem Echtzeit-Alarmierungen zu einem in der Organisation verwendeten SIEM System (SIEM = Security Information und Event Management) oder an für die Sicherheit zuständiges Personal gesendet werden.



Die Datenflusskontrolle der DeviceLock® DLP

DeviceLock
Proactive Endpoint Security

DeviceLock® Funktionen im Detail

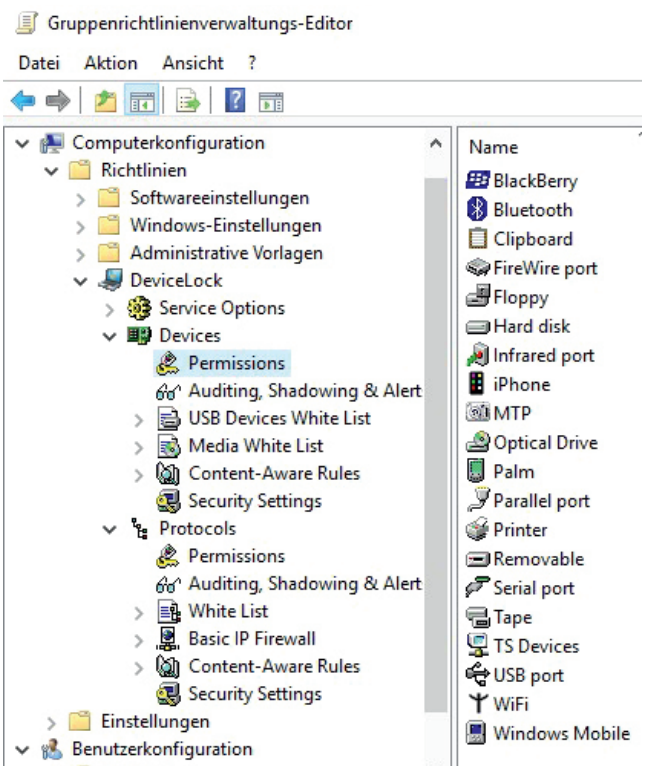
Neben Funktionsbereichen für die Kontrolle der lokalen Schnittstellen und der Netzwerk-/Webkommunikation bietet die DeviceLock® Endpoint DLP Suite eine vollständige Inhaltsfilterung. Mit DeviceLock vergeben Administratoren auf verschiedenen Ebenen Zugriffsrechte in Form von Parametern (z.B. schreiben, nur-lesen, formatieren) und Tages-/Uhrzeitangaben gemäß einer Unternehmensrichtlinie. Als Ebenen sind parallel die Schnittstelle, Geräteklasse, Typ, Modell und eindeutige Geräte-IDs konfigurierbar. Der Zugriff über Geräteklassen kann derart angepasst werden, dass auch in Abhängigkeit vom Verschlüsselungsstatus nur bestimmte Dateitypen bewegt oder gelesen werden dürfen. NetworkLock erweitert die Fähigkeit zur Kontextkontrolle auf die Netzwerk-/Webkommunikation und Anwendungen. ContentLock stellt sicher, dass nur zuvor geprüfte Daten mit für den Benutzer freigegebenen Informationen ihre Ziele erreichen

Gruppenrichtlinien/AD Integration. Eine DeviceLock-Konsole ist unmittelbar in die Microsoft Management Console (MMC) der Active Directory (AD) Gruppenrichtlinien-Verwaltung integriert. In Aussehen und Handhabung den Gruppenrichtlinien- und MMC-Oberflächen nachempfunden, erfordert die Lösung keine Einarbeitung in neue Strukturen oder den Erwerb einer speziellen Appliance zum zentralen Management. Die unmittelbare Integration als MMC-Snap-In ermöglicht die Steuerung über die Gruppenrichtlinienkonsole (GPMC) oder über die Konsole der Active Directory Users & Computers (ADUC). Es werden keine Skripts, ADMX-Vorlagen oder Schemaerweiterungen benötigt. Administratoren binden die Konfiguration der DeviceLock-Zugriffsrechte in ihre allgemeinen Systemmanagement-Aufgaben ein. Unabhängig von einer Gruppenrichtlinienumgebung bietet DeviceLock auch klassische Windows-Konsolen, mit denen Agenten auf jedem Novell, LDAP oder ‚Arbeitsgruppen' IP-Netzwerk von Windows und Apple macOS-Computern zentral verwaltet werden können. Hierbei werden die XML-basierten Richtlinien-Dateien über alle Konsolen hinweg ausgetauscht.

Web-Konsole. Umsetzung der administrativen DeviceLock-Konsolen auf einer Webseite zur Steuerung der DeviceLock-Komponenten über einen beliebigen Web-Browser.

RSoP-Unterstützung. Zur Ansicht der aktuell vergebenen Berechtigungen kann das Windows-Richtlinien-Ergebnissatz-Snap-In (RSoP) verwendet werden. Außerdem kann vorhergesagt werden, welche Richtlinie in einer bestimmten Situation angewendet wird.

(USB-)Geräte Whitelist-Zugriffskontrolle. DeviceLock unterstützt den USB-Modell und -Seriennummern-Level über ein Whitelisting. Administratoren nehmen z. B. firmeninterne USB-Geräte zentral auf und geben sie für eine beliebige Anzahl von Benutzern oder Gruppen frei. Diese haben gemäß ihren Rechten Zugriff auf die Geräte, wohingegen alle anderen Geräte und nicht aufgeführte Benutzer für den Datentransfer blockiert sind. Des Weiteren kann ein Gerät basierend auf seiner individuellen Seriennummer in die Whitelist aufgenommen werden, so dass alle modellgleichen Geräte desselben Herstellers weiterhin gesperrt sind. Offline sind auch befristete Zugriffsberechtigungen möglich, ohne dabei die normalen DeviceLock-Verfahren zur Festlegung und Bearbeitung von Zugangsrechten anwenden zu müssen. Diese werden mit Hilfe eines Challenge-Response-Verfahrens unter Mitwirkung der Administratoren definiert.



Integration der DeviceLock® Endpoint DLP Suite in die Microsoft Management Console der Active Directory Gruppenrichtlinien-Verwaltung.

DeviceLock® Funktionen im Detail

Virtuelle DLP. DeviceLocks virtuelle DLP Funktionen bieten die Möglichkeit, beliebige BYOD Geräte vor Insider-Datenlecks zu schützen, wenn diese mit führenden Remote-Desktop- und Anwendungsvirtualisierungslösungen wie Citrix XenApp/XenDesktop, Microsoft RDS und VMware Horizon View genutzt werden. Läuft DeviceLock auf einem VDI-Host oder Terminal Server, werden kontextuelle und inhaltsbasierte Endpunkt-DLP Steuerungen zum angeschlossenen BYOD-Gerät „weitergeleitet", um einen virtuelle Endpoint DLP Agent zu erstellen, der unkontrollierten Datenaustausch mit lokalen Peripheriegeräten, gehostete Anwendungen und Netzwerkverbindungen von dem BYOD Gerät innerhalb der Sitzung verhindert. Dieser Ansatz vereint DeviceLock DLP in physischen und virtuellen Windows und BYOD-Umgebungen.

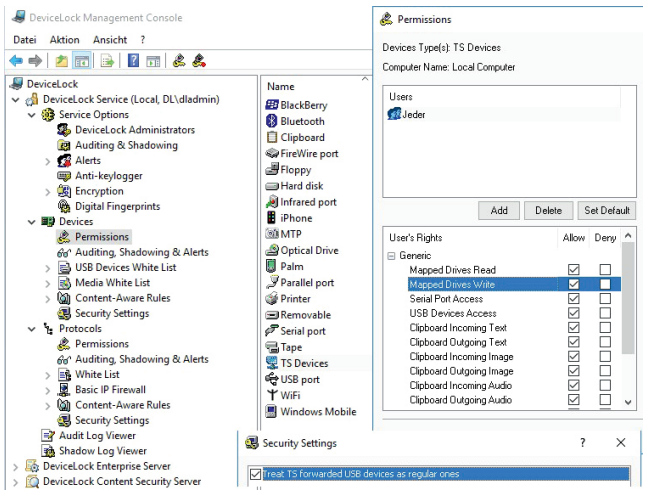
Kontrolle der Zwischenablage und Verhinderung von Screenshots. Mit DeviceLock ist es möglich, die Erstellung von Screenshots zu unterbinden und die Zwischenablage zu kontrollieren. So werden Datenlecks verhindert, die durch die Übertragung von Informationen zwischen verschiedenen Anwendungen und Dokumenten durch die Verwendung der Zwischenablage entstehen können.

Integration verschlüsselter Wechseldatenträger. Zur Sicherung der auf Wechseldatenträgern gespeicherten Informationen lassen sich in DeviceLock unterschiedliche Verschlüsselungstechnologien integrieren. Dadurch wird eine Verschlüsselungsrichtlinie im Unternehmen unterstützt, indem nur mit dieser Richtlinie konforme Datentransfers zugelassen werden. Entsprechend den Unternehmensanforderungen kann die passende Verschlüsselung gewählt werden. Unterstützt werden derzeit: Windows BitLocker To Go™ und PGP® Whole Disk Encryption, SafeDisk® SecurStar® DriveCrypt Plus Pack Enterprise (DCPPE) Software und Lexar Media S1100/S3000 Serie USB-Stick. Jedes weitere verschlüsselnde Endgerät kann verwendet und über die USB-Whitelist eindeutig verwaltet werden. Durch Technologie-Partnerschaften können – nach Prüfung der Voraussetzungen – zusätzliche Verschlüsselungsanwendungen implementiert werden.

Online-/Offline-Richtlinien. Abhängig vom Netzwerkstatus des PCs können angepasste Berechtigungen vergeben werden. Dadurch kann ein Anwender innerhalb eines Netzwerks (online) andere Berechtigungen als ‚offline' besitzen. Ein typischer Anwendungsfall ist die Verhinderung des ‚Bridging' durch eine Deaktivierung der WLAN-Schnittstelle an Notebooks, sobald diese an das Unternehmensnetzwerk angeschlossen werden.

Mobile Device Sync Control. Umfasst granulare Berechtigungen sowie Audit- und Datenspiegelungs-Regeln für mobile Geräte (Microsoft Windows Mobile®, Apple iPhone®/iPad®/iPod Touch®, Palm®, BlackBerry®, Android®, Windows Phone). Es kann eingestellt werden, welche Datenobjekte (Dateien, Bilder, E-Mails, Kontakte, Kalendereinträge etc.) bei Verbindung eines Gerätes mit dem Computer von bestimmten Benutzern/Benutzergruppen mit dem Unternehmens-PC synchronisiert werden dürfen.

Druckerüberwachung. DeviceLock kontrolliert Drucker (lokal, virtuell, Netzwerk). Durch die Unterbrechung, Analyse und Filterung sämtlicher Druckspooler-Operationen wird festgelegt, wer wann wohin drucken darf. Der Benutzerzugriff wird flexibel und zentral verwaltet. Bei über USB verbundenen Druckern können mittels Whitelisting spezifische Druckermodelle und/oder eindeutige Drucker-IDs verschiedenen Benutzern/Gruppen zugeordnet werden. Druck Ereignisse können protokolliert werden und die tatsächlichen Druckauftragsdaten können für das Logging oder zur späteren Analyse in durchsuchbarem PDF-Format schattenkopiert, gesammelt und zentral gespeichert werden.



Konfigurationsbeispiel für die Kontrolle von Geräten, die in eine Citrix/RDP-Session aufgenommen werden. Es können granulare Berechtigungen der Schreib- und Leserechte sowie der Zugriffsrechte auf serielle Schnittstellen und übernommene USB-Geräte erteilt werden.

DeviceLock® Proactive Endpoint Security

DeviceLock® Funktionen im Detail

Kontrolle der Netzwerk-/Webkommunikation. NetworkLock erweitert die Kontextkontrolle auf die Netzwerk-/Web-kommunikation. Die verwendeten Protokolle und Anwendungen werden portunabhängig erfasst und wahlweise gesteuert. Nachrichten und Sessions können mit dazugehörigen Parametern vollständig wiederhergestellt werden. Unterstützte Protokolle und Anwendungen: SMB Festplattenfreigaben, SMTP/SMTPS, HTTP/HTTPS, sowie Instant Messenger, Skype, FTP/FTPS, MAPI, IBM Notes (NRPC), SMB für Netzwerkfreigaben, WebSuche und Telnet-Sessions (siehe auch Seite 8, DeviceLock Funktionen im Detail).

Content Filtering. Mit dieser Funktion können durch Content Aware Rules granulare Berechtigungen für den Datentransfer auf Dateitypenebene vergeben werden. Dabei erfolgt eine Analyse des binären Dateiinhalts, um aus über 5.300 Dateitypen den Dateityp zu ermitteln. In Abhängigkeit der eingestellten Richtlinie, kann eine Kontrolle und ein Shadowing des Dateityps vorgenommen werden. Mit ContentLock werden Dateien, die auf oder von Wechseldatenträger/n und PnPGeräte/n kopiert werden, protokolliert und gefiltert. Damit wird sichergestellt, dass nur die zuvor geprüften Daten mit für den Benutzer freigegebenen Informationen ihre Ziele erreichen. Zudem werden verschiedene Dateiobjekte innerhalb der Netzwerk-/Webkommunikation analysiert und kontrolliert. ContentLock extrahiert aus 100+ Dateiformaten die Textinformationen und hält diese zur weiteren Klassifikation bereit. Neben binärer Inhaltsanalyse zur Bestimmung des Dateityps und der Auswertung von Dokumenteneigenschaften, wird sensibler (Text-) Inhalt mit Hilfe von Wortübereinstimmungen, Mustern regulärer Ausdrücke (RegExp) und Übereinstimmungen boolescher Kombinationen dieser Kriterien (Und/Oder/Nicht- Verknüpfungen) erkannt. Sowohl ein branchenspezifisches Schlagwortverzeichnis, als auch RegExp-Vorlagen sind bereits hinterlegt und können beliebig erweitert werden. Weitere Faktoren zu Inhaltsanalyse können Dokumenten-/Meta-Eigenschaften und verifizierte Dateitypen sein. ContentLock kann die Klassifizierungen, die Boldon James Classifier an Dateien und Dokumenten zugewiesen hat, erkennen und für die inhaltliche Filterung verwenden.

Data Fingerprinting wird zur Erkennung von unstrukturiertem textlichen und binärem Inhalt verwendet. Fingerabdrücke werden dabei abhängig von Wichtigkeit oder Geheimhaltungsgrad nach den zugeordneten Datenklassifizierungen in unterschiedlichen Stufen kategorisiert (z.B. “Restricted”, “Confidential”, “Secret”, “Top Secret”).

Endpunkt-Residente OCR. Ergänzend zur Inhaltsfilterung von textbasierten Datenobjekten, ermöglicht eine integrierte optische Zeichenerkennung (OCR), Textdaten aus Bildern in Dokumenten und Grafikdateien vieler Bildformate schnell, effizient und präzise zu extrahieren und zu untersuchen. Mit 30+ erkannten Sprachen, verwendet die hocheffiziente OCR anpassbare reguläre Ausdrücke, Schlüsselwort Wörterbücher sowie andere fortschrittliche Methoden der DeviceLock DLP, um vertrauliche Daten in grafischen Formen erkennen zu können und zu schützen. Einzigartig in der DeviceLock DLP ist die Integration der OCR-Funktionalität in den Komponenten: DeviceLock-Agent, DeviceLock Discovery Server und DeviceLock Discovery Agent. Die OCR-Architektur steigert den Funktionsumfang und die Leistungsfähigkeit der DeviceLock DLP enorm. Denn die auf den Endpunkten gespeicherten grafischen Objekte werden durch das lokal residierende OCR überprüft.

Echtzeit-Alerts. Administrative Alerts (z. B. bei erfolglosen Versuchen einer Policy-Änderung durch den Benutzer) und geräte-/protokollspezifische Alerts können mittels SYSLOG, SMTP- oder SNMP-Protokoll an konfigurierbare Empfänger oder externe Systeme, wie z. B. ein SIEM-System, versendet werden. Die granular konfigurierbaren Alerts können auch von der Content-Filtering-Technologie ausgelöst werden.

Schutz des DeviceLock-Diensts. Die konfigurierbare Funktion „DeviceLock Administrators“ verhindert lokal auf Windows und macOS Manipulationen an DeviceLock Richtlinieneinstellungen, auch von Benutzern mit lokalen Systemadministratorrechten. Ist diese Funktion aktiviert, können nur definierte DeviceLock-Administratoren über eine DeviceLock-Konsole oder ein Gruppenrichtlinienobjekt (GPO) den Agenten deinstallieren, aktualisieren oder die DeviceLock Einstellungen in irgendeiner Weise verändern.

Name	Type	Action(s)	Applies To	Protocol(s)	Send Alert	Log Event
Archives	File Type Detection	Deny: Outgoing Files	Permissions	HTTP	☐	☐
C# Source Code	Keywords	Deny: Outgoing Messages	Permissions	MAPI	☐	☑
Confidential	Keywords	Deny: Outgoing Files	Permissions	FTP	☑	☐
Credit Card Number	Pattern	Deny: Outgoing Messages	Permissions	Social Networks	☐	☐
MS Excel	File Type Detection	Deny: Outgoing Files	Permissions	File Sharing	☑	☐

Anwendung von Methoden der Inhaltsanalyse auf Protokolle der Web- und Netzwerkkommunikation.

DeviceLock® Protokollierung

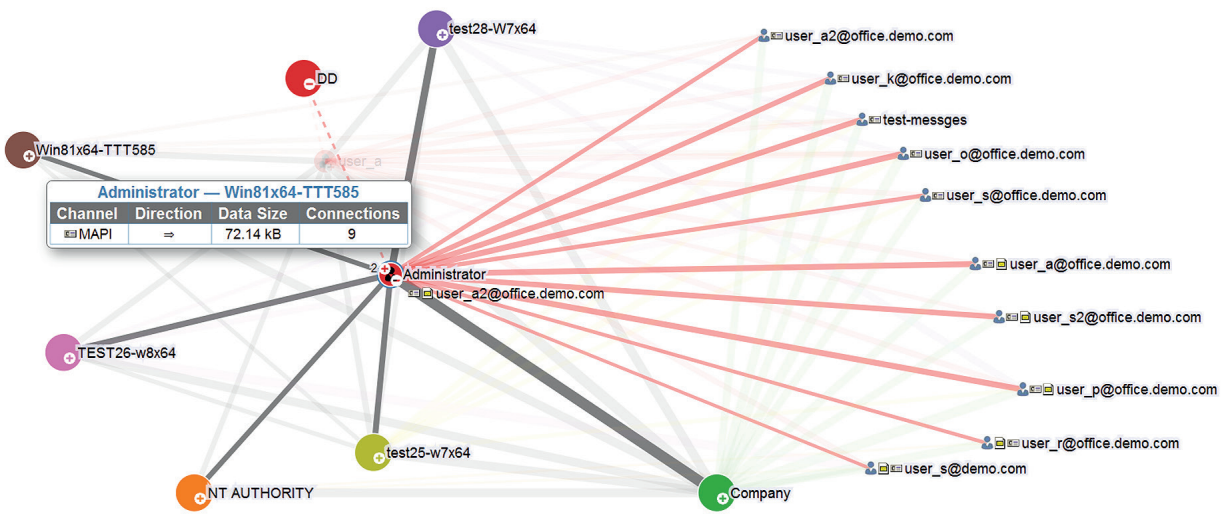
Die DeviceLock Endpoint DLP Suite fasst Informationen über Datenobjekte zusammen, die von Benutzern auf Wechseldatenträger, DVD/CD-ROMs, PDAs/Smartphones/MTP-fähige Geräte (Android, Windows Phone, etc.) oder über Webmail, Webformulare, etc. übertragen wurden. Über die Protokoll-/Datenspiegelungsfunktionen wird festgehalten, inwieweit unternehmensweite Datenschutzrichtlinien eingehalten oder verletzt wurden. Treten Datenlecks auf, bietet DeviceLock die nötigen Werkzeuge, um stichhaltige Protokolle auszuwerten und forensische Hinweise zur weiteren Verfolgung zu sammeln.

Audit Logging. Die DeviceLock-Audit-Funktion verfolgt Benutzer- und Dateiaktivitäten für bestimmte Gerätetypen, Ports und Protokolle auf einem verwalteten Computer. Es kann prüffähige Ereignisse vorfiltern nach Benutzer/Gruppe, Tag/Stunde, echtem Dateityp, Port/Gerätetyp/Protokoll, lesen/schreiben und nach erfolgreichen/verhinderten Vorgängen. DeviceLock verwendet das Standard- Subsystem für Ereignisprotokollierung unter Windows oder Apple macOS. In der spaltenbasierten Anzeige können Protokolle nach Spaltendaten sortiert und anhand beliebiger String-basierter Kriterien mit Wildcard-Operatoren gefiltert werden, um die gewünschte Ansicht der erfassten Prüfdaten zu erreichen.

Data Shadowing. Ermöglicht die Datenspiegelung für Datenkanäle, wie z.B. Wechseldatenträger, CD/DVD-Geräte, Drucker und Netzwerkkommunikation. Es wird eine vollständige Kopie der Daten gesichert und auf Wunsch über den DeviceLock Enterprise Server in ein gesichertes Verzeichnis (auf dem Server oder im Netzwerk) oder in einer SQL-Datenbank gespeichert. Wie auch beim Auditing können spezifische Filter gesetzt werden, um das Datenvolumen zu reduzieren. Beide Funktionen sind für höchste Effizienz im Hinblick auf die Netzwerklast ausgelegt. Sie bieten neben einer optimierten Serverauswahl und Bandbreitenregulierung die Möglichkeit, Speicherbeschränkungen zu definieren und somit das maximale Datenaufkommen zu limitieren.

Monitoring. Bietet Echtzeitüberwachung des DeviceLock-Dienstes (aktiv oder nicht), seiner Version sowie der Zusammensetzung und Integrität der Berechtigungen. Diese Informationen werden in das Überwachungsprotokoll geschrieben. Es kann eine „Master Policy" definiert werden, die automatisch an ausgewählte Computer verteilt wird, wenn eine Diskrepanz zu dieser hinterlegten Vorlage gefunden wird.

Grafische Auswertung. Die grafische Auswertungsfunktion unterstützt DeviceLock-Administratoren bei der Analyse der Datenflüsse über die Netzwerkendpunkte. Auswertungen können basierend auf Vorlagen in Form von angepassten Reporten durch konfigurierbare Parameter erstellt werden. Diese Reporte können auch per E-Mail an Verantwortliche versendet werden. DeviceLock-Administratoren können sehr einfach aus den Log-Daten der Benutzer-Kommunikation mittels interaktivem Relations-Diagramm einen Bericht der Kommunikationsbeziehungen zwischen Nutzern innerhalb und deren Kontakten außerhalb der Organisation bzw. des Unternehmens erstellen. Der HTML-basierte Bericht kann im Web-Browser oder der DeviceLock Management Konsole angezeigt werden. Aus den Log-Daten werden Benutzerverbindungen aus Anwendungen und Protokolle gezeigt. Informationen von Benutzerverbindungen werden als Knoten-Verbindung-Diagramm gezeigt. Dabei werden Domänen und Benutzer als Knoten und Kommunikationen zwischen den Knoten als entsprechende Verbindung dargestellt.



Grafischer Relations-Chart Report basierend auf Log Daten für blockierte Kommunikationsversuche aufgrund von Richtlinienverletzungen.

DeviceLock
Proactive Endpoint Security

DeviceLock® Produkt-Spezifikationen

Programm-Komponenten
- Agenten und Server: DeviceLock Agent (Windows und Apple macOS), DeviceLock Discovery Agent (Windows), DeviceLock Enterprise Server (DLES), DeviceLock Content Security Server (Discovery Server, Search Server)
- Management Konsolen: DeviceLock Gruppenrichtlinien Manager (MMC snap-in der Microsoft GPMC), DeviceLock Management Konsole, DeviceLock Enterprise Manager, DeviceLock Web-Konsole mit Apache

Geschützte Schnittstellen
- Windows: USB, FireWire, Infrarot, Seriell, Parallel
- Mac: USB, FireWire, Seriell
- Session terminal/BYOD: USB, Serial

Kontrollierte Gerätetypen (Partielle Liste)
- Windows: Disketten, CD-ROMs/DVDs/BD, Wechseldatenträger (Flash-Laufwerke, Speicherkarten, PC Cards, eSATA, etc.), Festplatten, Bandlaufwerke, WLAN-/Bluetooth-Adapter, Apple iPhone/iPod touch/iPad, Windows Mobile, Palm OS, BlackBerry, MTP-fähige Geräte (wie Android und Windows Phone), Drucker (lokal, Netzwerk, virtuell), Modems, Scanner und Kameras
- Mac: Wechseldatenträger, Festplatten, CD-ROMs/DVDs/BD, WLAN-/Bluetooth-Adapter
- Session terminal/BYOD: verbundene Laufwerke (Wechseldatenträger, optische Laufwerke, Festplatten), USB-Geräte

Kontrolle der Zwischenablage (Windows)
- Inter-/Intra-Anwendungs Kopieren-Einfügen-Operationen über Windows-Zwischenablage
- Kopiervorgänge zwischen Host und Gast OS Zwischenablagen
- Datentransfer von/nach Zwischenablagen von Windows und Desktop/Anwendungssitzung
- Screenshot-Operationen (Print Screen und 3rd-Party-Anwendungen)

Kontrollierte Netzwerkverbindungen
- Email: SMTP/SMTPS, Microsoft Outlook (MAPI), IBM Notes
- Webmail: AOL Mail, freenet.de, Gmail, GMX.de, Hotmail/Outlook.com, NAVER, Outlook Web App/Access (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail
- Soziale Netzwerke: Disqus, Facebook (+API), Google+, Instagram, LinkedIn, LiveJournal, MeinVZ.de, MySpace, Pinterest, StudiVZ.de, Tumblr, Twitter, Vkontakte (+API), XING.com
- Instant Messenger: ICQ Messenger, IRC, Jabber, Skype/Skype for Web/Skype for Business Web App, Telegram, Viber, WhatsApp, Yahoo! Messenger
- Cloud File Sharing Web Services: Amazon S3, Box, Cloud, Dropbox, freenet.de, GitHub, GMX.de, Google Docs/Google Drive, iCloud, MagentaCLOUD, MediaFire, MEGA, OneDrive, Sendspace, Web.de, WeTransfer, Yandex.Disk, 4shared
- Websuche: Google, Yandex, Bing, Baidu, Yahoo, Ask.com, AOL Search, Rambler, Wolfram Alpha, DuckDuckGo, WebCrawler, Search.com, Wayback Machine, Dogpile, StartPage, Excite, NAVER, Web.de
- Netzwerk-Protokolle: HTTP, HTTPS, FTP, FTPS, Telnet
- Andere: SMB Festplattenfreigaben, private Skype-Unterhaltungen, Skype Medien-gespräche, Torrent, Tor Browser

Content Aware Kontrollen
- Kontrollierte Kanäle: Speichergeräte (Wechseldatenträger, Disketten, optische CD/DVD/BD Laufwerke), Drucker (lokal, Netzwerk, virtuell), Zwischenablage (Windows, Desktop-/Anwendungssitzung), Mapped Drives (Desktop/Anwendungssitzung), Netzwerkkommunikation (E-Mail, Webmail, IM, soziale Netzwerke, Cloud File Sharing Dienste, HTTP/HTTPS, FTP/FTPS, SMB Festplattenfreigaben)
- Kontrollierte Inhaltstypen: textlicher Inhalt, Binärdaten, Datentypen
- Textinhalt-Objekte: Parsable Dateiformate (100+) und Archive (40+), Textdaten (in E-Mails, Nachrichten, Web-Formularen, etc.), Bilder (OCR-Verarbeitung), Oracle IRM- versiegelte Dokumente, nicht identifizierte Binärdaten, Klassifizierungen der Dateien und Dokumente, welche durch Boldon James Classifier zugewiesen wurden.
- Erkennungsmethoden für Textinhalt: Schlüsselworte und Schlüsselwort Wörterbücher (160+ vordefiniert, Benutzer konfigurierbar) mit morphologische Analyse (Englisch, Französisch, Deutsch, Italienisch, Russisch, Spanisch, Katalanisch Spanisch, Portugiesisch, Polnisch), RegExp-Vorlagen (90+ vordefiniert, Benutzer konfigurierbar), Daten-Fingerabdrücke für partiellen/exakten Dokumentenabgleich innerhalb von Datenklassifikationen (vorgefertigt, Benutzer konfigurierbar)
- Binäre Datenerkennungsmethode: Daten-Fingerabdrücke
- Kontrollierte Datentypen: verifizierte Dateitypen (5.300+), Datei/Dokumenteigenschaften, eingebettete Bildeigenschaften, Datentypen der Zwischenablage (Dateien, Textdaten, Bilder, Audio, nicht identifiziert), Sync-Protokoll-Objekte (Microsoft ActiveSync®, WMDC, Apple iTunes®, Palm® HotSync), Oracle IRM-versiegelte Dokumente (Sicherheitskontexte)
- Inhaltsbezogene Datenspiegelung: für alle kontrollierten Kanäle und Inhaltstypen
- OCR Funktionen: Endpunkt-Resident OCR-Verarbeitung, 30+ Grafikformate, 30+ Sprachen, integrierte DeviceLock Schlüsselwort Wörterbücher und reguläre Ausdrücke, gedrehte/gespiegelte/invertierte Bilder

Verschlüsselungsintegration
- Windows: Windows BitLocker To Go®, TrueCrypt®, SafeToGo, Symantec Drive Encryption, Infotecs SafeDisk®, SecurStar® Drive-Crypt® (DCPPE), Sophos® Safeguard Easy®
- Mac: Apple® macOS FileVault

Zentrale Log Erfassung
- Proprietäres sicheres Protokoll mit Traffic-Shaping/Priorisierung
- SYSLOG

Alarmierungs Methoden
- SMTP, SNMP, SYSLOG

Systemanforderungen
- Agenten: Windows NT/2000/XP/Vista/7/8/-8.1/10/Server 2003-2016 (32-/64-bit); Apple macOS 10.6 bis 10.13 (32/64-bit); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View; VMware Workstation/Player, Oracle VM VirtualBox, Windows Virtual PC; CPU Pentium 4, 512 MB RAM, HDD 400 MB
- Konsolen: Windows 2000/XP/Vista/7/8/-8.1/10/Server 2003-2016 (32-/64-bit); CPU Pentium 4, 512 MB RAM, HDD 1 GB
- DeviceLock Enterprise Server, DeviceLock Discovery Server, DeviceLock Search Server: Windows Server 2003-2016 (32/64-bit), Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2 × CPU Intel Xeon Quad-Core 2.33 GHz, RAM 8 GB, HDD 800 GB (bei lokaler SQL-DB); SQL Express/SQL Server 2005-2017

[www.devicelock.de]

DeviceLock Europe GmbH
Halskestr. 21
40880 Ratingen
Germany

Phone +49.2102.131840
Fax +49.2102.1318429
info@devicelock.de
www.devicelock.de

For DeviceLock offices in AMERICA, CANADA, UNITED KINGDOM and ITALY please refer to:

www.devicelock.com