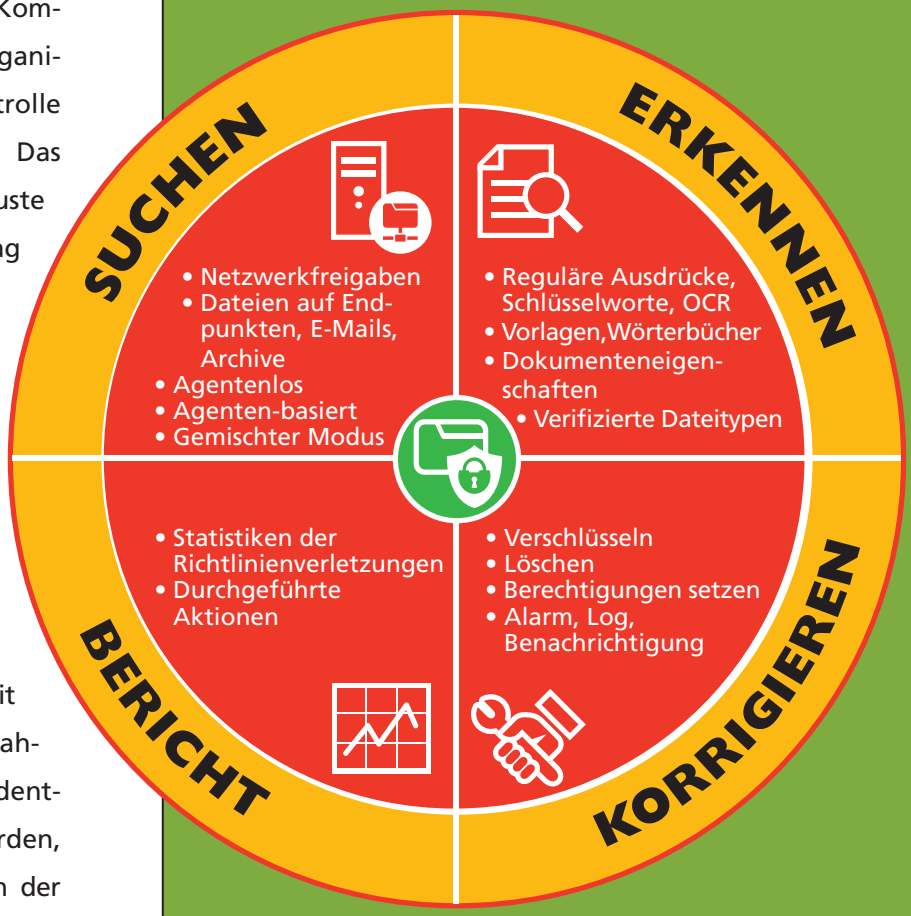
DeviceLock®

DISCOVERY

Einführung

DeviceLock Discovery ist eine funktionale Komponente der DeviceLock DLP Suite, die es Organisationen ermöglicht, Transparenz und Kontrolle über vertrauliche Daten zu gewinnen. Das Programm verhindert proaktiv Datenverluste und liefert damit einen wesentlichen Beitrag zur Compliance mit regulatorischen und unternehmerischen Datensicherheitsrichtlinien.

DeviceLock Discovery scannt automatisch „ruhende Daten“ auf Netzwerkfreigaben, Speichersystemen und Windows-basierten Computern innerhalb und außerhalb des Unternehmensnetzwerks und bietet Optionen, um Dokumente mit sensiblen Inhalten durch Korrekturmaßnahmen zu schützen. Optional können Incident-Management-Verfahren eingeleitet werden, indem Echtzeit-Alarmierungen zu einem in der Organisation verwendeten SIEM-System (SIEM = Security Information und Event Management) gesendet werden.



DeviceLock DISCOVERY

Struktur

Als eigenständige Lösung besteht DeviceLock Discovery aus den folgenden Komponenten:

- **DeviceLock Discovery Server** – ein Content-Discovery-Server-Dienst, der remote die Dateien auf Netzwerkfreigaben über das SMB/CIFS-Protokoll scannt sowie die DeviceLock Discovery-Agenten auf die Zielcomputer verteilt und verwaltet. Strukturell ist DeviceLock Discovery Server ein integraler Bestandteil des DeviceLock Content Security Server.

- **DeviceLock Discovery Agent** – eine kleine Discovery Client-Software, die auf den Endpunkten (Desktops, Laptops oder Server) für das Scannen der lokalen Dateisysteme und zugänglichen Netzwerkfreigaben verwendet wird, die nicht durch traditionelle DeviceLock-Agenten geschützt sind.

- **Management Konsole** – eine grafische Benutzerschnittstelle (GUI) für die zentrale Verwaltung aller DeviceLock Discovery-Komponenten. Je nach Kundenanforderungen und Besonderheiten der Umgebung können DeviceLock Administratoren für die Verwaltung zwei Arten von Konsolen wählen: die DeviceLock Management Konsole und die DeviceLock Web Konsole.

Wird Discovery zusammen mit anderen DeviceLock DLP-Komponenten verwendet, kann DeviceLock Discovery auch die integrierten Erkennungsfunktionen von DeviceLock-Agenten nutzen, um die auf Host-Computern und zugänglichen Netzwerkfreigaben gespeicherten Daten zu scannen.

Betrieb

Abhängig von der Netzwerktopologie und anderen Gegebenheiten der geschützten IT-Umgebung können DeviceLock Discovery-Scans in verschiedenen Modi durchgeführt werden: agentenlos (agentless), agentenbasiert (agent-based) und im gemischten Modus (mixed).

- Der agentenlose Modus wird vom DeviceLock Discovery Server verwendet, um Netzwerkfreigaben zu scannen. In diesem Modus werden die Dateien auf den Server heruntergeladen, auf dem dann die Inhaltsprüfung und -erkennung erfolgt. Anschließend werden die Korrekturmaßnahmen, die über das SMB-Protokoll umsetzbar sind, ausgeführt.

- Beim Modus „agentenbasiert“ werden DeviceLock-Agenten und Discovery-Agenten benutzt, um lokale Dateisysteme auf den Computern mit den installierten Agenten sowie Netzwerkfreigaben, die von diesen Computern aus zugänglich sind, zu scannen. In diesem Modus wird der Inhalt der lokalen Dateien lokal vom Agenten inspiziert. Anschließend führt dieser je nach Inhalt vorkonfigurierte Korrekturmaßnahmen durch. Dateien auf Netzwerkfreigaben werden auf den Computer, auf dem der Agent läuft, heruntergeladen. Dort prüft der Agent ihren Inhalt, erkennt Verletzungen der Richtlinien und bereinigt diese.

Neben der entscheidenden Fähigkeit, lokale Dateisysteme auf Unternehmenscomputern zu scannen, bietet der agentenbasierte Scan auch erhebliche Performance-Vorteile:

- Die Dateien müssen für den Scan nicht über das Netzwerk an den zentralen Server übermittelt werden.

- Durch die Verteilung der CPU-intensiven Inhaltsuntersuchung auf viele Endpunkte wird die Last auf dem Discovery-Server reduziert.

- Der gemischte Modus kombiniert agentenlose und agentenbasierte Scans, indem diese gleichzeitig von entsprechenden DeviceLock Komponenten durchgeführt werden. Dieses Hybridverfahren bietet nicht nur eine verbesserte Datensicherheit, sondern auch eine höhere Vielfalt der Scan-Modi. So können Administratoren die DeviceLock Content-Discovery-Aufgaben noch effizienter konfigurieren, um mit geringerer Netzwerkbandbreite gleichzeitig größere Performance zu erhalten.

Administratoren können DeviceLock Discovery-Scans manuell starten oder eine Ausführung nach Zeitplan festlegen. Als Scan-Ziele können sowohl Computer und Computergruppen als auch Netzwerkfreigaben und Speichersysteme im Unternehmensnetzwerk definiert werden. DeviceLock Discovery-Agenten lassen sich vom DeviceLock Discovery Server in einem vollautomatischen und für die Endanwender transparenten Prozess remote installieren und vom Zielcomputer wieder entfernen.

Inhaltserkennung

DeviceLock Discovery überprüft Textdaten in mehr als 120 Dateiformaten und in mehr als 40 Arten von verschachtelten Archiven.

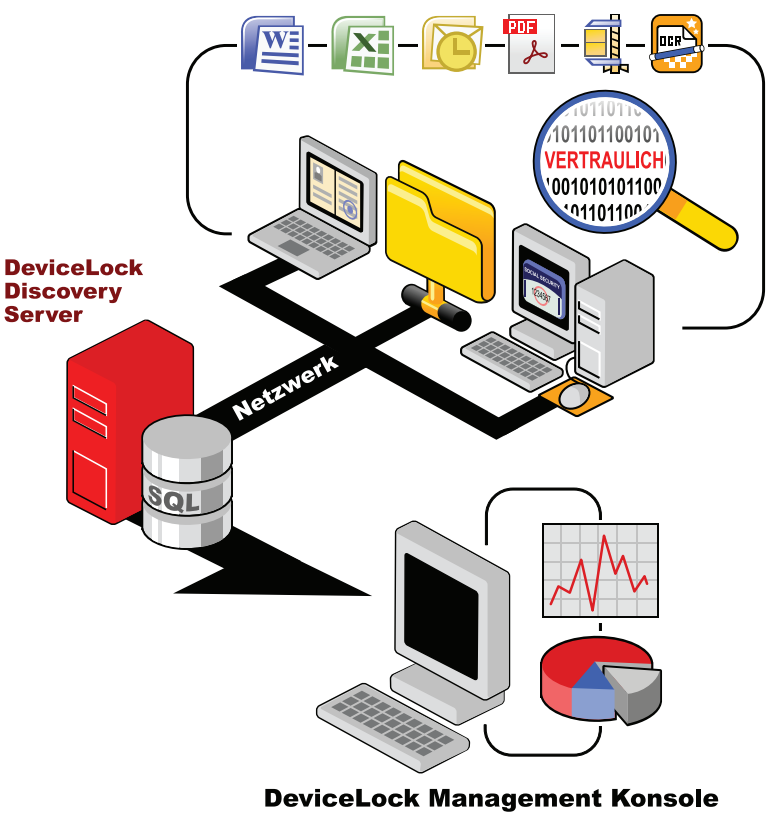
Vertrauliche Inhalte identifiziert DeviceLock Discovery mittels strukturierten Daten-Erkennungsmethoden wie Schlüsselwörtern und regulären Ausdrücken (RegExp). Um die Definition von Inhaltsfiltern zu erleichtern, enthält DeviceLock Discovery Hunderte von vorgefertigten branchen- und länderspezifischen Schlüsselwort-Wörterbüchern sowie RegExp-Vorlagen für gängige sensible Informationstypen wie z.B. Sozialversicherungsnummern, Kreditkarten, Bankkonten, Adressen, Führerscheine. Darüber hinaus können Kunden eigene Schlüsselwort-Wörterbücher und RegExp-Vorlagen entwickeln sowie die vorgefertigten für die eigenen Filter-Bedürfnisse ändern. Die Genauigkeit der Inhaltserkennung wird erhöht durch eine morphologische Analyse von Schlüsselwörtern in Englisch, Französisch, Deutsch, Italienisch, Portugiesisch, Russisch, Spanisch und Katalanisch.

Bestätigte Dateityperkennung (mehr als 4100+ Dateitypen werden erkannt) ist eine weitere Methode der Inhaltsuntersuchung, die in DeviceLock Discovery unabhängig oder in Kombination mit der Untersuchung des Textinhalts verwendet werden kann. Unabhängig von der Dateiendung oder dem Header wird der binäre Inhalt in einem signaturbasierten Verfahren geprüft, um den Dateityp verifiziert zu erkennen.

Darüber hinaus kann eine große Menge von Datei- und Dokumenteneigenschaften verwendet werden, um ein Dokument oder eine Klasse von Dokumenten für die Data-Leak-Prevention(DLP)-Kontrolle auszuwählen.

Durch die Verbindung von Inhaltsdefinitionen wird die Flexibilität der Content-Aware-Regeln weiter verbessert. Mehrere Inhaltskriterien mit verschiedenen Erkennungsmethoden und Datentypen können über logische (UND/ODER/NICHT-) Operatoren kombiniert werden, um Definitionen von praktisch unbegrenzter Komplexität festzulegen.

Zusätzlich zu der Inhaltserkennung in textbasierten Datenobjekten kann DeviceLock Discovery durch eine integrierte optische Zeichenerkennung (OCR) Textdaten aus Bildern in Dokumenten und Grafikdateien in vielen Bildformaten extrahieren und untersuchen. Mit 26 erkannten Sprachen, unter Verwendung von DeviceLock Schlüsselwort-Wörterbüchern und regulären Ausdrücken sowie durch Dutzende andere erweiterte Funktionen bietet diese hocheffiziente OCR die Möglichkeit, vertrauliche Daten in Datenbeständen mit grafischen Darstellungsformen zu entdecken und zu schützen. Einzigartig in DeviceLock Discovery ist dabei, dass das OCR-Modul in jeder umsetzenden Komponente eingesetzt werden kann: im DeviceLock Discovery Server, im DeviceLock Discovery Agent und im DeviceLock Agent. Die verteilte OCR-Architektur verbessert dabei die Gesamtleistung der Lösung enorm, weil auf den Endpunkten gespeicherte Grafikobjekte von den dortigen Agenten lokal gesucht und geprüft werden können. Somit wird die lokale Last auf dem Discovery Server genauso verringert wie der Scan-Datenverkehr im Unternehmensnetzwerk.



DeviceLock DISCOVERY

Maßnahmen

Sobald vertrauliche Inhalte in einer Datei erkannt wurden, die an der falschen Stelle gespeichert wurde, können eine Reihe von verhütenden Maßnahmen umgesetzt werden, um das Gefahrenpotenzial zu beseitigen:

- Log
- Alarm
- Benutzer benachrichtigen
- Berechtigungen setzen (für NTFS-Dateien)
- Verschlüsseln (mit EFS und nur für NTFS Dateien)
- Löschen
- Sicheres Löschen
- Archiv löschen (wenn eine Übertretung in einer Datei innerhalb eines Archivs gefunden wurde)

Lizenzierung

DeviceLock Discovery kann separat erworben und unabhängig von anderen DeviceLock DLP-Produkten verwendet werden.

DeviceLock Discovery kann als Upgrade für bestehende Installationen von DeviceLock oder der DeviceLock Endpoint DLP Suite lizenziert werden.

Alternativ kann DeviceLock Discovery mit DeviceLock und/oder mit der DeviceLock Endpoint DLP Suite erweitert werden.

Discovery: Produkt-Spezifikationen

Programm-Komponenten
- Discovery Agent
- DeviceLock Management Konsole
- DeviceLock Content Security Server (Discovery Server, Search Server)

Inhaltserkennung
- Für Windows-Endpunkte (Dateisysteme, E-Mail-Speicher angeschlossene Peripheriegeräte), Netzwerkfreigaben, Speichersysteme
- Textbasierter Inhalt, Datentypen: 4.100+ Dateitypen auf binärer Ebene, Dokumenten Eigenschaften, Text als Grafik (in Bildern) und Datentypen der Zwischenablage
- 120+ Formate (Microsoft Office, OpenOffice, Lotus 1-2-3, E-Mail- Verzeichnisse und Archive, CSV, DBF, XML, Unicode, GZIP, RAR, ZIP, etc.)
- Schlagwort-Übereinstimmung (vor- und selbstdefinierte Schlagwortverzeichnisse) und erweiterte Mustererkennung (RegExp) mit numerischen Bedingungen und booleschen „Und/Oder/Nicht"-Kombinationen
- Auf dem Endpunkt residente OCR Erkennung in 26 Sprachen mit integrierten DeviceLock Wörterbüchern und regulären Ausdrücken auch bei gedrehten oder gespiegelten Bildern

Systemanforderungen
- DeviceLock Agent: Windows XP/ Vista/7/8 oder Server 2003–2012 (32-/64-bit-Versionen); CPU Pentium 4, 64 MB RAM, HDD 200 MB
- DeviceLock Konsolen: Windows XP/ Vista/7/8 oder Server 2003–2012 (32-/64-bit-Versionen); CPU Pentium 4,2 GB RAM, HDD 200 MB
- DeviceLock Enterprise Server (optional): Windows Server ab 2003 R2; 2 × CPU Intel Xeon Quad-Core 2.33 GHz, RAM 8 GB, HDD 800 GB; MSDE or MS SQL Server 2008–2014

DeviceLock DISCOVERY

DeviceLock
Proactive Endpoint Security

DeviceLock Europe GmbH

Halskestr. 21
40880 Ratingen
Germany

Tel. +49.2102.131840
Fax +49.2102.1318429

info@devicelock.de
www.devicelock.de