DeviceLock ist ein führender Entwickler von einer Endpoint Data Leak Prevention Software und gab heute die DeviceLock DLP Suite 8 frei. Die DeviceLock DLP Suite 8 enthält die separat zu lizenzierende Komponente DeviceLock Discovery Server, mit dem Arbeitsstationen und Speichersysteme gescannt werden können, um bestimmte Arten von Inhalten nach vordefinierten Regeln zu identifizieren. Außerdem sind eine Optische Zeichenerkennung (OCR), die Unterstützung von AutoCAD-Dateien und viele weitere Neuerungen enthalten.

Was ist neu bei DeviceLock 8.0 (versus 7.3):

DeviceLock Discovery Server

- DeviceLock Discovery Server ist eine serverbasierte Komponente des DeviceLock Content Security Servers. DeviceLock Discovery Server scannt Arbeitsstationen der Benutzer-und Speichersysteme innerhalb und außerhalb des Unternehmensnetzwerks. Entsprechend vorher definierten Regeln werden bestimmte Arten von Inhalten gesucht und erkannt. Administratoren können Regeln zuweisen, welche der entdeckten Inhalte als vertraulich zu werten sind und die eigene Organisation nicht verlassen sollten.

DeviceLock:

- **Neue Funktion:** "Shadow Data Access"-Option wurde der DeviceLock Administrator Funktion hinzugefügt, um den Zugriff auf Schattenkopien nur mit entsprechender-Berechtigung zu erlauben. Dies gilt für den DeviceLock Service, den DeviceLock Enterprise Server und den DeviceLock-Agenten für Mac.
- Funktionserweiterung “Control log size”: Mit der neuen Implementierung wird die Protokollgröße gesteuert und die SQL Server Belastung durch den DeviceLock Enterprise Server (DLES) während der Logsammlung reduziert, wenn *"Überschreiben von Ereignissen bei Bedarf"* oder *"Ereignisse überschreiben, die älter sind als X Tage"*-verwendet wird.
- Verbesserte Loganzeige im DeviceLock Enterprise Server (DLES) und im DeviceLock Content Security Server. Innerhalb der DeviceLock Management Console wurde die Performance gerade bei einer großen Anzahl von Logeinträgen verbessert.
- Neue Audit-und Schattenkopie-Protokollberichte wurden hinzugefügt: "Am häufigsten gedruckte Dokumente", *"Aktivste Prozesse"* und *"Am häufigsten kopierte Dateien je Endung"*.
- Neuer Parameter *"TS-Geräte als normale Geräte melden"* hinzugefügt. Ermöglicht dem Benutzer während der Bericht Erzeugung, durchgereichte TS-Geräte wie normale physische Geräte zu behandeln.
- *"Log-Ereignis"* und *"Send Alert"* Flags in den Protokolleinstellungen der White List und den Content-Aware Rules überschreiben nun alle Log--und Alarmierungsoptionen auf Geräte- und Protokoll-Ebene.
- Zusätzliche neue administrative Warnung: *"Benachrichtigen, wenn Dienst deinstalliert wird."*
- *"Show Policy for Mac"* und *"Show Policy for Windows"*-Optionen wurden im Service-Settings-Editor und im Gruppenrichtlinien -Editor hinzugefügt. Mit diesen Optionen kann der Administrator die Parameter der DeviceLock Einstellungen verbergen, die nicht vom gerade konfigurierten Mac oder der gerade konfigurierten Windows-Plattform unterstützt werden.
- Die Einträge *"Remove ContentLock Policy"* und *"Remove NetworkLock Policy"* wurden dem Service Settings Editor hinzugefügt. Mit deren Hilfe kann der Administrator eine Einstellungsdatei (. dls) erstellen, die alle ContentLock oder NetworkLock Einstellungen entfernt, welche ansonsten zum DeviceLock Dienst übertragen würde.
- **Neue Funktion:** *"Log only“*. Diese Funktion ermöglicht es DeviceLock und Windows selbst dann funktionell zu bleiben, wenn eine Verletzung im Code des DeviceLock-Treibers mit der aktivierten

Option *"Unhook Protection"* gefunden wird. Anstatt einer Fehlermeldung über einen fatalen Fehler, wird ein Eintrag über diese Verletzung in das Audit-Log geschrieben.

- Allgemeine Verbesserungen, um mögliche Probleme auf lokalisierten (nicht englischen) Versionen von Windows mit der Zwischenablage, den Drucker- und MTP-Geräte Berechtigungen, sowie dem Auditing- und Shadowing zu vermeiden.
- Schnelleres Drucken bei Verwendung von Schattenkopien für den Gerätetyp Drucker.
- Besseres Speichermanagement des DeviceLock Dienstes.
- Die Optionen *"Display Available Devices Only"* und *"Report Available Devices Only"* wurden aus der DeviceLock Management Console und dem DeviceLock Enterprise Manager entfernt.
- Überarbeitete Integration der BitLocker To Go-Verschlüsselung von Windows 8.1.
- Verbesserte Unterstützung bei der Integration von PGP Whole Disk Encryption.
- Für eine einfachere Navigation und Anwendung wurde das Hauptinstallationspaket (setup.exe) optisch angepasst.
- Der DeviceLock-Agent für Mac bietet nun volle Unterstützung der Parameter " Log policy changes and Start/Stop events ".in den Service Optionen.
- Verbesserte grafische Oberfläche der Management Konsole.Die Webkonsole wurde mit allen Änderungen in der Management Konsole aktualisiert.

NetworkLock:

- Neuer Webmail-Dienst: Microsoft Outlook Web Access (OWA). Mithilfe des Service-Optionen Parameter *"OWA-Server"*, können Sie bestimmte Server-URLs festlegen, welche NetworkLock als genehmigte OWA-Server behandelt.
- Der Microsofts Umbenennung folgend, wurde SkyDrive in OneDrive umbenannt.
- Erweiterungen der File Sharing Kontrolle von Microsoft OneDrive, Google Drive, Dropbox, Yandex Disk und Amazon S3.
- Weiterentwickelte Webmail Kontrollen bei Hotmail, Gmail, Mail.ru, GMX.de, und web.de.
- Verbesserung im Bereich der Kontrolle sozialer Netzwerke bei Google+, Tumblr und Odnoklassniki.
- Weiterentwicklung der Whitelist Funktionalität für HTTP: Unter-URLs können granularer freigegeben werden, ohne einen Zugriff auf die gesamte Seite zu definieren. Zum Beispiel können Sie den Zugriff nur für *"Seite.de/Abschnitt/Unterabschnitt"* freigeben, ohne die gesamte *"Seite.de"*-Website zu ermöglichen.
- *"Log-Ereignis"* und *"Send Alert"*-Optionen stehen nun für alle unterstützten Protokolle in den White List Regeln zur Verfügung.
- Überarbeitung von Logging und Alarmierung im Bereich sozialer Netzwerke. Diese Aktionen finden nur noch dann statt, wenn der Benutzer versucht, tatsächlich auf Seiten sozialer Netzwerke zuzugreifen. Wenn der Benutzer nur auf Webseiten mit „like/share"-Buttons surft, die auf Webseiten verlinken, die unter der Kontrolle sozialer Netzwerke stehen, erfolgt kein Logging oder Alarmierung.
- Verbessertes Audit Log im Bereich Webmail und File Sharing, um übermäßige, nicht-informative Einträge zu vermeiden.
- Performance-Verbesserungen für den Umgang mit HTTPS-Verbindungen, wenn Platzhalter in den Protokolle White List Regeln für SSL benutzt werden.
- Verbesserter Umgang mit Platzhaltern in DNS-Namen bei deren Verwendung im Hosts-Feld von Protokoll Whitelisten oder der Basis IP Firewall.
- Neu gestaltete Technik zum Abfangen/Kontrollieren von Skype. Für diese Funktionalität wird das DLSkypePlugin nun nicht mehr verwendet.
- Weiterentwickelte Protokoll-Kontrollen für MAPI und Skype.

- Grundsätzliche Verbesserungen im Bereich Audit Log und Schattenkopien beim FTP-Protokoll.

ContentLock:

- Funktionserweiterung Optische Zeichenerkennung (Optical Character Recognition, OCR): Für eine weitere inhaltliche-Analyse durch inhaltsbasierten Regeln, ermöglicht die Verwendung der OCR-Technologie eine Extraktion von Text aus Bildern (z. B. gescannte Dokumente, Screenshots, etc.). Die integrierte OCR unterstützt die folgenden Sprachen: Bulgarisch, Dänisch, Deutsch, Englisch, Estnisch, Finnisch, Französisch, , Indonesisch, Italienisch, Katalanisch, Kroatisch, Lettisch, Litauisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Rumänisch, Russisch, Slowakisch, Slowenisch, Spanisch, Schwedisch, Tschechisch, Türkisch und Ungarisch.
- Die Möglichkeit einer Analyse von AutoCAD Dateien (dwg- und dxf-Dateien) im Hinblick auf enthaltenem Text, enthaltene Bilder oder eingefügte Dateien wurde hinzugefügt.
- Erweiterung der Liste der Dateitypenerkennung. Über 1.000 neue verifizierbare Dateitypen wurden hinzugefügt.
- Unterstützung für die Indizierung von Metadaten in Adobe Photoshop Bildern wurde hinzugefügt.
- Verbesserte Unterstützung für XLS-, DOC-, XLSX-, DOCX-, PPTX-, RTF-, EML-, RAR-, DBX- und PST-Formate bei inhaltsbasierten Regeln.
- In einer “komplexen” Regel können nun bis zu 50 einzelne, inhaltsbasierte Regeln mit Booleschen Operatoren (UND/ODER/NICHT) verbunden werden, um durch diese granularen Kriterien Datenbewegungen zu kontrollieren oder Schattenkopien anzufertigen.

DeviceLock Search Server:

- Zusätzliche Unterstützung für Synonym Textsuche in Englisch. Die Synonymsuche wird mit dem Symbol "&" am Ende des Wortes, für das Sie Synonyme finden wollen aktiviert. Wenn die Wörter in den gesammelten Daten von Audit Log und Schattenkopien enthalten sind, würde z.B. die Suche nach *„fast&“* auch das Synonym *„quickly“* finden.

Benutzerhandbuch:

- Für den leichteren Gesamtüberblick wurde das Benutzerhandbuch und die Hilfe-Dateien mit den Informationen über alle neuen v8.0 Features aktualisiert.

Alle Funktionsbereiche bilden als DeviceLock DLP 8 Suite den vollständigen Schutz vor einem Datenleck an allen Endpunkten (Laptop, Desktop oder Server), der Netzwerkkommunikation und nach Inhalten. DeviceLock ist für die unterschiedlichsten Bedrohungsszenarien granular skalierbar. Sprechen Sie mit uns: +49 (2102) 131840 oder schreiben Sie uns Ihren Wunschtermin für einen individuellen WebCast an info@devicelock.de.