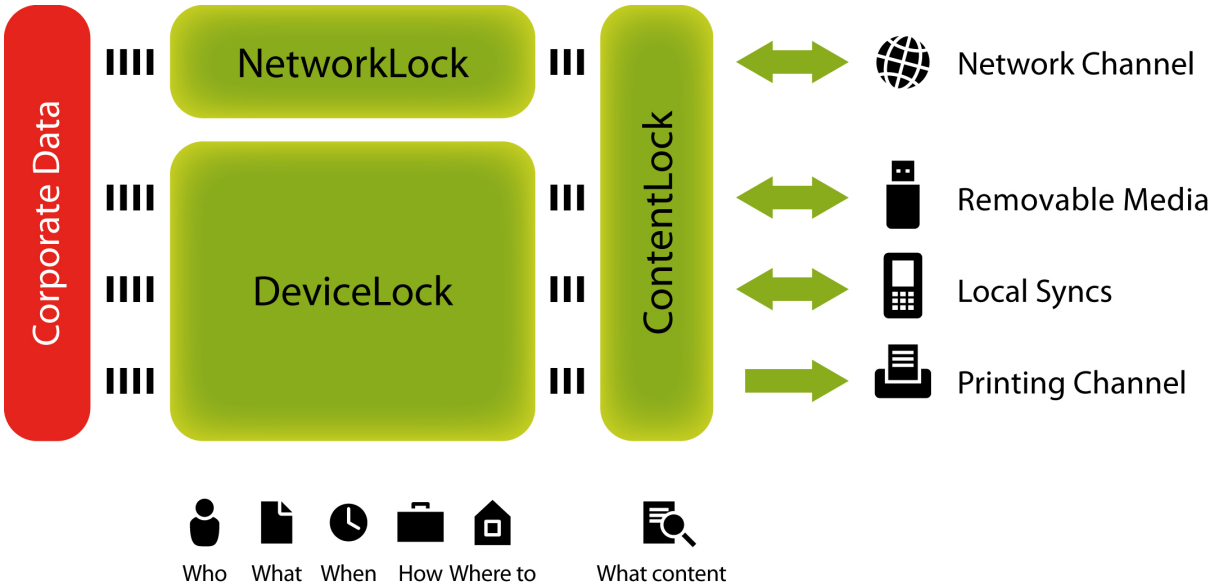
ZUR SOFORTIGEN VERÖFFENTLICHUNG

NEUE DEVICELOCK 7.0 ENDPOINT DATA LEAK PREVENTION SUITE JETZT IM HANDEL

Ratingen, 22. Februar 2011: DeviceLock, ein weltweit führender Anbieter von Endpoint Data Leak Prevention Software, gibt heute den Verkaufsstart der neuen DeviceLock 7.0 Endpoint DLP Suite bekannt. Die neue Version bietet umfassende Erweiterungen. So können Unternehmen erstmals die bewährte kontextbasierte Kontrolle von Datenflüssen auf ein breites Spektrum an Netzwerkkommunikationskanälen erweitern und mit der integrierten Inhaltsfilterung Datenschutzrichtlinien über alle Datenkanäle des Netzwerkendpoint hinweg durchsetzen.

Die DeviceLock 7.0 Endpoint DLP Suite erfüllt die Anforderungen von Unternehmen, die eine einfach zu handhabende und gleichzeitig kostengünstige Lösung suchen, um den nicht-autorisierten Datenabfluss von Microsoft Windows® Computern zu verhindern. Kern der Endpoint DLP Suite ist DeviceLock 7.0 für die umfassende kontextabhängige Kontrolle der lokalen Datenkanäle von Endpoint-Rechnern. Dazu zählen sämtliche Peripheriegeräte und die zugehörigen Anschlüsse, verbundene Smartphones und PDAs sowie alle lokal oder über das Netzwerk durchgeführten Druckvorgänge. Die Administration der DeviceLock-Agenten erfolgt immer komfortabel über eine zentrale Konsole. Optional können DeviceLock-Administratoren die ausgerollten Agenten aus der vertrauten Microsoft Windows Active Directory-Umgebung heraus über die Gruppenrichtlinienobjekte (GPOs) dynamisch verwalten und hier die erforderlichen DLP-Richtlinien zentral festlegen. Dabei können sie Zugriffsberechtigungen zum Beispiel nach Benutzer oder Benutzergruppen, Dateitypen, Schnittstellen, Datenflussrichtung (lesend/schreibend), Verschlüsselungsstatus, Wochentag und Uhrzeit vergeben.



Mithilfe des neuen, separat erhältlichen Moduls NetworkLock™ wird die kontextabhängige Kontrolle auf die meist genutzten Netzwerkprotokolle ausgeweitet. Hierzu zählen FTP/S, HTTP/S, SMTP/S, Telnet, Instant Messenger, Webmail-Services und Soziale Netzwerke wie Twitter™, Gmail™ und Facebook®. Ein weiteres neues Modul ist ContentLock™. Dieses ermöglicht die Überwachung und Filterung des Textinhalts von Dateien und Datenobjekten im Kontext ihrer Nutzung durch reguläre Ausdrücke (Regular Expressions), numerische Konditionierung und Boolesche Operatoren. Vorkonfigurierte Templates zur Erkennung von gemeinsamen Datenmustern, sensitiven Schlüsselwörtern, Dokumenteneigenschaften, Dateitypen und weiteren Faktoren sind bereits

enthalten. Sie lassen sich einfach konfigurieren oder kopieren, um unternehmensspezfische Regeln zu erstellen. Die komplette Suite bietet einen bislang einzigartigen Leistungsumfang unter Endpoint DLP-Lösungen im vergleichbaren Preissegment.

Die neue DeviceLock Version macht DLP auch für KMUs attraktiv

„Die Wikileaks-Skandale haben deutlich gezeigt, dass die Brisanz von Datenlecks kein Marketing-Hype ist, sondern eine reale Gefahr. Obwohl Datensicherheit mittlerweile von Unternehmen stärker gewichtet wird als Desaster Recovery, Identity- & Accessmanagement oder Regulatory Compliance, haben bislang nur etwa 15 Prozent eine DLP Lösung implementiert. Dies belegt eine Studie von Forrester Research aus dem Jahre 2010. Der Einsatz von DLP wurde bisher vornehmlich durch die damit verbunden hohen Kosten und die Komplexität der Lösungen verhindert," sagt Ashot Oganesyan, Gründer und Chief Technology Officer von DeviceLock. „Die neue DeviceLock Version beseitigt diese Hürde, da sie ein Maximum an Funktionalität und Zuverlässigkeit für ein Minimum an Anschaffungs- und Betriebskosten bietet. Wie das Wikileaks-Szenario mit der abtrünnigen CD veranschaulicht, sollten Unternehmen bei der Endpoint DLP zuerst die offensichtlichen Lücken von Ports, Geräten und Netzwerkkanälen durch kontextabhängige Kontrollen schließen und dann die Inhaltsfilterung für sensible oder verdächtige Datenflüsse hinzufügen. Die modulare Struktur von DeviceLock und das Lizenzmodell machen DLP für die breite Masse des Unternehmensmarkts praxistauglich und preislich attraktiv selbst für kleine und mittelständische Unternehmen."

Durch die Analyse von mehr als 80 Dateiformaten extrahiert und filtert ContentLock den Inhalt von Daten, die auf Wechsellaufwerke und Plug&Play-Speichergeräte kopiert oder über andere Ein- und Ausgabekanäle an Endpoint-Computern übertragen wurden. Dazu gehören zum Beispiel die Zwischenablage und – bei gleichzeitiger Verwendung von NetworkLock – die Netzwerkkommunikation über E-Mail und Webmail, Soziale Netzwerke, Instant Messenger Systeme, Webzugang, Dateitransfer und sogar Telnet-Sessions. Eine „Text-in-Picture" (TIP) Erkennungsfunktion sowie die Unterstützung von Archiv-Verzeichnissen bieten weiteren Schutz vor Datenlecks über Imagedateien und die Verwendung von Packprogrammen. NetworkLock ergänzt das Paket um eine portunabhängige Netzwerkprotokollierung, Applikationserkennung und -filterung, die Wiederherstellung von Nachrichten und Sessions mit der Extraktion von Dateien, Daten und Parametern sowie Ereignisprotokollierung und Datenspiegelungen.

Genauso effektiv wie DeviceLock derzeit mit TrueCrypt™, PGP™ und anderen Verschlüsselungs-produkten für Wechseldatenträger eingebunden werden kann, unterstützt DeviceLock 7.0 die in Windows 7 integrierte Datenverschlüsselung für mobile Datenträger BitLocker To Go™. DeviceLock-Kunden können die Microsoft-basierte Datenverschlüsselungstechnologie mit DeviceLock ohne Mehrkosten an ihren Windows 7-Endpoints nutzen. Da sich BitLocker To Go genauso wie DeviceLock zentral über das Microsoft Active Directory verwalten lässt, haben Unternehmen durch diese Kombination alle Möglichkeiten, Datenlecks an den Endpoints durch eine Medienverschlüsselung zu verhindern und dabei gleichzeitig die funktionellen und preislichen Vorteile zu nutzen.

Die Content-Filterung erhöht die Effizienz und Skalierbarkeit bei der Datenspiegelungsfunktion von DeviceLock auf allen Endpoint-Datenkanälen, einschließlich Wechsellaufwerke und Plug&Play - Datenträger, Netzwerkkommunikation, lokaler Synchronisation mit Smartphones und Dokumenten-druck. Jetzt können gespeicherte Datenströme im Hinblick auf genau die Informationen gefiltert werden, die für die Sicherheitsprüfung, Untersuchung einer Störung und die Spurensicherung von Bedeutung sind, bevor sie im Shadow Log gespeichert werden. Dadurch werden Speicherplatz und Bandbreitenbedarf im Netzwerk bei der Datenübermittlung des Shadow Logs an die zentrale Datenbank erheblich reduziert.

Die Endpoint-DLP von DeviceLock ist eine leicht bedienbare und skalierbare Lösung, die sich problemlos an die wachsenden Anforderungen im Unternehmen anpasst. Diese können ihre Endpoint-Datensicherheit durch Funktionen erweitern, die den Inhalt erkennen und das Netzwerk überwachen. Windows-Sicherheitsadministratoren arbeiten dabei mit dem vertrauten und bewährten MMC-Management Interface. Dadurch erfordert die Einarbeitung in DeviceLock und die entsprechende Konfiguration nur wenige Tage. Mit dem DeviceLock Group Policy Manager, einem maßgeschneiderten MMC-Snap-In für den Windows Group Policy Editor, können DeviceLock-Agenten unternehmensweit vollständig aus einer bestehenden Microsoft AD-Domäne heraus verteilt, konfiguriert und verwaltet werden.

Das Preismodell für die Komponenten der DeviceLock 7.0 Suite ist modular gestaltet. Dabei kann DeviceLock 7.0 als Kernmodul für die Kontrolle von Ports und Peripheriegeräten einzeln erworben werden. Da in der Installation der Suite alle Komponenten enthalten sind, können die Add-On-Module ContentLock und NetworkLock nach Bedarf lizensiert und aktiviert werden. So können Unternehmen je nach ihren Sicherheitsanforderungen die DLP-Funktionlitäten erweitern.

Über DeviceLock Inc.

Seit der Gründung im Jahr 1996 entwickelt und vertreibt DeviceLock Inc. (anfangs unter der Firmierung SmartLine) Endpoint Device Control und Data Leak Prevention-Softwarelösungen für kleine, mittelständische und Großunternehmen aller Branchen. Weltweit ist DeviceLock auf mehr als vier Millionen Computern in mehr als 60.000 Unternehmen und Behörden installiert und stellt sicher, dass alle Endpoint-Schnittstellen geschützt sind. Zum breiten Kundenstamm von DeviceLock Inc. zählen unter anderem Finanz- und Kreditinstitute, Landes- und Bundesbehörden, militärische Einrichtungen, Unternehmen des Gesundheitswesens, Bildungseinrichtungen und Telekommunikationsunternehmen. DeviceLock Inc. ist ein internationales Unternehmen mit Niederlassungen in San Ramon (Kalifornien, USA), London (Großbritannien), Ratingen (Deutschland) und Mailand (Italien).

Mehr Informationen zu DeviceLock erhalten Sie unter www.devicelock.com und www.devicelock.de

# # #

DeviceLock Europe GmbH
Mathias Knops
Halskestraße 21
40880 Ratingen
Tel.: +49 2102 89211-0
E-Mail: info@devicelock.de
Internet: http://www.devicelock.de

DeviceLock Pressekontakt
Marina Baader/Jürgen Höfling
presse-seitig
St.-Cajetan-Str. 10
81669 München
+49 89 45207500
marina.baader@presse-seitig.de
juergen.hoefling@presse-seitig.de