CenterTools

DriveLock und Windows 7

Warum Windows 7 alleine nicht ausreicht

CenterTools Software GmbH

Einleitung

Microsoft Windows 7 stellt einen großen Fortschritt in der Familie der Windows-Betriebssysteme dar. Viele der neuen Funktionen von Windows 7 werden Unternehmen bei der Verwaltung und Sicherung ihrer Netzwerkumgebungen unterstützen. Jedoch bieten einige der neuen Sicherheitsmerkmale von Windows 7 nur einen grundlegenden Schutz und sind schwierig zu verwalten. Bei der Bewertung von Windows 7 werden die meisten Unternehmen feststellen, dass Windows 7 allein nicht den erforderlichen Schutz bieten kann. Für eine effektive Datenverschlüsselung, Geräte- und Anwendungssteuerung werden Unternehmen weiterhin auf Lösungen von Drittanbietern wie CenterTools DriveLock zurückgreifen müssen. Dieses Whitepaper vergleicht den in Windows 7 enthaltenen begrenzten Schutz mit dem umfassenden Schutzpaket von DriveLock. Hierbei werden die folgenden Windows 7-Merkmale untersucht:

- Full Disk Encryption (*BitLocker*)
- Verschlüsselung von Wechseldatenträgern (*BitLocker To Go*)
- Anwendungssteuerung (*AppLocker*)
- Gerätesteuerung

Full Disk Encryption

BitLocker ist die Full Disk Encryption (Festplattenverschlüsselung), die in bestimmten Versionen von Windows Vista und Windows 7 enthalten ist. Bei richtiger Konfiguration bietet BitLocker einen starken und effektiven Schutz von vertraulichen Daten auf internen Festplatten. Jedoch ist die Anwendung nur dann möglich, wenn alle Computer bestimmte Systemanforderungen erfüllen. Windows bietet keine zentralen Überwachungsmöglichkeiten für BitLocker. Außerdem kann eine geteilte Pre-Boot-Authentifizierung aller Benutzer eines geschützten Computers die Sicherheit der Daten auf einem gemeinsam genutzten Rechner deutlich verringern.

Die folgende Tabelle führt die wichtigsten Unterschiede zwischen BitLocker und DriveLock Full Disk Encryption auf.

	Windows 7	DriveLock
Hardwareanforderungen	Um den BitLocker effektiv einzusetzen, muss der Computer einen Trusted Platform Module (TPM)-Chip enthalten. Es ist zwar möglich, den BitLocker ohne einen TPM-Chip zu benutzen, jedoch werden solche Konfigurationen von Microsoft nicht empfohlen, da sie schwierig anzuwenden sind und weniger Sicherheit bieten.	DriveLock benötigt keine spezielle Hardware für Full Disk Encryption.

	Windows 7	DriveLock
Unterstützte Client-Betriebssysteme	Nur in bestimmten teureren Windows Vista- und Windows 7-Editionen enthalten.	DriveLock wird von allen Windows XP-, Windows Vista- und Windows 7- Editionen unterstützt.
Unterstützung von Smartcard und Token	Die Smart Card- und Token-Authentifizierung steht während der Phase vor dem Booten nicht zur Verfügung.	DriveLock unterstützt zahlreiche Smart Card- und Tokentypen für die Pre-Boot-Authentifizierung.
Pre-Boot-Sicherheit	Der Schlüssel zur Festplattenverschlüsselung wird auf einem TPM-Chip gespeichert und unter Verwendung einer spezifischen PIN für diesen Computer geschützt. Bevor er Zugriff auf die Platte erhält, muss ein Benutzer die PIN eingeben. Benutzer, die mehrere BitLocker-geschützte Computer nutzen, müssen sich mehrere PINs merken. Jede Person, welche die PIN kennt (einschließlich früherer Angestellter), hat unbegrenzt Zugang zum Computer.	DriveLock unterstützt bis zu 2000 unterschiedliche Benutzer auf jedem Computer bei der Pre-Boot-Authentifizierung. Die Benutzer müssen nur ihre Windows-Zugangsdaten behalten, um die Authentifizierung durchzuführen. Wenn Angestellte das Unternehmen verlassen, können Pre-Boot-Accounts entfernt werden, um einen weiteren Zugang zu geschützten Computern zu vermeiden.
Single Sign-On für Windows.	Bei Windows 7 müssen sich die Benutzer zweimal authentifizieren, zuerst während der Pre-Boot-Phase und dann erneut beim Logon-Prompt von Windows.	DriveLock ermöglicht ein Single Sign-On. Die Benutzer authentifizieren sich während der Pre-Boot-Phase mit ihren Windows-Zugangsdaten und werden dann mit denselben Zugangsdaten automatisch in Windows eingeloggt.
Notanmeldung (Emergency-Logon)	Wenn ein Benutzer den Zugang zum Computer verloren hat, kann ein vorübergehender Zugang unter Verwendung eines 40 Zeichen umfassenden Schlüssels gewährt werden, bis ein Administrator die PIN für den TPM ändert. Jede Person, die diesen Schlüssel kennt, kann einen unbefristeten Zugang zum Computer erhalten.	Ein Administrator kann einmalige Zugangsdaten zum Anmelden für einen Benutzer bereitstellen, der sein Passwort vergessen hat. Hierbei wird ein Challenge/Response-Verfahren eingesetzt. Sobald der Benutzer sein Passwort ändert, können wieder normale Anmeldungsverfahren angewandt werden.

	Windows 7	DriveLock
Behandlung von beschädigten Festplatten	Viele Arten von Festplattenbeschädigung können dazu führen, dass Daten dauerhaft unzugänglich sind oder langwierige und schwierige Verfahren nötig sind, um die Festplatte zu entschlüsseln und den Zugang wiederherzustellen. Eine Wiederherstellung ist nicht möglich, wenn bestimmte Elemente der Festplattenstruktur nicht mehr gelesen werden können.	DriveLock erlaubt es den Administratoren, eine Verschlüsselung selbst von schwer beschädigten Festplatten zu entfernen, um einen Zugang zu allen Daten zu ermöglichen, die immer noch auf der physikalischen Festplatte vorhanden sind. Durch Fast Recovery können die Administratoren wichtige Dateien innerhalb von Minuten von einer beschädigten Festplatte auf Wechseldatenträger speichern. Die Daten können dann auf einen anderen Computer kopiert werden, damit die Benutzer ihre Arbeit schnell wieder aufnehmen können.
Zentrale Verwaltung	Die Administratoren können einige grundlegende BitLocker-Einstellungen unter Verwendung der Gruppenrichtlinien konfigurieren. Das Konfigurieren von Ausnahmen für einige Computer kann sehr schwierig sein. Selbst wenn BitLocker zentral verwaltet wird, muss ein lokaler Administrator den TP immer noch manuell für jeden Computer konfigurieren und die Festplattenverschlüsselung einleiten.	Die DriveLock-Einstellungen können mit den Gruppenrichtlinien einfach zentral konfiguriert werden. Gleichzeitig können problemlos Ausnahmen für einige Computer festgelegt werden. Die Festplattenverschlüsselung kann von einem zentralen Standort ohne örtlichen Zugang zum Computer eingeleitet werden.
Überwachung	Windows enthält keine Tools für eine effiziente Überwachung des Status der verschlüsselten Laufwerke im Netzwerk.	Das DriveLock Control Center ermöglicht einen Überblick über den Verschlüsselungsstatus im gesamten Unternehmen.

Nicht von Windows 7 unterstützte Full Disk Encryption-Szenarien

Die folgende Liste enthält nur einige Beispiele für übliche Full Disk Encryption-Anforderungen, die DriveLock problemlos erfüllt, die jedoch unter Windows 7 unmöglich oder nur schwierig zu konfigurieren sind:

- Single Sign-on unter Verwendung der Windows-Zugangsdaten.

- Gemeinsame Nutzung von Computern mit einer verschlüsselten Festplatte durch mehrere Benutzer, während separate Zugangsdaten für jeden Benutzer verwaltet werden, die nach dem Ausscheiden eines Nutzers widerrufen werden können.
- Einmalige Passwörter für eine Notanmeldung.

Gerätesteuerung

Windows 7 beinhaltet nur eine rudimentäre Gerätesteuerung, deren Verwaltung schwierig und mühsam ist. Statt einer dynamischen Ver- bzw. Entriegelung von Geräten für die Benutzer auf der Grundlage festgelegter Regeln schränkt Windows 7 die Installation von Gerätetreibern ein. Dies bedeutet, dass alle erforderlichen Gerätetreiber installiert sein müssen, bevor die Gerätesteuerung aktiviert wird. Die Änderung der Regeln zu einem späteren Zeitpunkt ist schwierig oder gar unmöglich. Außerdem stehen keine granularen Regeln zur Verfügung. Die meisten Regeln gelten weitgehend für bestimmte Geräteklassen. Die Einrichtung von Positivlisten (Whitelisting) für spezifische Geräte erfordert ein mühsames Editieren der Einstellungen für Registry und Gruppenrichtlinien.

Die nachstehende Tabelle vergleicht die Gerätesteuerung von Windows 7 mit den erweiterten Möglichkeiten von DriveLock.

	Windows 7	DriveLock
Benutzerspezifische Autorisierung von Geräten	Die Administratoren müssen manuell eine Liste der zulässigen Geräte erstellen, indem diese Geräte auf einem Computer installiert, die Hardwareeinstellungen für jedes Gerät gespeichert und diese Einstellungen schließlich in ein Gruppenrichtlinienobjekt (GPO) kopiert werden. Dies ist nicht besonders praktisch in einer Umgebung, in der es mehrere Computerkonfigurationen gibt. Die Geräte können nach Modell, jedoch nicht auf der Grundlage eines Gerätetyps oder einer spezifischen Seriennummer gesteuert werden.	DriveLock kann Computer auf installierte Geräte durchsuchen und es den Administratoren dann erlauben, diese Daten zu nutzen, um Whitelist-Richtlinien zu erstellen. Normalerweise müssen die Administratoren die Hardware-kennungen für jedes zulässige Gerät nicht kennen. Was noch wichtiger ist: DriveLock kann den Zugang von ganzen Geräteklassen erlauben oder verbieten oder den Zugang zu einem einzigen Gerät auf der Grundlage seiner Seriennummer erlauben.

	Windows 7	DriveLock
Gerätekontrolle	Windows 7 kann dies durchführen. Der Ausschluss von spezifischen Geräten aus einem Netzwerk stellt kein übliches Szenario dar und ist nicht sehr praktisch. Schon installierte Geräte können nicht blockiert werden.	Entsprechend den Regeln, die einen Zugang ermöglichen, kann DriveLock den Zugang gemäß Geräteklasse, Geräteseriennummer und Benutzer bzw. Gruppe blockieren. Das Blockieren gilt sogar für Geräte, die vor Anwendung der Richtlinie installiert wurden. Die Geräteinformationen über untersagte Laufwerke können von der Device Scanner Datenbank gesammelt werden, so dass ein Administrator das Gerät nicht auf einem Computer installieren und die Geräteinformationen manuell speichern muss.
Lese- und Schreibrechte für Wechseldatenträger steuern	Erlaubt es den Administratoren nur, jeglichen Zugang zu verschiedenen Typen von Wechseldatenträgern zu erlauben oder zu untersagen.	DriveLock erkennt mehr Gerätetypen und bietet eine äußerst granulare Steuerung. Der Lese- und Schreibzugang kann auf der Grundlage von Benutzer, Dateityp oder sogar eines spezifischen Geräts gesteuert werden.
Auditieren der Gerätenutzung	Windows 7 kann dies nicht durchführen.	Der DriveLock Device Scanner, das DriveLock Control Center sowie die Fähigkeiten zum Datenmitschnitt (File Shadowing) decken die Bedürfnisse der meisten Unternehmen für das Überwachen der Gerätenutzung und die Sammlung zum Nachweisen einer unerlaubte Nutzung ab.

	Windows 7	DriveLock
Vorübergehende Entriegelung von Geräten zur Durchführung von Ausnahmen	Windows 7 kann dies nicht durchführen.	DriveLock ermöglicht eine Online- und Offline-Entriegelung von Geräten für einen bestimmten Zeitraum. Dies erlaubt es dem Helpdesk-Personal, auf Situationen zu reagieren, in denen ein berechtigter Zugang zu Wechseldatenträgern benötigt wird, auch wenn die derzeit geltenden Richtlinien einen solchen Zugang verwehren.

Nicht von Windows 7 unterstützte Szenarien zur Gerätesteuerung

Die folgende Liste enthält nur einige wenige Beispiele für übliche Anforderungen an die Gerätesteuerung, die DriveLock ermöglicht, die jedoch mit Windows 7 unmöglich oder nur sehr schwierig konfiguriert werden können:

- Alle Benutzer können eine USB-Maus oder -Tastatur benutzen, jedoch keine Wechseldatenträger.
- Wechseldatenträger dürfen ausschließlich von Administratoren und Helpdesk-Personal verwendet werden.
- Es dürfen keine ausführbaren Dateien von Wechseldatenträgern auf einen Unternehmenscomputer kopiert werden (ausgenommen davon sind Administratoren).
- Alle auf USB-Speichersticks kopierten Daten sind zu verschlüsseln.
- Administratoren müssen verständigt werden, wenn ein Benutzer entgegen der Unternehmensrichtlinien einen Wechseldatenträger benutzt.
- Das Helpdesk-Personal muss zulassen können, dass ein Remote User eine Datei auf ein USB-Speicherstick kopiert, auch wenn dies normalerweise gegen die geltenden Richtlinien verstößt.
- Die Benutzer sollten nur vom Unternehmen ausgegebene USB-Speichersticks einsetzen dürfen.
- Es sollte den Nutzern erlaubt werden, Musik-CDs zu hören. Sie sollten jedoch keinen Zugang zu CDs mit Daten erhalten.

Verschlüsselung von Wechseldaten-trägern

BitLocker To Go gibt den Benutzern eine einfache Methode an die Hand, um alle Daten auf bestimmten Wechseldatenträgern zu verschlüsseln. Andere Medien wie z. B. CDs und DVDs können jedoch nicht verschlüsselt werden. Darüber hinaus ist der Zugang zu Daten auf verschlüsselte Speichersticks auf Computern mit früheren Windowsversionen nur lesend möglich. Die Verschlüsselung kann über die Gruppenrichtlinie zentral durchgesetzt werden. Die Administratoren können die Durchsetzung der Verschlüsselung und das zentrale Backup von

Recoveryinformationen für verschlüsselte Speichersticks konfigurieren. Bei der Durchsetzung von Verschlüsselungseinstellungen müssen die Unternehmen einen einheitlichen Ansatz verfolgen, da BitLocker keine Ausnahmen von den Richtlinieneinstellungen erlaubt. Der Recoveryprozess für verlorene Passwörter durch einen Recovery Agent erfordert einen physikalischen Zugang zu einem verschlüsselten Gerät. Für die Wiederherstellung durch einen Endbenutzer benötigt der Benutzer einen Recoveryschlüssel, der unbefristet für den Zugang zu einem Gerät verwendet werden kann. Dies gilt selbst nach dem Ausscheiden des Benutzers aus dem Unternehmen. Ein verschlüsseltes Gerät kann nicht zwecks Überprüfung der Einhaltung überwacht werden.

Die folgende Tabelle vergleicht Windows 7 BitLocker To Go mit den erweiterten Verschlüsselungsmöglichkeiten von DriveLock für Wechseldatenträger.

	Windows 7	DriveLock
Verschlüsselung von mobilen Daten	BitLocker To Go kann Daten auf USB-Speichersticks auf transparente Weise verschlüsseln. Es gibt jedoch auch bestimmte Einschränkungen wie die Tatsache, dass FAT das einzige unterstützte Dateisystem auf dem USB-Speicherstick ist. Zudem ist auf Windows XP oder Vista Client nur ein schreibgeschützter Zugang möglich.	DriveLock kann alle Daten auf oder von USB-Speichersticks und anderen Wechseldatenträgern transparent verschlüsseln. DriveLock kann auch durchsetzen, dass nur verschlüsselte Geräte auf einem Computer genutzt werden können. Mit DriveLock Mobile ist es möglich, einen verschlüsselten USB-Stick auch außerhalb einer DriveLock-Anlage (z. B. zu Hause) zu nutzen.
Geräteunterstützung	Es können ausschließlich USB-Medien verschlüsselt werden	DriveLock kann jede Art von Wechseldatenträger verschlüsseln und stellt einen Wizard zum Brennen von verschlüsselten CDs und DVDs bereit. Auf internen Festplatten können auch verschlüsselte Container eingerichtet werden.

	Windows 7	DriveLock
Wiederherstellung des Passworts	Vergisst ein Benutzer das Verschlüsselungspasswort, kann ein designierter Recovery Agent Zugang zu den Daten erhalten. Falls die Revoveryinformationen im Active Directory gespeichert waren, kann ein 40 Zeichen umfassender Schlüssel zur Wiederherstellung das Passworts ebenfalls abgerufen und dem Benutzer zur Verfügung gestellt werden. Jede Person, der dieser Schlüssel bekannt ist, wird in der Lage sein, einen unbefristeten Zugang zum Computer zu erhalten.	Vergisst ein Benutzer ein Verschlüsselungspasswort, kann das Helpdesk-Personal, dem eventuell ein Recovery Certificate zur Verfügung gestellt wurde, Zugang zu den Daten erhalten. Unter Einsatz eines Challenge/Response-Verfahrens kann ein Administrator auch einen einmaligen Code bereitstellen, um es einem Benutzer zu ermöglichen, das Passwort neu festzulegen.
Überwachung	Windows 7 verfügt weder über eine effektive Methode zur Überwachung der Nutzung von Wechseldatenträgern noch über eine Methode zur Feststellung, ob sie verschlüsselt sind und welche Daten auf diesen Geräten gespeichert werden.	DriveLock bietet eine umfassende Überwachung des Verschlüsselungsstatus, der Gerätenutzung und der Dateivorgänge mit dem DriveLock Control Center.

Nicht von Windows 7 unterstützte Szenarien für Wechseldatenträger

Die folgende Liste enthält nur einige wenige Beispiele für übliche Szenarien, die DriveLock ermöglicht, die jedoch mit Windows 7 unmöglich oder nur sehr schwierig konfiguriert werden können:

- Vollständiger Zugang mit Lese-/Schreibrechten zu verschlüsselten Laufwerken und Medien auf Computern, auf denen sich ältere Windowsversionen befinden
- Verschlüsselung von beschreibbaren optischen Medien wie CD-RW und DVD-RW
- Einmalige Codes für Daten-Recovery
- Zentrale Überwachung und Berichterstattung über Wechseldatenträger
- Erzwungene Verschlüsselung für bestimmte Laufwerke, während andere Laufwerke weiterhin unverschlüsselt bleiben
- Durchsetzung der Verschlüsselung für einige Benutzer, während andere Benutzer Zugang zu unverschlüsselten Datenträgern erhalten

Applikationskontrolle

Durch die Applikationskontrolle können Administratoren steuern, welche Anwendungen von den Benutzern gestartet werden können. Außerdem wird verhindert, dass nicht autorisierte Anwendungen auf einem Computer laufen. Windows 7 enthält AppLocker, einen stark

verbesserten Nachfolger der Richtlinien für Softwareeinschränkung (Software Restriction Policies), die in früheren Windowsversionen verfügbar waren. Sobald die Administratoren festlegen, welche Anwendungen auf einem Windows 7-Computer laufen dürfen, werden alle anderen Anwendungen automatisch blockiert. AppLocker kann effektiv sein, um die Nutzung von Anwendungen auf sehr standardisierten Desktops durchzusetzen, auf denen nur wenige Anwendungen laufen müssen. Es ist jedoch nicht praktisch, dieses Merkmal in den unterschiedlichen Computerumgebungen zu verwalten, die für die heutigen IT-Umgebungen typisch sind.

Die folgende Tabelle vergleicht Windows 7 AppLocker mit den erweiterten Möglichkeiten von Drive Lock.

	Windows 7	DriveLock
Systemanforderungen	Funktioniert nur mit Windows 7 und benötigt mindestens einen auf einem Windows Server 2008 R2 laufenden Domain Controller	Funktioniert mit Windows XP, Windows Vista und Windows 7. Es gibt keine Anforderung für eine Domain Controller-Version.
Festlegen, welche Anwendung laufen bzw. nicht laufen dürfen	Die Administratoren können Anwendungen auf der Grundlage eines Softwareherstellers, des Hash-Werts einer spezifischen Datei oder eines Speicherorts einer Datei festlegen. Die Regeln des Herstellers sind sehr flexibel und können eingesetzt werden, um alle signierten Programme, alle Programme vom selben Softwarehersteller, verschiedene Softwareversionen oder nur eine spezifische Version einer Anwendung zu erlauben. Anwendungsdateien im selben Ordner können in einem einzigen Schritt zu einer Regel hinzugefügt werden.	DriveLock kann dieselben Regeltypen wie Windows 7 anwenden. Darüber hinaus können integrierte Regeln für gängige Dateitypen wie alle Windows-Dateien eingesetzt werden, um schnell Regeln für Whitelists einzurichten. Durch die zusätzlichen Regeln für Dateibesitzer können die Benutzer problemlos alle Anwendungen ausführen, die von einem Administrator- oder Installationsaccount installiert wurden.
Erstellen von Regeln	Alle Anwendungen sind manuell zu White- oder Blacklists hinzuzufügen. Selbst in einem kleinen Netzwerk kann dies eine langwierige und mühsame Aufgabe darstellen.	DriveLock kann einen Referenzcomputer auf alle derzeit installierten Anwendungen durchsuchen und automatisch eine Whitelist-Schablone einrichten, damit alle diese Anwendungen laufen können. Es können auch Anwendungen von einer Online-Datenbank mit Hashes für über eine Million Anwendungen hinzugefügt werden.

	Windows 7	DriveLock
Verwaltung der Anwendungsregeln	Die meisten neuen Anwendungen müssen manuell zu den Regeln hinzugefügt werden, bevor die Nutzer die Anwendungen ausführen können. Die Softwareherstellerregeln können so konfiguriert werden, dass sie bei der Installation einer neuen Softwareversion nicht aktualisiert werden müssen.	Die DriveLock-Regeln, die auf den Zertifikaten der Softwarehersteller basieren, können auch so konfiguriert werden, dass sie aktualisierte Versionen eines Programms automatisch zulassen. Zusätzlich erlauben es die Regeln für Dateibesitzer, dass neue Anwendungen automatisch ausgeführt werden können, wenn sie von einem Administrator oder einem anderen designierten Benutzer installiert wurden.
Granularität	Jeder Satz AppLocker-Regeln wird auf allen Computern durchgesetzt, für die ein Gruppenrichtlinienobjekt gilt. Die Richtlinie kann separate Genehmigungen für verschiedene Benutzer und Gruppen beinhalten.	Zusätzlich zur Festlegung von Genehmigungen für Benutzer und Gruppen ermöglichen die DriveLock-Richtlinien eine wesentlich größere Granularität. Beispielsweise können Richtlinien so festgelegt werden, dass sie nur zu bestimmten Tageszeiten oder nur dann gelten, wenn ein Computer mit einem bestimmten Netzwerk verbunden ist.
Auditieren und Überwachen	Erfolgreiche und abgelehnte Versuche zum Start einer Anwendung werden nur im lokalen Windows-Ereignisprotokoll gespeichert.	Mit dem DriveLock Control Center können Administratoren die Nutzung der Anwendungen auf allen Client- Computern zentral auditieren und detaillierte Berichte erstellen.

Nicht von Windows 7 unterstützte Szenarien zur Applikationskontrolle

Die folgende Liste enthält nur einige wenige Beispiele für übliche Szenarien zur Applikationskontrolle, die DriveLock ermöglicht, welche jedoch mit Windows 7 unmöglich oder nur sehr schwierig konfiguriert werden können:

- Automatisches Whitelisting aller Anwendungen, die von bestimmten Administrator- oder Service Accounts installiert werden
- Blacklist- oder Whitelistregeln auf der Basis einer unternehmensweiten Anwendungsdatenbank
- Regeln basierend auf einer Online-Datenbank mit Millionen Anwendungen
- Auf Whitelist-Schablonen basierende Regeln, die alle ausführbaren Dateien einschließen, die Teil komplexer Anwendungen sind
- Regeldurchsetzung auf der Grundlage des Netzwerkstandorts (Büro, auf Reisen usw.)

Sicherheitsmanagement

Auch wenn jedes der in diesem Whitepaper beschriebenen Merkmale von Windows 7 zentral unter Einsatz der Gruppenrichtlinien verwaltet werden kann, müssen sich die Administratoren mit den Feinheiten der Komponente vertraut machen. Die Einrichtung der zentralen Speicherung von Recoveryschlüsseln ist schwierig und erfordert verschiedene Schritte für eine Full Disk Encryption und die Verschlüsselung von Wechseldatenträgern. Die Tools von Microsoft zur Wiederherstellung dieser Schlüssel sind wenig intuitiv und eingeschränkt. Außerdem gibt es keinen effektiven Mechanismus für eine zentrale Überwachung und Berichterstattung.

DriveLock verwendet eine integrierte Konsole zum Konfigurieren aller Einstellungen und für die Key Recovery. Diese Managementkonsole ist intuitiv und wurde so gestaltet, dass sie die Administratoren durch die häufigsten Aufgaben führt, um Fehler zu vermeiden, die sich negativ auf die Produktivität des Benutzers auswirken könnten. Die Managementkonsole enthält außerdem leistungsstarke Tools zur Durchsetzung der Richtlinien für Fehlerbehebung. Mit dem DriveLock Control Center können Administratoren umfassende Berichte über die Benutzeraktivität erstellen. Außerdem enthält es eine ausgereifte Drill-Down-Funktion, die den Nachweis einer unerlaubten Nutzung (forensic analysis) ermöglicht.

Schlussfolgerung

Bei sehr kleinen Unternehmen oder solchen mit einem äußerst begrenzten Hardwarebestand kann Windows 7 ausreichend sein, um die Gerätenutzung zu steuern. Jedoch ist CenterTools der Meinung, dass Windows 7 die Anforderungen an Gerätesteuerung und -sicherheit für die große Mehrheit der Unternehmen und Organisationen nicht erfüllt. Außerdem erfordert eine granulare Gerätesteuerung mit den in Windows 7 eingebauten Funktionen einen unverhältnismäßig hohen Aufwand an Verwaltungsressourcen. Unternehmen, die eine Migration auf Windows 7 durchführen, werden feststellen, dass zusätzliche Software erforderlich ist, um eine effektive und leistungsstarke Steuerung der mobilen Geräte zu ermöglichen. DriveLock bietet eine granulare und umfassende Gerätesteuerung, die sich durch einfache Implementierung, Verwaltung und Nutzung auszeichnet.