DriveLock

WHITEPAPER

DEVICE CONTROL

Überwachung und Steuerung externer Medien und Schnittstellen

Von Andreas Fuchs

EINLEITUNG

Wie viel Speicherplatz wird benötigt, um sensible Daten rund einer halben Million Menschen zu transportieren? Und zu verlieren? Ein einziger USB-Stick reicht. Das erfuhren vor wenigen Jahren die Einwohner und Einwohnerinnen der japanischen Stadt Amagasaki, als besagter USB-Stick mit ihren persönlichen Daten verloren ging.

Was war passiert? Ein Mitarbeiter eines IT-Dienstleisters der Stadtverwaltung hatte seine Tasche inklusive des USB-Sticks nach einem alkoholreichen Abend verloren. Dass es Richtlinien gab, gegen die der Mitarbeiter verstoßen hatte, ist bei einem Datenverlust dieses Kalibers im Grunde irrelevant. Denn für was gibt es Richtlinien, wenn sie durch eine einzelne unautorisierte Handlung problemlos umgangen werden können?

Unternehmen arbeiten mit enormen Mengen an sensiblen Informationen, die verarbeitet, transportiert und vor allem geschützt werden müssen. Trotz aller Digitalisierung und Vernetzung von Systemen sind externe Datenträger wie USB-Sticks, externe Festplatten aber auch Smartphones oder Bluetooth-Verbindungen regelmäßig im Einsatz, um Daten von A nach B zu transportieren. Dabei stellen sie ein erhebliches Sicherheitsrisiko dar.

WARUM?

Sie sind ein Einfallstor für Malware:
Infizierte USB-Geräte sind eine häufige Quelle für Malware – insbesondere in industriellen Umgebungen.

Sie ermöglichen Datenlecks und Datendiebstahl:
Über externe Geräte werden sensible Informationen schnell, einfach und häufig entwendet. Dabei ist es egal, ob Mitarbeitende in guter oder schlechter Absicht handeln. Daten, die sich unautorisiert und unverschlüsselt außerhalb des gesicherten Unternehmensnetzwerks befinden, sind ein kritisches Sicherheitsrisiko.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hebt in seinen Berichten regelmäßig die größten Cyber-Bedrohungen hervor. Infizierte USB-Geräte sind häufige Quellen für Viren und Malware – insbesondere in industriellen Umgebungen. Daher ist strenge Gerätekontrolle wichtig, um ihre Nutzung zu überwachen und einzuschränken.

DriveLock Device Control ist eine hochmoderne Sicherheitslösung, die Unternehmen effektiv vor Datenverlust und Malware-Angriffen schützt, die durch den Anschluss externer und unbefugter Geräte entstehen können. DriveLock Device Control ermöglicht Organisationen eine präzise Kontrolle über den Zugriff auf externe Speichermedien und Schnittstellen ohne den täglichen Betrieb für Nutzer einzuschränken – eine wichtige Voraussetzung und essenzieller Bestandteil jeder umfassenden Sicherheitsstrategie.

INHALT

1

FEATURES

FEATURES

DRIVELOCK DEVICE CONTROL UND ENCRYPTION 2-GO FEATURES:

- Nur gewünschte Geräte und externe Laufwerke werden zugelassen
- Proaktives Unterbinden von CD/DVD-Brennern
- Containerbasierte Verschlüsselung oder Verzeichnisverschlüsselung
- Konfigurierbare Benutzerauswahldialoge beim Anschluss externer Laufwerke
- Kein Dateitransfer über nicht zugelassene Medien
- Einfache Konfiguration integrierter Geräte
- Forensische Analyse und Reporting

ERGEBNIS:

- Vermeidung von mit Malware infizierten Fremd-USB-Sticks
- Datenabsicherung durch sichere Authentifizierung und Freigabeprozesse
- Einfache Skalierbarkeit dank Flexibilität mit minimalem Aufwand
- Zugangsberechtigungen für Mitarbeiter im gesamten Unternehmen
- Kein unerlaubter Datenausgang
- Individuell anpassbare Regelwerke für verschiedene Unternehmensbereiche
- Verschlüsselte „Corporate USB-Sticks" für Datenaustausch innerhalb des Betriebs

2

ANWENDUNGSFÄLLE

ANWENDUNGSFÄLLE

Ein anschauliches Beispiel für effektive Maßnahmen zur Kontrolle und Sicherung mobiler Datenträger findet man in medizinischen Einrichtungen, wo häufig sensible Daten weitergegeben werden. Der Einsatz externer Datenträger birgt daher ein erhebliches Sicherheitsrisiko. So könnten beispielsweise böswillige Akteure manipulierte USB-Sticks gezielt platzieren, um über sogenannte „Bad USB-Drop Attacks" Viren oder Malware ins Unternehmensnetzwerk einzuschleusen. Dieses Risiko besteht ebenfalls bei Smartphones, die sich über Bluetooth verbinden.

Unternehmen und Einrichtungen sollten effektive Maßnahmen ergreifen, um diese Risiken zu minimieren. Sie sollten überwachen und steuern, welche Geräte an ihre Systeme angeschlossen werden dürfen. Die Implementierung von Richtlinien ermöglicht es, den Zugang nur bestimmten, zuvor genehmigten mobilen Datenträgern und Anwendern zu gestatten. Sensible Daten müssen automatisch verschlüsselt werden, bevor sie auf USB-Sticks kopiert werden. Darüber hinaus kann auch die Datenübertragung über Bluetooth-Geräte kontrolliert werden, um unbefugten Zugriff und Datenlecks zu verhindern.

Diese Strategien ermöglichen es Unternehmen, ihre Netzwerke effektiv vor externen Bedrohungen zu schützen und gleichzeitig die Einhaltung von Datenschutzstandards zu gewährleisten.

Dieser Anwendungsfall zeigt, dass Device Control eine zentrale Rolle in modernen IT-Sicherheitskonzepten spielt und Sicherheitslücken schließt, die durch den Einsatz externer Geräte entstehen.

ANWENDUNGSFÄLLE

DriveLock wird in einer Vielzahl von Branchen und Szenarien eingesetzt, um die Datensicherheit zu erhöhen und die Einhaltung von Compliance-Anforderungen zu gewährleisten.

Finanzsektor: Banken und Finanzdienstleister setzen DriveLock ein, um den Datenaustausch über externe Geräte zu regulieren und finanzielle Informationen vor Diebstahl zu schützen.
Gesundheitswesen: Krankenhäuser nutzen DriveLock, um Patientendaten gemäß den HIPAA-Vorschriften zu schützen, indem der Zugriff auf Speichermedien strikt kontrolliert wird.
Öffentlicher Sektor: Behörden implementieren DriveLock, um die Sicherheit staatlicher Daten zu gewährleisten und unerlaubte Datenübertragungen zu verhindern.
Fertigungsindustrie: Hersteller verwenden DriveLock, um geistiges Eigentum in Form von Konstruktionsdaten und Patenten abzusichern und gleichzeitig die kritische Infrastruktur vor Schadsoftware zu schützen.

Bildungseinrichtungen: Schulen und Universitäten setzen DriveLock ein, um Forschungsdaten zu schützen und gleichzeitig die Compliance mit Datenschutzgesetzen sicherzustellen.
In all diesen Szenarien ermöglicht DriveLock eine Balance zwischen Sicherheit und Anwendungsfreundlichkeit und sorgt so dafür, dass Mitarbeitende ihre Aufgaben ohne unnötige Einschränkungen erfüllen können, während das Unternehmen zuverlässig vor Datenverlust und -Diebstahl geschützt ist.

> "Wir sind sehr zufrieden mit der Lösung von DriveLock. Diese funktioniert einwandfrei und ist so flexibel, dass sie uns zahlreiche Ausbaumöglichkeiten bietet. Auch für neue Anforderungen an die IT-Sicherheit sind wir mit DriveLock sehr gut aufgestellt."

Thomas Ochs, CIO Villeroy & Boch

3

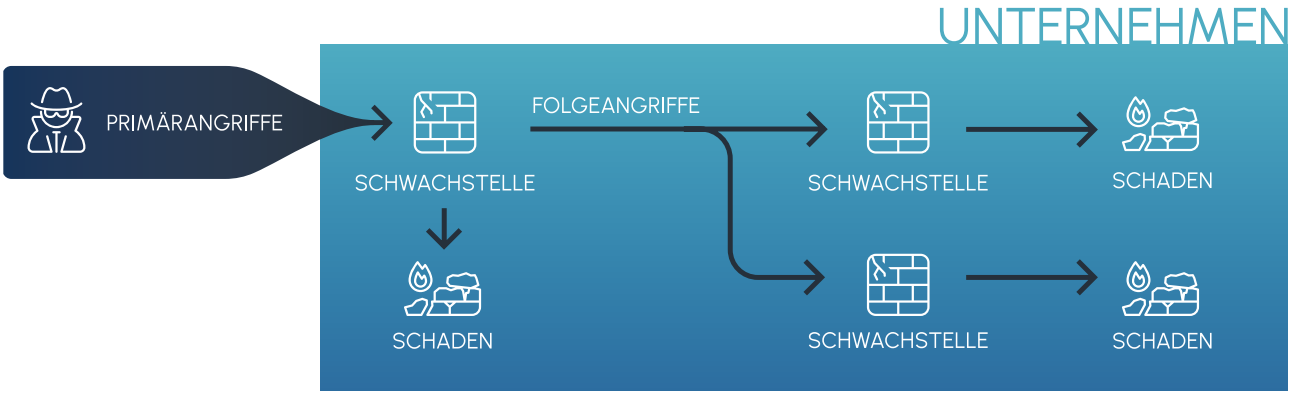
SCHLÜSSELASPEKTE

SCHLÜSSELASPEKTE

Die Bedeutung von Device Control lässt sich anhand mehrerer Schlüsselaspekte verdeutlichen

Prävention von Datenlecks und Datendiebstahl:
Ein zentrales Risiko, das von externen Geräten ausgeht, ist die Gefahr unbeabsichtigter Datenlecks oder gezielten Datendiebstahls. Angreifer können externe Geräte einsetzen, um sensible Informationen aus dem Unternehmensnetzwerk zu stehlen. Die Implementierung von Device Control hilft, diese Risiken zu minimieren. Diese Technologie beschränkt den Zugriff auf autorisierte Geräte und Benutzer, überwacht und kontrolliert Datenübertragungen und stellt sicher, dass alle Daten auf externen Medien obligatorisch verschlüsselt sind.

Schutz vor Malware und Ransomware:
Externe Geräte sind ein Einfallstor für Malware und Ransomware. Einmal eingedrungen, kann sich eine Schadsoftware schnell im Netzwerk verbreiten und erheblichen Schaden anrichten. Device Control kann die Einführung - verursacht durch einen Primärangriff - und Ausbreitung von Malware - verursacht durch einen Folgeangriff - verhindern, indem es nur vorab geprüfte und vertrauenswürdige Geräte zulässt.



Einhaltung von Compliance-Anforderungen:
Viele Industrien unterliegen strengen regulatorischen Anforderungen bezüglich des Umgangs mit sensiblen Daten (bspw. der DSGVO in Europa oder HIPAA in den USA). In der EU kommt nun die NIS2-Richtlinie hinzu, die ein Mindestmaß an Sicherheitsstandards verpflichtend macht.
Die DORA-Richtlinie (Digital Operational Resilience Act) der EU fordert robuste IT-Syteme zur Stärkung der digitale Widerstandsfähigkeit von Finanzinstituten, sie adressiert Cyberrisiken und schafft eine einheitliche Regulierung für den Finanzsektor. Viele Sicherheitsrichtlinien erfordern den Einsatz kritischer Security Controls wie Device Control. Sie unterstützt Unternehmen dabei, diesen Anforderungen gerecht zu werden und bietet die Grundlage für die Überwachung und Kontrolle des Datenzugriffs und -transfers über externe Geräte.

SCHLÜSSELASPEKTE

Innere Bedrohungen:
Device Control reduziert das Risiko interner Bedrohungen und verhindert den unautorisierten Transfer. Flexibilität und Produktivität: Ein modernes IT-Sicherheitskonzept muss Sicherheit gewährleisten, ohne die Produktivität zu beeinträchtigen. Device Control ermöglicht eine differenzierte Zugriffskontrolle, bei der nach Gerätetyp, Benutzergruppe oder sogar nach spezifischen Umständen (wie Netzwerkstandort) unterschieden werden kann. Dies stellt sicher, dass Mitarbeitende die notwendigen Werkzeuge für ihre Arbeit sicher nutzen können, ohne unnötige Hindernisse.

Vertrauen und Reputation:
Die Sicherung von Kundendaten und geistigem Eigentum ist entscheidend für das Vertrauen in ein Unternehmen und seine Reputation auf dem Markt.

Geschäftskontinuität:
Durch die Prävention von Sicherheitsvorfällen hilft Device Control dabei, die Betriebskontinuität zu wahren und teure Ausfallzeiten zu vermeiden.

Strategische Datennutzung:
Eine robuste Device Control-Strategie ermöglicht es Unternehmen, ihre Daten sicher und effektiv zu nutzen und somit Wettbewerbsvorteile zu erzielen.

Skalierbarkeit:
IT-Infrastrukturen wachsen und verändern sich ständig. Eine Device Control-Lösung muss daher in der Lage sein, mit dem Unternehmen zu skalieren.

Diversität der Geräte:
Die große Bandbreite und Diversität von Geräten und Betriebssystemen in modernen IT-Umgebungen stellt hohe Anforderungen an die Kompatibilität und Flexibilität von Device Control-Lösungen.

Benutzerfreundlichkeit:
Lösungen müssen sowohl sicher als auch benutzerfreundlich sein, um eine hohe Akzeptanz unter den Mitarbeitern zu gewährleisten.

Schnelle Reaktionsfähigkeit:
Im Falle eines Sicherheitsvorfalls muss eine Device Control-Lösung eine schnelle und effektive Reaktion ermöglichen, um den Schaden zu minimieren.

4

FUNKTIONEN

FUNKTIONEN

Device Control kommt mit einer Vielzahl an Sicherheitsfunktionen. Zu den Vorteilen gehören:

Detaillierte Kontrolle und Überwachung:
IT-Verantwortliche haben die Möglichkeit, präzise Vorgaben für unterschiedliche Arten von Geräten zu erstellen. Diese Regelungen dienen dazu, den Austausch von Daten mit externen Speichermedien sorgfältig zu kontrollieren. Darunter fallen USB-Sticks, externe Festplatten, Bluetooth-Geräte, Smartphones und weitere externe aber auch intern verbaute Geräte. Es können Listen mit zugelassenen oder blockierten Geräten angelegt werden, die auf Kriterien wie Hersteller, Modell oder Seriennummer basieren.

Verschlüsselung:
DriveLock bietet die sichere Verschlüsselung von Daten auf externen Medien an, um die Datenintegrität und -sicherheit zu gewährleisten, selbst wenn die Geräte das Unternehmen verlassen. Neben der eigenen Verschlüsselungsmethode kann DriveLock die Datenträger auch mit der integrierten BitLocker To Go Lösung von Microsoft verschlüsseln.

Dateifilter-Vorlagen zur präzisen Datenkontrolle:
DriveLock ermöglicht die Verwendung von Dateifiltern, um spezifische Lese- und Schreibberechtigungen für Wechseldatenträger zu definieren, einschließlich individueller Whitelist-Regeln. Mit vorgefertigten Filtervorlagen lassen sich leicht mehrere dieser Regeln nach Bedarf erstellen. Ein wesentliches Feature von DriveLock ist der Datei-Header-Check, der sicherstellt, dass eine Datei mit einer bestimmten Endung tatsächlich dem erwarteten Format entspricht und nicht einfach umbenannt wurden.

Regulierung des Datenvolumens:
DriveLock bietet die Möglichkeit, das Datenvolumen, das zwischen einem Wechseldatenträger und einem Endgerät transferiert wird, genau zu kontrollieren. Diese Funktion ermöglicht eine genaue Beschränkung der übertragbaren Datenmenge, was vor Datenmissbrauch schützt. Verhaltensanalyse: Erkennung von Anomalien im Benutzerverhalten, die auf potenzielle Sicherheitsverletzungen hinweisen können.

Integrierte Threat Prevention:
Schutz vor Malware und Zero-Day-Angriffen durch Integration mit Anti-Virus- und Anti-Malware-Lösungen. DriveLock erzwingt das Scannen des angeschlossenen Mediums auf Schadsoftware bevor der Zugriff freigegeben wird.

FUNKTIONEN

Flexible Richtliniendefinition:
DriveLock ermöglicht eine fein abgestimmte Definition von Zugriffsrechten auf externe Laufwerke sowie Geräte, die sich nach der Rolle des Nutzers und der Art des Geräts richtet. Zudem erlauben Zeit- und Kontextabhängige Regeln eine Anpassung der Zugriffsrechte basierend auf Uhrzeit, Standort oder Netzwerkumgebung.

Echtzeitüberwachung und Alarmierung:
Die Device Control-Lösung von DriveLock ermöglicht eine Echtzeitüberwachung des Gerätezugriffs und benachrichtigt Administratoren sofort über verdächtige Aktivitäten oder Verstöße gegen Sicherheitsrichtlinien. Dies ermöglicht es Administratoren, schnell auf potenzielle Sicherheitsbedrohungen zu reagieren und entsprechende Maßnahmen zu ergreifen.

Integrierte Security-Awareness-Lösungen:
Die Integration von Security-Awareness-Kampagnen ist ein entscheidender Schritt zur Maximierung der IT-Sicherheit in Unternehmen. Durch die Einbindung von Device Control in das Security-Awareness Modul können Mitarbeitende beim Anschließen eines Mediums gezielt über die Gefahren informiert werden, die von der unsachgemäßen Verwendung externer Geräte ausgehen. Das vernetzte Lernen stärkt nachhaltig ein verantwortungsvolles Handeln somit die Sicherheit des Unternehmens.

Auditierung:
DriveLock bietet eine gründliche Auditfunktion, die eine Vielzahl von Ereignissen wie Warnungen, Fehler, Informationsmeldungen und spezifische Audit-Ereignisse erfasst. Für jedes Ereignis werden detaillierte Informationen wie ID, Kritikalität und eine ausführliche Beschreibung bereitgestellt, was Administratoren hilft, Systemaktivitäten genau zu verfolgen und Sicherheitsprobleme effizient zu identifizieren und zu beheben.

Nachverfolgung durch Schattenkopien:
DriveLock bietet eine Funktion für Schattenkopien, die automatisch Kopien von Dateien anlegt, die von oder auf Wechseldatenträger übertragen werden. Diese Funktion dient der Nachverfolgung und Analyse von Dateiübertragungen, was insbesondere für die Aufklärung von Datenlecks von Bedeutung ist. Die Schattenkopien können sowohl auf individuellen Client-Systemen als auch zentral auf einem Server gespeichert werden, wobei Nutzer spezifische Einstellungen wie Dateiauswahl, Speicherlimits und Löschrichtlinien konfigurieren können. Über die DriveLock Management Konsole lassen sich diese Kopien einsehen und bei Bedarf für weitere Untersuchungen extrahieren und sichern.

FUNKTIONEN

Einfache und sichere Verwaltung von Bluetooth-Geräten:
Die DriveLock Lösung für das Management von Bluetooth-Geräten ermöglicht es Administratoren, den Einsatz dieser Geräte präzise zu kontrollieren. Sie können spezifische Gerätetypen wie Mäuse zulassen, während sie andere, potenziell unsichere Geräte sperren. Diese granulare Steuerung umfasst das Blockieren unerwünschter Funktionen und Dienste sowie die flexible Anpassung von Berechtigungen basierend auf Gerätehersteller, -klasse und -typ. DriveLock vereinfacht so die Konfiguration und steigert die Sicherheit, indem nur vertrauenswürdige Bluetooth-Geräte und -Dienste zugelassen werden.

Benutzerfreundliche Self-Service-Freigabe von Geräten:
DriveLock ermöglicht Endbenutzern, die Freigabe von externen Geräten selbst zu verwalten, sofern dies von Administratoren genehmigt wurde. Diese Flexibilität erlaubt es, dass die angeschlossenen Datenträger oder Geräte temporär genutzt werden können. Sowohl die Endbenutzer als auch der Helpdesk werden über solche Freigaben informiert, was den Verwaltungsaufwand reduziert und gleichzeitig die Sicherheitskontrollen aufrechterhält.

Workflow-gesteuerte Freigabeanfragen:
Damit können Endbenutzer direkt bei gesperrten Laufwerken oder Geräten Freigabeanfragen stellen. Administratoren reagieren zentral auf diese Anfragen, indem sie die Anfragen entweder genehmigen oder ablehnen. Nach der Entscheidung werden Endbenutzer mittels Push-Benachrichtigungen über den Status ihrer Anfrage informiert. Diese Funktion fördert eine effiziente und nahtlose Kommunikation zwischen Administratoren und Endbenutzern.

Durchgängige Richtlinienanwendung auch offline:
DriveLock gewährleistet, dass die festgelegten Richtlinien und Konfigurationen auch dann Anwendung finden, wenn Endbenutzer offline sind. Die konfigurierten Rechte und Einstellungen bleiben unverändert aktiv und sichern somit kontinuierlichen Schutz und Richtlinieneinhaltung auch ohne Netzwerkverbindung.

Sicherheitsmanagement in virtuellen Umgebungen:
DriveLock bietet Device Control für den Einsatz in Citrix-Umgebungen und auf Terminalservern. Für alle verbundenen Laufwerke eines Clients können einfache Berechtigungen vergeben werden, die auf dem verwendeten Verbindungsprotokoll basieren, z.B. Windows Terminal Services (RDP) oder Citrix XenApp (ICA).

FUNKTIONEN

Rollenkonzept:
DriveLock verfügt über ein besonders detailliertes administratives Rollenkonzept, das selbst die Verwaltung durch Helpdesk-Mitarbeiter umfasst.

Automatisierung und Benutzerfreundlichkeit:
Durch die Automatisierung der Richtliniendurchsetzung und eine intuitive Benutzeroberfläche minimiert DriveLock den administrativen Aufwand und verbessert die Nutzerakzeptanz.

Reporting und Compliance-Unterstützung:
Umfangreiche Berichtsfunktionen erleichtern die Überwachung der Gerätenutzung und unterstützen die Einhaltung von Compliance-Vorgaben.

Datenschutz nach DSGVO-Standards:
Die Datenmaskierungsfunktion ermöglicht es, sensible Benutzer- und Computerdaten in Übereinstimmung mit der DSGVO zu verbergen, indem echte Namen durch Platzhalter ersetzt werden. Dies verhindert die personifizierte Analyse des Benutzerverhaltens. Das Aktivieren und Deaktivieren der Funktion ist speziell berechtigten Personen vorbehalten, was durch ein Mehraugen-Prinzip für zusätzliche Sicherheit sorgt.

5

ÜBERSICHT

ÜBERSICHT

Schnittstellenkontrolle
Grundlegende Gerätekontrolle (ein/aus)
Steuerung aller Arten von Laufwerken (USB-Speicher, CD/DVD, SD usw.), aller Arten von Geräten (Drucker, Scanner, Kameras, Modems usw.), Smartphones (iOS, Android, Windows usw.) sowie von Controllern und Anschlüssen (COM, LPT, USB, Bluetooth usw.)
Erweiterte Einschränkungen für Gerätetypen/Benutzer/Computer
Bluetooth-Gerätesteuerung
Detaillierte Bluetooth-Verwaltung für Geräteklassen / Hersteller
Auditieren von Laufwerken & Geräten
Auditieren von Datei-Aktivitäten auf Laufwerken
Auditieren von Datei-Aktivitäten auf Smartphones
Erstellen von Schattenkopien bei Datei-Aktivitäten
Zugriffskontrolle für Laufwerke (Lesen/Schreiben/Ausführen)
Erweiterte Zugriffskontrolle / Dateifilterung (z.B.: EXE, PS1 sperren)
Zuweisen von Berechtigungen auf Computer, AD-Gruppen, OUs
Zuweisen von Berechtigungen auf Benutzer, Benutzer-AD-Gruppen
Zuweisen von Berechtigungen auf Azure-AD-Gruppen
Zuweisen von Berechtigungen auf eigene statische Gruppen
Zuweisen von Berechtigungen auf eigene dynamische Gruppen
Individuelles Ausnahmehandling für Sonderfälle
Autorisierung von Medien (CD/DVD)
Bidirektionale Dateifilterung - integriert und erweiterbar
Erzwungene Verschlüsselung von Wechseldatenträgern
Konfigurierbarer Audit-Only-Modus
Automatischer Lern-Modus für vorhandene Geräte
Integration mit Service-Management Lösung (direkter E-Mail-Versand aus Blockmeldung)
Erweiterbarkeit und Integration (Skriptausführung)
Festlegen von Reaktionen und Cmd auf spezifische Geräte-Ereignisse (z.B. beim Einstecken)
Individuell angepasste Benutzer-Benachrichtigungen

ÜBERSICHT

Schnittstellenkontrolle
Blockieren von Geräten mit Malware
Freigabe von Laufwerken erst nach erfolgreichem AV-Scan
Schnittstellenkontrolle für Thin Clients
Festlegung max. Anmeldeversuche und Sperrzeit (für Brute-Force-Schutz)
Notfallmanagement für die Freigabe von geblockten Geräten
Temporäre Geräte-Freigabe (online)
Temporäre Geräte-Freigabe via Challenge/Response (offline)
Möglichkeit der Selbstfreigabe für definierte Benutzergruppen
Laufwerksverschlüsselung über Windows Explorer Kontextmenü und Tray Icon
Umfangreiche Auswertungsmöglichkeiten für Laufwerke, Geräteklassen, Computer, etc.

Zusätzliche Sicherheitsmerkmale
Sicheres Löschen von Dateien und Ordnern
Datenmaskierung für Administration/Reporting/Auditing (GDPR)
Regelverarbeitung basierend auf Netzwerkprofil-Erkennung
EAL3+ zertifizierte Lösung

Verschlüsselung von Wechseldatenträgern
Erzwungene Verschlüsselung für alle externen Datenträger
Verwendung state-of the-art Verschlüsselungs-Algorithmen
Ausnahmeregelung für definierte AD-Benutzer/Computer/Gruppen
Ausnahmeregelung für definierte Laufwerke/Laufwerkstypen
Automatische Verschlüsselung für definierte Benutzer/Computer
Protokollierung der Dateiaktivitäten auf verschlüsselten Laufwerken
Verschlüsselung via BitLocker To Go
Verschlüsselung unter Citrix, RDSH, Linux, macOS (Encryption-2Go)
Passwort-Komplexitätsregeln inkl. Negativ-Wörterbuch
Wiederherstellung bei Verlust des Kennwortes (online)
Wiederherstellung bei Verlust des Kennwortes (offline)

ÜBERSICHT

Bereitstellung &Architektur
Managed Security as a Service (MSSP)
Richtliniengesteuerte Konfiguration
Unterstützung für Offline-Endgeräte

Administration & Verwaltung
Zentrale webbasierte Konsole
Granulares Rollen- und Rechteverwaltung
Entra- (Azure AD) Integration
SAML-Authentifizierung / Single Sign On
Vordefinierte Dashboards & Berichte
Regelmäßige Berichte via E-Mail

Inventarisierung & Eventverarbeitung
Inventarisierung von Hard- und Software
Einlesen & Verarbeitung von DriveLock- & Drittanbieter-Events
Forensischer Analysen zu angeschlossenen Laufwerken, zugehörigen Benutzern/Computern, zugegriffenen/übertragenen Dateien und mehr

DriveLock

Alles aus einer Hand:
DriveLock bietet seine Endpoint Protection-Lösungen als einen Baustein einer HYPERSECURE Platform zur Realisierung einer gesamtheitlichen Sicherheitsstrategie an.

Kontaktieren Sie uns.

DriveLock SE
Landsberger Straße 396
81241 München
Telefon +49 (0) 89 5463649-0
E-Mail info@drivelock.com