Ivanti Device Control

Datenverluste, die auf unabsichtliche oder manchmal auch böswillige Verwendung von Wechseldatenträgern bzw. -medien zurückzuführen sind, haben alarmierende Ausmaße erreicht. Ivanti® Device Control setzt Sicherheitsrichtlinien und Datenverschlüsselung bei der Nutzung von Wechseldatenträgern durch. Die Lösung zentralisiert die Verwaltung von Geräten und Daten unter Verwendung einer Whitelist bzw. eines „Default Deny"-Ansatzes (einer standardmäßigen Ablehnung) und bietet eine zusätzliche Schutzschicht vor Malware, die über physische Medien eingeführt werden.

Schützen Sie Daten vor Verlust oder Diebstahl

Da immer mehr Mitarbeiter remote arbeiten, ist ein Zugriff von außerhalb des Netzwerks erforderlich. Doch die möglichen Auswirkungen von Datenverlusten, seien sie unabsichtlich oder böswillig, sind ein wirkliches Problem. Heute gehören Wechseldatenträger/-medien zu den häufigsten Wegen, auf denen es zu Datenverlusten kommt, wenn es keine Begrenzungen für das Kopieren von Dateien, keine Verschlüsselung, keine Prüfpfade und keine zentrale Verwaltung gibt. Ivanti Device Control ermöglicht die sichere Verwendung solcher produktivitätssteigernden Werkzeuge, begrenzt aber gleichzeitig das Potenzial von Datenverlusten und deren Auswirkungen.

Hauptmerkmale

Whitelist bzw. „Default Deny"

Weist einzelnen Benutzern oder Benutzergruppen Berechtigungen für autorisierte Wechseldatenträger und -medien zu. Standardmäßig wird diesen Datenträgern bzw. Medien und Benutzern, die nicht explizit autorisiert wurden, der Zugriff verweigert.

Mit Richtlinien durchgesetzte Verschlüsselung für Wechselspeicher

Verschlüsselt Wechseldatenträger (z. B. USB-Flashlaufwerke) und Wechselmedien (z. B. DVDs/CDs) zentral und setzt zusätzliche Verschlüsselungsrichtlinien beim Kopieren auf Wechseldatenträger bzw. -medien durch.

Beschränktes Kopieren von Daten

Beschränkt die Datenmenge die jeder Benutzer pro Tag auf Wechseldatenträger und -medien kopieren darf; beschränkt ferner die Nutzung auf bestimmte Zeitfenster bzw. Tage.

Dateitypfilterung

Kontrolliert die Dateitypen, die auf und von Wechseldatenträgern/-medien verschoben werden dürfen, auf den einzelnen Benutzer bezogen; trägt dazu bei, die Verbreitung von Malware zu begrenzen.

Zentralisierte Verwaltung/Administratorenrollen

Definiert und verwaltet den Zugriff von Benutzern, Benutzergruppen, Computern und Computergruppen auf autorisierte Wechseldatenträger/-medien im Netzwerk. Standardmäßig wird diesen Datenträgern bzw. Medien und Benutzern, die nicht explizit autorisiert wurden, der Zugriff verweigert.

Temporärer bzw. geplanter Zugriff

Gewährt Benutzern temporären bzw. geplanten Zugriff auf Wechseldatenträger/-medien; wird dazu verwendet, für einen begrenzten Zeitraum „in der Zukunft" Zugriff zu gewähren.

Kontextbasierte Zugriffsrechte

Zugriffs- bzw. Nutzungsrichtlinien bleiben unabhängig vom Verbindungsstatus in Kraft und können speziell darauf abgestimmt werden, ob der Endpunkt mit dem Netzwerk verbunden ist oder nicht.

Rollenbasierte Zugriffskontrolle

Weist einzelnen Benutzern oder Benutzergruppen Berechtigungen basierend auf ihren Windows Active Directory- oder Novell eDirectory-Identitäten zu, die beide unterstützt werden.

Manipulationssicherer Agent

Installiert Agenten auf allen Endpunkten im Netzwerk. Agenten sind gegen ein nicht autorisiertes Entfernen geschützt – selbst für Benutzer mit Administratorrechten. Nur Device Control-Administratoren dürfen diesen Schutz deaktivieren.

Flexible bzw. skalierbare Architektur

Ermöglicht eine unternehmensweite Kontrolle und Durchsetzung mit Hilfe einer skalierbare Client-Server-Architektur und einer für Performance optimierten Datenbank. Unterstützt virtualisierte Serverkonfigurationen.

Funktionsweise von Ivanti Device Control

1. Erkennen Sie alle Wechselmedien, die derzeit mit Ihren Endpunkte verbunden sind oder jemals mit diesen verbunden waren.

2. Bewerten Sie alle Plug-und-Play-Geräte nach Klasse, Gruppe, Modell und/oder spezifischer ID und definieren Sie Richtlinien mit Hilfe eines Whitelist-Ansatzes.

3. Implementieren Sie Kopierbeschränkungen für Dateien, eine Filterung nach Dateityp sowie zwangsweise Verschlüsselungsrichtlinien für Daten, die auf Wechseldatenträger verschoben werden.

4. Überwachen Sie alle Richtlinienänderungen, Administratoraktivitäten und Dateitransfers, um eine kontinuierliche Richtliniendurchsetzung sicherzustellen.

5. Berichten Sie über die Geräte- und Datennutzung, um die Compliance mit unternehmenseigenen Richtlinien und gesetzlichen Vorschriften zu dokumentieren.

„Zu den wichtigsten Nutzeneffekten der Bereitstellung von Ivanti Device Control gehört die Whitelist-Funktion der Lösung, mit der sichergestellt wird, dass kein Gerät jemals verwendet werden kann, egal wie es eingesteckt wird, es sei denn, es wurde autorisiert. Flashspeicher-USB-Geräte stellen ein signifikantes Risiko dar, da sie potenziell als Vehikel für den Diebstahl von Unternehmensdaten oder die Einführung von Malware dienen könnten, die den Computer unbrauchbar machen und innerhalb kürzester Zeit andere PCs im selben Netzwerk infizieren könnten. Device Control ist ein wirklich starkes benutzerfreundliches Produkt. Daher hat sich Barclays für diese Lösung entschieden.“

Paul Douglas
ADIR Desktop Build Team Manager bei Barclays

Entdecken Sie die Vorteile von Ivanti Device Control

- Schützt Daten vor Verlust oder Diebstahl
- Ermöglicht die sichere Nutzung von Produktivitätstools
- Verbessert die Durchsetzung von Sicherheitsrichtlinien
- Bietet präzise Kontrolle dank Zugriffsbeschränkungen
- Verhindert Malware-Infiltrierung mit physischen Mitteln/Mapping zentralisierter und dezentralisierter Verwaltungsstrukturen
- Ermöglicht die Überwachung aller Dateitransfers zu Druckern und auf physische Medien

www.ivanti.de

+49 (0)69 941 757-0

contact@ivanti.de