

NORMAN® DeviceControl

WICHTIGE FUNKTIONEN

Whitelist/„Default Deny“
per Richtlinie erzwungene
Verschlüsselung für Kopien
auf Wechseldatenträgern

Datenkopierschutz

Filterung nach Dateityp

temporärer/planbarer Zugriff

kontextabhängige Berechtigungen

zentralisierte Verwaltung/
Administration

rollenbasierte Zugriffskontrolle

manipulationssicherer Agent

flexible/skalierbare Architektur

¹ Deloitte & Touche and Ponemon
Institute, Enterprise@Risk: 2007
Privacy & Data Protection Survey,
Dezember 2007

² Ponemon Institute,
2008 Annual Study:
Cost of Data Breach Study,
Februar 2009

Sicherheitsrichtlinien für Wechseldatenträger, Medien und Daten

Datenlecks, die von unabsichtlicher oder manchmal auch böswilliger Verwendung von Wechseldatenträgern herrühren, haben alarmierende Ausmaße erreicht. Über 85% der Datenschutz- und Sicherheitsbeauftragten haben mindestens einen solchen Vorfall gemeldet, knapp 64% sogar mehrere.¹



**Seien Sie gewappnet –
schützen Sie Ihre
Vermögenswerte**

Unternehmensweite Verwaltung der Datenträger

Zur Verbesserung der Produktivität müssen Unternehmen ihren Mitarbeitern und Partnern Datenzugriff gewähren. Je mehr Mitarbeiter von Remote-Standorten aus arbeiten, desto öfter ist Zugriff von außerhalb des Netzwerks erforderlich. Der potentielle Datenverlust – versehentlich oder böswillig herbeigeführt – stellt ein ernstzunehmendes Problem dar. Heutzutage sind Wechseldatenträger und -medien die gängigsten Wege, auf denen Daten nach außen gelangen: Es gibt keine Beschränkungen beim Kopieren, keine Verschlüsselung, keine Prüfpfade und keine zentrale Verwaltung.

Die Informationen in Kunden- und Firmendaten, wie z.B. persönlichen Daten und Daten zu geistigem Eigentum, sind manchen Millionen wert. Die Kosten der Datenwiederherstellung und die Verluste aus entgangenen Geschäftsgewinnen steigen rapide an. Die durchschnittlichen Gesamtkosten für eine Datensicherheitsverletzung werden auf 6,6 Millionen USD bzw. 202 USD pro betroffenen Datensatz geschätzt, die Verluste durch entgangenen Geschäftsgewinn auf 4,6 Millionen USD bzw. 139 USD pro Datensatz.²

Norman Device Control bietet:

- Richtlinien für die Nutzung von Wechseldatenträgern und Datenverschlüsselung
- zentrale Verwaltung von Geräten und Daten mit Whitelist/„Default Deny“-Methode
- Einsatz produktivitätssteigernder Tools und gleichzeitige Reduzierung von Datenlecks und deren Auswirkungen

Kundenmeinung:

„Einer der Hauptvorteile ist die Whitelist-Funktion, mit der sichergestellt wird, dass kein Gerät ohne Autorisierung verwendet werden kann – ganz egal auf welchem Weg es angeschlossen wird.“

NORMAN Application and Device Control

Norman Application Control schützt vor unbefugter Software und reduziert die Kosten für die Endpoint-Sicherheit.

Application Control bietet:

- Schutz Ihrer Endgeräte vor Malware, ohne Abhängigkeit von Signatur-Updates.
- Optimierte IT-Unterstützung durch weniger Support-Anfragen wegen unautorisierter Software.
- Verbesserte Systemverfügbarkeit und Service-Level durch Schutz vor bekannten und unbekanntem Bedrohungen.
- Überprüfung mit detaillierter Protokollierung aller Versuche Anwendung auszuführen und Richtlinien zu ändern.

So funktioniert Norman Device Control:

1. **Erkennt** alle Wechseldatenträger, die aktuell an den Endgeräten angeschlossen sind oder waren
2. **Analysiert** alle „Plug and Play“-Geräte nach Klasse, Modell und/oder spezifischer ID und definiert Richtlinien mittels Whitelist-Methode
3. **Implementiert** Kopier-Beschränkungen von Dateien, Dateityp-Filterungen und Verschlüsselungsrichtlinien auf dem Wechseldatenträger
4. **Überwacht** alle Richtlinienänderungen, Administratoraktivitäten und Dateiübertragungen, um sicherzustellen, dass die Richtlinien durchgängig umgesetzt werden
5. **Liefert einen Report** über die Einhaltung firmeneigener und rechtlicher Richtlinien durch Transparenz in Bezug auf Geräte- und Datennutzung



Wichtige Funktionen

- ▶ **Whitelist/„Default Deny“:** weist Benutzern oder Benutzergruppen Berechtigungen für autorisierte Wechseldatenträger/-medien zu; umgekehrt wird unautorisierten Wechseldatenträgern/-medien und Benutzern der Zugriff verweigert
- ▶ **Verschlüsselung von Wechseldatenträgern per Richtlinie:** zentrale Verschlüsselung von Wechseldatenträgern (z.B. USB-Flash-Laufwerke) und Medien (z.B. DVDs/CDs) sowie beim Kopieren auf Wechseldatenträger/-medien
- ▶ **Beschränkung von Datenkopien:** beschränkt die Datenmenge, die jeder Benutzer täglich auf Wechseldatenträger oder Medien kopieren darf und legt dafür bestimmte Zeitrahmen/Tage fest
- ▶ **Dateityp-Filterung:** legt die Dateitypen fest, die vom Benutzer von und auf Wechseldatenträger und Medien verschoben werden dürfen
- ▶ **Zentralisierte Verwaltung/Administration:** definiert und verwaltet zentral den Zugriff von Benutzern, Benutzergruppen, Computern und Computergruppen auf autorisierte Wechseldatenträger/-medien im Netzwerk; standardmäßig wird unautorisierten Wechseldatenträgern/-medien und Benutzern der Zugriff verweigert
- ▶ **Temporärer/planbarer Zugriff:** gewährt Benutzern temporäre bzw. zeitlich festgelegte Zugriffe auf Wechseldatenträger/-medien – auch zeitlich begrenzte Zugriffsrechte „in der Zukunft“
- ▶ **Kontextabhängige Berechtigungen:** nutzt verschiedene Rechte, in Fällen in denen das Endgerät an das Netzwerk angeschlossen ist, wenn es nicht angeschlossen ist oder unabhängig vom Verbindungsstatus
- ▶ **Rollenbasierte Zugriffskontrolle:** weist einzelnen Benutzern oder Benutzergruppen Berechtigungen zu, die auf ihrer Windows Active Directory- oder Novell eDirectory-Identität basierend
- ▶ **Manipulationssicherer Agent:** installiert auf jedem Endgerät Netzwerk-Agenten, die gegen unautorisierte Entfernung geschützt sind. Nur Device Control-Administratoren können diesen Schutz aufheben
- ▶ **Flexible/skalierbare Architektur:** bietet unternehmensweite Kontrolle mittels skalierbarer Client-Server-Architektur mit zentraler Datenbank, die für hohe Leistungen ausgelegt ist; Unterstützt virtualisierte Serverkonfigurationen

SYSTEMVORAUSSETZUNGEN

Server:
Windows Server 2003 & 2008

Client:
Windows XP Professional,
Windows 2000 Professional,
Windows Server 2003,
Windows Vista, Windows 7

Hauptvorteile

- schützt Daten vor Verlust/Diebstahl
- ermöglicht den sicheren Einsatz von Tools, wie USB-Sticks
- verbessert die Durchsetzung von Sicherheitsrichtlinien
- sorgt mit Zugriffsbeschränkungen für präzise Kontrolle



Norman zählt zu den führenden Unternehmen und Pionieren für die Entwicklung proaktiver Lösungen zur Absicherung von Unternehmensdaten und für die Entwicklung von Forensik-Tools zur Malware-Erkennung. Die Produkte von Norman schützen Endanwender und Netzwerke in Unternehmen jeder Größenordnung vor Malware und ermöglichen die Analyse von Schadcode. Norman wurde im Jahr 1984 in Oslo gegründet und vertreibt die Produkte weltweit über eigene Niederlassungen und ein ausgedehntes Partnernetz.

NORMAN®