

## WICHTIGE FUNKTIONEN

- Anwendungs-Whitelists
- automatische Anwendungserkennung
- Definition von Standarddateien
- automatische Autorisierung für Software-Updates
- Skript-/Makroschutz
- flexible Dateiautorisierung
- lokale Autorisierung
- Spread Check (Verbreitungsprüfung)
- Offline-Computerschutz
- Unterstützung von Active Directory und eDirectory

## Unautorisierte Software blockieren – senkt Kosten für die Sicherheit der Endgeräte

Wenn neue Malware-Bedrohungen auftreten oder Software Kompatibilitätskonflikte wegen fehlender Unterstützung verursacht, müssen IT-Beauftragte ihre Arbeit unterbrechen, um das Problem lösen. Egal, ob es sich um die Aktualisierung von Antivirensignaturen zum Schutz von Systemen und Daten handelt oder um das Wiederherstellen von Images auf Laptops nach Softwarekonflikten – im Endeffekt ergibt sich immer eine höhere Arbeitsbelastung im Support-Bereich und eine geringere betriebliche Effizienz.

### Gezielte Angriffe strategisch blockieren



## Endgeräte, Server, Kioske und POS-Systeme vor Malware schützen

Die Bedrohungen reißen nicht ab, und Antivirensoftware allein kann das Problem nicht lösen. Malware wird schneller entwickelt als die entsprechende Abhilfe. Das Ausmaß an Malware hat um über 500% zugenommen. Es wurde über 5,49 Millionen bekannte Malware gemeldet.<sup>1</sup> Zudem werden die Angriffe immer zielgerichteter und umgehen klassische Antivirenlösungen.

Mit Norman Application Control wird mittels Anwendungs-Whitelists die Ausführung bössartiger Codes verhindert. Diese Methode lässt nur autorisierte Anwendungen auf Laptops, PCs, Servern, Terminal-dienst-Servern und Thin Clients zu. Dies geschieht unabhängig von Antiviren-Signatur-Updates und spart Netzwerkbandbreite und IT-Ressourcen.

Wenn keine Virenangriffe zu vereiteln, keine Malware aufzuspüren und keine Systemabstürze verursachenden Anwendungen deinstalliert werden müssen, dann können Sie mehr Zeit auf strategische Aktivitäten verwenden, anstatt ständig nur Computerprobleme zu beheben.

## Norman Application Control bietet:

- Malwareschutz unabhängig von Signatur-Updates
- optimierten IT-Support mit weniger Helpdesk-Anfragen wegen unautorisierter Software
- verbesserte Systemverfügbarkeit und Service-Levels durch Abwehr bekannter und unbekannter Bedrohungen
- detaillierte Protokollierung aller ausgeführten Anwendungen und Richtlinienänderungen

### Kundenmeinung:

“Ich kann explizit auflisten, welche Anwendungen auf unseren Geräten ausgeführt werden dürfen. Alle anderen ausführbaren Dateien, einschließlich solcher, die bössartigen Code enthalten, funktionieren einfach nicht.”

<sup>1</sup> AVtest.org, 2008

## NORMAN Application and Device Control

Wechselmedien und -geräten sind die häufigste Ursache für Datenverlust – fehlende Beschränkungen bei Dateikopien, keine Verschlüsselung, keine Protokollierung und keine zentrale Verwaltung.

Die Informationen in Kunden- und Unternehmensdaten sowie geistigem Eigentum, haben einen Wert in Milliardenhöhe.

Device Control ermöglicht Ihnen

- die Durchsetzung von Richtlinien für Wechseldatenträger und Datenverschlüsselung
- zentrale Verwaltung von Geräten und Daten mittels Whitelist-Ansatz
- die Aktivierung produktivitätssteigernder Tools bei gleichzeitiger Einschränkung potenzieller Datenlecks und deren Auswirkungen.

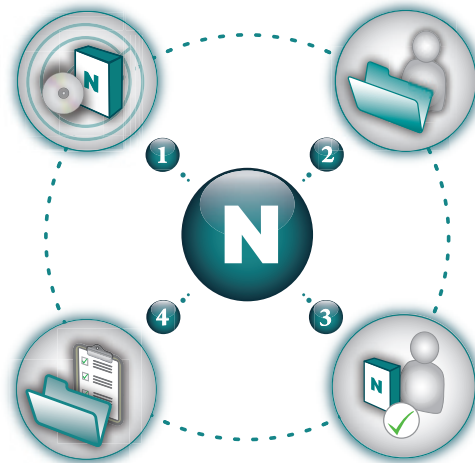
### SYSTEM VORAUSSETZUNGEN

Server:  
Windows Server 2003 & 2008

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

### So funktioniert Norman Application Control:

1. **Erkennen** aller ausführbaren Dateien, Profile erfassen und in vordefinierten Dateigruppen organisieren.
2. **Implementieren** von Berechtigungen für Anwendungen: basierend auf Datei-, Benutzer- und Gruppenfreigaben.
3. **Autorisieren** berechtigter Benutzer und Anwendungen durch Richtlinien. Wenn der Benutzer oder die Anwendung nicht über entsprechende Rechte verfügt, wird der Zugriff verweigert.
4. **Reporting** durch Erstellung eines detaillierten Protokolls über die Aktivitäten sowie die Prüfung der Gültigkeit der Softwarelizenzen.



### Wichtige Funktionen

- ▶ **Anwendungs-Whitelists:** eliminiert unbekannte oder unerwünschte Anwendungen in Ihrem Netzwerk. Automatische Anwendungserkennung zur Erstellung oder Aktualisierung von Whitelists
- ▶ **Automatische Erkennung von Anwendungen:** bietet flexible und schnelle Möglichkeiten zur Erstellung oder Aktualisierung von Whitelists
- ▶ **Spread Check (Verbreitungsprüfung):** das Risiko, bösartigen Code über das Netzwerk zu verbreiten, wird durch lokale Autorisierung vermindert; verdächtige Anwendungen, die auf zu vielen Computern lokal autorisiert sind, werden deaktiviert
- ▶ **Unterstützung von Active Directory und eDirectory:** vermindert den Einrichtung- und Wartungsaufwand für Benutzer durch die Nutzung bestehender Definitionen in Active Directory und eDirectory
- ▶ **Automatische Autorisierung für Software-Updates:** eliminiert das Risiko bei häufig aktualisierten Microsoft-Anwendungen versehentlich Benutzerzugriffsrechte einzuschränken
- ▶ **Skript-/Makroschutz:** erweitert die Anwendungsrichtlinien auf spezifische Skripts/Makros und ermöglicht die Arbeit ohne Beeinträchtigung des Schutzes
- ▶ **Flexible Dateiautorisierung:** bietet eine flexible und schnelle Möglichkeit neue und aktualisierte Anwendungen zu identifizieren, zu überprüfen und anschließend Whitelists zu erstellen
- ▶ **Lokale Autorisierung:** bietet dem Benutzer Flexibilität, ohne die administrative Kontrolle aufzugeben: Berechtigte Benutzer können Anwendungen lokal autorisieren, es wird jedoch ein Protokoll zur Überprüfung erstellt
- ▶ **Offline-Computerschutz:** stellt sicher, dass Remote-/nicht angemeldete Benutzer durchgehend geschützt sind, da auf jedem Gerät eine lokale Kopie der aktualisierten Hashes und Genehmigungen gespeichert wird
- ▶ **Standarddateidefinitionen:** beschleunigt und vereinfacht die Whitelist-Definition mit klassifizierten, bereits geladenen Whitelists aller unterstützten Betriebssysteme

### Hauptvorteile

- verhindert bekannte und unbekannte Bedrohungen
- blockiert gezielte Malware und Day-Zero-Angriffe
- erzwingt eine vertrauenswürdige Anwendungsumgebung
- verbessert die Serververfügbarkeit
- senkt die Betriebskosten für die Endgerätesicherheit



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®