

# Symantec™ Network Access Control Starter Edition

Endgeräte-Compliance leichter gemacht

## Überblick

Symantec Network Access Control Starter Edition ermöglicht einen einfachen Einstieg in die Implementierung einer Netzwerkzugangssteuerung. Die Lösung verfügt über einen Teil des Funktionsumfangs von Symantec Network Access Control, der auf dem Weg zu einer kompletten Symantec Network Access Control-Implementierung ohne Einschränkungen genutzt werden kann. Wie Symantec Network Access Control gewährt die Starter Edition nur solchen Endgeräten Zugang, die den definierten Sicherheitsrichtlinien eines Unternehmens entsprechen. Sie analysiert den Compliance-Status, nimmt automatisch Korrekturen vor und stellt sicher, dass der Zugang ordnungsgemäß und sicher erfolgt. Unternehmen können so die Zahl der Sicherheitsvorfälle deutlich reduzieren, die Konformität mit den Konfigurationsrichtlinien erhöhen und das Vertrauen darin verstärken, dass die Schutzmechanismen für Endgeräte adäquat funktionieren.

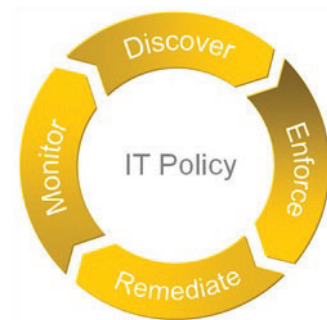
## Vorteile

Unternehmenskunden, die Symantec Network Access Control Starter Edition einsetzen, kommen so in den Genuss einer Reihe messbarer Vorteile. Dazu zählen:

- Geringere Verbreitung von Schadprogrammen wie Viren, Würmern, Spionageprogrammen und anderen Formen krimineller Software
- Geringeres Risiko durch die verstärkte Kontrolle der nicht verwalteten und verwalteten Endgeräte, die auf das Unternehmensnetzwerk zugreifen
- Bessere Netzwerkverfügbarkeit und seltenere Dienstbeeinträchtigung für die Anwender

- Nachweisliche Einhaltung von Unternehmensrichtlinien durch Endgeräte-Compliance-Informationen, die nahezu in Echtzeit bereitgestellt werden
- Geringere Gesamtbetriebskosten durch zentrale Verwaltungsarchitektur auf Unternehmensniveau
- Nachweisen der ordnungsgemäßen Funktionsweise des Endgeräteschutzes wie Symantec AntiVirus™ und die Client-Firewall
- Nahtlose Integration von Symantec™ Endpoint Protection

## Wichtige Funktionen



Symantec Network Access Control Starter Edition – Ablauf

## Netzwerkzugangssteuerungsverfahren

Netzwerkzugangssteuerung ist ein Verfahren, das für alle Arten von Endgeräten und Netzwerken angewendet werden muss. Es beginnt schon vor dem Verbindungsaufbau mit dem Netzwerk und setzt sich während der gesamten Verbindungsdauer fort. Wie bei allen Unternehmensprozessen dient auch hier eine Richtlinie als Grundlage für Bewertungen und Maßnahmen.

Das Verfahren der Netzwerkzugangssteuerung besteht aus vier Schritten:

- 1. Erkennung und Analyse von Endgeräten.** Dieser Schritt erfolgt, wenn Endgeräte eine Verbindung zum Netzwerk aufbauen und bevor sie auf die Ressourcen zugreifen. Durch die Integration in die bestehende Netzwerkinfrastruktur und die Nutzung intelligenter Agentensoftware können Netzwerkadministratoren sicher sein, dass neue Geräte beim Verbindungsaufbau mit dem Netzwerk auf die Mindestanforderungen der IT-Richtlinien geprüft werden.
- 2. Bereitstellung des Netzwerkzugangs.** Kompletter Netzwerkzugriff wird erst gewährt, wenn die Analyse abgeschlossen und festgestellt wurde, dass das Endgerät der IT-Richtlinie entspricht. Systeme, die nicht den Richtlinien entsprechen oder die Mindestsicherheitsanforderungen des Unternehmens nicht erfüllen, werden mit eingeschränktem oder gar keinem Zugang zum Netzwerk isoliert.
- 3. Korrekturmaßnahmen für Endgeräte, die nicht den Richtlinien entsprechen.** Mit Hilfe der automatischen Korrekturmaßnahmen für nicht konforme Endgeräte können Administratoren die Richtlinieneinhaltung schnell herstellen und den Geräten dann den Netzwerkzugriff gewähren. Der Korrekturprozess kann vollständig automatisiert werden und unbemerkt vom Benutzer ablaufen; es können dem Benutzer jedoch auch Informationen für die manuelle Korrektur angezeigt werden.
- 4. Proaktive Compliance-Überwachung.** Die Einhaltung von Richtlinien muss ständig gewährleistet sein. Aus diesem Grund überwacht Symantec Network Access Control in vom Administrator spezifizierten Abständen aktiv das Compliance-Niveau aller Endgeräte. Verändert sich der Compliance-Status eines Endgerätes, ändern sich damit auch die Netzwerkzugangsrechte des Endgeräts.

### **In jedem Netzwerk einsetzbar**

Der typische Unternehmensnutzer verbindet sich über verschiedenste Zugangsmethoden mit dem Netzwerk. Administratoren müssen daher Analyse- und Verbindungssteuerungen unabhängig vom Verbindungstyp flexibel und konsistent anwenden können. Als eine der ausgereiftesten Lösungen für die Netzwerkzugangssteuerung auf dem Markt ermöglicht es Symantec Network Access Control Starter Edition Netzwerkadministratoren, die Richtlinieneinhaltung über vorhandene Investitionen in die Netzwerkinfrastruktur und ohne Zusatzausstattung des Netzwerks aktiv durchzusetzen.

Ob Unternehmen nun einen der Symantec Network Access Control Gateway Enforcer verwenden, die sich direkt in das Netzwerk integrieren lassen, oder die Host-basierte Selbstüberwachungsoption, für die keine Netzwerk-Enforcer erforderlich sind – sie können sicher sein, dass die Benutzer und Endgeräte beim Kontakt mit dem Unternehmensnetzwerk richtlinienkonform sind.

---

### **Architektur von Symantec Network Access Control**

Die Architektur von Symantec Network Access Control beinhaltet drei Kernkomponenten: Richtlinienverwaltung, Endgeräteanalyse und Netzwerkdurchsetzung. Alle drei Komponenten arbeiten als eine Lösung zusammen und benötigen keine externen Elemente, um funktionsfähig zu sein. Wird die Host-basierte Durchsetzung der netzwerk-basierten Durchsetzung vorgezogen, sind nur die Komponenten für Richtlinienverwaltung und Endgeräteanalyse erforderlich.

### **Zentrale Richtlinienverwaltung und Berichterstellung**

Für den effizienten Betrieb jeder Lösung ist eine unternehmenstaugliche Verwaltungskonsolle von höchster Bedeutung. Symantec Endpoint Protection Manager verfügt über eine Konsolle auf Basis von Java™-Technologie für die zentrale Erstellung, Implementierung, Verwaltung und Berichterstellung der Agenten- und Enforcer-Aktivitäten. Der Richtlinienmanager ist auch für anspruchsvollste

Umgebungen skalierbar und bietet eine granulare Steuerung für alle administrativen Aufgaben in einer hochverfügbaren Architektur.

### Endgeräteanalyse

Symantec Network Access Control Starter Edition schützt das Netzwerk weitgehend vor Schadprogrammen und prüft zudem, ob Endgeräte beim Verbindungsaufbau mit dem Netzwerk über eine Konfiguration verfügen, die sie vor Online-Angriffen schützt. Ungeachtet des Ziels beginnt der Prozess immer mit der Analyse des Endgeräts. Die Prüfungen auf Virenschutz, Abwehr von Spionageprogrammen und installierte Patches sind einige der gängigsten Mindestanforderungen für den Netzwerkzugang. Die meisten Unternehmen erweitern die erste Implementierung für die Netzwerkzugangssteuerung jedoch recht bald über diese Mindestanforderungen hinaus.

Symantec Network Access Control Starter Edition beinhaltet Analysetechnologie in Form eines permanenten Agenten für die Bestimmung der Endgeräte-Compliance. Unternehmensinterne und andere verwaltete Systeme nutzen einen vom Administrator installierten Agenten, um den Compliance-Status zu bestimmen. Dieser prüft den Virenschutz, die Abwehr von Spionageprogrammen sowie die installierten Patches und komplexe Systemstatuseigenschaften wie Registriereinträge, laufende Prozesse und Dateiattribute. Permanente Agenten bieten detaillierte, genaue und zuverlässige Informationen zur Richtlinieneinhaltung und äußerst flexible Korrektur- und Reparaturfunktionen der Analyseoptionen.

### Durchsetzung

Bei Symantec Network Access Control Starter Edition können Unternehmen zwischen Gateway-basierter und Host-basierter Durchsetzung wählen:

- **Gateway Enforcer** ist ein Durchsetzungsgerät, das an Netzwerkengpassstellen eingesetzt wird. Es steuert den Verkehrsfluss durch das Gerät basierend auf der Richtlinieneinhaltung von entfernten Endgeräten. Unabhängig davon, ob es sich bei der Engpassstelle um Perimeternetzwerk-Verbindungspunkte, wie etwa WAN-Verbindungen oder VPNs, oder um interne Segmente handelt, die auf kritische Unternehmenssysteme zugreifen, bietet Gateway Enforcer auf effiziente Weise einen gesteuerten Zugang zu Ressourcen und Korrekturmaßnahmen.
- Die **Selbstüberwachung** nutzt die Host-basierten Firewall-Funktionen des Symantec Protection-Agenten, um die lokalen Agentenrichtlinien entsprechend des Endgeräte-Compliance-Status anzupassen. So können Administratoren den Zugriff auf jedes beliebige Netzwerk innerhalb oder außerhalb des Unternehmensnetzwerks für Geräte wie Laptops steuern, die sich zwischen verschiedenen Netzwerken bewegen.

### Support-Services

Symantec bietet verschiedene Beratungsleistungen, technische Schulungen und Support-Services an, die Unternehmen durch die Migration, Installation und die Verwaltung von Symantec Network Access Control Starter Edition führen und dabei unterstützen, das gesamte Potenzial ihrer Investition zu nutzen. Unternehmen, die die Sicherheitsüberwachung und -verwaltung auslagern wollen, bietet Symantec darüber hinaus Managed Security Services für Echtzeitschutz an.

**Produktfamilie Symantec Network Access Control Starter Edition**

	<b>Symantec Network Access Control</b>	<b>Symantec Network Access Control Starter Edition</b>
<b>Durchsetzung</b>		
LAN 802.1x	X	
DHCP	X	
Gateway	X	X
Selbstüberwachung	X	X
<b>Endgeräteanalyse</b>		
Permanenter Agent	X	X
Auflösbarer Agent	X	
Fernprüfung von Schwachstellen	X	

**Systemanforderungen**

**Unterstützte Plattformen**

*Symantec Endpoint Protection Manager*

- Microsoft® Windows® 2003 (32-Bit und 64-Bit)
- Microsoft Windows XP (32-Bit)
- Microsoft Windows 2000 – SP3 und höher (32-Bit)

*Symantec Endpoint Protection Manager-Konsole*

- Microsoft Vista (32-Bit und 64-Bit)
- Microsoft Windows 2003 (32-Bit und 64-Bit)
- Microsoft Windows XP (32-Bit und 64-Bit)
- Microsoft Windows 2000 – SP3 und höher (32-Bit)

*Symantec Network Access Control-Client*

Betriebssystem:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows XP Home Edition oder Professional
- Windows XP Tablet Edition
- Windows Server 2003 Standard oder Enterprise
- Mac OS X 10.4 oder höher

*Symantec Network Access Control Enforcer 6100 Serie*

Basis-Appliance-Option (Gateway und LAN)

Gehäuseeinheiten	1
Abmessungen	1.68" x 17.60" x 21.5"
Prozessor	1 2,8-GHz Intel Pentium 4-Prozessor
Arbeitsspeicher	1 GB
Speicher	1 160-GB (SATA)

Fail Open Appliance Option (Gateway and LAN)

Gehäuseeinheiten	1
Abmessungen	1.68" x 17.60" x 21.5"
Prozessor	1 2,8-GHz Intel Pentium 4-Prozessor
Arbeitsspeicher	1 GB
Speicher	1 160-GB (SATA)

**Besuchen Sie unsere Webseite**

*Visit our Web site*

[www.symantec.com/endpoint](http://www.symantec.com/endpoint)

*Um mit einem Produktspezialisten in Deutschland zu sprechen*

Rufen Sie folgende Rufnummer an: +49 (0) 69 6641 0315

*Um mit einem Produktspezialisten außerhalb Deutschlands zu sprechen*

Adressen und Telefonnummern der Symantec-Niederlassungen in den einzelnen Ländern finden Sie auf unseren Webseiten.

*Über Symantec*

Als einer der weltweit führenden Anbieter für Infrastruktursoftware vermittelt Symantec Unternehmen und Privatkunden Vertrauen in eine vernetzte Welt. Mithilfe von Softwareprogrammen und Dienstleistungen, die Sicherheitsrisiken abbauen, die Einhaltung gesetzlicher Vorschriften erleichtern sowie die Verfügbarkeit und Leistungsfähigkeit von Systemen steigern, trägt Symantec zum Schutz der Infrastruktur, Informationen und Interaktionen seiner Kunden bei. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien, und vertreibt seine Produkte in 40 Ländern. Weitere Informationen finden Sie unter [www.symantec.de](http://www.symantec.de).

*Symantec Dublin*

Ballycoolin Business Park

Blanchardstown

Dublin 15

Ireland

Phone: +353 1 803 5400

Fax: +353 1 820 4055

