

Symantec™ Network Access Control

Weitreichende Unterstützung für Endgeräte-Compliance

Überblick

Symantec Network Access Control ist eine umfangreiche, durchgängige Lösung für Netzwerkgerätesteuerung, mit deren Hilfe Unternehmen den Zugriff auf Unternehmensnetzwerke effizient und sicher realisieren können, weil sie in die bestehenden Netzwerkstrukturen integriert wird. Unabhängig davon, wie die Endgeräte mit dem Netzwerk verbunden sind, erkennt und analysiert Symantec Network Access Control ihren Compliance-Status, stellt den entsprechenden Netzwerkzugang zur Verfügung und bietet bei Bedarf Korrekturfunktionen. Die Endgeräte werden ständig auf Änderungen des Compliance-Status hin überwacht. Unternehmen können so die Zahl der Sicherheitsvorfälle in ihrer Netzwerkkumgebung deutlich reduzieren und das Compliance-Niveau mit internen IT-Sicherheitsrichtlinien erhöhen.

Mit Symantec Network Access Control werden die Implementierung und die Verwaltung der Netzwerkzugangssteuerung zu einem erreichbaren und kostengünstigen Ziel.

Autorisierung von Endgeräten, nicht nur von Benutzern

Unternehmen und Netzwerkadministratoren stehen bei den aktuellen Rechnerumgebungen vor der Schwierigkeit, dass ein immer größerer Benutzerkreis Zugriff auf die Unternehmensressourcen benötigt. Dazu zählen sowohl Mitarbeiter vor Ort als auch Mitarbeiter an anderen Standorten sowie Gäste, Vertragspartner und temporäre Mitarbeiter. Noch nie war es schwieriger, die Integrität von Netzwerkkumgebungen sicherzustellen. Es ist nicht mehr vertretbar, ohne vorherige Prüfung Zugang zu einem Netzwerk zu gewähren. Durch die deutliche Zunahme der Endgerätezahl und Endgerätetypen, die auf Unternehmenssysteme zugreifen, ist es erforderlich, den

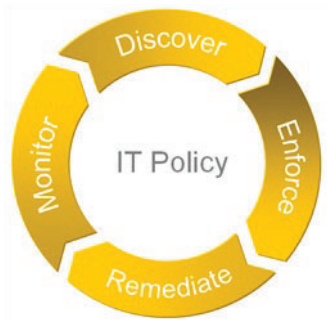
Status und das Sicherheitsniveau von Endgeräten festzustellen - bevor diese sich mit den Ressourcen verbinden und während sie verbunden sind. Symantec Network Access Control hilft dabei sicherzustellen, dass Endgeräte den IT-Richtlinien entsprechen, bevor eine Verbindung zum LAN, WAN, WLAN oder VPN des Unternehmens hergestellt wird.

Vorteile

Folgende messbare Vorteile können Unternehmen durch den Einsatz von Symantec Network Access Control erzielen:

- 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 in Echtzeit bereitgestellt werden
- Geringere Gesamtbetriebskosten durch zentrale Verwaltungsarchitektur auf Unternehmensniveau
- Nachweisen der ordnungsgemäßen Funktionsweise des Endgeräteschutzes wie Virenschutz und Client-Firewall
- Nahtlose Integration von Symantec™ AntiVirus™ Advanced Endpoint Protection

Wichtige Funktionen



Symantec Network Access Control-Verfahren

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 entweder 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.

Durchgängige Endgeräteabdeckung

Netzwerke bestehen aus neuen und alten Unternehmenssystemen, Vertragspartnersystemen, Gästesystemen, öffentlich zugänglichen Systemen, Systemen von Geschäftspartnern und allen möglichen anderen unbekannt Systemen. Die Administratoren haben häufig nur wenig oder gar keine Kontrolle über die Verwaltung einer Vielzahl dieser Endgeräte, müssen jedoch die Sicherheit und Verfügbarkeit des Netzwerks sicherstellen. Mit Symantec Network Access Control können Unternehmen das Verfahren für die Netzwerkzugangssteuerung auf beliebige Geräte anwenden: verwaltete oder nicht verwaltete, alte oder neue, bekannte oder unbekannte.

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 Netzwerkadministratoren, die Richtlinien Einhaltung über vorhandene Investitionen in die Netzwerkinfrastruktur und ohne Zusatzausstattung des Netzwerks aktiv durchzusetzen.

Ob Unternehmen nun eine der Symantec Network Access Control Enforcers nutzen, die sich direkt in das Netzwerk integrieren lassen, wobei bei einer Nur-Host-Durchsetzungsoption keine Netzwerkintegration erforderlich ist, oder einen auflösbaren Agenten, der in die Web-Anwendungsumgebung integriert ist – sie können immer sicher sein, dass die Anwender und Endgeräte bei Kontakt mit dem Unternehmensnetzwerk die Richtlinien erfüllen.

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.

Zentrale Richtlinienverwaltung und Berichterstellung

Für den effizienten Betrieb jeder Lösung ist eine unternehmenstaugliche Verwaltungskonsole von höchster Bedeutung. Der Symantec Endpoint Protection Manager verfügt über eine Konsole 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

Die Netzwerkzugangssteuerung schützt das Netzwerk vor Schadprogrammen und unbekanntem oder unbefugtem Endgeräten, prüft jedoch auch, 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 beinhaltet drei verschiedene Endgeräteprüftechnologien zur Bestimmung der Endgeräte-Compliance.

- **Permanente Agenten.** 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 Systemstatischeigenschaften wie Registriereinträge, laufende Prozesse und Dateiattribute. Permanente Agenten bieten detaillierte, genaue und zuverlässige Informationen zur Richtlinien Einhaltung und äußerst flexible Korrektur- und Reparaturfunktionen der Analyseoptionen.
- **Auflösbare Agenten.** Für Geräte, die nicht zum Unternehmen gehören, oder Systeme, die derzeit nicht von Administratoren verwaltet werden, stehen bei Bedarf und ohne Administrationsrechte Java-basierte Agenten für die Analyse des Endgeräte-Compliance-Status zur Verfügung. Am Ende der Sitzung entfernen sich diese Agenten automatisch selbst vom System.

- **Fernprüfung von Schwachstellen.** Mit der Fernprüfung von Schwachstellen erhalten Unternehmen Compliance-Informationen zur Durchsetzungsinfrastruktur von Symantec Network Access Control, und zwar auf Basis der Fernprüfungsergebnisse des Symantec Network Access Control Scanners für Schwachstellen. Die Fernprüfung erweitert die Informationserfassungsfunktion auf Systeme, für die es derzeit keine Technologie auf Agentenbasis gibt.

Durchsetzung

Die Weiterentwicklung der Netzwerkumgebung jedes einzelnen Unternehmens gestaltet sich unterschiedlich. Aus diesem Grund kann es keine einheitliche Durchsetzungsmethode geben, die alle Punkte im Netzwerk effektiv kontrollieren kann. Netzwerksteuerungslösungen müssen so flexibel sein, dass sie mehrere Durchsetzungsmethoden in die bestehende Umgebung einbinden können, ohne den Verwaltungs- und Instandhaltungsaufwand zu erhöhen. Bei Symantec Network Access Control können Unternehmen die am besten geeignete Durchsetzungsart für die verschiedenen Netzwerkbereiche auswählen, ohne dadurch die Betriebskomplexität oder Kosten zu erhöhen. Die netzwerkbasierenden Durchsetzungsmethoden sind entweder nur als Software oder als Appliance-Komponente verfügbar.

- **LAN Enforcer 802.1X** ist eine 802.1X RADIUS Proxy-Out-of-Band-Lösung, die mit allen wichtigen Switching-Anbietern funktioniert, die den 802.1X-Standard unterstützen. Der LAN Enforcer kann eine bestehende AAA-Identitätsverwaltungsarchitektur nutzen, die Benutzer und Endgeräte authentifiziert, oder als unabhängige RADIUS-Lösung für Umgebungen agieren, die lediglich eine Endgeräte-Compliance-Validierung benötigen. Der LAN Enforcer stellt in Abhängigkeit von den Authentifizierungsergebnissen einen Switch-Port-Zugang für verbundene Endgeräte bereit.
- **DHCP Enforcer** wird zwischen Endgeräten und der bestehenden DHCP-Dienstinfrastruktur implementiert und dient als DHCP-Proxy. Für alle durchgesetzten

Endgeräte werden einschränkende DHCP-Rechte-Zuordnungen vergeben, bis die Richtlinieneinhaltung bestätigt werden konnte. Dann wird dem Endgerät eine neue DHCP-Berechtigung zugewiesen. Die Integration von DHCP Enforcer mit dem Microsoft® DHCP Server-Plugin ermöglicht die schnelle Implementierung der Netzwerkzugangssteuerung ohne zusätzliche Geräte im Netzwerk.

- **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.

Cisco Network Admission Control und Microsoft Network Access Protection

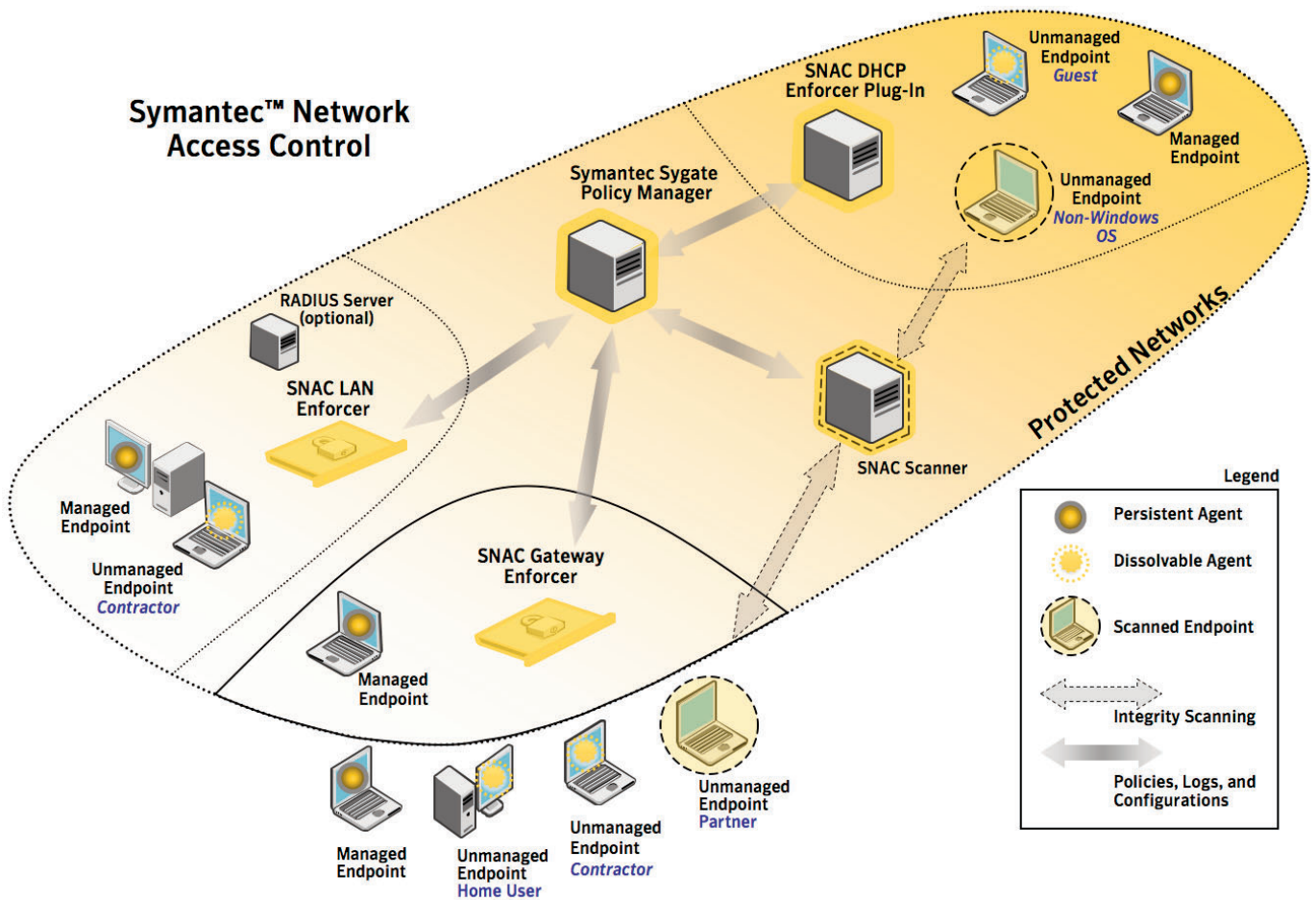
Symantec Network Access Control bietet durchgängige Steuerungsfunktionen, ohne dass zusätzliche Lösungen erforderlich sind, lässt sich jedoch in andere Technologien für Netzwerkzugangssteuerung integrieren und kann diese erweitern. Sicherheitsadministratoren können sich darauf verlassen, dass sie unabhängig von der Durchsetzungsmethode über eine umfangreiche Abdeckung und Kontrolle verfügen.

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 führen und sie 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

	Symantec Network Access Control	Symantec Network Access Control Starter Edition
Durchsetzung		
LAN 802.1x	X	
DHCP	X	
Gateway	X	X
Selbstüberwachung	X	X
Endgeräteanalyse		
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 Scanner

Betriebssystem:

- Windows 2000 Server SP4
- Windows 2003 Server SP1

Prozessor-Mindestanforderungen: Intel® Pentium®

4 1,8 GHz

Mindestens 1 GB RAM

1 GB freier Festplattenspeicher

Internet Explorer® 5.5 oder höher Windows 2000

Professional

Symantec Network Access Control Enforcer 6100 Serie

Basis-Appliance-Option (Gateway, LAN und DHCP)

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, LAN, and DHCP)

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)

Optional: Microsoft DHCP Server Plug-in (wird direkt auf Microsoft DHCP-Servern installiert, kein externes DHCP Enforcer-Gerät erforderlich)

Weitere Informationen

Besuchen Sie unsere Webseite

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.

Symantec Dublin

Ballycoolin Business Park

Blanchardstown

Dublin 15

Ireland

Phone: +353 1 803 5400

Fax: +353 1 820 4055

