

Symantec AntiVirus™ Enterprise Edition

Marktführender Virenschutz für alle Netzwerkbereiche

Symantec AntiVirus Enterprise Edition ist eine umfassende Lösung, die alle Netzwerkebenen wie Gateways, Netzwerkserver und Arbeitsstationen schützt. Diese Komplettlösung erleichtert den Aufbau eines effektiven Schutzes, denn es entfällt die aufwändige Zusammenstellung und Verwaltung von Produkten verschiedener Hersteller. Symantec AntiVirus Enterprise Edition verbindet bewährte Technologien mit Symantecs globaler Reaktionsinfrastruktur und sorgt so für leistungsstarken und skalierbaren Schutz vor Viren, bevor sie das Netzwerk infizieren können. Das Programm enthält zudem integrierte Filtertechnologien, mit denen sich unerwünschte E-Mail-Inhalte wie beispielsweise Werbe-E-Mails (Spam) blockieren lassen.

Die enorme Flexibilität der Symantec AntiVirus Enterprise Edition bietet Unternehmen den Vorteil, genau die Kombination von Virenschutzlösungen zu installieren, die den jeweiligen Anforderungen des Unternehmens entspricht. Mit dieser umfassenden Sicherheitslösung erhält das Unternehmen eine Vielzahl fortschrittlicher Technologien, die den Schutz jeder einzelnen Netzwerkebene abdecken.

> E-Mail (SMTP)-Gateway

Symantec AntiVirus™ für SMTP Gateways sorgt für integrierten Schutz vor Viren, Würmern, Trojanischen Pferden, Spam-E-Mails und anderen unerwünschten Inhalten, die über E-Mail in ein Netzwerk gelangen. Gefahren werden bereits zum frühestmöglichen Zeitpunkt im Netzwerk abgewehrt: am Internet-E-Mail-Gateway.

Symantec AntiVirus für SMTP Gateways wehrt Spam-E-Mails mit Hilfe eines mehrschichtigen Sicherheitssystems ab. Der integrierte Anti-Spam-Mechanismus kombiniert mehrere Erkennungsebenen mit unterschiedlichen Methoden zur Vermeidung von Fehlerkennungen. Dabei kommen verschiedene Erkennungstechniken zum Einsatz: benutzerdefinierte Listen zum Blockieren von Absendern, Unterstützung mehrerer Echtzeit-Negativlisten (Blacklists) sowie eine heuristische Anti-Spam-Engine. Benutzerdefinierte Positivlisten (Whitelists) sorgen dafür, dass legitime und vertrauenswürdige Domänen nicht von der Anti-Spam-Engine geprüft werden. Die Möglichkeit, Adressen in eine Positivliste einzutragen, vereinfacht die Korrektur von Fehlerkennungen. Die Kombination unterschiedlicher Erkennungsebenen und -methoden erhöht die Erkennungsrate und verringert das Auftreten von Fehlerkennungen.

> Internet (HTTP)-Gateway

Symantec™ Web Security schützt den Internet-Verkehr am HTTP/FTP-Gateway durch eine skalierbare, leistungsstarke Prüfung, die in einem einzigen Durchgang ausgeführt wird. Marktführende Virenschutz- und URL-Filtertechnologien sorgen für umfassende Sicherheit. Symantec Web Security ist die derzeit einzige Sicherheitslösung, die listenbasierte und heuristische Prüftechnologien für den Virenschutz und für die Filterung von unerwünschten Webinhalten kombiniert. Viren und unerwünschte Inhalte können so erst gar nicht in das Netzwerk eindringen. Und noch ein Vorteil: Bei dieser Sicherheitslösung stammen alle Softwarebestandteile aus einer Hand. Die neuen Funktionen zur zentralen Richtlinienverwaltung auf mehreren Servern vereinfachen die Administration und erhöhen die Skalierbarkeit.

DIE VORTEILE

- > Umfassende Lösung für den Schutz des gesamten Netzwerks vor Viren, Spam und anderen unerwünschten Inhalten
- > **NEU!** Mehrschichtiges Sicherheitssystem zur Abwehr von Spam-E-Mails durch die Kombination von Negativlisten (Blacklists) und heuristischen Erkennungsverfahren. Die Möglichkeit, Adressen in eine Positivliste (Whitelist) einzutragen, vereinfacht das Vermeiden und die Korrektur von Fehlerkennungen beim Internet-E-Mail-Verkehr.
- > **NEU!** Zentrale Überwachungsfunktionen zur Identifizierung von ungeschützten Knoten sowie von Knoten, die von Symantec AntiVirus™ Corporate Edition und ausgewählten Virenschutzlösungen anderer Hersteller gesichert werden
- > **NEU!** Unterstützung einer Vielzahl von Plattformen – jetzt auch für Windows® Server 2003, 64-Bit Intel® Itanium 2-Hardware und Netware® Secure Console
- > Umfassender Schutz auf der Internet-Gateway-, Netzwerkserver- und Arbeitsstationsebene durch die Verbindung wegweisender Virenschutztechnologien mit globalen Reaktionsteams
- > Maximale Verfügbarkeit des Systems durch eine zentrale, skalierbare Verwaltung und moderne Automatisierung – selbst in heterogenen Computerumgebungen
- > Leistungsstarker und skalierbarer Virenschutz für Internet-E-Mail- und Web-Gateways mit hohem Datenverkehr
- > Innovative Automatisierung und fortschrittliche Technologien bewirken auf allen führenden Unternehmensplattformen effektiven Schutz vor Viren sowie kurze Reaktionszeiten
- > Unterstützt durch Symantec™ Security Response, dem weltweit führenden Forschungs- und Unterstützungsteam für Internet-Sicherheit

> Groupware-Server

- Symantec AntiVirus™/Filtering für Microsoft Exchange schützt Microsoft Exchange-Server umfassend vor Viren, indem es Viren erkennt und entfernt sowie E-Mail-Inhalte nach zuvor festgelegten Regeln filtert.
- Symantec AntiVirus™/Filtering für Domino ist eine umfassende Lösung für den Schutz von Lotus® Domino™-Datenbanken. Das Programm sorgt für optimalen Schutz vor aktuellen und unbekanntem Viren – einschließlich sich schnell ausbreitender Würmer und polymorpher Viren. Über eine Schnittstelle, die nahtlos an die Notes-Umgebung angepasst ist, bietet Symantec AntiVirus/Filtering flexiblen, zuverlässigen Schutz für Domino-Server.

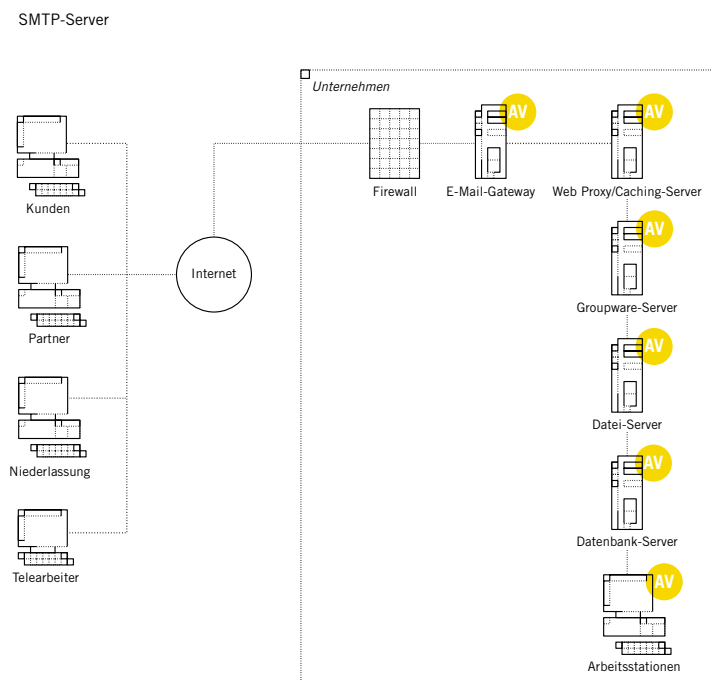
> Arbeitsstationen und Netzwerkserver

Symantec AntiVirus™ Corporate Edition sorgt unternehmensweit für skalierbaren, plattformübergreifenden Virenschutz für Arbeitsstationen und Netzwerkserver. Aber nicht nur sie werden umfassend geschützt. Symantec AntiVirus Corporate Edition bietet darüber hinaus auch zusätzlichen Virenschutz für Content-Storage-Umgebungen. Um Viren, Würmer und Trojanische Pferde in allen wichtigen Dateitypen – selbst in mobilem Code und komprimierten Dateiformaten – aufzuspüren, nutzt Symantec AntiVirus Corporate Edition branchenführende Virenschutztechnologien. Die Lösung arbeitet mit innovativen Diensten zur Virenprüfung und -reparatur, die nur geringe Ressourcen in der Netzwerk-Infrastruktur beanspruchen.

> Zentrale Verwaltung von Arbeitsstationen und Netzwerkservern

Symantec AntiVirus Enterprise Edition enthält zahlreiche Funktionen für die zentrale Verwaltung des Arbeitsstations- und Netzwerkservernschutzes. Mithilfe der skalierbaren Management-Konsole des Symantec System Center™ wird die unternehmensweite Installation von Virenschutzlösungen auf einer Vielzahl verschiedener Plattformen erheblich vereinfacht. Durch das anschließende Erstellen, Durchsetzen und Aktualisieren von Richtlinien sind Netzwerkserver und Arbeitsstationen jederzeit richtig konfiguriert. Über die zentrale Management-Konsole lassen sich sämtliche Netzwerkknoten überwachen. Administratoren können so leicht feststellen, welche Knoten ungeschützt und anfällig für Virenangriffe sind und welche Knoten von Symantec AntiVirus Corporate Edition, McAfee® VirusScan®, Trend Micro OfficeScan™, Computer Associates® oder Virenschutzlösungen anderer Hersteller geschützt werden. Das Symantec System Center ermöglicht auch die zentrale Verteilung von Virendefinitionen und Produkt-Updates. Dadurch werden die Installationskosten erheblich reduziert.

Umfassender unternehmensweiter Schutz



Virenschutz für alle neuralgischen Punkte im Netzwerk

➤ **Automatischer Virenschutzzyklus durch fortschrittliche Technologie**

Die Digital Immune System™-Technologie der Symantec AntiVirus Enterprise Edition koordiniert den Virenschutzzyklus auf intelligente Weise. Da die Weiterleitung möglicher Viren und die Bereitstellung von Virendefinitionen automatisiert ist, lässt sich auch die Bearbeitungszeit drastisch reduzieren. Zusammen mit einer fortschrittlichen Back-End-Infrastruktur bestehend aus Hardware-Ressourcen, einer hochentwickelten Systemarchitektur sowie den neuesten Prüf-Engines sorgt das Digital Immune System dafür, dass Unternehmen den bestmöglichen Service erhalten. Die folgenden Technologien verbessern die automatische Reaktionsfähigkeit der Lösung:

- Die modulare NAVEX™ Prüf-Engine-Technologie aktualisiert Virendefinitionen und Prüf-Engines, ohne dass die Software neu installiert oder das System neu gestartet werden muss. Dadurch wird maximale Systemverfügbarkeit gewährleistet, und die Total Cost of Ownership (TCO) werden gesenkt.
- LIVEUPDATE™ sorgt mit automatischen, zeitplangesteuerten Downloads der Virendefinitionen jederzeit für aktuellen Schutz.
- Die heuristische BLOODHOUND™-Technologie spürt neue Viren auf, indem sie virentypische Verhaltensmuster erkennt. Bloodhound erkennt bis zu 90 Prozent aller neuen Makro-Viren und bis zu 80 Prozent aller neuen und unbekanntes Programmdateiviren, darunter auch bösartigen mobilen Code.
- Mithilfe von Internet-basierten Technologien können verdächtige Dateien sicher über HTTPS an Symantec gesendet werden. Die daraufhin gelieferte Virensignatur kann zunächst getestet oder sofort automatisch an den infizierten Rechner bzw. das gesamte Unternehmen verteilt werden. Durch die automatisierte Bearbeitung wird die Reaktionszeit bei sich schnell ausbreitende Viren erheblich reduziert und Netzwerkausfallzeiten durch Virenangriffe werden minimiert.
- Der Quarantäne-Bereich bietet zusätzlichen Schutz. Alle nicht reparierbaren, virusinfizierten Dateien können in einen sicheren Bereich auf einem zentralen Server weitergeleitet werden. Vor der Übermittlung einer infizierten Datei werden alle unternehmensrelevanten Informationen aus der Datei gelöscht. Da der Virus aus der Arbeitsumgebung entfernt wird, lässt sich eine Ausbreitung des Virus im Unternehmen auf diese Weise wirksam verhindern.
- Mithilfe einer Technologie zur automatisierten Makrovirenanalyse und -reparatur analysiert SARA (Symantec AntiVirus Research Automation) alle Dateien, die an Symantec Security Response übermittelt werden. Anschließend wird per E-Mail eine neue Virensignatur zurückgesendet.

➤ **Unterstützt von Symantec™ Security Response**

Symantec AntiVirus Enterprise Edition wird weltweit von Symantec Security Response unterstützt, um so jederzeit einen 24-Stunden-Schutz zu gewährleisten. Dieses weltweit größte Team von Virenexperten arbeitet kontinuierlich an der Identifizierung und Bekämpfung von Viren, bevor diese das Netzwerk infizieren und sich im Unternehmen ausbreiten können. Symantec Security Response reagiert in kürzester Zeit auf Virenausbrüche und widmet sich der Erforschung möglicher zukünftiger Gefahren.

Weitere Informationen zu Symantec AntiVirus Enterprise Edition finden Sie unter www.enterprisesecurity.symantec.com oder www.enterprisesecurity.symantec.de.

VIRENSCHUTZ UND CONTENT FILTERING SIND WICHTIGE BESTANDTEILE DER SYMANTEC ENTERPRISE SECURITY-LÖSUNGEN. SYMANTEC ENTERPRISE SECURITY VERBINDET ERSTKLASSIGE TECHNOLOGIEN, UMFASSENDE SERVICES UND GLOBALE REAKTIONSTEAMS FÜR IHRE UNTERNEHMENSICHERHEIT.

SYSTEMANFORDERUNGEN

SYMANTEC ANTIVIRUS™ ENTERPRISE EDITION 8.6

SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 FÜR 32-BIT WINDOWS CLIENTS:

- Windows 98/98 SE/ME, Windows NT 4.0 Workstation/Server/Terminal Server mit SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Home/Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- Mindestens 32 MB RAM
- 46 MB freier Festplattenspeicher
- Intel Pentium-Prozessor (Prozessor ab Pentium II empfohlen)

SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 FÜR 64-BIT WINDOWS-CLIENTS:

- Windows XP 64-Bit Edition Version 2003; Windows Server 2003 Enterprise/Datacenter 64-Bit Editions
- 80 MB freier Festplattenspeicher
- Intel Itanium 2-Prozessor

SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 MANAGEMENT SERVER FÜR 32-BIT WINDOWS:

- Windows NT 4.0 Workstation/Server/Terminal Server mit SP6a; Windows 2000 Professional/Server/Advanced Server; Windows XP Professional; Windows Server 2003 Web/Standard/Enterprise/Datacenter
- 32 MB RAM (64 MB oder mehr empfohlen)
- 111 MB freier Festplattenspeicher (65 MB für Symantec AntiVirus Corporate Edition-Server-Dateien und 46 MB für das Client-Festplatten-Image)
- Intel Pentium-Prozessor (Prozessor ab Pentium II empfohlen)
- Für die Installation von AMS2 Server (optional) sind 15 MB freier Festplattenspeicher erforderlich.

SYMANTEC ANTIVIRUS CORPORATE EDITION 8.1 MANAGEMENT SERVER FÜR NETWARE:

- NetWare 5.x, 6 SP1
- 15 MB RAM (mehr als die standardmäßigen NetWare RAM-Anforderungen) für Symantec AntiVirus-NLMs
- 116 MB freier Festplattenspeicher (70 MB für Symantec AntiVirus Corporate Edition-Server-Dateien und 46 MB für das Client-Festplatten-Image)
- Intel Pentium-Prozessor (Prozessor ab Pentium II empfohlen)
- Für die Installation von AMS2 Server (optional) sind 20 MB freier Festplattenspeicher erforderlich.

UNTERSTÜTZUNG ÄLTERER BETRIEBSSYSTEME MIT NORTON ANTIVIRUS™ CORPORATE EDITION 7.6 FÜR WINDOWS 95-CLIENT:

- Mindestens 32 MB RAM
- Prozessor ab Intel 486 (Prozessor ab Pentium-Klasse empfohlen)
- 43 MB freier Festplattenspeicher (80 MB während der Installation)
- WINSOCK ab Version 2.0

FÜR NETWARE-SERVER:

- NetWare 4.11 mit SP9; NetWare 4.2 mit SP9; NetWare 5.x mit oder ohne SP2
- 3 MB RAM (zusätzlich zu den NetWare RAM-Standardanforderungen) für Norton AntiVirus-NLMs
- Erforderlich für NetWare 4.1x: LIBUPF (verfügbar mit Support Pack 7 oder höher)
- 70 MB freier Festplattenspeicher für Norton AntiVirus-Server-Dateien und 46 MB freier Festplattenspeicher für die Norton AntiVirus Client-Festplatten-Image
- 10 MB freier Festplattenspeicher für AMS2-Dateien (20 MB während der Installation)

Eine vollständige Auflistung der Systemanforderungen für das jeweilige Produkt finden Sie auf der Produkt-Webseite für Symantec AntiVirus Enterprise Edition unter <http://enterprisesecurity.symantec.de/>.

SYMANTEC SYSTEM CENTER:

- Windows NT 4.0 Workstation und Server mit SP6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional
- Microsoft Internet Explorer ab Version 5.5 mit Service Pack 2
- Microsoft Management Console 1.2. Wenn die MMC nicht bereits installiert ist, sind 3 MB Festplattenspeicher erforderlich (10 MB während der Installation).
- 10 MB freier Festplattenspeicher

SYMANTEC SYSTEM CENTER SNAP-INS:**Alert Management System-Konsole**

- 10 MB freier Festplattenspeicher zusätzlich zu den Symantec System Center-Anforderungen

Symantec AntiVirus Snap-In

- 5 MB freier Festplattenspeicher zusätzlich zu den Symantec System Center-Anforderungen

Tool zur Verteilung von AntiVirus Server

- 130 MB freier Festplattenspeicher zusätzlich zu den Symantec System Center-Anforderungen

Tool zur NT-Client-Installation

- 2 MB freier Festplattenspeicher zusätzlich zu den Symantec System Center-Anforderungen

SYMANTEC PACKAGER

Symantec Packager kann nur auf Windows NT-basierten Betriebssystemen ausgeführt werden. Für Symantec Packager gelten folgende Systemanforderungen:

Unterstützte Betriebssysteme:

- Windows NT Workstation 4.0/Server 4.0 mit SP6a; Windows 2000 Professional/Server mit SP2; Windows XP Professional
- Microsoft Internet Explorer ab Version 5.5
- Windows Installer 2.0 (Hinweis: Falls Windows Installer 2.0 nicht auf dem System vorhanden ist, wird er bei der Installation von Symantec Packager installiert.)
- Prozessor ab Pentium II 300 MHz
- 64 MB RAM (128 MB empfohlen)
- 60 MB freier Festplattenspeicher
- CD-ROM- oder DVD-Laufwerk

SYMANTEC PACKAGER-INSTALLATIONSPAKETE

Obwohl Symantec Packager nur auf Windows NT-basierten Betriebssystemen ausgeführt werden kann, können mit Symantec Packager erstellte Pakete auf den folgenden Betriebssystemen installiert werden:

- Windows NT 4.0 mit SP6a; Windows 98/ME/2000; Windows XP Home Edition/Professional Edition

QUARANTINE-KONSOLE:

- Windows NT 4.0 Workstation und Server mit SP6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional
- Microsoft Internet Explorer ab Version 5.5 mit Service Pack 2
- Microsoft Management Console 1.2. Wenn die MMC nicht bereits installiert ist, sind 3 MB Festplattenspeicher erforderlich (10 MB während der Installation).
- 35 MB freier Festplattenspeicher

QUARANTINE-SERVER:

- Windows NT 4.0 Workstation und Server mit SP6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Professional; Windows Server 2003 Web, Standard, Enterprise und Datacenter Editions
- Microsoft Internet Explorer ab Version 5.5 mit Service Pack 2
- 40 MB freier Festplattenspeicher
- Mindestens 250 MB für Auslagerungsdatei
- 500 MB bis 4 GB Festplattenspeicher für isolierte Elemente (empfohlen)

SYMANTEC ANTIVIRUS™/FILTERING 3.0 FÜR MICROSOFT® EXCHANGE 2000:**Server**

- Windows 2000 Server oder Advanced Server mit Service Pack ab Version 2
- Microsoft Exchange 2000 mit Service Pack ab Version 1
- 512 MB RAM für Microsoft Exchange 2000
- 95 MB freier Festplattenspeicher für die Installation, 120 MB für die Ferninstallation
- Mindestens 120 MB freier Festplattenspeicher für die Programmausführung
- Microsoft Management Console 1.2

Konsole

- Windows 2000 Professional mit Service Pack 2 oder Windows XP
- Microsoft Internet Explorer ab Version 5.01
- 200 MB freier Festplattenspeicher für die Installation

NORTON ANTIVIRUS™ FÜR MICROSOFT® EXCHANGE 2.5

- Windows NT Server 4.0 ab SP3, Windows 2000 ab SP1
- Microsoft Exchange 5.0 oder 5.5 mit den aktuellsten Service Packs, Exchange 2000
- Mindestens 64 MB RAM
- 20 MB freier Festplattenspeicher für die Installation; mindestens 50 MB freier Festplattenspeicher für die Programmverarbeitung
- Netscape® Navigator (ab Version 4.x) oder Microsoft Internet Explorer (ab Version 4.x), Java und JavaScript (Cookies müssen aktiviert sein)
- Upgrade-Server, auf denen Exchange 5.5 Service Pack 3 mit dem neuesten Hotfix ausgeführt wird. Verwenden Sie Microsoft Exchange ab Version 5.5.2651.76.

SYMANTEC ANTIVIRUS™/FILTERING 3.1 FÜR DOMINO™

- Windows 2000 mit Service Pack ab Version 2 oder Windows NT 4.0 mit Service Pack ab Version 6a
- Lotus Domino ab Version 5.0.8
- Lotus Notes Client ab Version 5.0.7a
- Mindestens 128 MB RAM
- 300 MB bis 1 GB freier Festplattenspeicher

SYMANTEC ANTIVIRUS™ FOR SMTP GATEWAYS 3.1**Solaris**

- SPARC-basiertes Solaris 7 oder 8
- Mindestens 256 MB RAM (512 MB oder mehr empfohlen für optimale Leistung)
- 50 MB für die Installation, mindestens 500 MB nach der Installation für die Mail-Verarbeitung
- Netscape® Navigator® ab Version 4.7 oder Microsoft® Internet Explorer ab Version 5.0

Windows 2000/NT®

- Prozessor ab Intel Pentium III oder IV oder kompatibler Prozessor
- Windows 2000 oder Server mit SP3
- Mindestens 256 MB RAM

- 50 MB für die Installation, mindestens 500 MB nach der Installation für die Mail-Verarbeitung

- Netscape Navigator ab Version 4.7 oder Microsoft® Internet Explorer ab Version 5.0

SYMANTEC™ WEB SECURITY 3.0**Windows 2000/NT®**

- PC mit Intel-Prozessor ab Pentium II oder kompatibelem Prozessor
- Windows NT Server 4.0 mit SP6a oder Windows 2000 Server mit SP2
- Mindestens 256 MB RAM

- Mindestens 500 MB freier Festplattenspeicher für Programmdateien, Online-Dokumentation, Konfigurationsdateien
- Zusätzlicher Festplattenspeicher erforderlich zum Speichern von Aktivitätsprotokollen und Cache. 400 MB empfohlen, für eine optimale Ausführung sollten ab 1 GB verfügbar sein.
- Internet-Zugang und CD-ROM-Laufwerk
- Korrekt konfiguierter DNS-Server mit A- und PTR-Datensätzen

- System unter Sun® SPARC
- Betriebssystem Solaris Version 7 oder 8
- Mindestens 256 MB RAM
- Mindestens 500 MB freier Festplattenspeicher für Programmdateien, Online-Dokumentation, Konfigurationsdateien

- Zusätzlicher Festplattenspeicher erforderlich zum Speichern von Aktivitätsprotokollen und Cache. 400 MB empfohlen, für eine optimale Ausführung sollten ab 1 GB verfügbar sein.
- Internet-Zugang und CD-ROM-Laufwerk
- Korrekt konfiguierter DNS-Server mit A- und PTR-Datensätzen

Solaris

- System unter Sun® SPARC
- Betriebssystem Solaris Version 7 oder 8
- Mindestens 256 MB RAM

- Mindestens 500 MB freier Festplattenspeicher für Programmdateien, Online-Dokumentation, Konfigurationsdateien

- Zusätzlicher Festplattenspeicher erforderlich zum Speichern von Aktivitätsprotokollen und Cache. 400 MB empfohlen, für eine optimale Ausführung sollten ab 1 GB verfügbar sein.
- Internet-Zugang und CD-ROM-Laufwerk
- Korrekt konfiguierter DNS-Server mit A- und PTR-Datensätzen

WORLD HEADQUARTERS:
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
001-408-253 9600
001-800-441 7234

DEUTSCHLAND:
Symantec (Deutschland) GmbH
Kaiserswerther Str. 115
D - 40880 Ratingen
Tel.: +49 (0) 69-6641 0315
E-Mail: enterprise.deutsch@symantec.com

ÖSTERREICH:
Symantec GmbH
Wipplingerstraße 34
A - 1010 Wien
Tel.: +43 (0)1- 532 85 33-0
E-Mail: info@symantec.at

SCHWEIZ:
Symantec Switzerland AG
Grindelstrasse 6
CH - 8303 Bassersdorf
Tel.: +41 (0) 1-838 49 00
Fax: +41 (0) 1-838 49 01
E-Mail: info@symantec.com

Symantec hat Niederlassungen in 38 Ländern. Adressen und Telefonnummern der Symantec-Niederlassungen in anderen Ländern finden Sie auf unseren Websites: www.symantec.com oder www.symantec.de

Informationen über Kundenservice und technischen Support finden Sie auf unserer Website