Symantec AntiVirus™ Corporate Edition

Umfassender Virenschutz für Arbeitsstationen und Netzwerk-Server in Unternehmen

Immer häufiger werden schädliche Viren in Umlauf gebracht, die sich mit enormer Geschwindigkeit verbreiten. Für Unternehmen ist daher das Thema Virenschutz ein Hauptanliegen. Allerdings bietet Virenschutz an der Firewall und am E-Mail-Gateway allein heute keinen ausreichenden Schutz mehr. Erst ein lückenloser Virenschutz auf den Arbeitsstationen und Netzwerk-Servern im gesamten Unternehmen kann die Betriebsbereitschaft des Systems und die Benutzerproduktivität dauerhaft gewährleisten.

Symantec AntiVirus™ Corporate Edition sorgt unternehmensweit für skalierbaren, plattformübergreifenden Virenschutz für Arbeitsstationen und Netzwerk-Server, um die Betriebsbereitschaft des Systems und die Benutzerproduktivität sicherzustellen.

Neue Funktionen in dieser Version

- Die ERWEITERTE BEDROHUNGSVERWALTUNG spürt unerwünschte Anwendungen wie beispielsweise Spyware- und Adware-Programme auf, deckt den Ausgangspunkt von Angriffen auf, die sich über geöffnete Dateifreigaben verbreiten, und beendet verdächtige Prozesse im Speicher, bevor sie Schaden anrichten können.
- Der ERWEITERTE E-MAIL-SCHUTZ verhindert, dass Client-Systeme Würmer per E-Mail verbreiten, und prüft Internet-E-Mail-Anhänge, die über POP3-E-Mail-Clients zugestellt werden.
- OPTIMIERTE FUNKTIONEN FÜR DEN SCHUTZ UND DIE VERWALTUNG VON REMOTE-BENUTZERN sorgen für die Einhaltung der Unternehmensrichtlinien auf Remote-Systemen, bevor diese Zugriff auf Unternehmensressourcen erhalten. Zudem werden damit Ereignisdaten auf Clients gespeichert, die nicht mit dem Netzwerk verbunden sind, und an den Management-Server weitergeleitet, sobald erneut eine Verbindung hergestellt wird.

Zentrale Konfiguration und Verwaltung

Die Management-Konsole des Symantec System Center™ ermöglicht die zentrale Konfiguration, Verteilung, Richtlinienverwaltung und Berichterstellung*. Über das Symantec System Center lassen sich mehrere Hunderttausend Server verwalten.

- Über ZENTRALE MANAGEMENT-FUNKTIONEN können einzelne Benutzer und Benutzergruppen als funktionale Einheiten verwaltet werden. Sie ermöglichen außerdem das Erstellen, Verteilen und Sperren von Sicherheitsrichtlinien und Einstellungen. Das Sperren von Einstellungen auf den Arbeitsstationen und Netzwerk-Servern hindert Benutzer daran, diese Einstellungen zu ändern. Arbeitsstationen und Netzwerk-Server können ebenfalls von der Management-Konsole aus konfiguriert und überwacht werden.
- AUTOMATISCHE VIRENREPARATUREN UND -WARNUNGEN. Sobald ein Virus entdeckt wird, erfolgt automatisch die Reparatur der infizierten Datei. Die Symantec System Center-Konsole benachrichtigt umgehend den IT-Administrator.
- SCHNELLE REAKTION BEI BEDROHUNGEN. Symantec AntiVirus Corporate Edition ermöglicht den sofortigen Start einer LiveUpdate-Sitzung auf einem bzw. mehreren Clients. Dadurch wird die Reaktionszeit bei sich schnell ausbreitenden Bedrohungen erheblich verkürzt. Für eine noch schnellere, automatisierte Reaktion wird eine Push-Technologie auf einem mit dem Symantec System Center verbundenen Management-Server installiert. Der Management-Server lässt sich so konfigurieren, dass Viren-Updates nach einem Zeitplan von Symantec oder einem zentralen LiveUpdate-Server heruntergeladen werden. Anschließend werden diese Updates an die sekundären Server verteilt und von dort an die Client-Systeme übertragen.
- NETZWERK-AUDIT-FUNKTION. Administratoren können feststellen, welche Knoten ungeschützt und anfällig für Virenangriffe sind und welche Knoten von Symantec AntiVirus, McAfee® VirusScan®, Trend Micro™ Office Scan™, Computer Associates® oder Virenschutzlösungen anderer Hersteller geschützt werden.

* Gegen eine zusätzliche Gebühr erhältlich.

DIE VORTEILE

- Fortschrittlicher, unternehmensweiter Virenschutz über eine einzige Konsole
- **NEU!** Erweiterte Funktionen für die Erkennung und Kategorisierung von Bedrohungen spüren unerwünschte Anwendungen auf, beispielsweise Spyware- und Adware-Programme.
- **NEU!** Die Bedrohungsverwaltung deckt den Ausgangspunkt von Angriffen auf, die sich über geöffnete Dateifreigaben verbreiten.
- **NEU!** Heuristische Technologie zur Erkennung von Würmern in ausgehenden E-Mail-Nachrichten verhindert, dass Client-Systeme Würmer per E-Mail verbreiten.
- **NEU!** Die Anhangsprüfung für Internet-E-Mail prüft alle eingehenden E-Mails, die über einen POP3-E-Mail-Client zugestellt werden.
- **NEU!** Symantec VPN Sentry prüft die Einhaltung der Unternehmensrichtlinien auf Remote-Systemen, bevor diese Zugriff auf Unternehmensressourcen erhalten.
- **NEU!** Mit der Funktion zum Speichern und Weiterleiten von Ereignisdaten werden Ereignisdaten auf Clients gespeichert, die nicht mit dem Netzwerk verbunden sind, und an den Management-Server weitergeleitet, sobald erneut eine Verbindung hergestellt wird.
- **NEU!** Die Speicherprüfungsfunktion erkennt Bedrohungen und beendet verdächtige Prozesse im Speicher, bevor sie Schaden anrichten können.
- Zentrale Überwachungsfunktionen identifizieren sowohl ungeschützte Knoten als auch solche Knoten, die von Symantec AntiVirus™ Corporate Edition und ausgewählten Sicherheitslösungen anderer Hersteller geschützt werden.
- Unterstützt von Symantec™ Security Response, einem führenden Forschungs- und Unterstützungsteam für Internet-Sicherheit

- GEMEINSAMER VERTEILUNGS- UND AKTUALISIERUNGSMECHANISMUS Das Symantec System Center™ ermöglicht die zentrale, plattformübergreifende Verteilung von Virendefinitionen und Produkt-Updates an Arbeitsstationen und Netzwerk-Server zahlreicher Plattformen. Dadurch werden die Kosten und der Verwaltungsaufwand für die unternehmensweite Verteilung von Virendefinitionsaktualisierungen gesenkt.
- Die BEDROHUNGSVERWALTUNG deckt den Ausgangspunkt von Angriffen auf, die sich über geöffnete Dateifreigaben verbreiten (beispielsweise Code Red und Nimda).
- VERSCHIEBEN VON CLIENTS ZWISCHEN SERVERN. Mithilfe der zentralen Management-Konsole lassen sich jetzt Clients per "Drag & Drop" von einem übergeordneten Server auf einen anderen verschieben.
- VERWALTUNG LOGISCHER GRUPPEN. Administratoren können Clients und Server innerhalb von Server-Gruppen zu logischen Gruppen zusammenfassen und mehrere funktionale Gruppen von einem einzigen übergeordneten Server aus verwalten. Insbesondere Unternehmen, die ähnliche funktionale Einheiten (beispielsweise Abteilungen oder Geschäftsbereiche) verwalten müssen, profitieren von dieser Funktion, da sich damit die Infrastrukturkosten erheblich reduzieren lassen.
- PRODUKT-PATCHING ermöglicht eine schnelle und kostengünstige Verteilung von Sicherheits-Patches und neuen Versionen.
- SPEICHERN UND WEITERLEITEN VON EREIGNISDATEN. Mit dieser Funktion lassen sich Ereignisdaten auf dem Client speichern, wenn dieser nicht mit dem Management-Server verbunden ist. Sobald der Client eine Verbindung herstellt, werden die Daten auf den Management-Server übertragen. Auf diese Weise wird gewährleistet, dass wichtige Ereignisdaten jederzeit für die Warnmeldungsfunktion, Protokollierung und Berichterstellung verfügbar sind.*
- PROBLEMLOSE MIGRATION. Das Installations-Tool sucht nach älteren Versionen von Norton AntiVirus™ Corporate Edition ab Version 7.x. Wird eine ältere Version gefunden, werden die Benutzereinstellungen beibehalten, die vorherige Technologie vom Client oder Server entfernt und die neue Lösung installiert.
- Ein DEINSTALLATIONSPROGRAMM FÜR SICHERHEITSSOFTWARE reduziert die Kosten für den Umstieg von einem Virenschutzprodukt eines anderen Herstellers auf Symantec AntiVirus Corporate Edition.
- AUTOMATISCHE ODER INTERAKTIVE INSTALLATIONSOPTIONEN für die flexible Installation auf Client-Rechnern im Hintergrund (automatischer Modus) oder mit Beteiligung von Seiten der Benutzer.
- EINGESCHRÄNKTE ODER VOLLSTÄNDIGE BENUTZEROBERFLÄCHE MIT KENNWORTSCHUTZ. Administratoren können festlegen, ob Benutzer vollständigen oder eingeschränkten Zugriff auf die Benutzeroberfläche erhalten.

Wegweisender Virenschutz

Um Viren, Würmer und Trojanische Pferde in allen wichtigen Dateitypen – selbst in mobilem Code und komprimierten Dateiformaten – aufzuspüren, nutzt Symantec AntiVirus Corporate Edition die wegweisenden Virenschutztechnologien von Symantec. Da die neue Version mit kleineren Virendefinitionsdateien auskommt und sich per Multi-Thread-Server-Rollout verteilen lässt, wird auch die für die Verteilung der Definitionen benötigte Zeit weiter verkürzt. Symantec AntiVirus Corporate Edition ist darüber hinaus eine hoch skalierbare Virenschutzlösung, die Engpässe vermeidet, indem sie selbst bei hohem Datenaufkommen für eine automatische Lastverteilung über mehrere Server sorgt.

- ERWEITERTE FUNKTIONEN ZUR ERKENNUNG UND KATEGORISIERUNG VON BEDROHUNGEN erkennen sowohl Viren als auch Bedrohungen, die nicht zur Kategorie der Viren gehören. Diese Funktionen spüren nicht autorisierte Programme auf, die die Sicherheit des Systems (z. B. Viren, Würmer und Trojanische Pferde) oder die Vertraulichkeit der Kundendaten (z. B. Spyware, Trackware und Adware) gefährden können. Auch Programme, die mit bösartigen Absichten verbreitet werden (z. B. Dialer, Scherzprogramme sowie Remote-Zugriffs- und Hacker-Tools) werden erkannt.

- VERHALTENSMUSTER-ERKENNUNG. Die heuristische Technologie für die Wurmerkennung erkennt bösartige Programme und verhindert, dass Client-Systeme Würmer per E-Mail verbreiten (z. B. SOBIG.F).
- ANWENDUNGSSICHERHEIT/MANIPULATIONSSCHUTZ. Diese Funktion protokolliert alle nicht autorisierten Registrierungsänderungen und authentifiziert die vom Symantec System Center auf einen Client übertragenen Richtlinien- und Definitionsaktualisierungen. Die Funktion erkennt außerdem, wenn der Echtzeit-Virenschutz über einen längeren Zeitraum hinweg deaktiviert ist, und schaltet ihn automatisch wieder ein.
- GEMEINSAME PRÜF-ENGINE. Unabhängig von der unterstützten Plattform oder Sprache wird nur eine einzige Virendefinitionsdatei an alle Arbeitsstationen und Server verteilt.
- Die erweiterbare NAVEX™ Prüf-Engine-Technologie aktualisiert Virendefinitionen und Prüf-Engines, ohne dass die Software neu installiert oder das System neu gestartet werden muss.
- OPTIMIERTE PRÜFVERFAHREN beanspruchen nur geringe Ressourcen in der vorhandenen Netzwerk-Infrastruktur. Komprimierte Dateien werden 50 Prozent schneller als in früheren Versionen geprüft, indem sie im Speicher dekomprimiert werden.
- ERKENNUNG UNBEKANNTER VIREN. Die heuristische BloodHound™-Technologie spürt unbekannte Viren anhand von virentypischen Verhaltensmustern auf. BloodHound erkennt bis zu 90 Prozent aller neuen Makro-Viren und bis zu 80 Prozent aller neuen und unbekannten Programmdateiviren, darunter auch bösartigen mobilen Code.
- Die ZENTRALQUARANTÄNE 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.
- AUTOMATISIERTER ANTWORTMECHANISMUS. Das Digital Immune System™ automatisiert das Einsenden von möglichen Viren zur weiteren Analyse und versorgt den betroffenen Rechner oder das gesamte Unternehmen mit Virensignaturen.
- E-MAIL-PRÜFUNG FÜR MICROSOFT® EXCHANGE- UND LOTUS DOMINO™-SERVER. Diese optionalen Komponenten prüfen eingehende E-Mail-Nachrichten und -Anhänge auf Microsoft Exchange- und Lotus Domino-Servern, um so eine unnötige Nutzung der E-Mail-Datenspeicher zu verhindern.
- PRÜFUNGSVERZÖGERUNG UND PRÜFPRIORITÄT. Mit diesen Optionen kann ein Benutzer einen vom Administrator geplanten Prüfvorgang auf einen späteren Zeitpunkt verschieben und die Prüfpriorität so anpassen, dass Prüfungen nur während Leerlaufzeiten durchgeführt werden.
- Die UNTERSTÜTZUNG FÜR KOMPRIMIERTE DATEIEN wurde optimiert und unterstützt die derzeit gängigsten Formate. Dazu gehören:

ArcManager
Cabinet-Dateien
Symantec Ghost Image
BinHex
LHA (LZH) Files
Multipurpose Internet Mail Extensions
RAR -Dateien
TAR -Archive
UUE -Archive
ARJ-Dateien
Executable Files
Komprimiertes GNU-Format
Hyper-Text Transfer Protocol
Komprimierte Microsoft-Dateien
OLESS Containers
Rich Text Format
MS-TNEF-Anhangsdateien
ZIP-Archivdateien

Optimierte Funktionen für die Verwaltung und den Schutz von Remote-Benutzern

- Die ANHANGSPRÜFUNG FÜR INTERNET-E-MAIL prüft alle eingehenden E-Mail-Nachrichtentexte und -Anhänge, die über einen POP3-E-Mail-Client wie beispielsweise Microsoft® Outlook®, Microsoft Outlook Express, Eudora® und Netscape Mail zugestellt werden.

- SYMANTEC VPN SENTRY gewährleistet, dass die Sicherheitsrichtlinien auf mobilen und Remote-Systemen, die über VPN eine Verbindung zum Unternehmensnetzwerk herstellen, eingehalten werden. Insbesondere prüft diese Funktion, ob die Virenschutz-Software installiert und der Echtzeitschutz aktiviert ist, die Virendefinitionsdateien auf dem neuesten Stand sind und die Client-Firewall installiert, aktiviert und mit den entsprechenden Richtlinien konfiguriert wurde.
- ROAMING SUPPORT Clients können eine Verbindung mit dem nächstliegenden übergeordneten Server herstellen, um Virendefinitionen und Richtlinien herunterzuladen. Dies ermöglicht eine optimale Bandbreitennutzung.
- Die BATTERIEPRÜFFUNKTION stellt fest, ob ein Laptop im Batteriebetrieb läuft und stellt eine geplante Prüfung so lange zurück, bis der Laptop wieder an das Stromnetz angeschlossen ist.

Weitere Informationen zu Symantec AntiVirus Corporate Edition 9.0 finden Sie unter http://enterprisesecurity.symantec.de.

VIRENSCHUTZ IST EIN WICHTIGER BESTANDTEIL DER SYMANTEC ENTERPRISE SECURITY-LÖSUNGEN. SYMANTEC ENTERPRISE SECURITY VERBINDET ERSTKLASSIGE TECHNOLOGIEN, UMFASSENDE SERVICES UND GLOBALE REAKTIONSTEAMS FÜR IHRE UNTERNEHMENSSICHERHEIT.

SYSTEMANFORDERUNGEN
SYMANTEC ANTIVIRUS™ CORPORATE EDITION 9.0

SYMANTEC ANTIVIRUS MANAGEMENT SERVER FÜR 32-BIT WINDOWS

- Windows® XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/ Terminal Server Edition SP6a
- 64 MB RAM
- 111 MB freier Festplattenspeicher
- 15 MB freier Festplattenspeicher für AMS2-Dateien (falls Sie AMS2 Server installieren)
- Microsoft Internet Explorer ab Version 4.01

SYMANTEC ANTIVIRUS MANAGEMENT SERVER FÜR NETWARE

- NetWare 5.1 ab SP3, 6.0 ab SP1
- 15 MB RAM für Symantec AntiVirus NLMs
- 116 MB freier Festplattenspeicher
- 20 MB freier Festplattenspeicher für AMS2-Dateien (falls Sie AMS2 Server installieren)

SYMANTEC ANTIVIRUS FÜR 32-BIT WINDOWS-CLIENTS

- Windows 98/98 SE/Me Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/Terminal Server Edition SP6a
- 32 MB RAM
- 55 MB freier Festplattenspeicher
- Microsoft Internet Explorer ab Version 4.01
- Intel Pentium-Prozessor 150 MHz (Prozessor ab Pentium II empfohlen)

SYMANTEC ANTIVIRUS FÜR 64-BIT WINDOWS-CLIENTS

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

SYMANTEC SYSTEM CENTER

- Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/ Terminal Server Edition SP6a
- Microsoft Management Console 1.2. Wenn die MMC nicht bereits installiert ist, sind 3 MB freier Festplattenspeicher erforderlich (10 MB während der Installation).
- 32 MB RAM
- 36 MB freier Festplattenspeicher
- Microsoft Internet Explorer ab Version 5.5 SP2

SYMANTEC SYSTEM CENTER SNAP-INS

Alert Management System-Konsole

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

Symantec AntiVirus-Snap-In

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

Symantec Client Firewall-Snap-In

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

AV Server Rollout Tool

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

NT Client Installation Tool

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

QUARANTÄNE-KONSOLE

- Windows XP Professional/2000 Professional/Server/Advanced Server/NT 4.0 Workstation
- Microsoft Management Console 1.2. Wenn die MMC nicht bereits installiert ist, sind 3 MB freier Festplattenspeicher erforderlich (10 MB während der Installation).
- 32 MB RAM
- 35 MB freier Festplattenspeicher
- Microsoft Internet Explorer ab Version 5.5 SP2

QUARANTÄNE-SERVER

- Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/ Terminal Server Edition SP6a
- 64 MB RAM
- 40 MB freier Festplattenspeicher
- Mindestens 250 MB für Auslagerungsdatei
- 500 MB bis 4 GB Festplattenspeicher für isolierte Elemente (empfohlen)
- Microsoft Internet Explorer ab Version 5.5 SP2

WORLD HEADQUARTERS:
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
Tel.: +1 (408) 253 9600
Fax: +1 (800) 441 7234

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

DEUTSCHLAND:
Symantec (Deutschland) GmbH
Lise-Meitner-Str. 9
D - 85737 Ismaning
Tel.: +49 (0) 69-6641 0315
E-Mail: enterprise.deutsch@symantec.com

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: infoline@symantec.com

Symantec hat Niederlassungen in über 35 Ländern. Adressen und Telefonnummern der Symantec-Niederlassungen in anderen Ländern finden Sie auf unseren Webseiten: www.symantec.com oder www.symantec.de

Informationen über Kundenservice und technischen Support finden Sie auf unserer Webseite: www.symantec.com/desupport/