

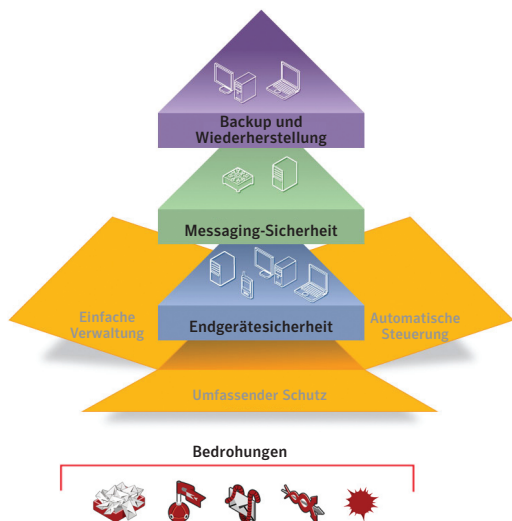
# Symantec™ Protection Suite Enterprise Edition

Zuverlässiger Schutz für Endgeräte- und Messaging-Umgebungen

## Übersicht

Die Symantec Protection Suite Enterprise Edition schafft eine sichere Umgebung für Endgeräte und Messaging, die weitestgehend vor komplexen Schadprogrammen, Datenverlusten und Spam-Bedrohungen schützt und sich nach einem Ausfall schnell wiederherstellen lässt. Senken Sie die Kosten für die Sicherheit Ihrer IT-Umgebung und verwalten Sie die Risiken moderner IT-Infrastrukturen effektiver mithilfe der bewährten Symantec-Technologien für Endgerätesicherheit, Messaging-Schutz und Systemwiederherstellung.

Die Symantec Protection Suite Enterprise Edition ist eine einzigartige Kombination aus leistungsstarken Technologien vom Marktführer in Sachen Schutz und Datensicherung, die es Unternehmen ermöglicht, ihre wichtigsten Ressourcen komplett zu sichern, einfach zu verwalten und automatisch zu kontrollieren.



## Endgerätesicherheit

### Mehr als Virenschutz

Die Symantec Protection Suite hat mehr zu bieten als erstklassigen, marktführenden Virenschutz und Schutz vor Spyware auf Signaturbasis. Sie bietet fortschrittliche Bedrohungsabwehr, die Ihre Endgeräte wie Laptops, Desktop-Computer, Server und mobile Geräte auch vor gezielten und neuartigen Angriffen effektiver schützt. Die Lösung umfasst gebrauchsfertige proaktive Technologien für die automatische Analyse des Anwendungsverhaltens und der Netzwerkkommunikation, um verdächtige Aktivitäten aufzuspüren und zu blockieren. Mithilfe von Kontrollfunktionen können Administratoren die Ausführung bestimmter Geräte- und Anwendungsaktivitäten verhindern, die als hohes Risiko gelten. Zudem umfasst die neue Suite eine integrierte softwarebasierte Netzwerkzugangskontrolle, die sicherstellt, dass Endgeräte den IT-Richtlinien entsprechen, unabhängig davon, wie oder von wo aus sie sich mit dem Netzwerk verbinden. Diese mehrschichtige Lösung sorgt für eine erhebliche Risikominderung und erhöht so das Vertrauen in den Schutz der Unternehmensressourcen. Der Endgeräteschutz der Protection Suite umfasst nun all diese Funktionen mit der Möglichkeit, einzelne Komponenten bei Bedarf zu aktivieren.

## Messaging-Sicherheit

### Spam-Abwehr und Messaging-Schutzfunktionen

Die Symantec Protection Suite bietet effektiven und weitestgehenden Schutz vor Spam-E-Mails und Viren für eingehende und abgehende E-Mails und Instant Messaging (IM). Die Messaging-Sicherheitskomponenten der Protection Suite können sowohl auf Messaging-Serverebene auf Microsoft® Exchange und Lotus

Domino® als auch auf Gateway-Ebene mit physischer oder virtueller Appliance-basierter Sicherheit eingesetzt werden. Die erweiterten Technologien zum Filtern von Inhalten und Verhindern von Datenverlusten unterstützen Unternehmen dabei, vertrauliche Daten zu kontrollieren, die Risiken durch Datenverluste zu verringern und behördliche Vorgaben sowie Anforderungen der Unternehmensführung zu erfüllen. Die Messaging-Sicherheit der Protection Suite ist einfach zu verwalten und weist eine Spam-Erkennung von über 97 Prozent und eine Rate von unter einer Fehlerkennung pro einer Million Nachrichten auf. Regelmäßige automatische Aktualisierungen, globale und selbstlernende lokale IP-Absenderanalysen und eine umfassende Berichterstellung gewährleisten, dass die Protection Suite effizient und erkennbar auf neue Spam-Bedrohungen reagiert, um die Netzwerkausfallzeit zu minimieren und die Produktivität der Mitarbeiter zu gewährleisten.

---

## Backup und Wiederherstellung

### *Vollständige System- und Datenwiederherstellung*

Die Symantec Protection Suite baut die Systemsicherung weiter aus und bezieht nun die plattenbasierte Systemwiederherstellung für Microsoft® Windows-basierte Desktops und Laptops mit ein. Dadurch sind Unternehmen in der Lage, ihre Systeme in nur wenigen Minuten anstatt von mehreren Stunden oder Tagen nach einem Ausfall oder einer Katastrophe wiederherzustellen – selbst auf nicht identischen Hardwareplattformen, in virtuellen Umgebungen oder an entfernten, unbeaufsichtigten Standorten.

---

## Vorteile

### **Lückenloser Schutz**

### ***Schutz auf mehreren Ebenen vom Endgerät bis zum Gateway***

**Einsatz bewährter Technologien** – Vertrauen Sie dem Schutz des marktführenden Anbieters von: Endgeräte- und Messaging-Sicherheit, Lösungen

zum Schutz vor Datenverlusten und Lösungen zur Systemwiederherstellung.

**Schutz vor weiteren Bedrohungen** – Schützen Sie Ihre Umgebung vor Datenverlusten, Schadprogrammen und Spam-E-Mails durch eine zuverlässige Identifizierung und Vermeidung von Risiken auf verschiedenen Plattformen.

**Durchgängiger Schutz** – Proaktiver Schutz für Endgeräte, Messaging-Server und Gateways, der über herkömmlichen Virenschutz sowie Abwehr von Spionageprogrammen hinausgeht.

**Schutz geistigen Eigentums** – Sichern Sie sensible Daten und wertvolle vertrauliche Informationen am Gateway mit dem fortschrittlichen Content Filtering und dem Schutz vor Datenverlusten.

**Vertrauen auf zuverlässige Untersuchungen** – Proaktiver Schutz mit Sicherheitsinformationen in Echtzeit, die eine Frühwarnung und Schutz vor neu entdeckten Risiken bieten.

**Schnelle und unkomplizierte Wiederherstellung** – Einzelne Dateien und Ordner innerhalb von Sekunden oder ganze Windows-Systeme innerhalb von Minuten zuverlässig wiederherstellen, selbst auf nicht identischer Hardware oder in virtuellen Umgebungen.

## Einfache Verwaltung

### ***Einheitliche Verwaltung und Administration***

**Implementierung & Betrieb vereinfachen** – Einfache Implementierung mit einer minimalen Unterbrechung für die Umgebung dank einfacher Verwaltung und optimierter Systemressourcen.

**Einfache Verwaltung** – Die rationalisierte Verwaltung mit optimierten Workflows für wichtige Sicherheitsaufgaben nimmt Administratoren und Endbenutzern unproduktive Aufgaben ab.

**Flexible und skalierbare Konfiguration** – Einhaltung von IT-Richtlinien mit granularer Kontrolle über Richtlinien und Funktionen, die einfach zu konfigurieren und wahlweise einsetzbar sind.

**Komplexität der Umgebung vermeiden** – Einsatz integrierter und wichtiger Endgerät- und Messaging-Sicherheitstechnologien als kombinierte Lösung mit koordinierter Verwaltung.

**Optimierte Prozesse** – Zusätzliche Arbeitsschritte und Kosten vermeiden; nur eine Entscheidung, nur ein Kauf und nur ein Anbieter für komplette Sicherheit.

**Betriebskosten senken** – Zeitaufwand, Kosten und Fachwissen für die Verwaltung mehrerer Technologien reduzieren.

#### **Automatische Steuerung**

***Backup und Wiederherstellung, Überwachung, Aktualisierung, und Durchsetzung erfolgen automatisiert***

**Richtlinieneinhaltung sicherstellen** – Einhaltung von IT-Richtlinien und gesetzlichen Vorgaben auf problemlose Weise durchsetzen und nachweisen.

**Vertrauliche Informationen steuern** – Fluss vertraulicher Informationen per E-Mail und IM sowie an Endgeräten festlegen und steuern.

**Mühevolle Updates** – Dank dem Symantec Global Intelligence Network, einer der größten Infrastrukturen der Welt zur Erforschung von Sicherheitsbedrohungen, schneller an Risiken anpassen und innerhalb von Minuten Maßnahmen ergreifen.

**Verbesserte Übersicht über Ihre Umgebung** – Mehr Übersicht über Aktionen, Ereignisse und den Status von Endgeräten und der Messaging-Infrastruktur durch aufschlussreiche Berichte.

**Ausfallzeit minimieren** – Sorgt durch die Wiederherstellung von ereignisgesteuerten und geplanten Wiederherstellungspunkten aus dafür, dass Ihre Systeme schnell wieder einsatzbereit sind.

---

#### **Produkteigenschaften**

**Virenschutz und Antispyware** – Für einen leistungsstarken Schutz vor Schadprogrammen, mit marktführendem Virenschutz, fortschrittlichem Schutz vor Spionageprogrammen, neuem Rootkit-Schutz, geringerem Speicherbedarf und neuen dynamischen Leistungsanpassungen, für eine durchgängige Produktivität der Benutzer.

**Schutz vor Netzwerkbedrohungen** – Eine regelbasierte Firewall-Engine und die Abwehr allgemeiner Bedrohungen (Generic Exploit Blocking – GEB) stoppen eine Vielzahl von Schadprogrammen, bevor sie in das System gelangen.

**Proaktiver Bedrohungsschutz** – Schützt mithilfe von TruScan Proactive Threat Scan, das nicht auf Bedrohungssignaturen angewiesen ist, besser vor neuen Formen von Bedrohungen (d. h. Zero-Day-Bedrohungen).

**Nur ein Agent und eine Verwaltungskonsole** – Ein einziger Agent enthält folgende Technologien: Virenschutz, Schutz vor Spionageprogrammen, Desktop-Firewall, Intrusion Prevention System (IPS), Geräte- und Anwendungskontrolle sowie Netzwerkzugriffskontrolle. Sämtliche Technologien werden über eine einzige Konsole verwaltet.

**Virenschutz für Linux, Mac und Windows Mobile** – Viren aus E-Mail-Anhängen, Internet-Downloads und anderen Quellen entfernen, um das Unternehmensnetzwerk zu schützen. Ermöglicht Sicherheit während des mobilen Computereinsatzes durch umfassenden Virenschutz vor böswilligen Angriffen, die auf Windows Mobile-Betriebssysteme abzielen.

**Spam-Abwehr und Messaging-Schutzfunktionen** – Die auf Symantec Brightmail™ basierende Spam-Abwehr-Technologie arbeitet mit einer Effektivität von über 97 Prozent und einer Rate von unter einer Fehlerkennung pro einer Million Nachrichten. Sie ist damit eine der branchenweit genauesten Lösungen.<sup>1</sup>

- Prüft eingehende und abgehende E-Mails auf Einhaltung von Richtlinien und gesetzlichen Bestimmungen.
- Beinhaltet Incident Management- und Reporting-Funktionen. Dies versetzt Unternehmensnutzer in die Lage, Richtlinien festzulegen und Verstöße dagegen zu analysieren und damit umzugehen.
- Fortlaufend automatische Spam-Signatur-Aktualisierungen und Reputation Scoring zur Unterstützung eines effektiven Echtzeitschutzes vor neuen Bedrohungen.
- Leistungsstarker Schutz, der durch über 40 VB100-Preise in Folge seit 1999 bestätigt wurde – ein Rekordergebnis in der Branche.
- Echtzeitanalyse und -berichterstattung, durch die sich die E-Mail- und IM-Nutzung besser verfolgen und Wachstumsmuster erkennen lassen.

**Systemwiederherstellung** – Ermöglicht die schnelle, zuverlässige Wiederherstellung von Computerdaten und -systemen.

- Erstellen von Backups des gesamten Systems im Betrieb ohne Beeinträchtigung der Benutzerproduktivität.
- Startseitenansicht zeigt unmittelbar den Backup-Status von Computersystemen.
- Backups werden automatisch gestartet, wenn Symantec ThreatCon eine individuell festgelegte Gefahrenstufe erreicht oder überschreitet.

1. Symantec Brightmail Gateway erhielt von InfoWorld die Auszeichnung „Technology of the Year“ für Best Mail Security, InfoWorld – 7. Januar, 2008, [http://www.infoworld.com/slideshow/2008/01/149-2008\\_technology-5.html](http://www.infoworld.com/slideshow/2008/01/149-2008_technology-5.html)

### Die Wahl des richtigen Endgeräteschutzprodukts

Schutztechnologie	10 bis 99 Plätze		über 100 Plätze	
	Symantec Endpoint Protection Small Business Edition	Symantec Protection Suite Small Business Edition	Symantec Endpoint Protection	Symantec Protection Suite Enterprise Edition
<b>Endgeräteschutz</b>				
Virenschutz/Abwehr von Spionageprogrammen	•	•	•	•
Desktop-Firewall	•	•	•	•
Intrusion Prevention	•	•	•	•
Blockierung allgemeiner Bedrohungen	•	•	•	•
Geräte- und Anwendungskontrolle			•	•
Virenschutz für Macintosh®		•		•
Virenschutz für Linux®			•	•
Virenschutz für Windows® Mobile				•
Netzwerkzugangskontrolle – Selbstüberwachung				•
<b>Messaging-Sicherheit</b>				
Virenschutz/Spam-Abwehr/Antiphishing		•		•
Spam-Filter mittels Reputationsanalyse				•
Inhaltsfilter/Einhaltung von Regelungen		•		•
Verhindern von Datenverlusten				•
Microsoft® Exchange		•		•
Gateway-Software im Abonnement und Lotus Domino®				•
<b>Backup und Wiederherstellung</b>				
Backup von Desktops und Laptops im laufenden Betrieb		•		•
Wiederherstellung auf beliebiger Hardware		•		•
Backups bei Gefährdungen		•		•

**Hinweis:** Symantec Protection Suite Enterprise Edition Messaging Security-Funktionen stehen für Exchange, Domino auf Windows-Betriebssystemen, Gateway und Instant Messaging zur Verfügung. Symantec Protection Suite Small Business Edition Messaging Security ist nur für Exchange verfügbar.

## Systemanforderungen

Hardware/Software	Betriebssysteme/Browser	Speicher (Minimum)	Festplatte (Minimum)
<b>Endpoint Protection Client-Arbeitsstationen und Server</b>			
Prozessor: Intel® Pentium® oder kompatibel, 32-Bit und 64-Bit Hinweis: Itanium® wird nicht unterstützt	Windows® 32-Bit und 64-Bit: - 2000 Professional, Server, Advanced Server, Datacenter Server, Small Business Server (ab Service Pack 3) - XP Home Ed., Professional Ed., Tablet PC Ed., Embedded Ed., Media Center Ed. (ab Service Pack 1) - Server 2003 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Vista® Home Basic, Home Premium, Business, Enterprise, Ultimate - Server 2008 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed.  Linux® 32-Bit und 64-Bit: - Red Hat® Enterprise Linux 3.x, 4.x, 5.x - SUSE Linux Enterprise (Server/Desktop) 9.x, 10.x - Novell® Open Enterprise Server (OES/OES2) - VMware ESX 2.5, 3.x - Ubuntu 7.x, 3.x - Debian 4.x	256 MB RAM	600 MB
<b>Endpoint Protection Management Server</b>			
Prozessor: Intel Pentium oder kompatibel, 32-Bit und 64-Bit Hinweis: Itanium wird nicht unterstützt	Windows 32-Bit und 64-Bit: - 2000 Server, Advanced Server, Datacenter Server, Small Business Server (Service Pack 3 oder höher) - XP Professional Ed. (Service Pack 1 oder höher) - Server 2003 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Server 2008 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed. - Essential Business Server Standard Ed., Premium Ed.	1 GB	2 GB
<b>Endpoint Protection-Verwaltungskonsole</b>			
Prozessor: Intel Pentium oder kompatibel, 32-Bit und 64-Bit Hinweis: Itanium wird nicht unterstützt	Windows 32-Bit und 64-Bit: - 2000 Professional, Server, Advanced Server, Datacenter Server, Small Business Server (ab Service Pack 3) - XP Professional Ed. (ab Service Pack 1) - Server 2003 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed., Small Business Server, Computer Cluster Server, Storage Server - Vista Home Basic, Home Premium, Business, Enterprise, Ultimate - Server 2008 Standard Ed., Enterprise Ed., Datacenter Ed., Web Ed. - Small Business Server Standard Ed., Premium Ed. - Essential Business Server Standard Ed., Premium Ed.	512 MB	15 MB
<b>Endpoint Protection-Datenbank</b>			
	Eingebettete Datenbank bereitgestellt. Auch unterstützt: - Microsoft SQL Server 2000 (ab Service Pack 3) - Microsoft SQL Server 2005		4 GB
<b>AntiVirus für Linux-Clients</b>			
(nicht vom Endpoint Protection Manager verwaltet)	Linux 32-Bit und 64-Bit: - Red Hat® Enterprise Linux 3.x, 4.x, 5.x - SUSE Linux Enterprise (Server/Desktop) 9.x, 10.x - Novell® Open Enterprise Server (OES/OES2)  Nur Linux 32-Bit: - VMware ESX 2.5, 3.x		
<b>AntiVirus für Macintosh-Administrationsserver</b>			
- Xserve G5, Xserve, Power Mac G5, Power Mac G4, Macintosh Server G4, Power Macintosh G3 (Blue & White), Macintosh Server G3 (Blue & White), iMac, eMac, Mac-Mini-Computer - FireWire integriert	Mac OS X Server 10.4.11-10,5.x Hinweis: Mac OS X Server 10.4 und 10.5 beinhaltet Apache und MySQL	256 MB RAM 512 MB RAM für stark beanspruchte Server, auf denen zahlreiche Dienste ausgeführt werden	4 GB

Hardware/Software	Betriebssysteme/Browser	Speicher (Minimum)	Festplatte (Minimum)
<b>AntiVirus für Macintosh-Administrationskonsole</b>			
	<ul style="list-style-type: none"> <li>- Mac OS X + Safari 1.2x, Firefox 2</li> <li>- Windows XP Pro + Internet Explorer 6 SP2</li> <li>- Red Hat Linux + Netscape 7</li> </ul>		
<b>AntiVirus für Macintosh-Client</b>			
- G4 800 MHz	Mac OS X 10.4.11-10,5.x	192 MB RAM	40 MB
<b>Mobile AntiVirus für Windows Mobile</b>			
	<p>Mobiles Endgerät:</p> <ul style="list-style-type: none"> <li>- Microsoft Windows Mobile 6 Standard, Professional</li> <li>- Microsoft Windows Mobile 5.0 SmartPhone und Pocket PC</li> </ul> <p>Administrations-Tools:</p> <ul style="list-style-type: none"> <li>- Microsoft Windows 2000, XP und 2003 Server</li> </ul>		2.5 MB
<b>Mail Security für Exchange</b>			
<p>Prozessor:</p> <ul style="list-style-type: none"> <li>- 32-Bit-Intel-Prozessor der Serverklasse (für Server 2003 x64 oder Server 2008 x64)</li> <li>- 64-Bit-Intel-Prozessor, der Extended Memory 64-Technologie oder AMD 64-Bit unterstützt (für Exchange Server 2007)</li> </ul> <p>Softwarekomponenten:</p> <ul style="list-style-type: none"> <li>- .NET Framework v.2</li> <li>- Microsoft Data Access Components (MDAC) ab Version 2.8</li> <li>- Microsoft DirectX® 9.0</li> </ul>	<p>Microsoft Windows:</p> <ul style="list-style-type: none"> <li>- 2000 Server, Advanced Server, Data Center (ab Service Pack 4)</li> <li>- Server 2003 Standard Ed., Enterprise Ed., Data Center Ed. (ab Service Pack 1)</li> <li>- Server 2003 x64 oder R2 x64 Standard Ed., Enterprise Ed.</li> <li>- Server 2008 x64 Standard Ed., Enterprise Ed.</li> <li>- Small Business Server Standard Ed., Premium Ed.</li> </ul> <p>Wenn nur die Konsole installiert wird: Windows 2000 (ab Service Pack 4), Windows 2003 (ab Service Pack 1), Windows XP (ab Service Pack 1)</p>	<ul style="list-style-type: none"> <li>- 512 MB RAM</li> <li>- 1 GB RAM für Windows Server 2003 x64 oder Windows Server 2008 x64</li> <li>- 2 GB RAM für Exchange Server 2007</li> </ul>	325 MB
<b>Mail Security für Domino</b>			
	<p>Microsoft Windows:</p> <ul style="list-style-type: none"> <li>- 2000 Server, Advanced Server</li> <li>- Server 2003 Standard Ed., Enterprise Ed.</li> </ul> <p>Lotus:</p> <ul style="list-style-type: none"> <li>- Domino® Server 6.5.x, 7.x</li> <li>- Notes® Client 6.5.x, 7.x</li> </ul>	128 MB RAM (256 MB RAM empfohlen)	300 MB
<b>Brightmail Gateway</b>			
<p>Physische Appliances:</p> <ul style="list-style-type: none"> <li>- Brightmail 8300 Serie</li> <li>- Mail Security 8300 Serie</li> <li>- Mail Security 8200 Serie</li> </ul> <p>Virtuelle Appliances:</p> <ul style="list-style-type: none"> <li>- min. 2 CPUs, 4 CPUs empfohlen</li> </ul>	<p>Administrator-Konsole:</p> <p>Microsoft Internet Explorer 6.0, 7.0</p> <p>Firefox 2.0</p> <p>Virtuelle Appliances:</p> <p>VMware ESX und ESXi 3.x</p>	<p>Virtuelle Appliances:</p> <p>2 GB (4 GB empfohlen)</p>	<p>Virtuelle Appliances:</p> <p>min. 30 GB</p>
<b>Backup Exec System Recovery Desktop Edition</b>			
<p>Prozessor:</p> <ul style="list-style-type: none"> <li>- Mindestens 233 MHz oder nach Anforderung des Betriebssystems</li> </ul> <p>Softwarekomponenten:</p> <ul style="list-style-type: none"> <li>- .Net Framework v.2</li> </ul>	<p>Windows(R) 32-Bit- oder 64-Bit-Betriebssysteme:</p> <ul style="list-style-type: none"> <li>- Windows Vista(R) Ultimate, Business, Enterprise</li> <li>- Windows XP Media Center Ed., Professional Ed., Home Ed. (ab SP2)</li> </ul> <p>Virtuelle Plattformen (für konvertierte Wiederherstellungspunkte):</p> <ul style="list-style-type: none"> <li>- VMware ESX Server 2,0, 3.0 und 3.5</li> <li>- VMware Server 1.0</li> <li>- VMware GSX Server 3.x (ersetzt durch VMware Server)</li> <li>- VMware Workstation 4, 5 und 6</li> <li>- Microsoft Hyper-V</li> <li>- Microsoft Virtual Server 2005 R2 und höher</li> <li>- Citrix XenServer 4.x</li> </ul>	<ul style="list-style-type: none"> <li>- Agent: 512 MB</li> <li>- Benutzeroberfläche und Recovery Point Browser: 512 MB</li> <li>- Recovery Disk: min. 512 MB (dediziert), min. 768 MB bei mehrsprachiger Version</li> <li>- LightsOut Restore-Funktion: 1 GB</li> </ul>	<p>250-390 MB</p> <p>Außerdem:</p> <p>Ausreichend freier Festplattenspeicher auf einer lokalen Festplatte oder einem Netzwerkserver für die Speicherung von Wiederherstellungspunkten</p>

### Services

Symantec bietet verschiedene Beratungsleistungen, technische Schulungen und Support-Services an, die Unternehmen durch die Migration, Installation und die Verwaltung von Symantec Protection Suite führen und dabei unterstützen, das gesamte Potenzial Ihrer Investition zu nutzen. Die Essential Support Services geben Unternehmen die Gewissheit, dass ihre kritischen Ressourcen rund um die Uhr geschützt sind. Unternehmen, die die Sicherheitsüberwachung und -Verwaltung auslagern wollen, bietet Symantec darüber hinaus Managed Security Services für Echtzeitschutz an.

### *Besuchen Sie unsere Website*

<http://www.symantec.de>

### *Um mit einem Produktspezialisten in Deutschland zu sprechen*

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

### *Um mit einem Produktspezialisten zu sprechen*

Detaillierte Kontaktinformationen für verschiedene Länder finden Sie auf unserer Website.

### *Über Symantec*

Symantec ist einer der weltweit führenden Anbieter auf dem Gebiet der Informationssicherheit, Datenspeicherung und der Systemverwaltung und bietet Unternehmen und Privatkunden effektive Lösungen zur Absicherung und Verwaltung ihrer Daten. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien, und verfügt über Niederlassungen in mehr als 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

### *Symantec (Deutschland) GmbH*

Humboldtstr. 6  
85609 Aschheim  
Germany  
Tel: +49 (0)89 943 02-0  
Fax: +49 (0)89 943 02-950  
[www.symantec.de](http://www.symantec.de)

### *Symantec (Austria) GmbH*

Wipplinger Strasse 34  
1010 Wien  
Österreich  
Tel: +43 1 532 85 33  
Fax: +43 1 532 85 33 33 33  
[www.symantec.at](http://www.symantec.at)

### *Symantec AG*

Andreasstr. 15  
8050 Zürich  
Schweiz  
Tel: +41 (0)44 305 72 00  
Fax: +41 (0)44 305 72 01  
[www.symantec.ch](http://www.symantec.ch)

Confidence in a connected world.

