

Symantec™ Enterprise Security Manager

Einhaltung von Sicherheitsrichtlinien und gesetzlichen Bestimmungen

Übersicht

Symantec Enterprise Security Manager™ versetzt Unternehmen in die Lage, die Konformität ihrer Informationssysteme mit Sicherheitsrichtlinien, Standards und gesetzlichen Bestimmungen zu definieren und zu bewerten sowie Sicherheitslücken aufzudecken. Sämtliche Aufgaben werden über eine einzige Konsole ausgeführt. Durch die Integration mit der Symantec™ Security Management Solution können Unternehmen die Daten zur Richtlinieneinhaltung mit Sicherheitsereignisdaten aus einer Vielzahl anderer Sicherheitsquellen abgleichen. Zu diesen Quellen gehören beispielsweise Firewalls, Intrusion Detection-Systeme, Virenschutzprodukte und Lösungen zur Schwachstellenanalyse. So können Unternehmen den Wert ihrer bestehenden Sicherheitslösungen optimieren und eine allgemeine Verbesserung des Sicherheitszustands erzielen. Die proaktive Sicherheitsstrategie von Symantec Enterprise Security Manager ermöglicht ein schnelles Eindämmen und Beseitigen von Sicherheitsbedrohungen. Unternehmen können so Ressourcen und Kosten sparen.

Vorteile

- **NEU!** Nachrichten-/Richtlinienprüfungen liefern ausführliche Beschreibungen und Handlungsanweisungen für eine schnellere Reparatur anfälliger Systeme.
- **NEU!** Die verbesserte LiveUpdate-Integration erleichtert und beschleunigt den Abruf und die Installation von Sicherheitsaktualisierungen.
- **NEU!** Das optionale Network Assessment-Modul erkennt und informiert über Schwachstellen, ohne dazu einen Agenten auf den Zielnetzwerkgeräten, beispielsweise Routern, Switches oder andere Geräten, zu installieren.

- **NEU!** Die Internationalisierung wichtiger Manager, Agenten und Programme ermöglicht den Einsatz mit nicht-englischsprachigen Betriebssystemen.
-

Weitere Funktionen

- Enthält neue Vorlagen zur Richtlinienbewertung zu wichtigen Verordnungen wie Sarbanes-Oxley oder PCI-DSS sowie zu GLBA, HIPAA, NERC, FISMA, VISA CISP und ISO 17799. Darüber hinaus bietet die Lösung auch Unterstützung für das Revised International Capital Framework (BASEL II).
- Über 3.000 Sicherheitsprüfungen, um sicherzustellen, dass wichtige IT-Systeme die Sicherheitsrichtlinien eines Unternehmens einhalten:
 - Kontoinformation
 - Standardkonten und -kennwörter
 - Rechte und Berechtigungen für Benutzer und Gruppen
 - Kennwortintegrität
 - Sicherheitskonfigurationseinstellungen der einzelnen Systeme
 - Patch-Nummern der Betriebssysteme
 - Registrierungseinstellungen
 - Virenschutzaktualisierungen
 - Dateiattribute
- Flexible und leistungsstarke Berichte zur Richtlinieneinhaltung im gesamten Unternehmen, darunter 75 vordefinierte Berichte sowie mit dem erweiterten Berichterstellungs-Tool generierte Ad-hoc-Berichte
- Berichte für das Unternehmensmanagement enthalten eine Bewertung der Richtlinieneinhaltung im Unternehmen insgesamt, Problembehebung und unternehmensweite Trends

- Granulare Berichte für technische Manager informieren detailliert über die Richtlinieneinhaltung auf folgenden Ebenen: System, Betriebssystem oder Geschäftsbereich
- Integration mit anderen Symantec™ Security Management Solution-Produkten für einen ganzheitlichen Überblick über Sicherheitsrisiken und -prioritäten

Systemanforderungen

Symantec Enterprise Security Manager 6.5

Konsole

- Windows Server 2003
- Windows 2000 Professional/Server/Advanced Server mit Service Pack ab Version 1.0
- Windows XP Professional
- Microsoft Windows NT 4.0 Server oder Workstation mit Service Pack ab Version 6a

Manager

Microsoft Windows

- Windows Server 2003
- Windows 2000 Professional/Server/Advanced Server mit Service Pack ab Version 1.0

UNIX

- Sun Solaris 2.8, 2.9
- HP-UX 11 (PA-RISC), 11i (11.11) (PA-RISC)
- IBM AIX 5L 5.1, 5.2

ESM Server-Agent

Microsoft Windows

- Windows Server 2003 (x86)
- Windows Server 2003 64-Bit (Itanium)
- Windows 2000 Professional/Server/Advanced Server mit Service Pack ab Version 1.0

- Windows NT 4.0 Server oder Workstation mit Service Pack ab Version 6a
- Windows XP Professional

UNIX

- Sun Solaris 2.51, 2.6, 2.7, 2.8, 2.9, 2.10
- HP-UX 10.20, 11 (PA-RISC), 11i v1 (11.11) (PA-RISC)
- HP-UX 11i v2 (11.23) (Itanium)
- IBM AIX 4.2.1, 4.3.3, 5L 5.1, 5L 5.2, 5L 5.3
- HP Tru64 OSF-1.4.0 D-5.1A
- SGI Irix 6.2, 6.3, 6.4
- Sequent DYNIX/ptx 4.4.2

Linux

- Red Hat Linux 6.2, 7.0, 7.1, 7.2, 7.3, 8, 9
- Red Hat Linux ES 2.1 (x86), ES 3.0 (x86), AS 3.0 64-Bit (Itanium, Opteron und Xeon), WS 3.0 64-Bit (Opteron und Xeon)
- SUSE Linux SS und ES 8.0 (x86), ES 9.0 (x86)

Novell NetWare

- NetWare 4.2, 5.0, 5.1, 6.0, 6.5

Digital VMS Midrange

- OpenVMS 7.2, 7.3 (Alpha-Prozessor)

IBM OS/400 Midrange

- IBM iSeries (OS/400) V5R1, V5R2

ESM Application Audit-Module

Web-Server

- IIS Web Server 4.0 (Windows)
- iPlanet 4.x (Solaris)
- Apache Web Server 1.3, 2.0 (Linux)

Datenbanken

- Oracle 8.0.x, 8i, 9i, 9.2 (Solaris, HP-UX, AIX)

- Microsoft SQL Server 2000 (Microsoft Windows 2000)
- IBM DB2 UDB 7.2 unter Windows (Informationen zu unterstützten Windows-Versionen finden Sie im Abschnitt zu den Servern, auf denen Microsoft Windows ausgeführt wird ["Servers Running Microsoft Windows"].)

Firewalls

- Check Point Provider-1 (Solaris 8)

E-Mail-Server

- MS Exchange Server 2000 (Windows)

ESM-Richtlinien für Standards und gesetzliche Bestimmungen

Betriebssystemrichtlinien

Standards

- ISO 17799:2000
- ISO 17799:2005 Überarbeitet
- SANS Top 20 für Windows, UNIX und Linux
- CIS Benchmark für Solaris
- CIS Benchmark für Windows 2000 Server und Arbeitsstation

Gesetzliche Bestimmungen

- SOA - Sarbanes-Oxley Act Section 404 (COSO, CobiT)
- VISA CISP
- HIPAA - Health Insurance Portability And Accountability Act von 1996
- GLBA - Gramm-Leach-Bliley Act von 1999
- NERC Standard 1200
- FISMA (NIST 800-53 Entwurf)
- Basel II Capital Accord (ISO 17799:2000)
- PCI DSS - Payment Card Industry

Datenbankrichtlinien

Standards

- ISO 17799:2000

Gesetzliche Bestimmungen

- SOA - Sarbanes-Oxley Act Section 404 (COSO, CobiT)
- Basel II Capital Accord (ISO 17799:2000)
- PCI DSS - Payment Card Industry

Symantec-Berichterstellung auf Unternehmensebene Anforderungen für den Bericht-Server

Empfohlene Hardware

- Geringe Anzahl Berichtsbenutzer (bis zu 500 Berichtsbenutzer, mehrere 100 Symantec ESM-Agenten)
 - 1 Server
(Dualer Prozessor mit 2 GHz)
(4 GB RAM / Prozessor)
- Große Anzahl Berichtsbenutzer (10.000 Berichtsbenutzer, bis zu 10.000 Agenten)
 - 3 Server
 - Ein ReportNet Web-Server
(Dualer Prozessor mit 2 GHz)
(2 GB RAM / Prozessor)
 - Zwei ReportNet-Anwendungs-Server
(Quad-Prozessor mit 2 GHz)
(2 GB RAM / Prozessor)

Weitere Informationen

Besuchen Sie unsere Webseite

<http://enterprisesecurity.symantec.de/>

Um mit einem Produktspezialisten zu sprechen

Symantec verfügt über Niederlassungen in 40 Ländern. Die Adressen und Telefonnummern der Niederlassungen in den einzelnen Ländern finden Sie auf unserer Webseite.

Über Symantec

Symantec ist einer der weltweit marktführenden Anbieter auf dem Gebiet der IT-Sicherheit. Mit seiner breiten Palette an Software, Appliances und Services hilft es Privatanwendern, kleineren und mittleren Unternehmen sowie Großunternehmen, ihre IT-Infrastruktur zu sichern und zu verwalten. Die Produktmarke Norton ist im Einzelhandel weltweit führend und hat zahlreiche Auszeichnungen der Branche erhalten. Das Unternehmen hat seinen Hauptsitz in Cupertino, Kalifornien, und vertreibt seine Produkte in 40 Ländern. Weitere Informationen finden Sie unter www.symantec.de.

