

SOPHOS
und **utimaco**



FOR MICROSOFT EXCHANGE

Reviewer's Guide

 email **security and control**



PureMessage für Windows/Exchange
Produkttour

WILLKOMMEN

Herzlich Willkommen beim Reviewer's Guide für Sophos PureMessage™ für Microsoft® Exchange, einer Produktkomponente von Sophos E-Mail Security and Data Protection. Dieser Guide wird Sie mit den Hauptfunktionen von Sophos PureMessage für Microsoft Exchange vertraut machen, Ihnen einen Einblick in die zentrale Management-Konsole der Lösung verschaffen und Aufschluss über die verfügbaren Funktionen zum Enforcement unternehmensweiter E-Mail-Richtlinien geben.

Wie all unsere Lösungen ist Sophos PureMessage für Microsoft Exchange das Ergebnis von mehr als 20 Jahren Erfahrung beim Schutz von Unternehmen, Bildungseinrichtungen und Behörden. Sophos PureMessage für Microsoft Exchange schützt den E-Mail-Gateway und Exchange-Informationsspeicher vor E-Mail-Bedrohungen wie Spam, Phishing, Viren und Spyware. Mit PureMessage für Microsoft Exchange kontrollieren Sie den Informationsfluss aus Ihrem und in Ihr Unternehmen, beugen dem Verlust vertraulicher Daten vor und verhindern die missbräuchliche Nutzung Ihres E-Mail-Systems.

Dank seiner präventiven Erkennungs- und Schutzmechanismen zur Sicherung vor zunehmend komplexen und sich schnell ausbreitenden Bedrohungen genießt Sophos innerhalb der IT-Branche ein ausgezeichnetes Renommee und kann einen hohen Grad an Kundenzufriedenheit verzeichnen. In allen Sophos Lizenzen ist umfassender Support durch unser weltweites Netzwerk von Support-Technikern rund um die Uhr und an 365 Tagen im Jahr inbegriffen. Der breite Funktionsumfang von PureMessage für Microsoft Exchange wird durch das unvergleichliche Know-how der SophosLabs™ gekrönt: Unser globales Netzwerk aus Bedrohungsanalysecentern reagiert stets zuverlässig auf neue Bedrohungen.

Informationen zum Preis und zum Erwerb von PureMessage für Microsoft Exchange erhalten Sie bei Ihrem Sophos Account Manager vor Ort.

Auf unserer Homepage erfahren Sie, wer für Ihren Standort zuständig ist:

www.sophos.de/companyinfo/contacting

Eine Testversion können Sie über folgende Adresse anfordern:

www.sophos.de/puremessage-download

INHALT

1	EIN KURZER ÜBERBLICK	4
2	ZENTRALE VERWALTUNG ÜBER EINE EINZIGE KONSOLE	6
	Dashboard	6
	Activity Monitor (Aktivitätsanzeige)	7
	Integration von und Synchronisierung mit Active Directory	8
	Benutzer und Gruppen	8
3	UNTERNEHMENSWEITES RICHTLINIEN- ENFORCEMENT	9
	Vereinfachte Einrichtung & Durchsetzung von Richtlinien	9
	Leistungsstarker Anti-Malware-Scan	10
	Branchenführender Spamschutz	10
	Inhaltsfilterung	12
	Disclaimer	13
	Quarantäne-Management	14
4	UMFASSENDES REPORTING	15
	Reporting-Tool	15
	Diagramme	16
	ANHÄNGE	
I	Sophos Produkte für Unternehmen	17
II	Andere Produkte und Services von Sophos	18
III	Systemanforderungen für Sophos	19

Mit Sophos PureMessage für Microsoft Exchange haben Sie die Wahl, entweder die Sophos Standard-Anti-Virus- und Anti-Spam-Richtlinien zu verwenden, oder aber eigene Richtlinien zu erstellen. Für Inhalte und Attachments stehen des Weiteren zahlreiche Filteroptionen zur Verfügung.

Nach dem Lesen dieses Guides werden Sie ein tieferes Verständnis dafür entwickeln, wie PureMessage für Microsoft Exchange kosteneffizienten und verlässlichen Schutz vor bekannten und unbekanntem Computer-Bedrohungen bereitstellt und Ihnen eine umfassende Kontrolle sämtlicher E-Mails innerhalb Ihres Unternehmens ermöglicht.

Besondere Vorteile von PureMessage für Microsoft Exchange

Unübertroffene Erkennung von Malware	Erkennung von bis zu 98% aller Spam-E-Mails und Schutz vor E-Mail-Betrügereien, einschließlich Phishing-Attacken. Erkennung, Desinfektion, Löschung oder Isolierung von Viren, Trojanern, Würmern und schädlicher Spyware in eingehenden und ausgehenden E-Mails
Proaktiver Schutz	Einsatz des Genotype-Verfahrens zum Abfangen neuer Bedrohungen und gefährlicher Anwendungen
Hohe Genauigkeit	Ausgewogener Einsatz zahlreicher Spam-Erkennungsmethoden sorgt für genaue Ergebnisse und reduziert False Positives.
Schutz von geistigem Eigentum	Leistungsstarke Steuerung des Inhaltsscans zum Schutz vor Datenverlust
Compliance mit geltenden Richtlinien	Umfassende Richtlinien-Umgebung zur Unterstützung komplexer Sicherheitsbestimmungen bzw. gesetzlicher Vorschriften
Globaler Schutz	Schutz globaler Unternehmen vor Spam und Viren im mehrsprachigen E-Mail-Verkehr, darunter auch in solchen Sprachen, die Doppel-Byte-Zeichen verwenden
Automatische Updates	Automatische Updates mit dem neuesten Schutz aus den SophosLabs, dem globalen Netzwerk aus Bedrohungsanalysecentern
Delegierte Administration	Verwaltung u.a. von Richtlinien, Quarantäne und Reports für Gruppen, Abteilungen oder Kunden
Endbenutzer-Kontrollen	Endbenutzer-Quarantäne-Überblick, Allow Lists und Block Lists

Farbige Anzeigen auf dem Dashboard geben den Status eines jeden Servers an. Eine grüne Anzeige signalisiert, dass alle Prozesse ordnungsgemäß verlaufen, eine rote Anzeige dient als Warnung. Oft ist ein rotes Warnsignal darauf zurückzuführen, dass PureMessage einen Virenausbruch erkannt hat und Korrekturmaßnahmen vornimmt. In einigen Fällen kann die rote Anzeige darauf hindeuten, dass der Scan für den Exchange-Informationsspeicher oder AutoUpdate, meist als Folge einer Unterbrechung der Internet-Verbindung, nicht verfügbar sind.

Activity Monitor (Aktivitätsanzeige)

Über die Konsole besteht Zugriff auf den Activity Monitor (Aktivitätsanzeige), welcher die Anzahl der von PureMessage verarbeiteten E-Mails in Echtzeit anzeigt. Wie Abbildung 3 veranschaulicht, wird dieser Wert in drei Kategorien unterteilt, nach denen die Lösung automatisch sucht, z.B. E-Mails mit anstößigen Inhalten, verschlüsselte Attachments oder unangemessene Ausdrücke (Details hierzu in Kapitel 3). Um die Wirksamkeit Ihrer Einstellungen zu analysieren und ggf. Anpassungen vorzunehmen, kann der Counter jederzeit gestoppt werden. Zusätzlich zu der Bereitstellung einer genauen Übersicht über die Anzahl der in Ihrem Unternehmen eingehenden E-Mails kann der Activity Monitor das Helpdesk dabei unterstützen festzustellen, ob ein Netzwerk oder eine bestimmte Gruppe im Netzwerk Opfer einer Spam-Kampagne geworden sind.

Umfassende Kontrolle

Die Konsole von PureMessage für Microsoft Exchange bietet komfortable Funktionen zur richtlinienbasierten Verwaltung und verfügt über benutzerfreundliche Funktionen, die von einem zentralen Punkt ausgeführt werden können.

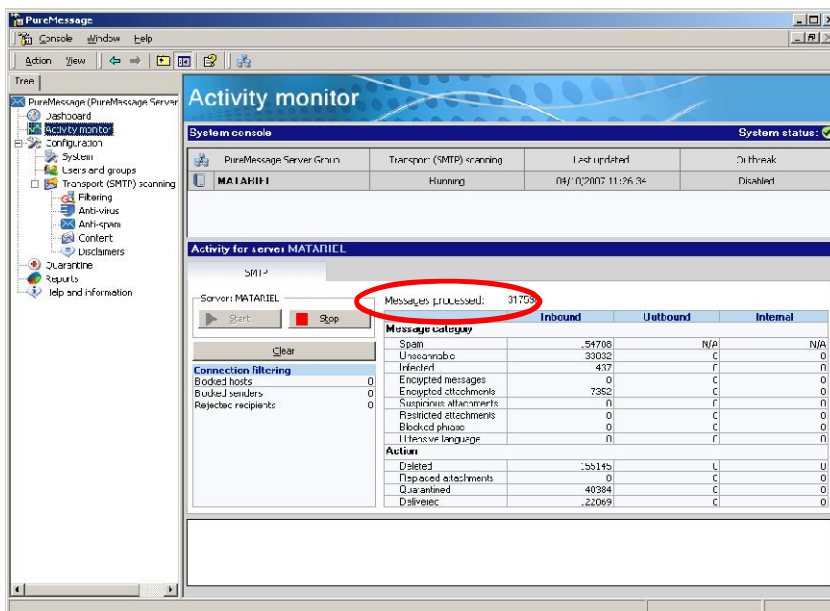


Abbildung 3: Der Activity Monitor verschafft sofortigen Einblick in das E-Mail-Volumen und weitere Daten

3: UNTERNEHMENSWEITES RICHTLINIEN-ENFORCEMENT

Vereinfachte Einrichtung und Durchsetzung von Richtlinien

PureMessage für Microsoft Exchange gibt Ihnen die Möglichkeit, unternehmensweite E-Mail-Richtlinien zentral zu konfigurieren und einheitlich durchzusetzen. So kontrollieren Sie den Informationsfluss Ihres Unternehmens und verhindern, dass Daten bewusst oder versehentlich aus Ihrem Unternehmen gelangen bzw. unerwünschte Inhalte Verbreitung finden.

Eine richtig konfigurierte E-Mail-Richtlinie spielt beim Kampf gegen E-Mail-Angriffe auf Ihr Netzwerk eine entscheidende Rolle. Deshalb liefern wir PureMessage für Microsoft Exchange mit einer Reihe vorbereiteter Standardrichtlinien aus, die auf Basis unseres umfangreichen Know-hows im Bereich Viren- und Spamschutz-Enforcement speziell entwickelt wurden. Wie Abbildung 5 zeigt, durchlaufen E-Mails zahlreiche Verfahren und werden an bestimmten Punkten auf Viren, Spam und unangemessene Inhalte gescannt. Wird eine E-Mail als verdächtig identifiziert, wird diese entweder gesperrt, abgewiesen, in die Quarantäne verschoben oder nach Ermittlung ihrer Unbedenklichkeit zugestellt. Sie können die Standardrichtlinien verändern oder eigene Richtlinien erstellen, die Ihren individuellen Anforderungen gerecht werden; Ausnahmen für einzelne Benutzer und Gruppen sind möglich.

PureMessage für Microsoft Exchange ermöglicht Ihnen außerdem die Konfiguration individueller Richtlinien zur E-Mail-Richtung: Sie können

Richtlinienflexibilität

Administratoren haben die Freiheit, Richtlinien individuell anzupassen. So können sie z.B. festlegen, dass mit eingehenden E-Mails anders verfahren wird als mit ausgehenden E-Mails oder aber Ausnahmen für ausgewählter Benutzer oder Gruppen definiert werden.

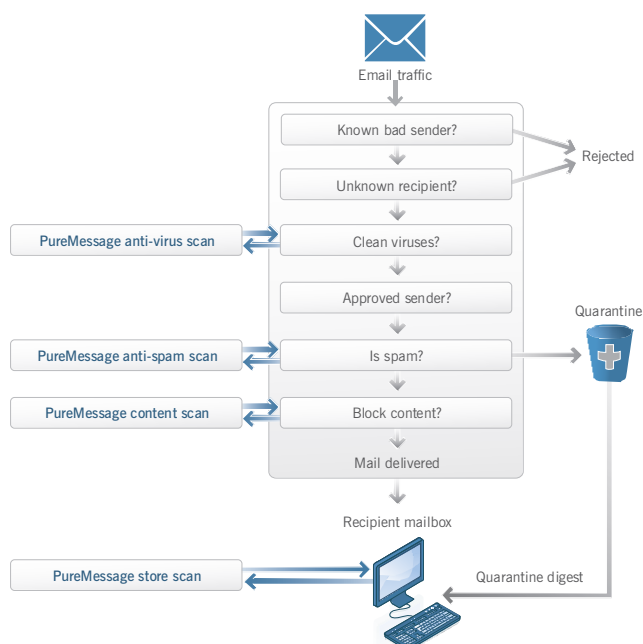


Abbildung 5: Richtlinien können für unterschiedliche Verfahren bei der Verarbeitung von E-Mails individuell angepasst werden

bedient sich PureMessage für Microsoft Exchange bei der Filterung verdächtiger E-Mails zahlreicher Methoden: Eine Filterung führt z.B. einen Test auf Milliarden unterschiedlicher Schreibweisen des Wortes „Viagra“ durch.

Unter Einsatz eines Scoring-Systems ermittelt die Lösung beim ersten Scan, ob es sich bei einer E-Mail um Spam oder vermuteten Spam handelt. Wie das Beispiel in Abbildung 6 zeigt, wird eine E-Mail mit einem Spam-Wahrscheinlichkeitswert von 90 bis 100 als Spam kategorisiert, während E-Mails mit einem Wert von 50 bis 90 unter die Kategorie vermuteter Spam fallen. Natürlich können Sie diese Schwellenwerte an die individuellen Anforderungen Ihres Unternehmens anpassen.

Das Spam-Scoring kann mit dem übergreifenden E-Mail-Fluss verglichen und die Abfangrate spezifischer Spam-Wahrscheinlichkeitswerte als Standard-Report reproduziert werden. Um eine Feinabstimmung des Scoring-Systems zu ermöglichen, ermittelt der Report in diesem Beispiel, wie hoch die Spam-Wahrscheinlichkeit von E-Mails ist und wie viele E-Mails im Vergleich zu den Kategorie-Einstellungen gesperrt werden. Wenn Sie Microsoft Exchange 2003 oder eine neuere Version einsetzen, kann PureMessage die Spam-Wahrscheinlichkeit als einen Microsoft Schwellenwert der SCL-Bewertung (Spam Confidence Level [SCL]) berechnen. Bei einer solchen Konfiguration des Systems werden alle E-Mails, die Endbenutzern mit einer höheren SCL-Bewertung als dem PureMessage-Wert zugestellt werden, automatisch in den Junk-Mail-Ordner von Microsoft Outlook umgeleitet.

Oft überlisten Spammer unachtsame Benutzer, indem Sie E-Mails mit schädlichen Hyperlinks versenden und dann zum Klicken auf den betreffenden Link auffordern. Wie bereits erwähnt, bekämpft PureMessage für Microsoft Exchange solche Vorgänge mittels Spammer Asset Tracking:

- Prüfen der in einer E-Mail enthaltenen URLs und Sperren von Nachrichten, die Links zu Spammer-Domains enthalten
- URI-Filterung und Sperrung von E-Mails, die auf missbrauchte, Freeweb und andere verdächtige Websites verlinken

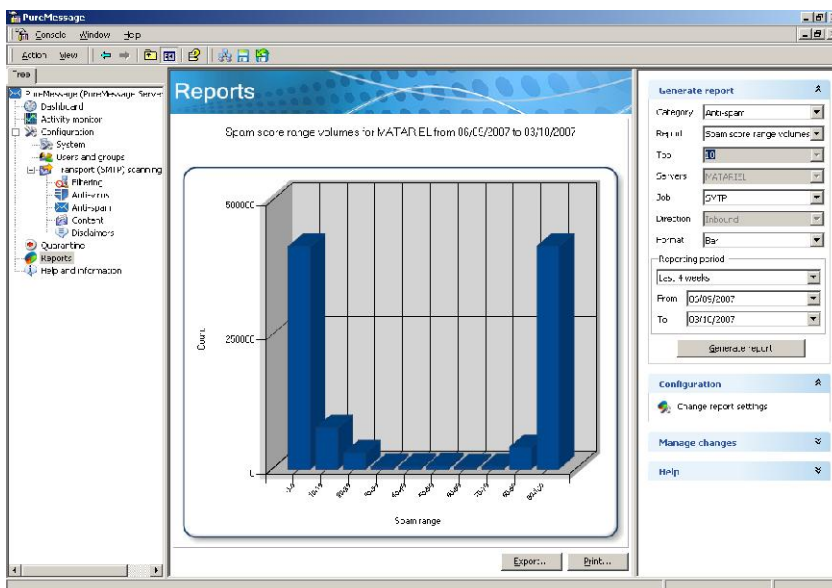


Abbildung 7: Unmittelbare Reports zeigen, wie viel Spam gesperrt wurde

Disclaimer

Mit der Disclaimer-Option können Sie alle ausgehenden E-Mails mit individuellen Texten versehen. Diese Option kann auch nur für bestimmte Gruppen oder einzelne Benutzer verwendet werden. Wie Abbildung 8 zeigt, können E-Mails der Vertriebsabteilung mit Werbetexten und E-Mails der IT-Abteilung mit Helpdesk-Informationen versehen werden. Sie haben ferner die Möglichkeit, Ausnahmen zu definieren: E-Mails vom Sales- oder IT Director sollten z.B. Informationen enthalten, die für deren Empfängerkreis angebracht sind.

Disclaimer können sich auch an bekannte Spammer oder andere Sender der Block List richten und diese darüber informieren, dass ihre E-Mail gesperrt und ggf. korrigierende Maßnahmen vonseiten Ihres Unternehmens getroffen wurden.

Spammer versenden oft E-Mails an Benutzer, die gar nicht existieren und hoffen darauf, dass die E-Mail an einen Mitarbeiter mit einem ähnlichen Namen gelangt. Recipient Validation (Empfänger-Validierung) gleicht eingehende E-Mails mit Active Directory ab. Als Spam identifizierte E-Mails können mit einem Disclaimer versehen werden, der den Sender über die Identifizierung seiner E-Mail als Spam und die Konsequenzen informiert. Da diese Maßnahme am Gateway greift, wird das Spam-Volumen automatisch und ohne Einfluss auf Verarbeitungsgeschwindigkeit und Bandbreite reduziert.

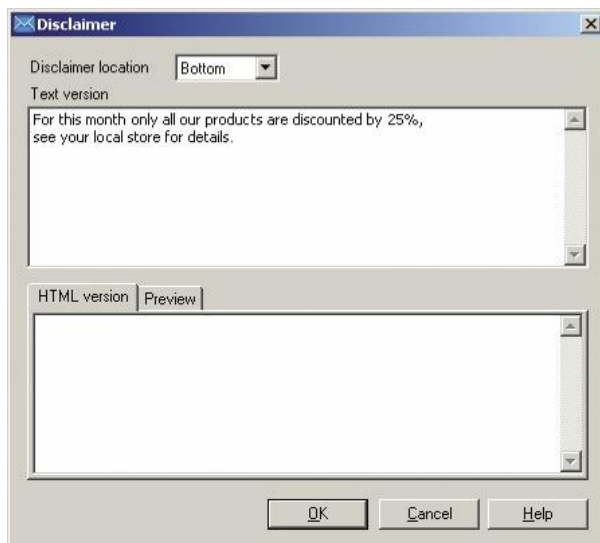


Abbildung 8: Ausgehende E-Mails können mit Disclaimern versehen werden

4: UMFASSENDE REPORTING-FUNKTIONEN

Reporting-Tool

PureMessage für Microsoft Exchange verfügt über umfangreiche Reporting- und Protokolloptionen, die genau die Daten aufzeichnen, die Sie zur Analyse Ihrer Traffic- und Filteroptionen benötigen. Sie können Reports mit Details zu sämtlichen Aspekten Ihres E-Mail-Netzwerks erstellen: Trends beim E-Mail-Durchsatz, Spamregel-Übereinstimmungsraten, Datenträgerverwendung und jegliche Vorfälle, die korrigierende Maßnahmen erfordern. Diese Daten können in Folge exportiert und für weitergehende Analysen in andere Office-Anwendungen wie Textverarbeitungs- und Tabellenkalkulationsdokumente eingefügt werden.

Reports können über die bereitgestellten Filter definiert und angepasst werden (siehe Abbildung 10). Verfügbare Optionen:

- Standard-Report-Formate
- Darstellungsformat
- Report-Zeitraum
- Server-Status
- E-Mail-Richtung

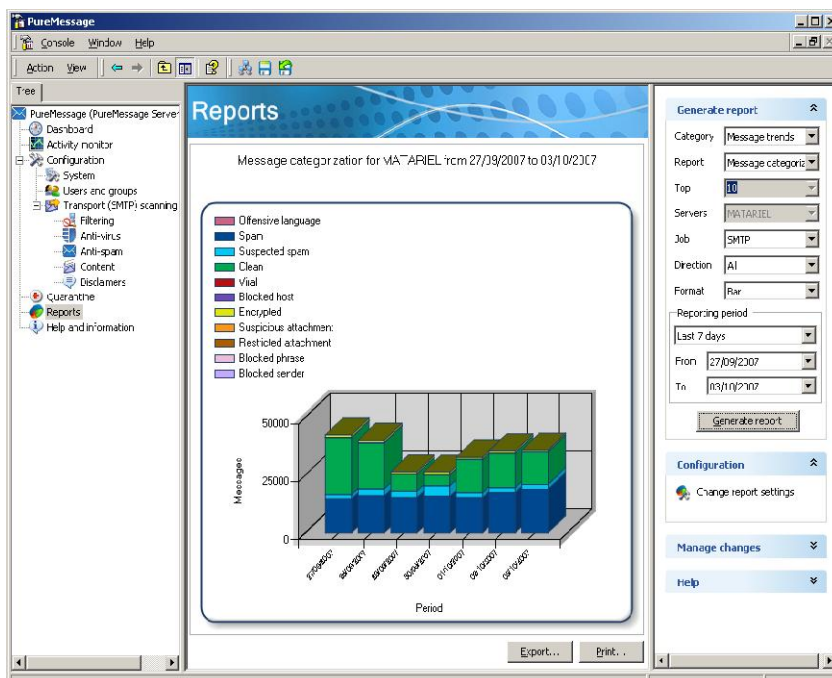


Abbildung 10: Reports können über den erweiterten Filter individuell angepasst werden

ANHANG I: SOPHOS PRODUKTE FÜR UNTERNEHMEN

Sophos Security and Data Protection

Sophos Security and Data Protection™ bietet Ihnen integriertes Bedrohungsmanagement für die gesamte Unternehmensinfrastruktur. Zusätzlich zu E-Mail Security and Data Protection beinhaltet Sophos Security and Data Protection:

Sophos Endpoint Security and Data Protection

Sophos Endpoint Security and Data Protection™: Mit den zentralen Verwaltungsfunktionen der Sophos Enterprise Console™ schützt Sophos Endpoint Security and Control Netzwerke vor Malware und sorgt für die lückenlose Kontrolle unerwünschter Anwendungen. Ein einziger Client erkennt Viren, Spyware, Adware, verdächtige Dateien, verdächtiges Verhalten und Controlled Applications wie VoIP-Anwendungen und Spiele. In Kombination mit einer Client-Firewall können zudem Zero-Day-Bedrohungen und unbefugte Hackerzugriffe abgewendet werden.

Sophos Web Security and Control

Sophos Web Security and Control™ ist eine voll integrierte Lösung zum Schutz vor Bedrohungen aus dem Internet. Sie bietet eine stabile Infrastruktur für sicheres Browsing ohne den bislang für effektive Internet-Sicherheit erforderlichen Verwaltungsaufwand.

Sophos NAC Advanced

Sophos NAC Advanced™ regelt den Netzwerkzugang für, nicht verwaltete, unbefugte und Gastcomputer, um anhand einer zentral festgelegten, auf Richtlinien basierenden Auswertung Computer zu identifizieren und zu isolieren, die nicht mit den Richtlinien übereinstimmen.

APPENDIX III: SYSTEMANFORDERUNGEN

Die neueste Version von PureMessage für Microsoft Exchange unterstützt Microsoft Exchange 2007 und Windows Server 2003 (64-Bit-Edition). Das Produkt kann jedoch auch weiterhin als Standalone Windows SMTP Gateway-Lösung zum Schutz Exchange-fremder E-Mail-Server zum Einsatz kommen.

Die Installation ist auf allen Exchange 2000-, 2003- und 2007-Servern möglich und kann auch eine Edgeserverrolle auf einem Standard-Windows IIS SMTP Server übernehmen. Bei einer solchen Konfiguration können E-Mails auch ohne Installation von Exchange gescannt werden.

Betriebssysteme	
Version	Grad der Unterstützung
Windows 2000 und ältere Versionen (alle Editionen)	Nicht unterstützt
Windows Server 2003 und Windows Server 2003 R2 (einschließlich Small Business Edition)	Unterstützt ab SP2. R2 erforderlich für CCR
Windows XP	Unterstützt ab SP3
Windows Server 2008 (einschließl. Essential Business Server und Small Business Server)	Offiziell unterstützt ab SP2 SP1-Unterstützung hinzugefügt in CC01
Windows Vista	Offiziell unterstützt ab SP2
Windows Server 2008 (einschließl. Essential Business Server und Small Business Server, falls vorhanden)	Unterstützt ab RTM
Windows 7	Unterstützt ab RTM

Microsoft Exchange Server	
Version	Grad der Unterstützung
Exchange 2000 und älter	Nicht unterstützt
Exchange 2003	Unterstützt ab SP2
Exchange 2007	Offiziell unterstützt ab SP2 SP1-Unterstützung hinzugefügt in CC01
Exchange 2010	Unterstützt ab RTM

Microsoft SQL Server	
Version	Grad der Unterstützung
SQL 2000/MSDE	Wird inoffiziell unterstützt
SQL 2005/Express	Vor SP3 inoffiziell unterstützt, SP3 offiziell unterstützt
SQL 2008/Express	Vor SP1 inoffiziell unterstützt, SP1 offiziell unterstützt

SOPHOS und utimaco

SOPHOS GmbH Tel.: 01805 767 467 (12 Cent/Min) E-Mail: info@sophos.de

Boston, USA | Oxford, UK

© Copyright 2010. Sophos Plc. Alle Rechte vorbehalten. Alle Marken sind Eigentum ihres jeweiligen Inhabers.

rg/100512

