

# SOPHOS



## puremessage

FOR LOTUS DOMINO

Reviewer's Guide





# WILLKOMMEN

Willkommen zum Reviewer's Guide für Sophos PureMessage™ für Lotus Domino, einer der Sophos E-Mail Security and Data Protection-Lösungen. Dieser Reviewer's Guide gibt IT-Administratoren einen Überblick über die Produktmerkmale von PureMessage™ für Lotus Domino und geht im speziellen auf Strategien zum Enforcement von Unternehmensrichtlinien sowie auf die umfassenden Reporting-Funktionen dieses Produkts ein.

Wie all unsere Lösungen ist Sophos PureMessage für Lotus Domino das Ergebnis von mehr als 20 Jahren Erfahrung beim Schutz von Unternehmen, Bildungseinrichtungen und Behörden. Diese Lösung schützt Ihren E-Mail Gateway und Ihre Domino Server umfassend vor Spam und Malware. Mit PureMessage für Lotus Domino 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.

Alle Sophos Lösungen sind auf maximale Bedienerfreundlichkeit und einfache Verwaltbarkeit ausgelegt. Sie genießen aufgrund ihrer proaktiven Schutzmechanismen, die zuverlässig zunehmend komplexe und schnelle Sicherheitsbedrohungen abwehren, branchenweit höchstes Ansehen. 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 Lotus Domino 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 Lotus Domino erhalten Sie von Ihrem Sophos Account Manager.

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

[www.sophos.de/companyinfo/contacting](http://www.sophos.de/companyinfo/contacting)

Eine Testversion können Sie über folgende Adresse anfordern:

[www.sophos.de/puremessage-download](http://www.sophos.de/puremessage-download)



# INHALT

<b>1</b>	<b>EIN KURZER ÜBERBLICK</b>	<b>6</b>
	Vielfach ausgezeichnete Technologie	6
	Installation und Verwaltung	7
<b>2</b>	<b>UNTERNEHMENSWEITES RICHTLINIEN-ENFORCEMENT</b>	<b>8</b>
	Vereinfachte Einrichtung & Durchsetzung von Richtlinien	8
	Leistungsstarke Malware-Überprüfung	10
	Branchenführender Spamschutz	10
	Inhaltsfilterung	11
	Disclaimer	12
	Quarantäne-Management	12
<b>3</b>	<b>UMFASSENDE PROTOKOLLE UND STATISTIKEN</b>	<b>14</b>
	Diagramme	15
	<b>ANHÄNGE</b>	
	I    Sophos Enterprise-Produkte	16
	II   Andere Produkte und Services von Sophos	17
	III  Systemvoraussetzungen für Sophos	19

# 1 EIN KURZER ÜBERBLICK

PureMessage für Lotus Domino verhindert, dass Spam und Malware in Ihre E-Mail-Infrastruktur und Ihre Domino 8 Server gelangen. Dieses Produkt bietet kostengünstigen und proaktiven Schutz vor bekannten und unbekanntem Bedrohungen, verhindert durch den Einsatz erweiterter Technologien zur Inhalts- und Attachment-Filterung Datenverluste und unterstützt Sie aktiv beim Enforcement unternehmensweiter E-Mail-Nutzungsrichtlinien. Standardrichtlinien zum Viren- und Spamschutz stellen sicher, dass Sie PureMessage für Lotus Domino so schnell wie möglich einsetzen können. Im Anschluss steht es Ihnen frei, von unseren bedienerfreundlichen Funktionen zu profitieren und eigene Richtlinien

## Simple Security

Mit individuellen und Standardrichtlinien sowie umfassender Überprüfung für E-Mails und deren Attachments schützen Sie Ihre Domino Server/Ihr Unternehmen vor Spam, Malware und Datenverlusten.

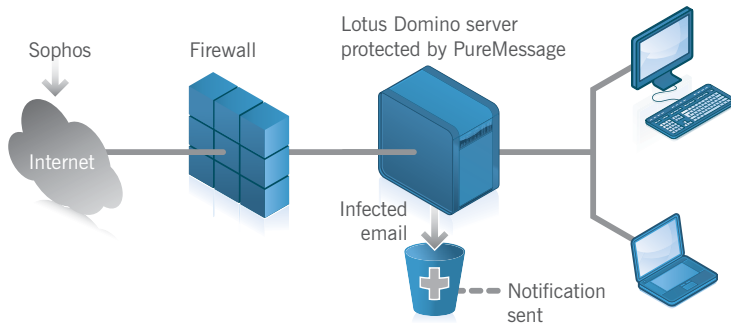


Abbildung 1: Eingehende, ausgehende und interne E-Mails werden auf verschiedenste Bedrohungen geprüft.

zu erstellen, die auf Ihre individuellen Bedürfnisse abgestimmt sind. Sämtliche Richtlinien können einzelnen Usern oder Gruppen zugeordnet werden. So erhalten Sie umfassende Kontrolle über die E-Mail-Nutzung in Ihrem Unternehmen.

## Vielfach ausgezeichnete Technologie

PureMessage überprüft E-Mails und Attachments beim Netzwerkeingang und -ausgang und innerhalb Ihrer Domino Server (Abbildung 1). Es spürt Viren, Trojaner, Würmer, Spyware, Spam und sensible Daten auf und schützt so nicht nur die Integrität Ihrer E-Mail-Infrastruktur, sondern auch Ihre vertraulichen Daten.

Die Sophos Genotype® Technologie erkennt ganze Viren- und Spamfamilien und schützt Sie bereits vor Bedrohungen, noch bevor diese ausgeführt werden können. So werden Malware und 99,9% des gesamten Spamaufkommens im Vorfeld abgefangen.

Noch mehr Schutz bieten Obfuscation Detection, URL-Tracking, Heuristiken und Fingerprinting von Inhalten, während SXL (Sophos eXtensible Lists) mit Echtzeit-Spamschutz auch neueste Bedrohungen abwehrt.

## Die besonderen Merkmale von PureMessage für Lotus Domino

<b>Unübertroffene Erkennung von Spam und Malware</b>	Erkennung von über 99,9% aller Spam-Mails und Schutz vor E-Mail-Betrügereien wie Phishing-Attacken. Erkennt, desinfiziert, löscht oder isoliert Viren, Trojaner, Würmer und schädliche Spyware in eingehenden und ausgehenden E-Mails.
<b>Proaktiver Schutz</b>	Setzt Genotype-, Behavioral Genotype®- und Sender Genotype-Technologie gezielt zur Bekämpfung neuer Bedrohungen und gefährlicher Anwendungen ein.
<b>Hohe Genauigkeit</b>	Ausgewogener Einsatz zahlreicher Spam-Erkennungsmethoden sorgt für genaue Ergebnisse und reduziert False Positives.
<b>Verhinderung von Datenverlust</b>	Leistungsstarke Steuerung der Inhaltsüberprüfung für E-Mails und Attachments zum lückenlosen Schutz vor Datenverlust
<b>Einhaltung von Richtlinien</b>	Umfangreiche Richtlinienumgebung zur Umsetzung komplexer und gesetzlicher Anforderungen
<b>Globaler Schutz</b>	Schützt globale Unternehmen vor Spam und Viren im mehrsprachigen E-Mail-Verkehr, darunter auch in solchen Sprachen, die Doppel-Byte-Zeichen verwenden.
<b>Automatische Updates</b>	Automatische Updates mit dem neuesten Schutz aus den SophosLabs, dem globalen Netzwerk aus Bedrohungsanalysecentern
<b>Enduser-Funktionen</b>	Enduser-Quarantäne-Überblick, Allow Lists und Block Lists
<b>Umfassender Support</b>	Uneingeschränkter Support per Telefon, E-Mail und online – rund um die Uhr, an 365 Tagen im Jahr

### *Umfassender Einblick*

Über eine Domino-basierte Konsole verwalten Sie die Quarantäne, verfolgen E-Mails und haben Einsicht in den gesamten E-Mail-Traffic und Bedrohungsaktivitäten.

PureMessage für Lotus Domino erhält im Laufe des Tages immer wieder Updates aus den SophosLabs, mit denen Sie stets vor den neuesten Viren- und Spamskampagnen geschützt sind.

## Installation und Verwaltung

Eine Konsole im Stil von Domino ermöglicht die zentrale Verwaltung über mehrere Server und bietet automatisiertes Quarantäne-Management, E-Mail-Nachverfolgung und Reporterstellung zum gesamten E-Mail-Traffic sowie zur Bewegung bedrohlicher Daten. Sie können PureMessage für Lotus Domino auf Standalone- und replizierten Serverumgebungen installieren und User und Gruppen über das Notes Address Book (NAB) einbinden.

## Zwei Versionen

PureMessage für Lotus Domino ist in zwei verschiedenen Ausführungen mit unterschiedlicher Preisstruktur erhältlich:

- Virenschutz
- Integrierter Viren- und Spamschutz mit Inhaltsfilterung

## 2 UNTERNEHMENSWEITES RICHTLINIEN-ENFORCEMENT

### Vereinfachte Einrichtung und Durchsetzung von Richtlinien

PureMessage für Lotus Domino 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 Lotus Domino mit einer Reihe vorbereiteter Standardrichtlinien aus, die auf Basis unseres umfangreichen Know-hows im Bereich Viren- und Spamschutz-Enforcement speziell entwickelt wurden. E-Mails und ihre Attachments werden auf Viren, Spam, unangemessene Inhalte, Stichwörter und andere sensible Daten geprüft (Abbildung 2). Eine als verdächtig eingestufte E-Mail wird entweder geblockt oder in die Quarantäne verschoben. Die E-Mail kann in bestimmten Fällen auch zugelassen und in Folge zugestellt werden. Sie können die

### Flexible Richtlinien

Sie können Richtlinien so anpassen, dass mit eingehenden, ausgehenden und internen E-Mails unterschiedlich verfahren wird.

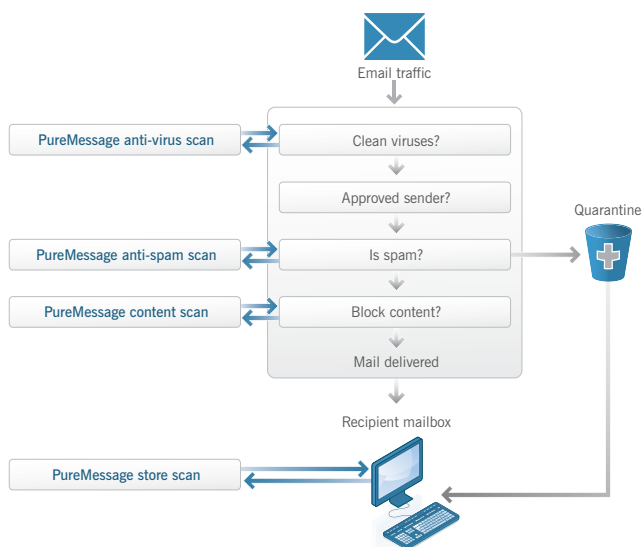


Abbildung 2: E-Mails werden mehrmals überprüft, bevor Sie in den Posteingang gelangen.

Standardrichtlinien umändern oder eigene Richtlinien erstellen, die Ihren individuellen Anforderungen gerecht werden; Ausnahmen für einzelne User und Gruppen sind möglich.

PureMessage für Lotus Domino ermöglicht Ihnen außerdem die Konfiguration individueller Richtlinien zur E-Mail-Richtung: Sie können also separate Richtlinien für eingehende, interne und ausgehende E-Mails definieren.

Richtlinien können so verfasst werden, dass sie bestimmte Wörter oder Ausdrücke im E-Mail-Body oder der Betreffzeile erkennen. Diese Überprüfung kann auch auf Attachments mit allen gängigen Dateiformaten ausgeweitet werden.

Um Ihnen bei der Verwaltung maximale Flexibilität einzuräumen, werden Richtlinien zur E-Mail- und Speicher-Überprüfung (Abbildung 3) unabhängig voneinander gehandhabt. Jede Richtlinie setzt sich aus einer Reihe von Jobs zusammen und eine unbegrenzte Anzahl an Jobs kann konfiguriert und priorisiert werden. Um einen schnellen unternehmensweiten Einsatz von PureMessage für Lotus Domino zu ermöglichen, verfügt die Software bereits bei Auslieferung über vorkonfigurierte Standardjobs.

### Intelligente Überprüfungsverfahren

Richtlinien können bestimmte Wörter oder Ausdrücke in E-Mails und Attachments (alle gängigen Programme) erkennen.

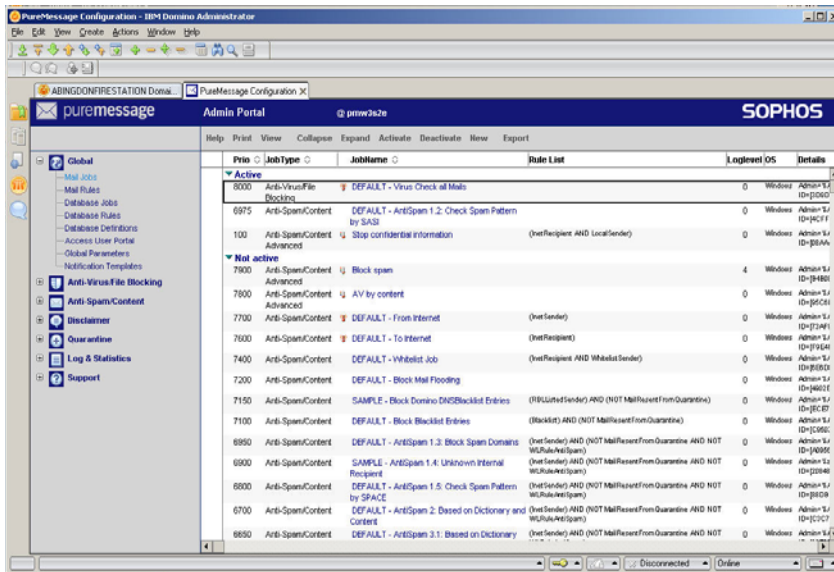


Abbildung 3: Richtlinien, die E-Mails und Speicher überprüfen, werden über eine festgelegte Job-Anzahl definiert und können individuell auf Ihre Bedürfnisse angepasst werden.

Jeder einzelne Job verfügt wiederum über eine Reihe von Aspekten, die ganz nach Ihren Bedürfnissen konfiguriert werden können. So kann z.B. festgelegt werden, bei welchen Arten von E-Mails der Job zum Einsatz kommen soll und auf welche Informationen E-Mails und Attachments geprüft werden sollen (Abbildung 4).

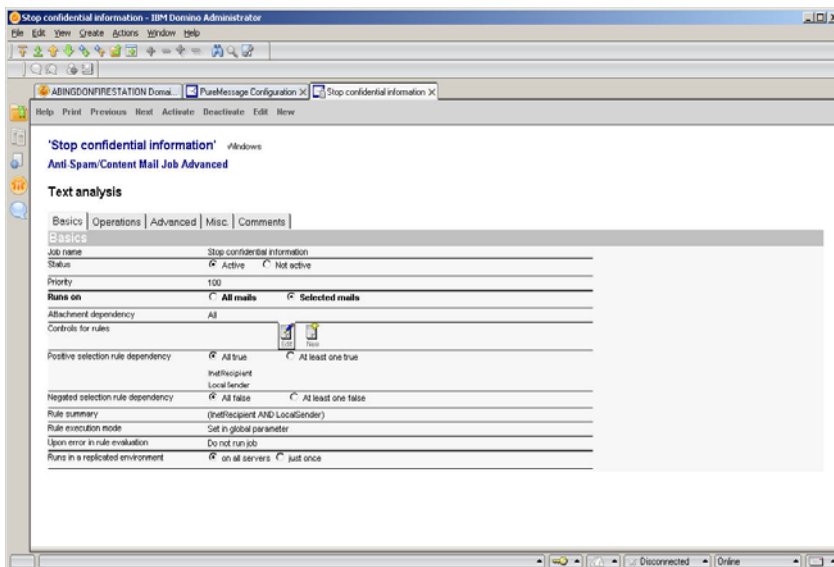


Abbildung 4: Jeder Job kann auf unterschiedliche Arten konfiguriert werden.

Je nach Job können auch andere Eigenschaften konfiguriert werden. Sie können z.B. festlegen, welche Bereiche der E-Mail genau überprüft werden sollen, welche Schwellenwerte zum Einsatz kommen sollen, ob die E-Mail gesperrt oder in die Quarantäne verschoben werden soll bzw. welche Benachrichtigungen erstellt werden sollen.

### Leistungsstarke Malware-Prüfung

PureMessage für Lotus Domino ist mit unserer leistungsstarken Malware Detection Engine ausgerüstet: Diese überprüft nicht nur sämtliche E-Mails, die auf einem Domino Server eingehen bzw. diesen verlassen, sondern auch Domino E-Mail-Speicher. PureMessage für Lotus Domino schützt vor Mischbedrohungen (z.B. Kombination aus Viren, Spam und Denial-of-Service-Attacken) und ermöglicht auch Überprüfungen im Hintergrund. In diesem Fall erfolgen Überprüfungsläufe entweder in regelmäßigen Abständen oder fortlaufend.

### Umfassender Bedrohungsschutz

PureMessage für Lotus Domino schützt vor Mischbedrohungen (z.B. eine Kombination aus Viren, Spam und Denial-of-Service-Attacken).

### Branchenführender Spamschutz

Bei 97% aller geschäftlichen E-Mails handelt es sich um Spam. Um Spam aktiv zu bekämpfen, bedient sich PureMessage für Lotus Domino bei der Filterung verdächtiger E-Mails zahlreicher Methoden: Eine Filterung führt z.B. einen Test auf Milliarden unterschiedlicher Möglichkeiten durch, mit denen das Wort "Viagra" buchstabiert werden kann.

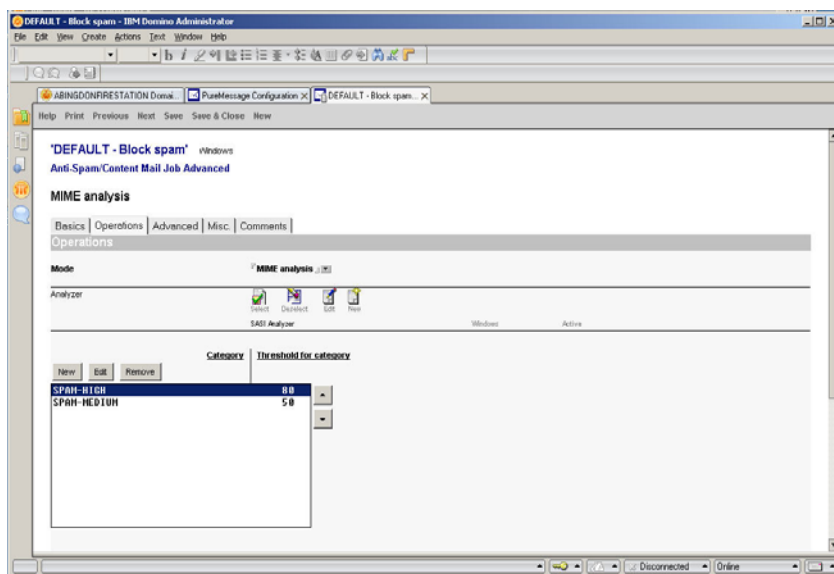


Abbildung 5: Ein Scoring-System legt fest, ob eine E-Mail als Spam behandelt wird.

Über ein Scoring System legt PureMessage für Lotus Domino im Rahmen des ersten Überprüfungslaufs den Risikolevel einer E-Mail fest. Im vorliegenden Beispiel (Abbildung 5) wird jede E-Mail mit einem Spam Rating von 80 als hohes Spam-Risiko eingestuft. E-Mails mit einem Spam Rating von 50 gelten als mittleres Spam-Risiko. Sie entscheiden, ob die E-Mail in die Quarantäne verschoben, gelöscht oder zugestellt werden soll.

### Schädliche Hyperlinks

Oft überlisten Spammer unachtsame User, indem Sie E-Mails mit schädlichen Hyperlinks versenden und dann zum Klicken auf den betreffenden Link auffordern. PureMessage für Lotus Domino beugt

diesen kriminellen Machenschaften durch Spammer Asset Tracking vor und führt konkret folgende Maßnahmen durch:

- Prüfen der in einer E-Mail enthaltenen URLs und Sperren von Nachrichten, die Links zu Spammer-Domains enthalten
- URL-Filterung und Sperrung von E-Mails, die auf missbrauchte, Freeweb- und andere verdächtige Websites verlinken
- Gegenprüfung mit der Sophos IP Block List für bekannte Spam-Server, offene Proxys und missbrauchte Systeme

### Inhaltsfilterung

Durch seine erweiterten Funktionen zu Inhaltsfilterung, die für die lückenlose Überprüfung von Attachments und E-Mail-Inhalten sorgen, kontrolliert PureMessage für Lotus Domino den Datenfluss aus Ihrem Unternehmen. Die Inhaltsfilter von PureMessage für Lotus Domino schützen Ihre Daten durch Einsatz zahlreicher Methoden:

#### Attachment-Typ

PureMessage für Lotus Domino kann zur Sperrung bestimmter Anwendungen konfiguriert werden. Hierzu zählen z.B. ausführbare Dateien, die als Sicherheitsbedrohung gelten, oder Anwendungen, die die Mitarbeiterproduktivität potenziell beeinträchtigen (z.B. MP3s). Sowohl Attachment-Body, Betreffzeile und E-Mail-Text können überprüft werden.

#### Ausdruck/regulärer Ausdruck

Diese Richtlinie sucht nach vollständigen und unvollständigen Ausdrücken und regulären Ausdrücken, die Sie als inakzeptabel bzw. als Sicherheitsrisiko erachten. PureMessage für Lotus Domino wird mit einer Reihe von Standard-Wörterbüchern (Abbildung 6) ausgeliefert, die übliche vertrauliche Ausdrücke und anstößige Sprache enthalten. Wörterbücher können individuell angepasst werden.

### Reputation Scanning

PureMessage für Lotus Domino führt auf Basis der IP-Adresse des sendenden Servers bei sämtlichen empfangenen E-Mails einen Reputation-Check durch.

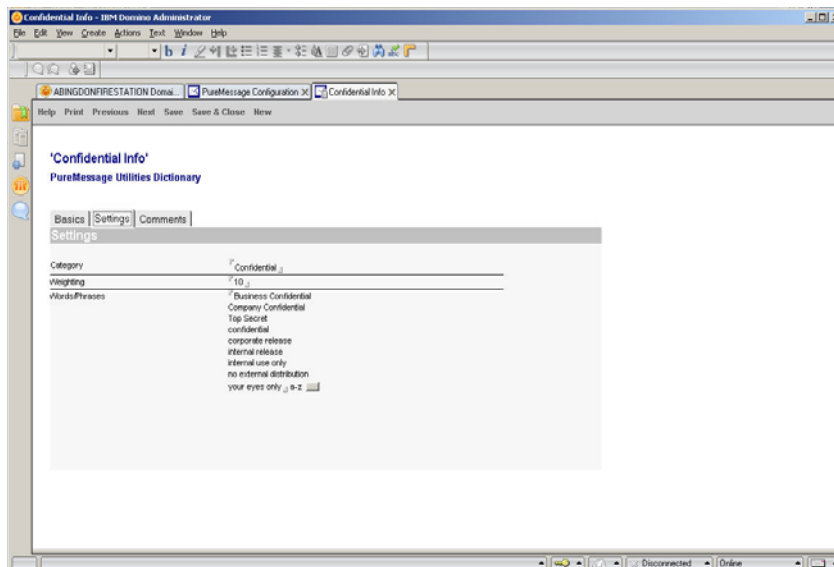


Abbildung 6: Dieses Wörterbuch führt Stichwörter und andere vertrauliche Daten auf, die geblockt werden sollen.

PureMessage für Lotus Domino führt Inhaltsanalysen in gängigen Dateiformaten wie Word und Excel durch und ermittelt, ob diese zuvor definierte Wörter oder Ausdrücke enthalten (z.B. "Finanzbericht"). Sie können Listen von Ausdrücken erstellen und auch Platzhalter berücksichtigen, die unvollständigen Ausdrücken entsprechen. Außerdem haben Sie die Möglichkeit, auch reguläre Ausdrücke zur Richtlinie hinzuzufügen. So können spezifische Zahlen- und Code-Formate wie Kreditkartennummern oder andere personenbezogene Daten identifiziert und nach Ihren Vorgaben behandelt werden.

Nach Definition der Inhaltsrichtlinie können beim Abfangen einer E-Mail eine der folgenden Maßnahmen und jede Ausnahme angewandt werden:

Zu den Standard-Maßnahmen zählen:

- Löschen
- Nur protokollieren
- Mit Text ersetzen
- Quarantäne
- Quarantäne und zustellen

Mit der letzten Option können Sie eine blinde Kopie einer E-Mail in die Quarantäne verschieben. Diese Maßnahme erweist sich vor allem bei der Überwachung sensibler Daten in ausgehenden E-Mails als nützlich.

### True File Type-Erkennung

True File Type-Erkennung spürt ausführbare Attachment-Dateien auf, die versuchen, sich als harmlose Dateien zu tarnen (z.B. als jpegs oder Textverarbeitungsdokumente).

### Disclaimer

Mit der Disclaimer-Option können Sie ausgewählte Texte zu allen ausgehenden E-Mails hinzufügen. Diese Option kann auch nur für bestimmte Gruppen oder einzelne User verwendet werden. So könnten z.B. E-Mails vom Sales Team um Werbeslogans erweitert werden oder E-Mails aus der IT-Abteilung Helpdesk-Informationen enthalten. 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.

### Quarantäne-Management

Sie können Ihre Richtlinien so definieren, dass alle als Malware und Spam klassifizierte E-Mails sowie E-Mails mit unangemessenen Inhalten in die zentrale Quarantäne verschoben werden (Abbildung 7). In der Quarantäne können Sie die E-Mail in Folge gefahrlos prüfen und eine Reihe von Maßnahmen vornehmen, z.B:

- Weiterleiten einer Kopie in Ihren Posteingang
- Freigabe der E-Mail an ursprünglichen Empfänger
- Löschen der E-Mail aus der Quarantäne
- Desinfektion der E-Mail
- Löschen schädlicher Attachments
- Hinzufügen des Senders zur globalen Allow oder Block List

### *Hinzufügen von Text*

Sie können sämtliche ausgehenden E-Mails mit ausgewählten Texten versehen und Ihre Korrespondenz so auf einen bestimmten Empfängerkreis anpassen.

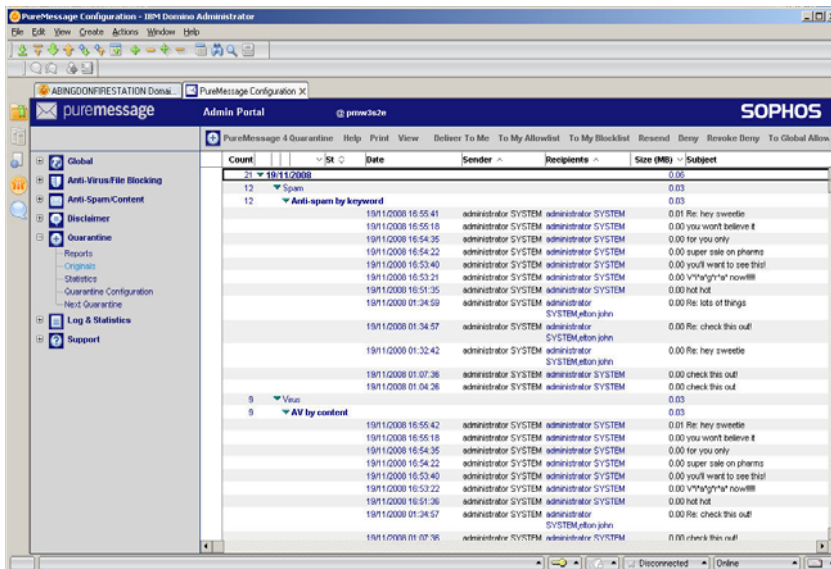


Abbildung 7: In der Quarantäne können Sie E-Mails, die als Bedrohung eingestuft wurden, gefahrlos prüfen.

### Signifikante Zeiteinsparungen

Mit PureMessage für Lotus Domino können Sie Ihre User mit der Verwaltung ihrer eigenen Spam-Mails betrauen. So bleibt der IT-Abteilung mehr Zeit, sich auf ihre Hauptaufgaben zu konzentrieren.

Außerdem steht es Ihnen frei, spezifische Details einzelner E-Mails einzusehen und zu ermitteln, welcher Job zum Verschieben in die Quarantäne geführt hat (Abbildung 8). In diesem Beispiel fing der Job Spam nach Stichwörtern ab.

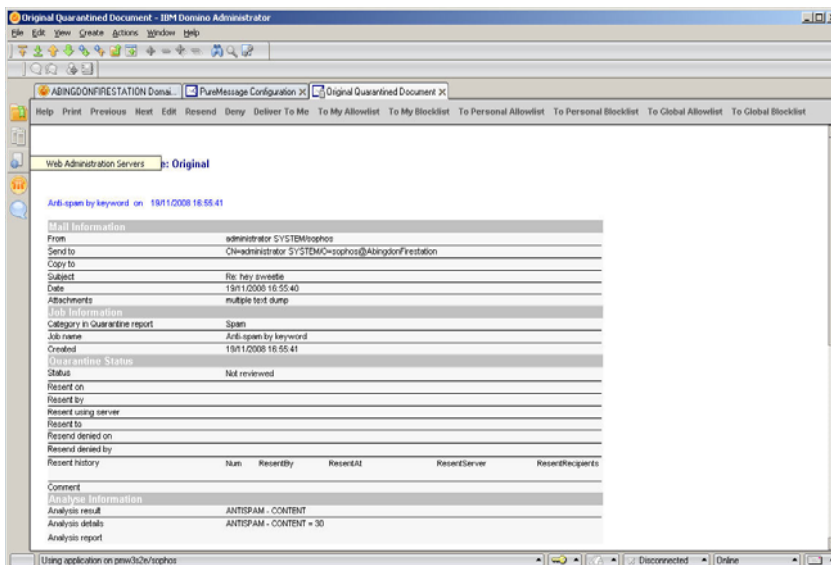


Abbildung 8: Einsicht in Details zu einzelnen E-Mails gibt Aufschluss darüber, warum eine E-Mail als verdächtig eingestuft und in die Quarantäne verschoben wurde.

Über eine webbasierte Benutzeroberfläche können Sie Endusern Zugriff auf Quarantäne-E-Mails einräumen und diese auffordern, bei dringenden Belangen (z.B. falsche Kategorisierung einer E-Mail) mit Ihnen in Kontakt zu treten. User können die Freigabe einer Quarantäne-E-Mail beantragen oder das Hinzufügen eines Absenders zur Allow oder Block List erwirken.

Mitarbeiter mit der Verwaltung ihres eigenen Spams zu betrauen, bringt zahlreiche Vorteile mit sich: Alle eingehenden E-Mails werden richtig identifiziert und Ihre IT-Mitarbeiter können sich auf ihre Hauptaufgaben konzentrieren. Bitte beachten Sie jedoch, dass bei E-Mails, die Malware enthalten könnten, besondere Vorsicht geboten ist und nur geschulte Fachkräfte mit einer Desinfektion betraut werden sollten.

## 3 UMFASSENDE PROTOKOLLE UND STATISTIKEN

PureMessage für Lotus Domino verfügt über umfangreiche Reporting-, Diagramm- und Protokoll-Optionen, die Ihnen die Analyse von E-Mail-Traffic, Quarantänen und Filter-Optionen erleichtern.

Sie können Reports mit Details zu sämtlichen Aspekten Ihres E-Mail-Netzwerks erstellen: Trends beim E-Mail-Durchsatz, Spam-Regel-Übereinstimmungsraten und jegliche Vorfälle, die korrigierende Maßnahmen erfordern. Diese Daten können in Folge exportiert und für weitergehende Analysen und zur Erstellung von Management-Reports in andere Office-Anwendungen wie Textverarbeitungs- und Tabellenkalkulationsdokumente eingefügt werden.

Reports können definiert und über erweiterte Filter individuell angepasst werden. Einige Beispiele:

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

### *Eingehende Analysen*

Sämtliche von PureMessage für Lotus Domino erfassten Daten können zur späteren Ansicht und Analyse exportiert werden.

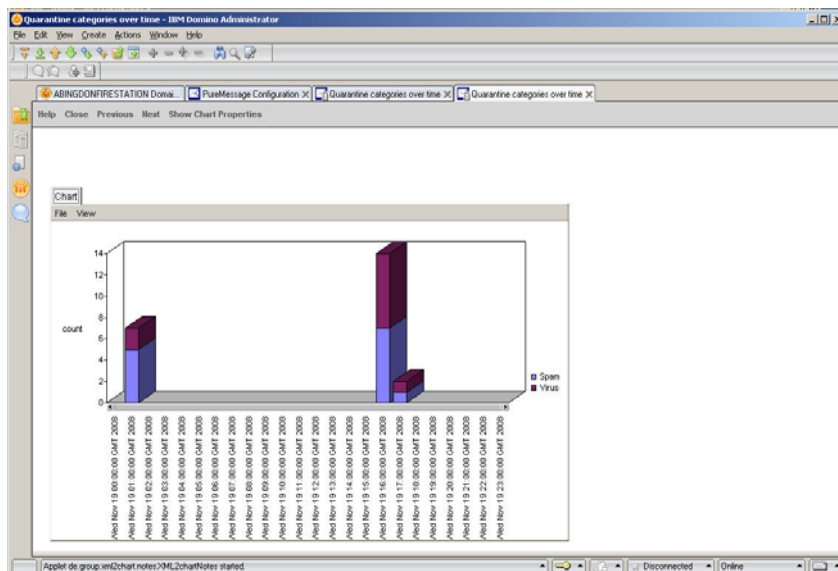


Abbildung 9: Erstellung angepasster Reports und Export in gängige Textverarbeitungs- und Tabellenkalkulationsprogramme

## Diagramme

Außerdem haben Sie mit PureMessage für Lotus Domino Zugriff auf zahlreiche Standard-Report-Diagramme, u.a.:

- Quarantänen nach Kategorie
- Anzahl in die Quarantäne verschobener E-Mails
- Traffic Reports
- E-Mail nach Trends

### *Standard Reporting*

Umfangreiche Reporting-Optionen ermöglichen eine schnelle und effiziente Datenanzeige- und analyse.

# ANHANG I: SOPHOS ENTERPRISE-PRODUKTE

## 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 umfasst Sophos Security and Data Protection:

**Sophos Endpoint Security and Data Protection™:** Mit den zentralen Verwaltungsfunktionen der Sophos Enterprise Console™ schützt Sophos Endpoint Security and Data Protection 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. Unser Endpoint-Schutz umfasst außerdem integrierte Network Access Control.

### **Sophos Web Security and Control™:**

Das Herzstück dieses Produktes ist unsere Web Appliance, welche lückenlosen Schutz vor sämtlichen Bedrohungen aus dem Internet bietet. Sophos Web Security and Control liefert eine komplette Infrastruktur für sicheres Internet-Browsing und sorgt mit bedienerfreundlichen Verwaltungsfunktionen gleichzeitig für maximale Effektivität sämtlicher Abläufe.

**Sophos NAC Advanced™:** Diese Lösung regelt den Netzwerkzugriff für Gast-, nicht verwaltete und unbefugte Computer, um anhand einer zentral festgelegten, auf Richtlinien basierenden Auswertung Computer zu identifizieren und zu isolieren, die nicht mit den Richtlinien übereinstimmen.

**Safeguard Enterprise Encryption:** Dieses Produkt aus dem Hause Utimaco ist nun über Sophos erhältlich, da das auf Verschlüsselungstechnologien spezialisierte Unternehmen Utimaco seit kurzem der Sophos Gruppe angehört. Safeguard Enterprise Encryption ergänzt Sophos' Lösungen für Endpoint, Gateway und Network Access Control und verhindert durch zentral verwaltete Festplattenverschlüsselung effektiv Datenzugriff, -verlust oder -diebstahl auf Laptops, Desktops und Wechseldatenträgern. Safeguard Enterprise Encryption kann außerdem die Verwendung von Wechseldatenträgern, optischen Medienlaufwerken und Wireless Networking Protokollen ermitteln und blockieren.

## ANHANG II: ANDERE PRODUKTE UND SERVICES VON SOPHOS

### SAV Interface:

Mit SAV Interface™ können Software-Anbieter, OEMs, ISPs und ASPs Sophos Malware-Erkennungstechnologie in ihre eigenen Firewalls, Gateways und Lösungen integrieren. SAV Interface™ ist außerdem Teil der E-Mail Security and Data Protection und der Web Security and Control Lizenz.

### Sophos Small Business Solutions

*Sophos Small Business Solutions* bieten vielfach ausgezeichneten und bewährten Schutz vor Viren, Spyware und Spam für Unternehmen mit wenigen oder keinen IT-Fachkräften.

### Sophos Professional Services

Sophos Professional Services bieten Unternehmen fundiertes Know-how, um die Endpoint- und Gateway-Lösungen von Sophos optimal in Ihr Netzwerk zu integrieren. Erfolgreiche Unternehmen auf der ganzen Welt nutzen unsere Services. Sie können Sophos Lösungen nicht nur zeitsparend an Ihre spezifischen Anforderungen anpassen, sondern auch deren effizienten Einsatz und maximalen ROI (Return on Investment) sicherstellen. Um das Maximum aus Ihrem Investment herauszuholen, bieten wir Ihnen sowohl Standard- als auch individuelle Support-Packages, mit denen Sie ganz auf Wunsch vor Ort oder über Remote-Verbindung von unserem Know-how profitieren können.

### Sophos Alert Services

*Sophos ZombieAlert™ Service* warnt Ihr Unternehmen sofort, wenn Spammer Computer in Ihrem Netzwerk dazu missbrauchen, Spam-Mails zu versenden oder Denial-of-Service-Attacken durchzuführen.

*Sophos PhishAlert™ Service* warnt Sie nahezu in Echtzeit vor Phishing-Kampagnen, damit Sie die nötigen Schritte einleiten können, um die falsche Website zu schließen und so Ihre Kunden zu schützen.

Sophos WebAlert Service warnt Ihr Unternehmen automatisch, wenn eine Ihrer Webseiten mit Malware infiziert werden sollte.

Weitere Informationen zu den Sophos Alert Services finden Sie auf den folgenden Webseiten:

[www.sophos.com/products/enterprise/alert-services/phishalert.html](http://www.sophos.com/products/enterprise/alert-services/phishalert.html)  
(englisch)

[www.sophos.de/products/enterprise/alert-services/zombiealert.html](http://www.sophos.de/products/enterprise/alert-services/zombiealert.html)

[www.sophos.com/products/enterprise/alert-services/webalert.html](http://www.sophos.com/products/enterprise/alert-services/webalert.html)  
(englisch)

### Branchenführender Support rund um die Uhr

Dank des in der Lizenz inbegriffenen technischen Supports können Sie sich bei Problemen jederzeit an unser erfahrenes Support Team wenden. Kontaktieren Sie für individuellen Support unsere technischen Mitarbeiter per Telefon oder E-Mail oder nutzen Sie einfach unsere webbasierte Support-Knowledgebase. Die Experten in unseren weltweit präsenten Supportcentern bauen beim Rekonstruieren, Analysieren und Beheben von Problemen auf einschlägige Erfahrung und bewährte Verfahren.

Wir verfügen über technische Supportcenter in Deutschland, Frankreich, Großbritannien, Italien, Australien, Japan, Kanada, Singapur und den USA. Jedes dieser Center bietet ein hohes Niveau an Fachkompetenz, Professionalität und Dienst am Kunden.

Weitere Informationen finden Sie auf [www.sophos.de/support](http://www.sophos.de/support)

# ANHANG III: SYSTEMVORAUSSETZUNGEN PUREMESSAGE FÜR LOTUS DOMINO

## E-Mail-Server\*

- Lotus Domino Server R7, R8.0x und R8.5 (32-/64-Bit)

## Betriebssystem

- Windows 2000 Server
- Windows Server 2003 (32-/64-Bit)
- Windows Server 2008 (32-/64-Bit)

\*Lotus Domino Server R6 wird von PureMessage für Notes/Domino v3 unterstützt.

# SOPHOS

Boston, USA | Oxford, UK

© Copyright 2009. Sophos GmbH. Alle Rechte vorbehalten. Alle aufgeführten Marken sind Eigentum der jeweiligen Inhaber.  
rg/091210

