

# Microsoft® Forefront Security for Exchange Server

## Multiengineschutz vor den neuesten E-Mail-Bedrohungen

**Microsoft Forefront Security for Exchange Server umfasst mehrere Scanmodule führender Sicherheitshersteller, die zum Schutz der Exchange Server-Messagingumgebung von Unternehmenskunden vor Viren, Würmern und Spam in eine einzige Lösung integriert sind.**

*Microsoft Forefront Security for Exchange Server ist Teil der Microsoft Forefront-Familie von Sicherheitsprodukten. Dieses Produkt war als Antigen für Exchange bekannt. Es umfasst mehrere Scanmodule, die sich leicht integrieren lassen. Mit Sicherheitsfunktionen auf mehreren Ebenen sorgt es für den umfassenden Schutz von Exchange-Messagingservern, optimiert die Serverleistung und vereinfacht die Sicherheitsverwaltung.*

Auch heute noch sind durch E-Mail verbreitete Virenangriffe die kostspieligste Bedrohung für die Unternehmen, da durch Angriffe oft erhebliche Zeit- und Produktivitätsverluste\* entstehen. Viren, Würmer, Spam und andere Schadsoftware können die Kommunikation lahmlegen, die Serverressourcen überfordern, Systeme zum Absturz und produktive Arbeit zum Stillstand bringen. Im Jahre 2006 verwendeten etwa 97 Prozent aller Unternehmen Antivirensoftware. Dennoch fielen 65 Prozent dieser Unternehmen Virenattacken zum Opfer.\*

Weshalb? Einer der Gründe ist der Versuch, alle geschäftskritischen Server im Unternehmen durch Software zu schützen, die nur über ein einziges Antivirenscanmodul verfügt. Wenn dieses Modul die neueste Bedrohung nicht schnell genug erkennt, kann sich der Virus im gesamten Unternehmen verbreiten, indem er in jeden Netzwerkknoten, der dasselbe anfällige Scanmodul verwendet, eindringt.

Überaus restriktive Abwehrmaßnahmen sind jedoch auch mit Nachteilen verbunden.

Wenn eine ganze Nachricht blockiert wird, obwohl nur ein Teil davon suspekt ist, werden den Benutzern wichtige E-Mails vorenthalten. Wenn jede Nachricht an jedem Server gescannt wird, verzögert sich die Zustellung, und es ergibt sich ein unnötiger Ressourcenaufwand. Installation und Verwaltung von mehreren, nicht integrierten Antivirenprodukten erhöht den Verwaltungsaufwand. Das redundante Scannen alter E-Mails, unabhängig davon, wie alt sie sind, zehrt an den Serverressourcen.

Und das Ergebnis ist letzten Endes immer gleich – langsamere E-Mailzustellung, größere Verwundbarkeit an einem kritischen Ausfallpunkt („Single Point of Failure“), hohe Verwaltungskosten und Produktivitätsverluste.

### **Bessere Chancen ohne zusätzlichen Overhead**

Mit umfassenden Antivirenmaßnahmen auf mehreren Ebenen, verbesserter Serverleistung und -verfügbarkeit sowie vereinfachter Sicherheitsverwaltung für Exchange Server-Systeme kann Microsoft Forefront Security for Exchange Server zur Lösung dieser Probleme beitragen.

### **Umfassender Schutz vor den neuesten Bedrohungen**

Forefront Security for Exchange Server wird mit mehreren Antivirenengines von führenden Sicherheitsherstellern ausgeliefert. Damit ist umfassender Schutz vor den neuesten Bedrohungen gewährleistet. Bis zu fünf Scanmodule können gleichzeitig auf mehreren Ebenen in der gesamten Exchange Server-Umgebung eingesetzt werden. Wenn ein Modul während eines Updates offline ist, scannen die anderen Module die Exchange 2007-Edge-, -Hub- und -Speicherserver weiter – auch bei E-Mails von Mobilgeräten. Signaturupdates erfolgen schnell und automatisch für alle Module, sodass neue Bedrohungen erkannt werden können, während sie sich noch in der Entstehung befinden.

Zur Spamabwehr aktiviert Forefront Security for Exchange Server die Premiumantispam- und -contentfilter von Exchange 2007. Automatische Updates sorgen dafür, dass diese Filter stets auf dem neuesten Stand sind. Die Heuristik- und Dateifilterungstechnologien schützen Unternehmen vor neuen Bedrohungen, da sie Viren anhand von Verhaltensmustern identifizieren und gefährliche Dateien (wie ausführbare Dateien) auch noch erkennen, wenn die Dateinamenerweiterung geändert worden ist.

### **Optimierte Leistung sorgt für rasche Beförderung der E-Mail**

Forefront Security for Exchange Server lässt sich in Exchange 2007 integrieren, sodass E-Mails, die bereits am ersten Server gescannt worden sind, nicht noch einmal unnötig gescannt werden. Wenn wiederholte Scans während des Transports wegfallen, kann die E-Mail schneller befördert werden, und die Server werden nicht überlastet. Zur Verbesserung der Leistung am Speicherserver werden die Mailboxen selektiv auf nur die wahrscheinlichsten Viren gescannt. Ein solches inkrementales Scannen im Hintergrund setzt Serverressourcen frei, da viele Megabytes alter E-Mails nicht immer wieder unnötig gescannt werden.

### **Vereinfachte Verwaltung entlastet das IT-Personal**

Automatische Signatur- und Modulupdates, Migrationsschutz für Exchange 2007-Server und zentralisierte Kontrolle und Verwaltung reduzieren den Kosten- und Verwaltungsaufwand. Die Microsoft Forefront Server Security Management Console ermöglicht eine zentrale Konfiguration, Bereitstellung und Aktualisierung von Forefront Security for Exchange Server. Zudem wird auch der System Center Operations Manager unterstützt, mit dem die Exchange Server im gesamten Unternehmen überwacht werden können.

\* CSI/FBI-Umfrage 2006.

## Welche Funktionen bietet Microsoft Forefront Security for Exchange Server?

### Umfassender Schutz

- **Multienginescanning, kein Single Point of Failure.** Bis zu fünf Antivirenschamodule können gleichzeitig eingesetzt und verwaltet werden, wobei unterschiedliche Kombinationen für die Exchange 2007-Transportserver (Edge- und Hubserver) und -Speicherserver (Mailbox/Public Folder) möglich sind. Selbst wenn ein Scanmodul offline ist oder eine Bedrohung nicht erkennt, wird die E-Mail noch von den anderen Modulen gescannt; es gibt also keinen Single Point of Failure. Module von AhnLab, Authentium, CA, Kaspersky Labs, Microsoft, Norman Data Defense, Sophos und VirusBuster sind im Lieferumfang enthalten
- **Premiumspamabwehr.** Die Premiumantispamservices von Exchange 2007, darunter der Microsoft-IP-Reputationsfilter sowie Contentfilterung durch die Intelligent Message Filter (IMF) und Antispamsignaturdateien, sind auch über Forefront Security for Exchange Server verfügbar. Diese Spamabwehrtools werden während der Installation aktiviert und mehrmals täglich aktualisiert
- **Schutz auf mehreren Ebenen.** Scans können an verschiedenen Kontrollpunkten installiert und aktiviert werden. Sollte also beispielsweise ein Scan am Edgeserver fehlschlagen, wird die E-Mail nochmals am Hubserver gescannt. Dieser Schutz auf mehreren Ebenen ist eine wichtige Sicherheitsmaßnahme, die dazu beitragen kann, Attacken abzufangen, bevor sie das Netzwerk oder die Produktivität der Endbenutzer beeinträchtigen können
- **Schutz vor neuen und verborgenen Bedrohungen.** Mittels integrierter Heuristiktechnologie kann Schadcode anhand von Verhaltensmustern identifiziert werden, und Dateitypen, die als Virenträger bekannt sind (z. B. .exe), können über konfigurierbare Dateifilterregeln erkannt werden – auch dann noch, wenn die Dateinamenerweiterung geändert worden ist. Forefront Security for Exchange Server kann weiterhin komprimierte Anhänge (z. B. .zip-Dateien) entpacken und diese nach Entfernung eines infizierten oder unerwünschten Objekts selektiv wieder neu packen
- **Abwehr neuer Bedrohungen durch Produkte mehrerer Hersteller.** Forefront Security for Exchange Server bietet bessere Chancen, neue Attacken schnell abzuwehren, da mehrere Sicherheitshersteller daran arbeiten, den Kunden Abwehrmittel gegen die

neuesten Viren bereitzustellen. Durch automatische Downloads wird sichergestellt, dass die erste effektive Lösung, sobald sie verfügbar ist, in das System der Kunden gelangt

### Optimierte Leistung

- **Leistungsoptimierung.** In-Memory-Scanning (Daten müssen nicht auf die Festplatte gespoolt werden) und Multithreadscanning (es können mehr Mails gleichzeitig verarbeitet werden) verbessern die Serverleistung und erhöhen den Maildurchsatz. Forefront Security for Exchange Server ermöglicht dem IT-Personal, mithilfe von Leistungskontrollen für die dynamische Verwaltung und den eingesetzten Modulen für den jeweiligen Scanjob, ein ausgewogenes Verhältnis von Serverleistung und Schutzstufe zu erzielen
- **Effizienteres Scannen während des Transports und im Speicherserver.** Redundante Scans der E-Mail werden eliminiert. Forefront Security for Exchange Server versieht jede E-Mail mit einem AV-Transportstempel, wenn sie erstmals an einem Exchange 2007-Edge- oder Hubserver gescannt wird. Die E-Mail wird dann ohne weitere Scans zugestellt. Dadurch wird die Verarbeitungslast am Hub- und am Speicherserver reduziert. Und durch Einschränkung des Bereichs für Hintergrundscans kann das erneute Scannen von Wochen oder gar Monate alten E-Mails im Speicherserver eliminiert werden. Inkrementale Scans im Hintergrund können so eingestellt werden, dass nur die Objekte gescannt werden, bei denen die Wahrscheinlichkeit einer Infektion am höchsten ist, so z. B. solche, die einige Tage alt sind
- **Keine Unterbrechung des E-Mailflusses während des Updatevorgangs.** Die Signaturdateien der Scanmodule können aktualisiert werden, ohne dass die E-Mail angehalten oder in eine Warteschlange eingereiht werden muss. Wenn ein Scanmodul während eines Updates offline ist, scannen die anderen Module dank der mehrere Scanmodule umfassenden Lösung von Forefront Security for Exchange Server weiter
- **Effektive E-Mail-Clusterunterstützung.** Die E-Mail ist auch dann geschützt, wenn ein Server ausfällt und die E-Mail auf einen anderen Knoten verlagert wird. Forefront Security for Exchange Server sorgt dafür, dass sowohl aktive als auch passive Knoten stets mit neuesten Konfigurationsinformationen und Signaturen aktualisiert werden. Die unterstützten Clusterkonfigurationen umfassen auch Exchange 2007-CCR-Cluster

### Vereinfachte Verwaltung

- **Forefront Server Security Administrator.** Diese integrierte, zentrale Verwaltungskonsole ermöglicht eine komplette Konfiguration von Forefront Security for Exchange Server, entweder vor Ort oder im Remotebetrieb
- **Zentrale webbasierte Verwaltungskonsole.** Wenn Forefront Security for Exchange Server über die Microsoft Forefront Server Security Management Console verwaltet wird, können IT-Administratoren die Server leicht im Remotebetrieb verwalten, umfassende Berichte erstellen und sich ggf. über Ausbrüche in der gesamten Infrastruktur benachrichtigen lassen. Diese browserbasierte Konsole ermöglicht zentrale Konfiguration, Bereitstellung und Aktualisierung für alle Forefront-Serversicherheitsprodukte
- **Automatische Updates aus einer Hand.** Die Aktualisierung der einzelnen Scanmodule kann ohne Intervention durch das IT-Personal erfolgen. Microsoft fragt seine AV-Hersteller regelmäßig nach neuen Signaturen und Modulupdates ab. Diese Updates werden dann innerhalb weniger Minuten an einer Virendatenbank getestet, bestätigt und zum automatischen Download durch Forefront Security for Exchange Server- oder Forefront Server Security Management Console-Systeme ins Netz eingestellt
- **Migrationschutz.** Bei einer Migration zu Exchange 2007 ist die gesamte Messagingumgebung geschützt. Kunden, die Forefront Security for Exchange Server erwerben, um ihre Exchange 2007-Server zu schützen, erhalten auch Lizenzen für Microsoft Antigen for Exchange, Microsoft Antigen for SMTP Gateways und Antigen Spam Manager, sodass sie ihre Microsoft Exchange Server 2003- und Microsoft Exchange Server 2000-Umgebungen schützen können
- **Verfügbar in 11 Sprachen.** Unternehmen können die Sicherheit ihrer Messagingserver in 11 Sprachen verwalten: Chinesisch (traditionell und vereinfacht), Deutsch, Englisch, Französisch, Italienisch, Japanisch, Koreanisch, Portugiesisch (Brasilien), Russisch und Spanisch
- **Integrierte Überwachung.** Mittels eines Management Packs für System Center Operations Manager können Administratoren den Status der mit Forefront Security for Exchange Server überwachten Umgebung im Rahmen der betrieblichen Verwaltungsverfahren des Unternehmens verfolgen

### Systemanforderungen für Microsoft Forefront Security for Exchange Server

Für die vorstehend beschriebenen Features und Funktionen sind Windows Server® 2003, Microsoft Exchange Server 2007, eine x64-Architektur, 512 MB RAM pro Server (1 GB empfohlen) und 300 MB Festplattenspeicher erforderlich. Forefront Security for Exchange Server unterstützt auch Exchange auf Microsoft Cluster Servern.

Weitere Informationen zu Microsoft Forefront Security for Exchange Server finden Sie unter [www.forefront.de](http://www.forefront.de)

