

- **Esclusivo rilevamento in tempo reale dello spamming per una protezione immediata**
- **Blocca fino al 97% di e-mail indesiderate**
- **Riconosce lo spamming indipendentemente da lingua, contenuto o formato dei messaggi**
- **Servizio antispying economicamente vantaggioso**
- **Analisi dello spamming in quarantena**
- **Completamente integrato con Firebox X**
- **Nessun aggiornamento di regole o configurazioni complesse**



Tecnologia eco-compatibile



Stronger Security, Simply Done™

Blocca lo spamming in tempo reale con spamBlocker

Lo spamming, che rappresenta circa il 70% del traffico e-mail globale, è qualcosa di più di un semplice fastidio. Rallenta il traffico della rete, diffonde virus, sparge attacchi di spyware e phishing e induce utenti in buona fede a visitare siti Web sospetti, progettati per raccogliere dati personali o aziendali sensibili. Ora è possibile bloccare lo spamming immediatamente, prima che raggiunga il server di posta interno o il client email, e senza compromettere le prestazioni, aggiungendo il potente spamBlocker di WatchGuard per le appliance UTM (Unified Threat Management) Firebox® X.

Blocco spamming in tempo reale

spamBlocker si basa su un esclusivo rilevamento in tempo reale per fornire una protezione immediata dall'attacco di spamming. È il migliore servizio sul mercato per il riconoscimento in tempo reale degli attacchi di spamming, con una percentuale di e-mail bloccate che raggiunge il 97%.

Blocco indipendente da lingua o formato

spamBlocker utilizza Commtouch® Recurrent Pattern Detection (RPD™), una tecnologia leader del mercato che consente di monitorare Internet rilevando schemi riconoscibili all'interno del traffico e-mail mondiale. Attraverso il blocco e il monitoraggio degli attacchi di spamming appena essi si manifestano, la tecnologia RPD blocca lo spamming indipendentemente da lingua, contenuti e formato del messaggio, compreso lo spamming basato sugli immagini.

Soluzione economicamente vantaggiosa

spamBlocker è completamente integrato in Firebox X, ed elimina quindi la necessità di acquistare e gestire una soluzione antispying aggiuntiva per la propria rete. Non sono necessarie costose licenze per singolo utente: un singolo abbonamento fornisce protezione su tutta la rete per tutti gli utenti configurati a monte del Firebox X.

Impareggiabile facilità di utilizzo

È possibile configurare e mettere in funzione Gateway AV/IPS in pochi minuti: l'interfaccia intuitiva assicura una gestione corrente semplice e lineare. Nelle appliance Firebox X Peak™ e Core™, e nelle appliance Firebox X Edge su reti Peak o Core, Gateway AV/IPS viene gestito tramite il potente WatchGuard System Manager (WSM). Le appliance stand-alone Firebox X Edge utilizzano una intuitiva interfaccia Web.

L'amministratore ha la possibilità di:

- Bloccare*, consentire e contrassegnare i messaggi di posta per una facile identificazione e per l'inoltro alle cartelle dedicate

- Decidere in che modo elaborare i messaggi e quali utenti o gruppi possono ricevere spedizioni di massa
- Utilizzare in modo flessibile whitelist per accettare posta da domini attendibili

**Solo server di posta SMTP*

Quarantena integrata

spamBlocker include una funzione di quarantena* integrata per archiviare i messaggi email sospettati di essere spamming. Gli utenti finali possono esaminare questi messaggi tramite una pagina Web a bassa larghezza di banda, piuttosto che scaricare lo spamming nel proprio client email. In questo modo gli utenti possono personalizzare la protezione dallo spamming, riducendo al tempo stesso le attività di amministrazione IT.

**Disponibile solo per le appliance Firebox X Core e Peak*

Nessun aggiornamento di regole o configurazioni complesse

Dal momento che spamBlocker comunica in maniera protetta e automatica e in tempo reale con Commtouch allo scopo di identificare lo spamming e il traffico legittimo, non è necessario attendere la ricezione di nuove regole antispying per disporre subito del più accurato filtraggio antispying. spamBlocker si affida alla suddivisione in categorie di centinaia di migliaia di e-mail al giorno senza i costi e i tempi lunghi associati al training di un filtro antispying.

Tasso minimo di falsi positivi

I programmi che tentano di definire parole chiave e contenuti in maniera aggressiva allo scopo di rilevare lo spamming spesso determinano un tasso di falsi positivi inaccettabilmente elevato, bloccando le comunicazioni legittime insieme allo spamming. spamBlocker non si affida a parole chiave o ai contenuti per suddividere in categorie lo spamming e le comunicazioni business-critical attraversano la rete mentre le e-mail indesiderate vengono immediatamente bloccate.

Real-time Outbreak Monitor

Point to outbreak for more information



New Outbreaks				
Location:	Subject:	URL:	Massiveness:	Attackers:
United Sta...	never scrub your toi...	.greatcleaners...		37
United Sta...	arrange all your bil...	.jumpshark.com		43

Source: Commtouch Online-Lab



WatchGuard è in partnership con Commtouch, sviluppatore dell'innovativa tecnologia Recurrent Pattern Detection (RPD). Utilizzando sofisticati algoritmi per analizzare in tempo reale il traffico Internet globale alla ricerca di schemi ricorrenti, la tecnologia RPD è in grado di identificare un attacco di spamming non appena esso si manifesta.

Visitare il Real-time Outbreak Monitor all'indirizzo www.watchguard.com/spamblocker

I servizi di protezione in abbonamento potenziano la protezione

Per potenziare la funzionalità di prevenzione attacchi Zero Day del Firebox® X, è possibile aggiungere servizi in abbonamento per raggiungere livelli ancora superiori di protezione. In Firebox X è possibile attivare con facilità i servizi di protezione utilizzando una semplice chiave di licenza. È facile e non è necessario acquistare hardware aggiuntivo. Insieme a spamBlocker, la nostra suite di servizi di protezione include:

- **Gateway AntiVirus/Intrusion Prevention Service:** la potente scansione al gateway basata su firme blocca spyware, virus, worm, trojan horse conosciuti e altro malware prima che siano in grado di penetrare nella rete.
- **WebBlocker:** consente di gestire la navigazione sul Web degli utenti per aumentare la produttività, prevenire eventuali responsabilità e diminuire i rischi per la protezione bloccando l'accesso a contenuti Web nocivi o inappropriati.

Questi servizi in abbonamento completamente integrati sono semplici da distribuire e gestire in Firebox X. Il costo di ogni servizio viene determinato per appliance e non per utente e pertanto un solo abbonamento fornisce protezione per tutta la rete e per tutti gli utenti configurati a monte del Firebox X.

Versione di prova GRATUITA per 30 giorni

È possibile ricevere una versione gratuita di 30 giorni di **Gateway AntiVirus/Intrusion Prevention Service, spamBlocker e WebBlocker** per la appliance Firebox X Peak, Core, o Edge. Per informazioni dettagliate, contattare il proprio rivenditore.

UTM Bundle - Unica soluzione, una sola licenza, un grande prezzo

Tutto il necessario per la gestione unificata delle minacce (UTM), inclusa l'appliance. Ogni bundle offre una convenienza eccezionale e include:

- Appliance di protezione Firebox X Peak, Core o Edge
- Abbonamenti di 1 anno a spamBlocker, Gateway AV/IPS e WebBlocker
- Abbonamento di 1 anno a LiveSecurity® Service per guida e supporto esperti

Firebox® X Peak™ UTM Bundle

Firebox X5500e UTM Bundle	WG55503
Firebox X6500e UTM Bundle	WG56503
Firebox X8500e UTM Bundle	WG58503
Firebox X8500e-F UTM Bundle	WG58513

Firebox® X Core™ UTM Bundle

Firebox X550e UTM Bundle	WG50553
Firebox X750e UTM Bundle	WG50753
Firebox X1250e UTM Bundle	WG51253

Firebox® X Edge UTM Bundle

Firebox X10e UTM Bundle	WG50016
Firebox X20e UTM Bundle	WG50026
Firebox X55e UTM Bundle	WG50061
Firebox X10e Wireless UTM Bundle – Nord America	WG50017
Firebox X10e Wireless UTM Bundle – Internazionale	WG50018
Firebox X10e Wireless UTM Bundle – Cina	WG50019
Firebox X10e Wireless UTM Bundle – Giappone	WG50018-JP
Firebox X20e Wireless UTM Bundle – Nord America	WG50027
Firebox X20e Wireless UTM Bundle – Internazionale	WG50028
Firebox X20e Wireless UTM Bundle – Cina	WG50029
Firebox X20e Wireless UTM Bundle – Giappone	WG50028-JP
Firebox X55e Wireless UTM Bundle – Nord America	WG50062
Firebox X55e Wireless UTM Bundle – Internazionale	WG50063
Firebox X55e Wireless UTM Bundle – Cina	WG50064
Firebox X55e Wireless UTM Bundle – Giappone	WG50063-JP

UTM Software Suite per reti Firebox X

Con un singolo acquisto e a un prezzo eccezionale, è possibile aggiungere la nostra potente suite di servizi di protezione in abbonamento alla rete Firebox X e-Series esistente. UTM Software Suite trasforma Firebox X in una completa soluzione di gestione unificata delle minacce con:

- Abbonamenti di 1 anno a spamBlocker, Gateway AV/IPS e WebBlocker
- Abbonamento di 1 anno a LiveSecurity Service per guida e supporto esperti

Firebox® X Peak™ UTM Software Suite

Firebox X5500e UTM Software Suite	WG017449
Firebox X6500e UTM Software Suite	WG017450
Firebox X8500e UTM Software Suite	WG017451
Firebox X8500e-F UTM Software Suite	WG017452

Firebox® X Core™ UTM Software Suite

Firebox X550e UTM Software Suite	WG017446
Firebox X750e UTM Software Suite	WG017447
Firebox X1250e UTM Software Suite	WG017448

Firebox® X Edge UTM Software Suite

Firebox X10e UTM Software Suite	WG017453
Firebox X10e-W UTM Software Suite	WG017456
Firebox X20e UTM Software Suite	WG017454
Firebox X20e-W UTM Software Suite	WG017457
Firebox X55e UTM Software Suite	WG017455
Firebox X55e-W UTM Software Suite	WG017458

spamBlocker - Requisiti di sistema

Firebox X Edge

Software appliance	v8.6
Amministrazione	Windows 2000, Windows NT, Windows XP o Windows Vista per supportare WatchGuard System Manager o l'interfaccia Web
Supporto	Abbonamento LiveSecurity Service attivo

Firebox X Peak o Core

Software appliance	Fireware® 9.1
Amministrazione	Windows 2000, Windows NT, Windows XP o Windows Vista per supportare WatchGuard System Manager
Supporto	Abbonamento LiveSecurity Service attivo

Per maggiori informazioni su spamBlocker, visita: www.watchguard.com/services

E-MAIL: italy@watchguard.com · VENDITE: +39-335-7030721 · WEB: www.watchguard.com