

Panda GateDefender Performa

LA PRIMA LINEA DI DIFESA



La rete di ogni azienda che si collega a Internet è esposta al rischio di minacce legate ai contenuti.

Il 99% circa delle infezioni che colpisce le reti aziendali è trasmesso tramite Internet. Il 70% di tutto il traffico Internet che interessa le aziende è inappropriato o non adatto alla produzione.

Oggi una delle principali preoccupazioni per le organizzazioni è la perdita di dati sensibili.

Il primo strumento di difesa contro le minacce provenienti dai contenuti è una soluzione di protezione perimetrale in grado di bloccare in modo preventivo tutti i contenuti indesiderati o pericolosi e impedire la perdita di informazioni critiche.

"È una questione di sopravvivenza per tutti i fornitori AV che sono sempre più alla ricerca di soluzioni per reinventarsi mentre i loro prodotti cercano di bloccare nuovi tipi di infezioni. I servizi basati su cloud e sull'"Intelligenza collettiva" sono il passo necessario per combattere il malware. Per sopravvivere, credo che ogni fornitore AV dovrà adottare un approccio del genere". Andrew Jaquith, gruppo Yankee

La soluzione: Panda GateDefender Performa

Panda GateDefender Performa è un dispositivo scalabile ed estremamente affidabile per la protezione perimetrale, offre la massima protezione della rete aziendale contro tutte le minacce basate sul contenuto ed è facilmente integrabile in qualsiasi tipo di rete senza dover adattare l'architettura esistente.

Offre massima protezione grazie all'"Intelligenza Collettiva" per combattere tutti i rischi in ingresso e in uscita nel perimetro della rete aziendale. Panda GateDefender Performa prevede cinque tipi di protezione:

- **Filtro antimalware:** protegge automaticamente contro tutti i tipi di software dannoso.
- **Content Filter:** consente la definizione di differenti criteri di protezione aziendale dai contenuti inappropriati.
- **Protezione antispam:** protegge la posta elettronica dai messaggi di posta indesiderata.
- **Protezione per le applicazioni di instant messaging e P2P:** impedisce l'utilizzo non appropriato delle risorse della rete aziendale.
- **Protezione filtro dei contenuti Web:** limita l'accesso alle pagine Web con contenuto non adatto alla produzione.



Indipendentemente dalle dimensioni della rete o dal flusso di traffico, sono disponibili quattro modelli hardware per soddisfare le esigenze di protezione dell'azienda:

Traffic flow	GateDefender Performa 9050	GateDefender Performa 9100	GateDefender Performa 9200	GateDefender Performa 9500
HTTP (Mbps)	275	320	420	510
SMTP (messages/s)	115	135	200	220
Concurrent connections	600	1800	3600	7200

One step ahead...

"Entro il 2010, le soluzioni più adeguate dovranno offrire la scansione in ingresso sui protocolli per bloccare i contenuti inappropriati e la scansione in uscita tra i protocolli".

Gartner

Panda GateDefender Performa ha operato in questo modo da quando è apparso la prima volta sul mercato nel 2004, confermando la leadership e l'innovazione di Panda Security.

Benefici

- **Rafforza il sistema di gestione del rischio** in quanto è estremamente efficace nel rilevare e pulire le minacce sconosciute presenti nel perimetro senza alcun intervento da parte dell'amministratore.
- **Migliora la produttività dei dipendenti** grazie alla rimozione dello spam dall'e-mail aziendale, limitando l'utilizzo delle applicazioni di messaggistica istantanea e di condivisione dei file e controllando i contenuti Web a cui hanno accesso gli utenti.
- **Contribuisce a garantire la conformità alle normative di legge:** impedendo la perdita di dati sensibili con criteri di protezione personalizzati in base alle esigenze dei singoli utenti.
- **Elimina la necessità di infrastrutture IT complesse** poiché funziona come bridge trasparente, consentendo l'installazione semplice senza modificare l'architettura di rete.
- **Garantisce la continuità dell'attività aziendale** bloccando il traffico superfluo (circa il 70% di tutto il traffico) e ottimizzando l'utilizzo della banda.
- **Riduce i costi operativi** grazie agli aggiornamenti continui che consentono al dispositivo di funzionare in modo automatico già subito dopo l'installazione.

Funzionalità chiave

- **Tecnologia preventiva integrata:** i motori euristici, l'"Intelligenza collettiva" e la quarantena lavorano unite nel perimetro per ottimizzare il rilevamento delle minacce e garantire la protezione delle informazioni sensibili.
- **Protezione completa:** la protezione perimetrale contro le minacce basate sui contenuti Web offre la migliore protezione contro malware e contenuto potenzialmente pericoloso (Panda); spam (Cloudmark) e contenuto Web non adatto alla produzione (Cobion). Il dispositivo limita inoltre l'utilizzo di applicazioni potenzialmente pericolose quali i programmi di messaggistica istantanea (IM) e P2P.
- **Criteri di protezione flessibili:** è possibile creare e definire differenti profili utente e gruppi per stabilire criteri di protezione specifici per ogni utente della rete, rafforzando in tal modo il sistema di gestione del rischio. Tutti i contenuti in ingresso e in uscita vengono analizzati in base al tipo di contenuto e al profilo specifico di ogni mittente o destinatario.
- **Connessione immediata:** il dispositivo può essere configurato offline e diventa operativo non appena viene collegato, riducendo in tal modo i costi operativi.
- **Bilanciamento del carico/alta disponibilità:** analizza grandi quantità di traffico. Le performance sono sempre eccellenti grazie al bilanciamento del carico automatico e nativo che assicura un'elevata disponibilità del servizio in caso di guasto imprevisto.
- **Protezione automatica:** gli aggiornamenti continui delle firme e dei report grafici in tempo reale garantiscono il funzionamento automatico del dispositivo già subito dopo l'installazione.
- **Amministrazione centralizzata:** tutti i moduli di protezione della rete possono essere configurati da una singola console.
- **Monitoraggio centralizzato:** i report definiti dall'amministratore per tutti i moduli di protezione sono disponibili da una singola console.
- **Flusso di traffico garantito:** l'opzione di bypass impedisce l'interruzione del flusso di dati in caso di guasti del sistema, assicurando in tal modo continuità per l'attività aziendale.

PANDA
SECURITY

One step ahead.

Protezione del perimetro

L'hardware e il software di Panda GateDefender Performa sono stati progettati per offrire elevate performance e massima protezione nel principale punto di immissione delle informazioni nelle reti aziendali. Analizza i protocolli più diffusi: HTTP, FTP, SMTP, POP3, IMAP4 e NNTP.

Protezione preventiva completa

Panda GateDefender Performa rileva e blocca tutti i tipi di minacce che viaggiano in Internet prima che entrino nella rete. Protegge il sistema da

Virus	Worm	Spyware
Phishing	Dialer	Strumenti di hacking
Trojan	Joke	Rischi per la sicurezza

Grazie al motore euristico genetico e all'"Intelligenza Collettiva" di Panda, è inoltre in grado di rilevare malware sconosciuto.

Security Compliance

Il filtro del contenuto Web consente agli amministratori di rete di definire criteri di protezione personalizzati. È possibile configurare filtri per file e messaggi di posta elettronica e applicati a destinatari o mittenti specifici. In questo modo si impedisce la perdita di dati sensibili e si eliminano altri potenziali rischi.

Filtro antispam

Il modulo antispam incluso in Panda GateDefender Performa migliora la produttività bloccando lo spam prima che entri nella rete.

Utilizzo ottimizzato di Internet

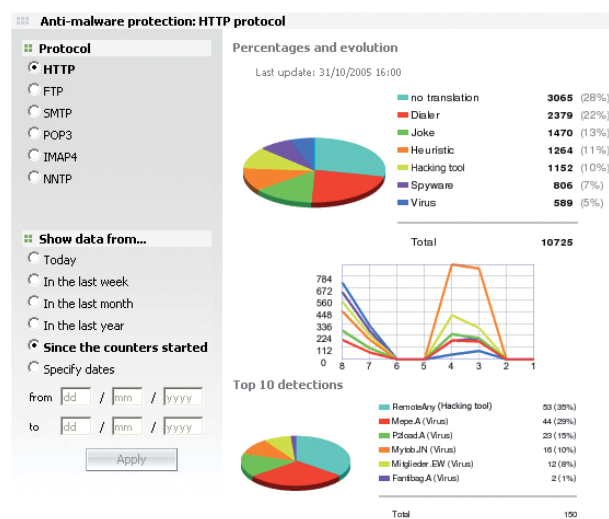
Il filtro del contenuto Web ottimizza la produttività degli utenti della rete in quanto impedisce l'accesso a pagine Web dal contenuto inappropriato o non inerente all'attività lavorativa.

Utilizzo efficace delle risorse

Panda GateDefender Performa può bloccare le applicazioni P2P (peer-to-peer) e di messaggistica istantanea (IM), ottimizzando l'utilizzo delle risorse di rete.

Monitoraggio del sistema in tempo reale

La console offre report grafici in tempo reale sull'attività di ogni modulo di protezione. È inoltre possibile configurare report periodici riepilogativi per ogni tipo di protezione.



Amministrazione centralizzata

Tutti i moduli di protezione disponibili possono essere configurati da una singola console.

Criteri di protezione per ogni utente

Panda GateDefender Performa è integrabile con LDAP e Active Directory. La possibilità di definire profili utente e gruppi consente agli amministratori di assegnare differenti criteri di protezione per gli utenti in base alle esigenze specifiche.

Disponibilità delle informazioni garantita

Panda GateDefender prevede tre tipi di quarantena:

- Quarantena per file che non possono essere puliti o che possono contenere malware sconosciuto
- Quarantena per spam o probabile spam
- Quarantena per file bloccati dai criteri di protezione

L'accesso alla quarantena consente l'eliminazione o il recupero dei file archiviati. I file sospetti vengono inviati a PandaLabs per essere puliti e quindi recuperati in modo automatico.

Connessione immediata

Il dispositivo opera in modalità bridge trasparente, senza necessità di reindirizzare il traffico di rete. È configurata prima dell'installazione e viene controllata tramite una console Web.

Monitoraggio centralizzato

Il sistema invia notifiche personalizzate tramite SMTP, SNMP e/o Syslog. Gli amministratori possono scegliere il metodo da utilizzare per ogni tipo di evento.

Elevata scalabilità

Panda GateDefender Performa garantisce un bilanciamento del carico automatico e nativo per l'ottimizzazione delle operazioni di rete.



Flusso di traffico garantito

I modelli hardware per le organizzazioni di grandi dimensioni includono un'opzione di bypass per assicurare la continuità del flusso di traffico in caso di guasto del sistema.

