

Quali sono le funzionalità principali del motore antispam di Cisco Email Security Appliance (ESA)?

Cisco Anti-Spam è in grado di bloccare la più ampia gamma di minacce a livello mondiale

- Progettato appositamente per identificare le minacce note, tra cui spam, phishing e attacchi originati da zombie, nonché minacce nuove e in evoluzione
- L'unica soluzione per combinare i sistemi di e-mail e di reputazione Web per rilevare minacce miste. A differenza delle tecniche basate sui contenuti, questi sistemi di reputazione sono indipendenti dalla lingua.
- L'accesso in tempo reale a Sender Base, la rete di monitoraggio del traffico web e della posta elettronica più grande al mondo, determina l'identificazione di nuove minacce non appena queste iniziano.
- Progettato e gestito da un team di esperti di sicurezza altamente qualificati. Il personale di ricerca locale in Asia, Europa e America Latina contribuisce al collaudo e alla formazione dei sistemi
- Basato sull'esclusivo Context Adaptive Scanning Engine (CASE) di Cisco, che combina tecniche orientate ai contenuti e indipendenti dai contenuti, evitando classificazioni errate basate su uno stretto contesto dei messaggi.
- Supportato 24 ore su 24, 7 giorni su 7 dal Threat Operations Center per garantire l'analisi dei messaggi a loop chiuso.

Cisco Anti-Spam non comporta alcun sovraccarico amministrativo

- Configurare e dimenticare, con una GUI facile da usare.
- Nessuna necessità di ottimizzazione, training o scrittura di filtri.
- Consente agli utenti finali di concentrarsi sulle attività aziendali principali anziché rivedere manualmente i messaggi.

Cisco Anti-Spam offre prestazioni leader del settore

- Cisco aggiorna dinamicamente l'ordine in cui le regole vengono eseguite utilizzando il nostro algoritmo di uscita anticipata in attesa di brevetto per eliminare la scansione non necessaria.
- Cisco trasferisce quante più analisi possibile al cloud di rete utilizzando il punteggio abilitato per la rete, riducendo i requisiti di elaborazione.
- I messaggi vengono scansati una sola volta per rilevare più minacce, ottimizzando il throughput complessivo delle nostre appliance.