Cisco Web Security Appliance (WSA) fornisce la protezione da malware e spyware?

Sommario

Domanda

Cisco Web Security Appliance (WSA) fornisce la protezione da malware e spyware?

Cisco Web Security Appliance (WSA) offre la protezione gateway più completa del settore contro spyware e malware basato sul Web. Ciò include tutto, da Adware (che causa i problemi di supportabilità più elevati e consuma notevoli risorse di rete) a minacce più dannose come Trojan, Hijackers del browser, Oggetti helper del browser, Phishing, Pharming, Monitor di sistema, Keylogger, Worm, ecc.

I principali elementi di differenziazione della soluzione Cisco Web Security includono:

1. Un monitor integrato per il traffico di layer 4 (L4) esegue la scansione di tutte le porte alla velocità wire-speed, rilevando e bloccando malware e attività "phone-home". Tenendo traccia di tutte le 65.535 porte di rete, L4 Traffic Monitor blocca in modo efficace il malware che tenta di ignorare la porta 80 e impedisce anche le attività P2P e IRC non autorizzate.
2. Elaborazione livello proxy: Cisco Web Security Appliance include anche un proxy Web a prestazioni estremamente elevate, oltre a funzionalità integrate di cache e accelerazione dei contenuti. Basato sul sistema operativo proprietario di Cisco, AsyncOS, l'accessorio proxy Web Cisco è in grado di supportare fino a 100.000 connessioni simultanee, 10 volte più dei tradizionali server proxy basati su UNIX. Essere un proxy Web consente un'ispezione completa dei contenuti a livello dell'applicazione, un requisito fondamentale per garantire l'accuratezza contro il malware basato sul Web.
3. I primi filtri di reputazione Web del settore forniscono un potente livello esterno di difesa. Sfruttando SenderBase®, i filtri Cisco Web Reputation analizzano oltre 50 diversi parametri relativi al traffico Web e alla rete per valutare accuratamente l'affidabilità degli URL. Per pesare singolarmente ogni parametro e generare un singolo punteggio su una scala da -10 a +10 vengono utilizzate tecniche sofisticate di modellazione della sicurezza. I criteri configurati dall'amministratore vengono applicati in modo dinamico in base ai punteggi della reputazione.
4. Scansione accelerata delle firme mediante il motore di streaming e vettorizzazione dinamica (DVS Engine). A differenza delle soluzioni di architettura legacy che si basano su ICAP e su un'implementazione multi-box per garantire la scansione dei malware, Cisco WSA ha introdotto DVS Engine per una soluzione di scansione integrata on-box. Questa piattaforma innovativa impiega sofisticate tecniche di analisi e vettorizzazione degli oggetti, insieme alla scansione in streaming e alla memorizzazione dei verdetti nella cache, con un conseguente

aumento fino a 10 volte della velocità di scansione rispetto alle soluzioni basate su ICAP di prima generazione.

5. Il sistema antimalware Cisco, leader del settore, sfrutta il motore DVS e diversi tipi di firma di Webroot per fornire la migliore protezione contro la più ampia varietà di minacce basate sul Web. Queste minacce possono spaziare da attacchi adware, dirottatori di browser, phishing e pharming a minacce più dannose come trojan, monitor di sistema e keylogger. WSA offre il più grande database di firme malware del settore sul gateway.