Panoramica

Vantaggi

- **Protezione continua e in tempo reale contro le minacce** attraverso il controllo continuo 24 ore su 24, 7 giorni su 7 del traffico globale.
- **Migliore monitoraggio e analisi** della rete estesa prima, durante e dopo un attacco.
- **Soluzione facile da implementare** grazie agli aggiornamenti automatici e alle opzioni di implementazione semplici, veloci e flessibili.
- **Controllo accurato delle policy e del comportamento degli utenti** con visibilità completa sensibile al contesto da un'unica interfaccia di gestione.
- **Costi ridotti** grazie all'integrazione con l'infrastruttura di sicurezza esistente.
- **Risparmio di tempo per il reparto IT** dato dal minor numero di dispositivi da gestire, supportare e amministrare.

Cisco Web Security Appliance

Figura 1. Protezione in tutte le fasi dell'attacco

La sicurezza solida e integrata per tutta la rete

Le tecnologie Web interattive di oggi offrono alle aziende modi sempre più innovativi per promuovere i prodotti, interagire con clienti e fornitori, lavorare in maniera più produttiva e ridurre i costi. Tuttavia, queste tecnologie non sono prive di vulnerabilità, che espongono le stesse aziende a rischi per la sicurezza non trascurabili. Per contrastare le minacce sempre più sofisticate per la sicurezza Web, c'è bisogno di proteggere e controllare non solo tutti gli endpoint, ma anche le altre risorse della rete, compresi i dispositivi mobili, le applicazioni mobili, le applicazioni Web e i browser Web.

Cisco® Web Security Appliance (WSA) integra la protezione anti-malware avanzata, la visibilità e il controllo delle applicazioni, la gestione delle policy per l'uso consentito, la reportistica dettagliata e la mobilità sicura, tutto in un'unica piattaforma facile da gestire. Cisco WSA non solo aiuta le aziende ad adattarsi alle nuove esigenze di sicurezza e controllo del traffico Web, ma è anche più semplice da implementare, richiede meno attività di manutenzione, comporta spese operative inferiori e offre latenza ridotta. Nelle reti ampie, Cisco Web Security Virtual Appliance (WSAV) consente di implementare la sicurezza Web dove e quando è necessario.

Caratteristiche principali e componenti della soluzione

Le funzionalità presenti in entrambi i modelli sono:

Cisco Talos

Il sistema di intelligence delle minacce in tempo reale più grande del settore fornisce avvisi tempestivi e l'analisi delle vulnerabilità: 100 terabyte (TB) di dati sulla sicurezza al giorno, 13 miliardi di richieste Web al giorno, 150 milioni di endpoint e 1,6 milioni di dispositivi di sicurezza supportati. Cisco SIO e Sourcefire VRT sono i due servizi di rilevamento delle minacce nel cloud che formano Talos. Cisco Talos riceve gli aggiornamenti automatici ogni 3-5 minuti, fornendo la protezione continua e in tempo reale contro le minacce.

Filtri di reputazione Web di Cisco

Insieme all'intelligence sulle minacce di Cisco Talos, i filtri di reputazione Web di Cisco offrono la protezione dal malware Web di tipo zero-day usando la reputazione dinamica. La funzionalità seleziona in tempo reale il motore di analisi più appropriato in base alla reputazione dell'URL, al tipo di contenuto e all'efficacia del motore di analisi. Inoltre migliora il numero dei rilevamenti eseguendo prima l'analisi degli oggetti ad alto rischio quando il carico delle analisi è superiore.

Advanced Malware Protection

Advanced Malware Protection (AMP) è una funzionalità aggiuntiva concessa in licenza a tutti i clienti che acquistano Cisco WSA. AMP potenzia le funzionalità di rilevamento e blocco del malware già presenti in Cisco WSA con capacità di valutazione della reputazione dei file, reportistica dettagliata sul comportamento dei file, analisi continua dei file e avvisi di verdetti retrospettivi. Sfrutta le vaste reti di intelligence di sicurezza nel cloud di Cisco e Sourcefire (ora parte di Cisco).

Monitoraggio del traffico del layer 4

Il monitoraggio del traffico del layer 4 analizza continuamente le attività, rilevando e bloccando le comunicazioni "phone-home" dello spyware. Tenendo traccia di tutte le applicazioni di rete, questa funzionalità blocca in modo efficace il malware che tenta di eludere le soluzioni di sicurezza Web tradizionali. Inoltre, aggiorna dinamicamente il proprio elenco di entità dannose con gli indirizzi IP dei domini di malware noti.

Protezione degli utenti in roaming

Cisco WSA protegge i dati richiesti dai laptop che usano il roaming attivando una VPN che reindirizza il traffico dei dati sensibili all'access point Web principale per l'analisi in tempo reale, prima di consentire l'accesso. In più, l'integrazione di Cisco WSA con Cisco Identity Services Engine (ISE) permette agli amministratori di creare una policy in Cisco WSA basata sulle informazioni del profilo o dell'appartenenza ai gruppi raccolte da Cisco ISE.

Application Visibility and Control

La funzionalità di ispezione sensibile al contesto permette di applicare le policy e controllare il comportamento delle applicazioni e degli utenti da una singola interfaccia di gestione intuitiva. È possibile definire facilmente le policy per controllare l'uso di centinaia di applicazioni Web 2.0 e oltre 150.000 microapplicazioni. Così facendo, diventa possibile utilizzare applicazioni come Facebook o Dropbox e al tempo stesso impedire agli utenti di svolgere certe attività, come l'uso della chat o il caricamento di documenti. I clienti possono anche definire le quote di tempo e di larghezza di banda personalizzate per utente, gruppo e policy.

Controlli Cisco per l'uso del Web

Questi controlli integrano il filtro URL tradizionale con un database di URL aggiornato dinamicamente per difendere dai rischi legati a conformità, responsabilità legale e produttività. Il motore Cisco Dynamic Content Analysis (DCA) analizza il contenuto delle pagine alla ricerca di URL sconosciuti per classificarli in tempo reale. Le classificazioni vengono aggiornate in modo dinamico ogni 3-5 minuti da Cisco Talos.

Data Loss Prevention

Le regole di Data Loss Prevention (DLP) basate sul contesto impediscono ai dati riservati di uscire dalla rete. Cisco WSA utilizza Internet Content Adaptation Protocol (ICAP) per l'integrazione con soluzioni DLP di terze parti per fornire la protezione avanzata.

Implementazione semplice

Cisco WSA è una soluzione completa che semplifica l'implementazione tramite l'integrazione di varie funzionalità di sicurezza Web in una singola appliance. Grazie all'architettura semplificata, Cisco WSA taglia i costi dell'IT riducendo il numero di dispositivi da gestire, supportare e amministrare. Nelle reti ampie, Cisco Web Security Virtual Appliance consente di implementare le sicurezza Web dove e quando è necessario.

Ulteriori informazioni

Per ulteriori informazioni su Cisco Web Security Appliance, visitare http://www.cisco.com/go/wsa.

Per scoprire i potenziali benefici di Cisco WSA per la propria azienda, contattare un rappresentante di vendita, un partner di canale o un tecnico sistemista Cisco.

C45-730937-01 10/14