McAfee Web Gateway Cloud Service

Tramite il cloud la sicurezza web protegge ovunque

Vantaggi principali

- La sicurezza web dal rapporto costi/benefici più conveniente, senza bisogno di hardware o software in sede.
- Va oltre la protezione di base: l'emulazione del comportamento previene il malware del giorno zero in pochi millisecondi, mentre viene elaborato il traffico.
- Protezione estesa per gli utenti fuori rete. Il cloud cancella il tradizionale perimetro della rete.
- Efficienza di gestione senza paralleli grazie alla piattaforma McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud come console di gestione unificata per tutti i servizi nel cloud di Intel Security.
- Architettura collaudata: McAfee® Web Gateway Cloud Service si fonda su una versione multitenant di McAfee Web Gateway, l'appliance in sede scelta dalle aziende di tutto il mondo.

La difesa contro le sofisticate minacce del web richiede una tecnologia avanzata, ma senza aumentare costi e complessità. La sicurezza web dal cloud permette ai team della sicurezza di ottenere gli stessi vantaggi della protezione dalle minacce avanzate offerta dalle appliance in sede, ma senza il costo dell'hardware e delle risorse necessarie per mantenerlo. Dato che l'accesso al web viene sempre di più eseguito fuori dal perimetro della rete, il cloud diviene il punto di contatto continuo per dispositivi e utenti in movimento. Anziché proteggere il traffico che arriva a un unico sito, è più efficiente metterlo in sicurezza quando esce dall'endpoint. La connessione al cloud degli endpoint, o addirittura di sedi intere, offre protezione ovunque, creando all'esterno della rete un nuovo perimetro dal quale non si esce mai.

Protezione ubiqua e dal costo efficiente

La gestione delle appliance di sicurezza web in sito è costosa e distoglie da altre attività gli addetti alla sicurezza, già oberati di lavoro. La distribuzione della sicurezza web come servizio cloud abbassa il costo totale di proprietà. Non più appliance hardware da acquistare, possedere e mantenere. Tutte le risorse precedentemente usate per la manutenzione delle appliance, costituita da upgrade e applicazioni di patch, possono essere riassegnate a iniziative più strategiche nel reparto informatico o della sicurezza.

Nella distribuzione ibrida si possono usare sia l'appliance che il servizio cloud. La maggior parte delle aziende sceglie questo modello per mantenere la titolarità e il controllo della appliance in rete, oltre che per estendere la protezione cloud ai piccoli uffici remoti e agli utenti in viaggio.

I team informatici che reinstradano il traffico dagli uffici remoti sui circuiti Multiprotocol Label Switching (MPLS) per il filtraggio da parte di un'appliance gateway web posta sulla rete, traggono immediatamente vantaggio dalla sicurezza web fornita tramite il cloud. Il reinstradamento del traffico è costoso e aggiunge complessità alla rete. Invece, gli uffici remoti possono passare direttamente per il cloud al fine di proteggersi, eliminando i circuiti MPLS e semplificando l'architettura di rete.

Infine, l'accesso dei dipendenti al web non è più limitato al perimetro, che lasciava gli utenti e dispositivi fuori rete privi di protezione e invisibili al reparto IT. Il passaggio della sicurezza web al cloud inverte il perimetro. Il traffico web proveniente dagli utenti e dispositivi fuori rete può essere automaticamente instradato dall'endpoint al cloud, mantenendo la connessione sicura quando si lavora da casa, da un aeroporto,

da un caffè o da qualsiasi altro luogo all'esterno della rete. La rete non è più concentrata sul traffico interno ai confini fisici, ma si estende al di fuori, ovunque si sposti un endpoint.

Architettura globale ad alte prestazioni

McAfee Web Gateway Cloud Service, studiato per la grande impresa, permette a molte organizzazioni di aumentare notevolmente le prestazioni attualmente rilevate in sede. Per esempio, in sede, quando c'è bisogno di aumentare la capacità, il reparto IT deve procurarsi e installare una nuova appliance, il che può richiedere giorni o settimane. Nel nostro cloud per gli aumenti di capacità occorrono circa 15 minuti, grazie all'elasticità con cui è progettato il servizio.

Quando un'appliance in sede si guasta e necessita di una riparazione, può rendere non disponibile Internet oppure danneggiare lo stato della sicurezza, se in caso di guasto rimane aperta. Nell'eventualità di un guasto presso uno dei nostri centri dati, il servizio cloud reinstrada automaticamente tutto il traffico web verso il centro dati più vicino e più veloce, assicurando immediatamente la continuità.

La nostra architettura di servizio nel cloud è inoltre progettata per comunicare con la dorsale di Internet presso i maggiori punti di interscambio (IXP). Ciò elimina i salti di reinstradamento dei provider Internet (ISP) intermedi, che non fanno altro che aggiungere latenza alla connessione. Con meno salti verso i principali fornitori di contenuti come Microsoft Office 365 e Google, tramite il nostro servizio nel cloud gli utenti ottengono spesso una connessione più rapida che se si connettessero direttamente all'Internet aperto.

McAfee Web Gateway Cloud Service è globale. Per visualizzare sedi attuali e lo stato dei centri dati in cui viene elaborato il traffico web, visita **https://trust.mcafee.com**. Il contenuto web può essere inviato nella lingua locale così, a prescindere da dove si connette, un utente può vedere i risultati di ricerca locali di Google.

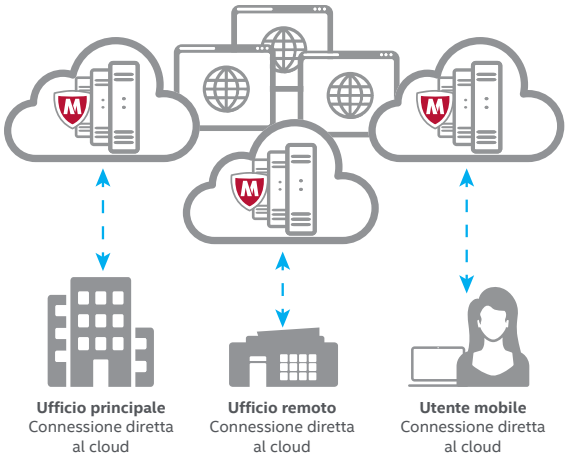

Figura 1. Distribuzione di McAfee Web Gateway Cloud Service.

Protezione contro le minacce sofisticate

I team della sicurezza spesso non riescono a tenere il passo con il malware altamente sofisticato e gli attacchi mirati che eludono le difese tradizionali, drenano risorse e provocano una costante situazione di emergenza per correggere gli endpoint. A differenza del tradizionale filtraggio URL e dei metodi basati sulle firme per la prevenzione delle minacce web, McAfee Web Gateway Cloud Service protegge gli endpoint dal malware del giorno zero e di quello senza file, tramite l'emulazione in linea di file, JavaScript e HTML. Ciò consente di prevenire il malware del giorno zero prima che raggiunga un utente. I tassi di blocco aumentano inoltre di circa il 20% rispetto al filtraggio URL e alla soluzioni basate sulle firme. Le operazioni di sicurezza traggono vantaggio dai costi inferiori e dalla maggiore flessibilità delle risorse, riducendo il numero complessivo degli eventi legati al malware.

Le minacce web vengono spesso inviate tramite il traffico cifrato, per occultarlo alle difese di sicurezza web. Quasi tutte le applicazioni cloud, come l'archiviazione nel cloud o i media sociali, usano il traffico cifrato per impostazione predefinita. McAfee Web Gateway Cloud Service decifra completamente e ispeziona il traffico HTTPS crittografato, consentendo di prevenire il malware e dando visibilità alle applicazioni cloud nei canali crittografati.

Dove si trova McAfee Web Gateway Cloud Service?
Visita **https://trust.mcafee.com** per gli aggiornamenti in tempo reale e la visibilità sui siti dei centri dati, lo stato della disponibilità e molto altro.

Per la maggior parte degli addetti informatici è difficile controllare la proliferazione delle applicazioni cloud, particolarmente dello "shadow IT" e dei rischi causati dai servizi scelti dagli utenti. Con la piena visibilità in tutto il traffico web, compreso quello HTTPS, i report preincorporati mostrano i siti web visitati, le applicazioni cloud usate e i corrispondenti punti dati, al fine di valutare i rischi. Lo Shadow IT viene facilmente scoperto confrontando ciò che viene effettivamente usato con ciò che è stato proibito dal reparto IT. Le applicazioni cloud, specialmente quelle per l'archiviazione, sono sempre più usate anche come meccanismi di invio del malware. L'identificazione delle applicazioni che hanno portato il malware può informare le decisioni sulle policy aziendali. Con la visione completa di quali servizi cloud vengono usati, si possono applicare oltre 1600 controlli delle applicazioni cloud, che minimizzano i rischi prevenendo caricamenti e messaggistica oppure bloccando totalmente le applicazioni.

Gestione efficiente della sicurezza

La gestione della sicurezza su svariate console e per molteplici policy è gravosa, specialmente quando la protezione web in sede e quella basata sul cloud vengono gestite separatamente. In un ambiente ibrido c'è una sola console di gestione per le distribuzioni in sede e nel cloud, una singola serie di policy e una sola interfaccia per la reportistica.

Quando impiegato da solo, senza hardware o software in sede, McAfee Web Gateway Cloud Service viene gestito insieme alla sicurezza endpoint da McAfee ePO Cloud, la console di gestione unificata per tutti i servizi di sicurezza basati sul cloud di Intel Security, dando un'efficienza senza precedenti alla gestione della sicurezza.

Fornire la sicurezza web ai dispositivi endpoint è difficile, specialmente per quanto riguarda instradamento e autenticazione. McAfee Client Proxy, un client endpoint opzionale, automatizza l'instradamento e l'autenticazione verso il nostro servizio cloud, assicurando una connessione pervasiva nel cloud con una coerente imposizione delle policy. McAfee Client Proxy funziona senza problemi in un ambiente ibrido con appliance in sede, instradando in maniera intelligente il traffico nella rete verso l'appliance e quello fuori rete verso il servizio cloud. Sono disponibili ulteriori opzioni di instradamento e autenticazione, selezionabili a seconda delle necessità dell'organizzazione.

Ulteriori informazioni

Ulteriori informazioni sono disponibili sul sito **mcafee.com/it/products/web-protection.aspx**.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com