McAfee Enterprise Log Manager

Riduci i costi di conformità grazie a raccolta, archiviazione e gestione automatiche.

Acquisendo e memorizzando i log in modo appropriato, il costo della conformità si riduce con una chiara registrazione di tutte le operazioni effettuate che non può essere messa in dubbio. McAfee® Enterprise Log Manager acquisisce, comprime e memorizza tutti i file di log. L'integrazione con McAfee Enterprise Security Manager fornisce funzionalità avanzate di ricerca, analitica, correlazione, segnalazione e reportistica. Tutti gli eventi e gli avvisi forniscono un semplice accesso one-clic al file di log della fonte originale, così che anche le attività di analisi ne traggano beneficio.

Se si tratta di un file di log, McAfee Enterprise Log Manager lo acquisisce, lo firma e lo memorizza. McAfee automatizza la gestione e l'analisi dei log per tutte le tipologie di log, inclusi i log relativi agli eventi di Microsoft Windows, ai database, alle applicazioni e i syslog. I log vengono firmati e convalidati, assicurandone l'autenticità e l'integrità, una necessità per la conformità con le normative. Una serie di regole e report predefiniti per la conformità semplificano la dimostrazione che l'azienda è conforme e le policy sono state applicate.

Utilizzando questo ambiente integrato di raccolta, gestione e analisi dei log permette di rafforzare il profilo di sicurezza e migliora in modo significativo la capacità dell'azienda di adempiere a standard quali PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA e SOX.

Gestione intelligente dei log

McAfee Enterprise Log Manager acquisisce i log in modo intelligente, memorizzando i log corretti per la conformità e analizzando i log corretti per la sicurezza. È possibile conservare i log nel loro formato originale per il tempo necessario a soddisfare le specifiche esigenze di conformità. Dal momento che i file di log originali non vengono alterati, McAfee supporta la catena di custodia e le attività di non-repudiation.

Le esigenze in termini di conservazione delle informazioni dipendono dalla fonte del log e dai differenti requisiti di conformità che si devono soddisfare. McAfee Enterprise Log Manager utilizza pool di storage facilmente personalizzabili per

Vantaggi principali

- Acquisizione e conservazione di log universali per soddisfare i requisiti di conformità
- Memorizzazione e conservazione flessibile appropriata per la fonte di ogni log
- Supporta la catena di custodia (CoC) e l'analisi
- Analisi dei log e ricerca
- Memorizza i log localmente o tramite una rete SAN (Storage Area Network) gestita
- Completamente integrato con McAfee® Enterprise Security Manager
- Opzioni di distribuzione ibride flessibili includono appliance fisiche e virtuali

garantire che i log siano memorizzati in modo corretto e per il corretto periodo di tempo. Scegli la miglior opzione di archiviazione per le tue esigenze: storage su disco utilizzabile sulle appliance e schede fiber channel opzionali per reti SAN ad alta velocità.

I file di log da soli non ci dicono tutto ciò di cui abbiamo bisogno. Contengono elementi di prova importanti e sono un collegamento fondamentale per stabilire la catena di custodia, ma sollevano anche nuove domande. Per esempio, possiamo vedere un nome utente in un log di accesso, ma non sono presenti informazioni sul ruolo o i privilegi di quell'utente. Potremmo anche sapere a quale sistema si è avuto accesso, ma potremmo non sapere nulla su quali tipi di informazione vengono utilizzati da quel sistema o chi dovrebbe avervi accesso.

Integrato con McAfee Enterprise Security Manager

McAfee Enterprise Log Manager è una parte integrata opzionale di McAfee Enterprise Security Manager. McAfee Enterprise Log Manager memorizza i log, mentre McAfee Enterprise Security Manager può analizzare in modo approfondito e normalizzare le informazioni relative al log, rendendolo immediatamente disponibile per indagini di sicurezza e reazione agli incidenti in tempo reale.

Quando viene generato un evento di sicurezza, i file degli eventi analizzati vengono collegati direttamente al file di log sorgente e al record di log specifico, permettendo un accesso immediato durante i processi di gestione e analisi degli eventi. Nessun passaggio ulteriore, applicazione aggiuntiva da lanciare o tempo extra sprecato per effettuare ricerche manuali tra i log.

Un contesto completo per l'analisi

McAfee Enterprise Security Manager e McAfee Enterprise Log Manager insieme offrono informazioni sul contesto per ogni singolo log, rendendo ogni singolo record di log analizzato più prezioso. Tra le informazioni possono essere inclusi:

- La fonte o la destinazione dell'indirizzo IP
- Il contesto dell'identità
- Il nome dell'host o del servizio utilizzato
- Informazioni sulla vulnerabilità provenienti da uno scanner per la valutazione delle vulnerabilità
- Informazioni sulla topologia di rete
- Informazioni su policy e privacy

Pool di storage flessibili

I pool di storage della soluzione McAfee Enterprise Log Manager aggiungono flessibilità sulla modalità in cui i log vengono conservati nel lungo periodo. I pool di storage sono gruppi virtuali di storage utilizzabile che possono essere distribuiti tra vari gruppi di dispositivi di storage fisici (storage locale, NFS, SAN, CIF e altri) per soddisfare diverse esigenze di gestione dei log.

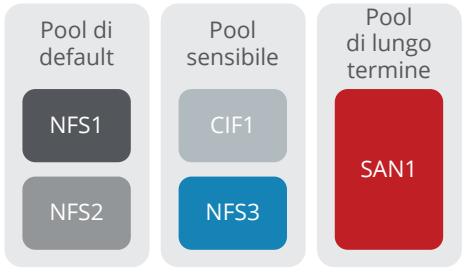

Figura 1. Pool di storage flessibili supportano la conservazione personalizzata dei log.

Un pool di storage può includere diversi dispositivi e i dati possono essere assegnati a un pool particolare sulla base del dispositivo sorgente, in modo che i log possano essere memorizzati in sedi separate in base alla loro rilevanza in termini di sicurezza, conformità, riservatezza o altri criteri. Per esempio, i log che sono importanti per la conformità dovrebbero essere memorizzati in un pool che include diversi dispositivi di storage di rete ridondanti. I log meno critici potrebbero essere memorizzati su sistemi meno ridondanti, mentre i log più utili per le analisi dovrebbero essere memorizzati in locale per analitiche più rapide.

Implementazione rapida

McAfee Enterprise Log Manager e McAfee Enterprise Security Manager possono essere distribuiti insieme utilizzando un'unica appliance combinata o distribuita per supportare anche le reti aziendali di più ampie dimensioni. Opzioni di distribuzione ibride flessibili includono appliance fisiche e virtuali.

Integrato con l'infrastruttura aziendale

Mentre la maggior parte delle soluzioni per la gestione dei log operano in modo isolato, McAfee Enterprise Log Manager opera congiuntamente a altri sistemi per la sicurezza delle informazioni. Attraverso McAfee Enterprise Security Manager, si collega al resto dell'infrastruttura di sicurezza per semplificare le operazioni di sicurezza, migliorare l'efficienza complessiva e ridurre i costi. È possibile integrare la gestione intelligente dei log con analitiche potenti, ispezione di rete, monitoraggio degli eventi legati al database e molto altro.

Ulteriori informazioni

Pr maggiori informazioni, visitare **www.mcafee.com/it/products/siem/index.aspx**.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it