McAfee Embedded Control

Integrità dei sistemi, controllo sulle modifiche e rispetto delle policy in un'unica soluzione

La soluzione McAfee® Embedded Control mantiene l'integrità del sistema consentendo solo l'esecuzione di codice autorizzato e l'implementazione di modifiche autorizzate. Crea automaticamente una whitelist dinamica del "codice autorizzato" sul sistema embedded. Dopo che la whitelist è stata creata e abilitata, il sistema viene mantenuto nella configurazione di base sicuramente funzionante, in modo che nessun programma o codice al di fuori della serie autorizzata possa essere eseguito, e non sia possibile effettuare modifiche non autorizzate. McAfee Integrity Control — che riunisce McAfee Embedded Control e la console McAfee ePolicy Orchestrator® (McAfee ePO™) — fornisce rapporti integrati sulla conformità e le verifiche per facilitare il rispetto di molteplici requisiti di conformità.

Principali vantaggi

- Limitazione del rischio di sicurezza grazie al controllo delle applicazioni eseguite sui dispositivi embedded e alla protezione della memoria di tali dispositivi.
- Permette di fornire l'accesso, mantenere il controllo e ridurre i costi di assistenza.
- Applicazione selettiva.
- Implementazione senza necessità di manutenzione.
- Rende i dispositivi conformi e pronti per i processi di verifica.
- Visibilità in tempo reale.
- Processo di verifica completo.
- Archivio delle modifiche ricercabile.
- Riconciliazione a ciclo chiuso.

La soluzione McAfee Embedded Control è stata studiata per risolvere il problema del crescente rischio di sicurezza derivante dall'adozione di sistemi operativi commerciali nei sistemi embedded. McAfee Embedded Control è una soluzione con ingombro ridotto, basso impiego di risorse e indipendente dalle applicazioni che offre una sicurezza che non richiede manutenzione. La soluzione McAfee Embedded Control converte un sistema basato su un sistema operativo commerciale in una "scatola nera" che assomiglia a un sistema operativo proprietario chiuso. Impedisce l'esecuzione di qualsiasi programma non autorizzato presente sul disco o iniettato nella memoria e qualsiasi modifica non autorizzata a una configurazione di base autorizzata. Questa soluzione permette ai produttori di godere dei vantaggi derivanti dall'uso di un sistema operativo commerciale senza incorrere in rischi aggiuntivi o rischiare di perdere il controllo sul modo in cui i sistemi vengono utilizzati sul campo.

Integrità dei sistemi assicurata

Controllo dei programmi eseguibili

Con la soluzione McAfee Embedded Control, possono essere eseguiti solo i programmi elencati all'interno della whitelist dinamica di McAfee. Gli altri programmi (exe, dll, script) sono considerati come non autorizzati: ne viene impedita l'esecuzione e il blocco viene registrato per impostazione predefinita. In questo modo si evita l'esecuzione illegittima di worm, virus, spyware e altro malware che si sia eventualmente installato.

Controllo della memoria

La funzione di controllo della memoria assicura che i processi in esecuzione siano protetti contro tentativi malevoli di assumerne il controllo. Il codice non autorizzato immesso all'interno di un processo in esecuzione viene bloccato, interrotto e registrato. In tal modo, i tentativi di assumere il controllo di un sistema attraverso exploit di tipo buffer overflow, heap overflow, stack execution e similari vengono resi inefficaci e registrati[1].

Integrazione con McAfee GTI: il modo intelligente per affrontare le minacce globali negli ambienti air-gap

McAfee Global Threat Intelligence (McAfee GTI) è un'esclusiva tecnologia McAfee che traccia la reputazione di file, messaggi e mittenti in tempo reale tramite milioni di sensori sparsi in tutto il mondo. Questa funzione utilizza le informazioni provenienti dal cloud per stabilire la reputazione di tutti i file presenti nell'ambiente di elaborazione, classificandoli come autorizzati, pericolosi e sconosciuti. Grazie all'integrazione con la tecnologia GTI, un malware inserito per errore in una whitelist viene immediatamente segnalato. La funzione di controllo della reputazione di GTI è accessibile sia negli ambienti software connessi a Internet, sia negli ambienti McAfee ePO isolati.

Controllo delle modifiche

La soluzione McAfee Embedded Control rileva le modifiche in tempo reale. Consente di individuare l'origine delle modifiche e verifica che siano state implementate nei sistemi di destinazione appropriati. Compila inoltre un audit trail delle modifiche e le consente solo secondo modalità autorizzate.

McAfee Embedded Control permette di imporre i processi di controllo delle modifiche specificando i mezzi autorizzati per apportarle. È possibile controllare chi può applicare le modifiche, quali certificati sono necessari per autorizzare le modifiche, che cosa può essere modificato (per esempio, si possono limitare le modifiche ad alcuni file o directory) e quando si possono applicare le modifiche (per esempio, l'aggiornamento di Microsoft Windows può essere possibile solo durante determinati periodi della settimana).

La funzione di modifica proattiva verifica ogni modifica prima che venga applicata ai sistemi di destinazione. Con questo modulo abilitato, gli aggiornamenti ai sistemi software possono essere effettuati solo in modo controllato.

Il modulo di localizzazione delle modifiche in tempo reale registra tutte le modifiche allo stato di sistema, incluso codice, configurazione e il registro. Gli eventi relativi alle modifiche vengono registrati nel momento in cui si verificano, in tempo reale, e inviati al controller di sistema a fini di aggregazione e archiviazione.

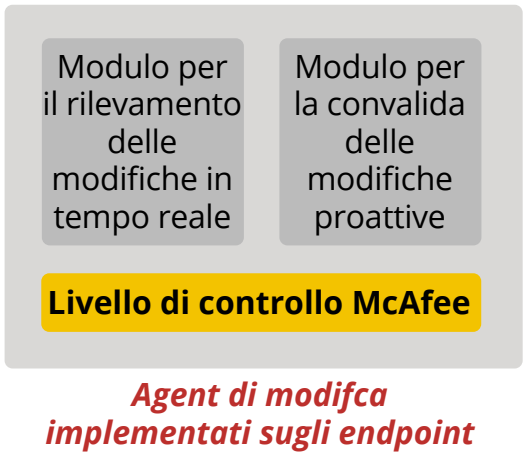

Figura 1. Livello di controllo McAfee.

Il modulo controller di sistema gestisce le comunicazioni tra il controller di sistema e gli agent e aggrega e memorizza le informazioni sugli eventi di modifica provenienti dagli agent nel sistema indipendente di registrazione.

Figura 2. Moduli per la reportistica, le ricerche e le analisi.

Verifica e rispetto delle policy

La soluzione McAfee Integrity Control mette a disposizione dashboard e rapporti che permettono di rispettare i requisiti per la conformità; vengono generati attraverso la console McAfee ePO, che fornisce un'interfaccia utente basata su web per utenti e amministratori.

La soluzione McAfee Embedded Control consente di gestire conformità e verifiche in modo integrato, a ciclo chiuso, in tempo reale. È dotata inoltre di un sistema di registrazione a prova di manomissione per le attività autorizzate e i tentativi abusivi.

La sicurezza integrata McAfee

Le soluzioni di sicurezza integrate McAfee aiutano i produttori a garantire che i loro prodotti e dispositivi siano protetti da minacce e attacchi informatici. Le soluzioni McAfee si avvalgono di un'ampia gamma di tecnologie tra cui whitelisting delle applicazioni, protezione antivirus e antimalware, gestione dei dispositivi, crittografia, rischio e conformità: tutte fanno affidamento su McAfee Global Threat Intelligence, la soluzione più all'avanguardia del settore. Le nostre soluzioni possono essere personalizzate per soddisfare i requisiti progettuali specifici del dispositivo di un produttore e le relative architetture.

Per saperne di più

Per ulteriori informazioni, visitate il sito **www.mcafee.com/it/partners/oem-alliances/index.aspx** o rivolgetevi al rappresentante locale McAfee.

Funzionalità	Descrizione	Vantaggio
Integrità di sistema garantita		
Difesa dalle minacce esterne	Garantisce che possa essere eseguito solo codice autorizzato. Il codice non autorizzato non può essere immesso nella memoria. Il codice autorizzato non può essere manomesso.	▪ Elimina l'esigenza di applicare patch in emergenza, riduce numero e frequenza dei cicli di applicazione delle patch, consente di eseguire un numero maggiore di test prima dell'applicazione delle patch, riduce il rischio di sicurezza per i sistemi che presentano difficoltà nell'applicazione delle patch. ▪ Riduce il rischio di sicurezza legato ad attacchi zero-day polimorfi tramite malware come worm, virus, trojan e attacchi con iniezione di codice come buffer overflow, heap overflow e stack overflow. ▪ Mantiene l'integrità dei file autorizzati, garantendo che il sistema in produzione sia in uno stato noto e verificato. ▪ Riduce il costo delle operazioni limitando i processi di patching e i tempi di fermo per il recovery non programmati e migliora la disponibilità del sistema.
Difesa dalle minacce interne	La funzione di blocco dell'amministratore locale offre la possibilità di impedire persino agli amministratori di modificare i programmi autorizzati a operare su un sistema protetto, se non presentati da una chiave autentica.	▪ Protegge dalle minacce interne. ▪ Blocca i programmi eseguiti su sistemi embedded in produzione e impedisce le modifiche anche da parte degli amministratori.

SCHEDA TECNICA

Funzionalità	Descrizione	Vantaggio
Controllo avanzato delle modifiche		
Aggiornamenti autorizzati sicuri da parte del produttore	Garantisce che su sistemi embedded sul campo possano essere implementati solo gli aggiornamenti autorizzati.	▪ Garantisce che sui sistemi sul campo non possano essere implementate modifiche out-of-band. Impedisce le modifiche non autorizzate al sistema prima che provochino periodi di inattività e generino chiamate al servizio di assistenza. ▪ I produttori possono scegliere di mantenere il controllo su tutte le modifiche, oppure autorizzare solo agent fidati del cliente a controllare le modifiche.
Verifica le modifiche che sono state effettuate all'interno di una finestra temporale approvata	Assicura che le modifiche non siano state implementate al di fuori delle finestre di modifica autorizzate.	▪ Impedisce le modifiche non autorizzate nei periodi delicati dal punto di vista fiscale o durante le ore lavorative di punta per evitare interruzioni operative e/o violazioni della conformità.
Sistemi di aggiornamento autorizzati	Garantisce che solo i sistemi di aggiornamento autorizzati (persone o processi) possano implementare le modifiche sui sistemi di produzione.	▪ Garantisce che sui sistemi di produzione non possano essere implementate modifiche out-of-band.
Verifica e conformità in tempo reale, a ciclo chiuso		
Rilevamento delle modifiche in tempo reale	Rileva le modifiche nel momento in cui si verificano nell'azienda.	▪ Garantisce che sui sistemi di produzione non possano essere implementate modifiche out-of-band.
Processo di verifica completo	Acquisisce informazioni complete su ogni modifica del sistema: autore, natura, localizzazione e modalità.	▪ Una registrazione precisa, completa e definitiva di tutte le modifiche del sistema.
Identificazione delle origini della modifica	Collega le singole modifiche alla loro origine: autore della modifica, sequenza degli eventi che hanno portato alla modifica, processo/programma interessato.	▪ Convalida le modifiche approvate; identifica rapidamente le modifiche non approvate e aumenta la percentuale di modifiche andate a buon fine.
Basso impiego di risorse operative		
Implementazione senza necessità di manutenzione	Il software si installa in pochi minuti, senza necessità di configurazione o impostazioni iniziali. Nessuna necessità di configurazione in corso d'opera.	▪ Funzionamento immediato. Attiva subito dopo l'installazione. Non richiede alcun impiego di risorse per la manutenzione continua. È quindi la scelta migliore per la configurazione di una soluzione di sicurezza con spese operative ridotte.
Senza regole, senza firme, nessun periodo di apprendimento, indipendente dalle applicazioni	Non dipende da regole o da database di firme; è efficace subito su tutte le applicazioni senza necessità di periodi di apprendimento.	▪ Nel corso del ciclo di vita del server, richiede solo interventi sporadici da parte dell'amministratore. ▪ Protegge i server fino all'applicazione delle patch o i server privi di patch con spese operative ridotte. ▪ La sua efficacia non dipende dalla qualità di alcuna regola o policy.

Funzionalità	Descrizione	Vantaggio
Ingombro ridotto, basso impiego di risorse in fase di esecuzione	Occupa meno di 20 MB di spazio su disco. Non interferisce con le prestazioni dell'applicazione in fase di esecuzione.	▪ È pronta per essere implementata su qualsiasi sistema di produzione mission-critical senza influire sulle prestazioni in fase di esecuzione o sui requisiti di memoria.
Garanzia di assenza di falsi positivi o falsi negativi	Viene registrata solo l'attività non autorizzata.	▪ La precisione dei risultati riduce le spese operative rispetto ad altre soluzioni di prevenzione delle intrusioni su host grazie alla drastica diminuzione del tempo necessario per analizzare i registri su base quotidiana o settimanale. ▪ Migliora l'efficienza dell'amministratore, riduce le spese operative.

1. Disponibile solo per piattaforme Microsoft Windows.

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