McAfee Cloud Workload Security

Proteggi i carichi di lavoro nella tua infrastruttura ibrida. Più sicuro. Più rapido. Più semplice.

Con l'evoluzione dei data center aziendali, ogni giorno sempre più carichi di lavoro vengono migrati in ambienti cloud. La maggior parte delle aziende ha un ambiente ibrido che combina carichi di lavoro on premise e cloud, tra cui i container, che sono in costante mutazione. Ciò introduce una sfida alla sicurezza in quanto gli ambienti cloud (privati e pubblici) richiedono nuovi approcci e strumenti per la protezione. Le aziende devono avere visibilità centralizzata di tutti i carichi di lavoro cloud con una protezione completa contro il rischio di errori di configurazione, malware e violazioni dei dati.

McAfee® Cloud Workload Security (McAfee® CWS) automatizza l'individuazione e la protezione di carichi di lavoro elastici e container per eliminare i punti ciechi, offre protezione dalle minacce avanzate e semplifica la gestione multicloud. McAfee offre una protezione che consente a una singola policy automatizzata di proteggere efficacemente i carichi di lavoro durante la transizione attraverso gli ambienti virtuali privati, pubblici e multicloud, garantendo l'eccellenza operativa dei team preposti alla sicurezza informatica.

Protezione avanzata dei carichi di lavoro: casi di utilizzo

Discovery automatica

Le istanze di carichi di lavoro e container Docker non gestite creano lacune nella gestione della sicurezza e possono offrire agli aggressori il punto d'appoggio di cui hanno bisogno per infiltrarsi nell'azienda.

McAfee CWS individua le istanze di carichi di lavoro elastici e i contenitori Docker in ambienti Amazon Web Services (AWS), Microsoft Azure, OpenStack e VMware. Inoltre, verifica costantemente nuove istanze. Ottieni una visione centralizzata e completa dei vari ambienti ed elimina punti ciechi operativi e di sicurezza che portano a un'esposizione ai rischi.

Informazioni approfondite sul traffico di rete

Utilizzando traffico di rete nativo fornito dai carichi di lavoro cloud, McAfee CWS è in grado di incrementare e applicare le informazioni provenienti dai feed di dati di McAfee® Global Threat Intelligence (McAfee® GTI). Le informazioni migliorate sono in grado di mostrare proprietà come punteggio di rischio, geolocalizzazione e altre importanti informazioni sulla rete. Queste informazioni possono essere utilizzate per creare azioni di remediation automatizzate per proteggere i carichi di lavoro.

Vantaggi principali

- La visibilità costante delle istanze dei carichi di lavoro elastici elimina gli "angoli ciechi" operativi automatizzando l'attività di distribuzione delle policy, una volta difficoltosa.
- Gestione centralizzata e carichi di lavoro automatizzati riducono drasticamente la complessità di ambienti ibridi e multicloud.
- Visualizzazione e individuazione delle minacce di rete senza necessità di installare un agent.
- Le difese dalle minacce ottimizzate per i computer virtuali offrono contromisure multi-livello.
- L'integrazione con strumenti di automazione come Chef e Puppet applica sicurezza ai carichi di lavoro cloud pubblici e privati al momento della distribuzione.

Seguici su

Integrazione in strutture di distribuzione

McAfee CWS crea script di distribuzione per consentire la distribuzione e la gestione automatiche dell'agent McAfee® sui carichi di lavoro cloud. Questi script permettono l'integrazione in strumenti come Chef, Puppet e altre strutture DevOps per la distribuzione dell'agent McAfee su carichi di lavoro eseguiti da fornitori di servizi cloud, come AWS e Microsoft Azure.

Consolidamento degli eventi

McAfee CWS permette alle aziende di utilizzare un'unica interfaccia per gestire numerose tecnologie di contrattacco sia per ambienti on premise che cloud. Ciò include anche l'integrazione in tecnologie aggiuntive, come AWS GuardDuty, McAfee® Policy Auditor e McAfee® Network Security Platform.

- Gli amministratori possono sfruttare le funzioni di monitoraggio continuo e i comportamenti non autorizzati identificati da AWS GuardDuty, fornendo un ulteriore livello di visibilità delle minacce. Questa integrazione permette ai clienti di McAfee CWS di visualizzare gli eventi GuardDuty, che includono connessioni di rete, scansioni delle porte e richieste DNS per istanze EC2, direttamente all'interno della console McAfee CWS.
- McAfee Policy Auditor esegue controlli basati su agent per verifiche di configurazione note o definite dall'utente per la conformità con Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Center for Internet Security Benchmark (CIS Benchmark) o altri standard industriali. McAfee CWS segnala ogni verifica fallita per la visibilità immediata di un'errata configurazione per i carichi di lavoro nel cloud.
- McAfee Network Security Platform è un'altra piattaforma di sicurezza cloud che esegue ispezioni di rete per il traffico in ambienti ibridi come AWS e Microsoft Azure. Esegue ispezioni più approfondite a livello di pacchetto rispetto al traffico di rete e segnala eventuali discrepanze o avvisi tramite McAfee CWS. Questo fornisce visibilità tramite un unico riquadro di visualizzazione per gli ambienti multicloud per l'attività di remediation.

Applicazione di policy di gruppo per la sicurezza di rete

McAfee CWS permette a utenti e amministratori di creare policy di gruppo di riferimento e verificare le policy che sono in esecuzione sui carichi di lavoro rispetto a tali linee guida. Qualsiasi scostamento o modifica rispetto alle linee guida può creare un avviso nella console McAfee CWS per l'attività di remediation. Gli amministratori possono anche configurare manualmente i gruppi di sicurezza di rete nativi da McAfee CWS; iin questo modo possono controllare direttamente le policy dei gruppi di sicurezza nativi in cloud.

Cosa contraddistingue McAfee Cloud Workload Security: principali caratteristiche e vantaggi

Supporto di build nel cloud in modalità nativa

Utilizzando McAfee CWS, i clienti possono consolidare la gestione di diversi cloud pubblici e privati in un'unica console di gestione, tra cui AWS EC2, computer virtuali Microsoft Azure, OpenStack e VMware Vcenter.

Vantaggi principali (segue)

- Una facile protezione multilivello da malware avanzato e intrusioni
- Individuazione e monitoraggio di container Docker proteggendoli grazie alla micro-segmentazione.
- Protezione dell'ambiente utilizzando azioni correttive direttamente dalla soluzione.

Cloud Workload Security

Visibilità e **controllo** completi

McAfee CWS importa e permette ai clienti l'esecuzione in cloud con il supporto di build nel cloud in modalità nativa per Amazon Elastic Container Service for Kubernetes (Amazon EKS) e Microsoft Azure Kubernetes Service (AKS).

Semplice gestione centralizzata

Un'unica console offre una gestione centralizzata coerente delle policy di sicurezza in ambienti multi-cloud per server, server virtuali e carichi di lavoro cloud. Gli amministratori possono anche creare diverse autorizzazioni basate su ruolo all'interno del software McAfee® ePolicy Orchestrator® (McAfee ePO™), che consente loro di definire ruoli utenti in modo più specifico e appropriato.

Visualizzazione di rete con la micro-segmentazione

Visualizzazione di rete nativa in cloud, segnalazione di rischio prioritario e funzionalità di micro segmentazione offrono consapevolezza e controllo per prevenire la progressione laterale degli attacchi all'interno di ambienti virtualizzati e da fonti dannose esterne. La funzionalità di spegnimento o quarantena con un singolo clic aiuta a ridurre i potenziali errori di configurazione e aumenta l'efficienza dell'attività di remediation.

Protezione avanzata della virtualizzazione

La suite McAfee CWS protegge i computer virtuali nel cloud privato dal malware utilizzando McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus). E lo fa senza abusare delle risorse di base o richiedere costi operativi aggiuntivi. McAfee MOVE AntiVirus permette alle aziende di scaricare la sicurezza su computer virtuali dedicati per l'analisi ottimizzata del loro ambiente virtualizzato.

Gli utenti ottengono una protezione anti-malware tramite McAfee® Endpoint Security for Servers. Questa soluzione può pianificare in modo intelligente attività che richiedono un elevata quantità di risorse, come l'analisi su richiesta, per evitare l'impatto su processi aziendali critici.

Contrassegno e automatizzazione della sicurezza del flusso di lavoro

Assegna le giuste policy a tutti i carichi di lavoro automaticamente con la possibilità di importare informazioni sui tag AWS e Microsoft Azure nel software McAfee ePO e assegnare le policy sulla base di tali tag. I tag AWS e Microsoft Azure esistenti sono sincronizzati con i tag del software McAfee ePO in modo che siano gestiti automaticamente.

Remediation automatica

L'utente definisce le policy software McAfee ePO. Se McAfee CWS individua un sistema che non è protetto dalle policy di sicurezza del software McAfee ePO e che contiene un malware o un virus, questo sistema verrà messo automaticamente in quarantena.

Protezione adattiva dalle minacce

McAfee CWS integra contromisure complete, che includono apprendimento automatico, contenimento delle applicazioni, antimalware ottimizzato per i computer virtuali, whitelisting, monitoraggio dell'integrità dei file e micro segmentazione, per proteggere i carichi di lavoro da minacce come il ransomware e gli attacchi mirati. McAfee® Advanced Threat Protection respinge gli attacchi sofisticati mai rilevati in precedenza utilizzando tecniche di apprendimento automatico per classificare i payload dannosi in base agli attributi del codice e al comportamento.

Controllo delle applicazioni

Il whitelisting delle applicazioni previene attacchi noti e sconosciuti autorizzando l'esecuzione solo delle applicazioni attendibili e bloccando qualsiasi payload non autorizzato. McAfee® Application Control offre protezione dinamica sulla base di intelligence sulle minacce globale e locale e la capacità di mantenere i sistemi aggiornati senza disabilitare le funzioni di sicurezza.

Monitoraggio dell'integrità dei file

La funzione di monitoraggio dell'integrità dei file di McAfee® effettua un controllo costante per garantire che directory e file di sistema non siano stati compromessi da malware, hacker o malintenzionati interni all'azienda. I dettagli completi della verifica forniscono informazioni su come i file sui carichi di lavoro del server variano e segnalano la presenza di un attacco attivo.

Copertura di sicurezza adeguata per il tuo ambiente multicloud

McAfee CWS consente di mantenere la massima qualità della sicurezza e sfruttare il cloud. Copre molteplici tecnologie di protezione, semplifica la gestione della sicurezza e impedisce alle minacce informatiche di avere un impatto negativo sulle attività aziendali, per restare focalizzati solo sulla crescita dell'azienda. Di seguito un confronto delle caratteristiche delle diverse soluzioni disponibili.

Caratteristiche	McAfee Cloud Workload Security Basic	McAfee® Cloud Workload Security Essentials	McAfee® Cloud Workload Security Advanced
Gestione centralizzata (Piattaforma di McAfee ePO)	✓	✓	✓
Supporto multi-cloud (AWS, Microsoft Azure, VMware)	✓	✓	✓
Utilizzo della micro-segmentazione per mettere in quarantena carichi di lavoro e container	✓	✓	✓
McAfee MOVE (senza agent e multipiattaforma)	✓	✓	✓
Prevenzione delle minacce di McAfee Endpoint Security per i sistemi operativi server (Windows e LInux)	✓	✓	✓
Firewall basato su host	✓	✓	✓
Gestione nativa del firewall per AWS e Microsoft Azure (Gruppi di sicurezza)	✓	✓	✓
Prevenzione delle intrusioni su host e degli exploit	✓	✓	✓
Importazione di informazioni sui tag AWS e Microsoft Azure all'interno del software McAfee ePO	✓	✓	✓
Remediation automatica su carichi di lavoro non conformi	✓	✓	✓
Protezione adattiva dalle minacce con l'apprendimento automatico		✓	✓
Visualizzazione del traffico di rete e microsegmentazione		✓	✓
Analisi del traffico di rete nativo in cloud combinato con il punteggio di reputazione di McAfee GTI		✓	✓
Integrazione con McAfee® Virtual Network Security Platform (McAfee® vNSP)		✓	✓
Whitelisting dinamico per i server tramite McAfee Application Control			✓
Registrazione continua delle verifiche tramite la funzione di monitoraggio dell'integrità dei file di McAfee			✓
Protezione di file e cartelle tramite McAfee® Change Control per i server			✓

Maggiori informazioni

Per maggiori informazioni visitare: **www.mcafee.com/it/products/host-ips-for-desktop.aspx**.

Le caratteristiche e i benefici offerti dalle tecnologie McAfee dipendono dalla configurazione del sistema e potrebbero richiedere l'abilitazione di hardware, software o l'attivazione del servizio. Ulteriori informazioni sono disponibili sul sito www.mcafee.com/it. Nessun sistema informatico può essere assolutamente sicuro.

McAfee
Together is power.

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