McAfee Cloud Workload Security

**Protezione dei carichi di lavoro cloud privati e pubblici.
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 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 multi-cloud. McAfee offre protezione ineguagliata che consente a una singola policy automatizzata di proteggere efficacemente i carichi di lavoro durante la transizione attraverso gli ambienti virtuali privati, pubblici e ibridi, garantendo l'eccellenza operativa dei team preposti alla sicurezza informatica.

Visibilità in tempo reale

Discovery automatica

Le istanze di carichi di lavoro e container Docker non rilevati creano lacune nella gestione della sicurezza e possono offrire agli aggressori il punto d'appoggio di cui hanno bisogno per infiltrarsi nell'azienda. McAfee Cloud Workload Security individua istanze elastiche dei carico di lavoro e container Docker in ambienti Amazon Web Services (AWS), Microsoft Azure e VMware ed effettua un controllo costante per le 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.

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.
- Individua e monitora i container Docker e li protegge grazie alla micro-segmentazione.
- Le difese dalle minacce ottimizzate per i computer virtuali offrono contromisure multi livello.
- Gestione centralizzata e flussi di lavoro automatizzati riducono drasticamente la complessità di ambienti ibridi e multi-cloud.
- 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:

Protezione dei carichi di lavoro attuale

Protezione dalle minacce avanzate

McAfee Cloud Workload Security 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. La protezione dalle minacce avanzate , incluso l'apprendimento automatico, 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.

Consolidamento degli eventi

McAfee Cloud Workload Security permette alle aziende di utilizzare un'unica interfaccia per gestire numerose tecnologie di contrattacco sia per ambienti on premise che cloud. Tra questo sono incluse tecnologie di terze parti, come AWS GuardDuty. 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 Cloud Workload Security 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 Cloud Workload Security. Gli eventi relativi alle connessioni di rete GuardDuty vengono mappati all'interno di un diagramma di flusso quando il traffico corrisponde al traffico rilevato da McAfee Cloud Workload Security.

Protezione avanzata della virtualizzazione

McAfee Cloud Workload Security protegge i computer virtuali del cloud privato dal malware senza affaticare le risorse di base o richiedere costi operativi aggiuntivi. Ottieni una protezione antimalware che pianifica in modo intelligente le attività che richiedono un elevato impiego di risorse, come la scansione su richiesta, quando l'hypervisor non è sovraccarico.

Visualizzazione della rete con 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.

Vantaggi principali (segue)

- Protezione multi livello, di facile utilizzo, per difendersi da malware avanzato e intrusioni.
- Visualizzazione e individuazione delle minacce di rete senza necessità di installare un agent.
- Protezione dell'ambiente utilizzando azioni correttive direttamente dalla soluzione.

Cloud Workload Security

Visibilità e **controllo** completi

Monitoraggio dell'integrità dei file

Il monitoraggio dell'integrità dei file 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.

Controllo delle applicazioni

Il whitelisting delle applicazioni previene gli attacchi noti e sconosciuti autorizzando l'esecuzione solo delle applicazioni attendibili e bloccando qualsiasi payload non autorizzato. Il controllo delle applicazioni 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.

Gestione semplificata

Coerenza grazie alla 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.

Distribuzione automatizzata

Grazie al supporto per gli strumenti di automazione della distribuzione di aziende come Chef, Puppet e Ansible, è possibile distribuire automaticamente la tecnologia di sicurezza in più ambienti cloud.

Copertura di sicurezza migliorata

McAfee Cloud Workload Security permette di mantenere la massima qualità della sicurezza e sfruttare il cloud. Copre molteplici tecnologie di protezione, semplifica la gestione della sicurezza e impedisce alle cyber minacce 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.

SCHEDA TECNICA

Caratteristiche	Cloud Workload Security Basic	Cloud Workload Security Essentials	Cloud Workload Security Advanced
Gestione centralizzata (Piattaforma McAfee® ePO™)	✓	✓	✓
Supporto multi-cloud (AWS, Azure, VMware)	✓	✓	✓
Utilizzo della micro-segmentazione per mettere in quarantena carichi di lavoro e container	✓	✓	✓
Prevenzione delle minacce per i sistemi operativi server (Windows e LInux)	✓	✓	✓
Prevenzione delle intrusioni su host e degli exploit	✓	✓	✓
Gestione della crittografia cloud	✓	✓	✓
Gestione nativa del firewall per AWS e Azure (Gruppi di sicurezza)	✓	✓	✓
McAfee® Management for Optimized Virtual Environments (senza agent e multi piattaforma)	✓	✓	✓
Firewall basato su host	✓	✓	✓
Protezione adattiva dalle minacce con l'apprendimento automatico		✓	✓
Visualizzazione del traffico di rete e micro segmentazione		✓	✓
Analisi del traffico di rete cloud nativa combinata con il punteggio di reputazione di Global Threat Intelligence		✓	✓
Application Control for Servers			✓
File Integrity Monitoring			✓
Change Control for Servers			✓
Integrazione con McAfee® Virtual Network Security Platform		✓	✓

Ulteriori informazioni

Per ulteriori informazioni, visitare il sito: **https://www.mcafee.com/it/products/cloud-workload-security.aspx**.

McAfee
Together is power.

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