McAfee Public Cloud Server Security Suite

Sicurezza completa per i carichi di lavoro nel cloud di AWS e Azure

Vantaggi principali

- Progettata per i carichi di lavoro in AWS e Azure.
- Scoperta istantanea.
- Valutazione della sicurezza e neutralizzazione delle minacce.
- Sicurezza scalabile.
- Protezione completa.
- Utilizza la console di gestione McAfee® ePolicy Orchestrator® (McAfee ePO™).
- Le opzioni di distribuzione includono Chef, Puppet e OpsWorks.
- Dimostra la conformità.
- Si integra con le altre soluzioni di Intel Security.

Le grandi imprese che stanno includendo nella propria strategia dei centri dati le istanze dei server dei cloud pubblici (spesso basando su di esse la strategia stessa) sono coscienti del fatto che un modello di responsabilità condivisa[1] sia una considerazione importante. I fornitori di cloud pubblici come Amazon Web Services (AWS) e Microsoft Azure proteggono il perimetro, mentre agli utenti spetta di proteggere i contenuti. Ma in che modo le imprese lungimiranti possono proteggere i propri carichi di lavoro nel cloud dagli attacchi del giorno zero e dalle minacce avanzate persistenti (APT), mantenendo al contempo i costi in linea con la propria strategia cloud? Alcune delle principali sfide affrontate dalle imprese che adottano il cloud:

- È sempre più difficile tenere il passo con le minacce zero day e avanzate.
- La mancanza di visibilità e di una gestione centralizzata complicano estremamente le cose quando si possiedono più infrastrutture cloud.
- La riduzione delle prestazioni è una preoccupazione per la sicurezza dei carichi di lavoro nel cloud.

McAfee® Public Cloud Server Security Suite permette di scoprire e proteggere istantaneamente i carichi di lavoro in AWS e Azure, proteggendo in modo completo, uniforme e continuo dalle minacce, con minimo impatto sulle prestazioni. Puoi scoprire numerosi centri dati e account nel cloud, computer virtuali e minacce emergenti.

La protezione completa offerta da McAfee Public Cloud Server Security Suite include le funzioni base di antivirus e prevenzione delle intrusioni, oltre a quelle avanzate di whitelisting che protegge dalle minacce del giorno zero, di controllo delle modifiche per soddisfare i requisiti di conformità normativa e di gestione della crittografia per la protezione dei dati. Una singola console facilita la gestione di più cloud e l'imposizione delle policy. Le opzioni di distribuzione flessibile tramite gli strumenti DevOps Chef, Puppet e OpsWorks eliminano le interruzioni, con un impatto minimo.

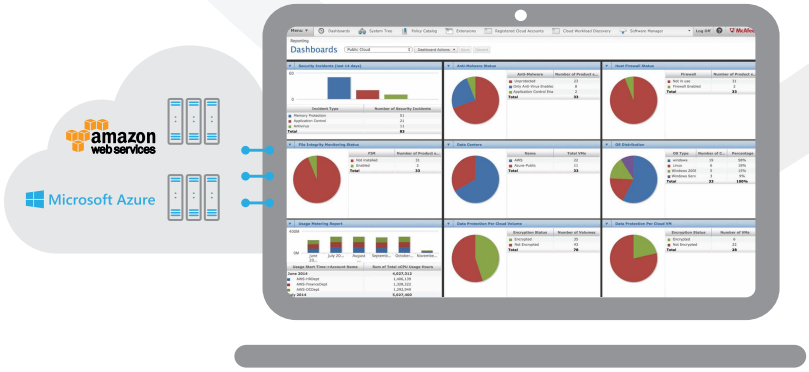

Figura 1. Una singola console di gestione per molteplici infrastrutture nel cloud e molteplici tecnologie Intel Security.

intel Security

Piattaforme supportate

- Windows Server 2008, 2008 R2, 2012, 2012 R2
- Linux (Red Hat, CentOS, SUSE, Ubuntu, Amazon Linux)

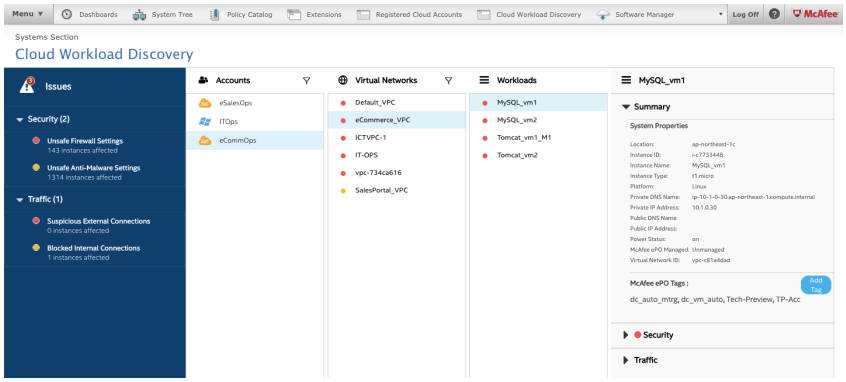

Figura 2. Individuazione e monitoraggio di molteplici infrastrutture nel cloud e minacce emergenti.

Scopri le infrastrutture e le minacce nel cloud

Per avere un maggiore controllo sull'infrastruttura e sulle minacce nel cloud hai bisogno di maggior visibilità su di esse.

- In pochi minuti puoi scoprire tutte le reti virtuali o i cloud privati virtuali (VPC), oltre ai modelli e ai carichi di lavoro nelle infrastrutture cloud di AWS e Azure. Possedere informazioni dettagliate sugli account dell'infrastruttura cloud, sapere quali sono gli utenti che hanno accesso a quali parti dell'infrastruttura, capire in che modo i carichi di lavoro sono assegnati a modelli e VPC e l'avere un'istantanea rapida della struttura dei sistemi associata all'infrastruttura cloud sono i primi passi da compiere per proteggere in modo adeguato la tua infrastruttura cloud.
- In una sola interfaccia hai la visibilità su più cloud. Sfrutta le informazioni end-to-end sulle minacce, comprese le loro origini, per controllare meglio la sicurezza.
- Visualizza il traffico fra i carichi di lavoro e gestisci il modo in cui le informazioni scorrono fra di essi e vengono utilizzate dall'esterno dell'organizzazione.

Monitora il cloud e reagisci più rapidamente agli allarmi di sicurezza

Dato che una rapida remediation è sempre più importante, con questa soluzione puoi valutare rapidamente i problemi della sicurezza a un livello più approfondito e prendere le azioni immediate.

- Identifica i problemi che richiedono attenzione urgente e prendi le misure appropriate in base al codice dei colori assegnati alle minacce.
- Crea etichette personalizzate e assegnale ai carichi di lavoro in base alle tue specifiche esigenze.
- Prendi le misure correttive per risolvere i problemi legati alla sicurezza; adotta le policy necessarie oppure definisci le reputazioni delle minacce per difendere l'infrastruttura dalle violazioni future.
- Gestisci il firewall cloud con delle policy su misura di singoli carichi di lavoro o gruppi di carichi. Gestisci le policy per i gruppi di sicurezza AWS al fine di controllare il traffico per una o più istanze.
- Identifica il traffico sospetto nei VPC e prendi le misure correttive per impedire che le informazioni critiche cadano nelle mani sbagliate.

Protezione completa contro le minacce

McAfee Public Cloud Server Security Suite utilizza un unico agent che offre multipli livelli di protezione ed è a sua volta gestibile tramite una singola console su multiple piattaforme cloud. Questa soluzione può essere distribuita anche con gli strumenti DevOps, per la migliore esperienza possibile.

Per saperne di più

Visita la pagina del prodotto: **www.mcafee.com/it/products/public-cloud-server-security-suite.aspx**.

Acquistabile anche su **AWS Marketplace**.

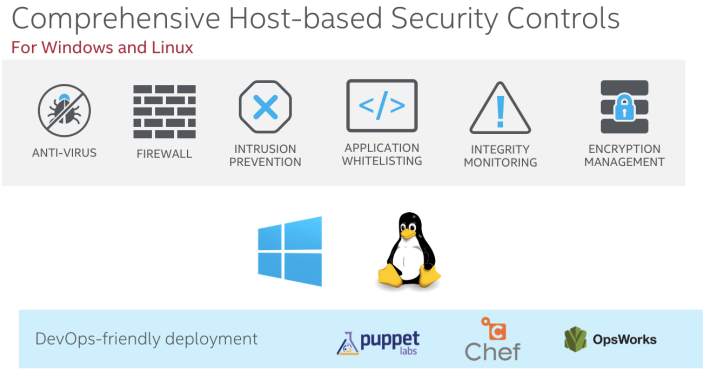

Figura 3. Protezione completa per i carichi di lavoro nel cloud pubblico.

Funzione	Vantaggi
Opzioni di distribuzione con Chef, Puppet e AWS OpsWorks	• Gli strumenti di distribuzione DevOps consentono di pianificare in anticipo la protezione con una distribuzione facile. • La sicurezza viene integrata nelle operazioni.
Scoperta dei carichi di lavoro nel cloud	• La visibilità istantanea nelle infrastrutture cloud permette di scoprire i centri dati virtuali, i carichi di lavoro nel cloud e i firewall cloud. • Rapidi avvisi di minaccia con valutazione automatica della condizione di sicurezza. • Remediation più rapida delle minacce grazie agli allarmi ordinati in base alla criticità e ai passi da compiere per reagire rapidamente dopo la ricezione degli allarmi.
Un'unica console di gestione per molteplici soluzioni di sicurezza dell'infrastruttura cloud (software McAfee ePO)	• Estremamente vantaggiosa per gli ambienti ibridi. • Gestibilità da un singolo pannello per i carichi di lavoro fisici, virtuali, cloud e per le policy. • Integra le tecnologie di sicurezza nel cloud e in sito di Intel Security e dei suoi partner. • Abbassa il costo totale di proprietà grazie ai processi di sicurezza integrati e alle rapide misure risolutive.
Antimalware	• Massima difesa contro il malware. Salvaguarda file e sistemi da virus, spyware, worm, trojan e altri rischi per la sicurezza. Rileva e rimuove il malware e consente agli utenti di configurare in modo semplice le policy per gestire gli oggetti in quarantena.
Firewall host	• Proteggi i carichi di lavoro dagli accessi non autorizzati e dagli attacchi.
Prevenzione delle intrusioni su host	• Blocca il traffico di rete nocivo o indesiderato, blocca precocemente gli attacchi noti e del giorno zero grazie a una tecnologia brevettata e premiata. • Impedisce di apportare modifiche indesiderate ai carichi di lavoro tramite la limitazione dell'accesso a porte, file, condivisioni, chiavi di registro e valori di registro specifici. • La protezione della memoria impedisce ai programmi anomali o alle minacce di invadere i limiti del buffer e di sovrascrivere la memoria adiacente, registrando contemporaneamente i dati in un buffer. Gli exploit da overflow del buffer consentono l'esecuzione di codice arbitrario sul computer dell'utente.
Whitelisting delle applicazioni	• Protegge contro le minacce del giorno zero e le minacce persistenti avanzate senza la necessità di aggiornare le firme. • Rinforza la sicurezza e abbassa i costi di proprietà grazie al whitelisting dinamico, che accetta automaticamente il nuovo software aggiunto tramite i canali affidabili. • Riduce i cicli di applicazione delle patch grazie al whitelisting sicuro delle applicazioni e alla protezione avanzata della memoria.
Monitoraggio dell'integrità dei file	• Permette il rilevamento continuo delle modifiche eseguite a livello di sistema nei siti remoti e distribuiti. • Previene le manomissioni bloccando le modifiche non autorizzate ai file di sistema critici, alle directory e alle configurazioni. • Segue e convalida ogni tentativo di modifica in tempo reale sul carico di lavoro, applicando le policy per il controllo delle modifiche in base a intervalli di tempo, origine o ticket approvati.
Gestione della crittografia	• Cripta i dati archiviati nei volumi AWS EBS con l'Advanced Encryption Standard (AES) di AWS. • I volumi con dati preesistenti possono essere crittografati facilmente. • Si integra con il Key Management Service (KMS) di Amazon per la crittografia.

1. **http://www.mcafee.com/it/resources/white-papers/wp-cloud-security-primer-techtarget.pdf**

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