Protezione dei carichi di lavoro nel cloud

Come proteggere i carichi di lavoro negli hybrid cloud

vmware®

Sommario

Quadro di sintesi

L'hybrid cloud rappresenta il motore della digital transformation. Oggi, più del 90% delle aziende dichiara di adottare una strategia multi-cloud che si avvale, nella maggior parte dei casi, dell'uso congiunto di public cloud e private cloud.[1] La buona notizia è che questo approccio offre la flessibilità e la scalabilità necessarie per favorire una rapida innovazione, mentre la cattiva notizia è che accresce la complessità e i rischi, rendendo la sicurezza un componente essenziale nei private cloud e nei public cloud.

Mentre i team aziendali distribuiscono e gestiscono i carichi di lavoro cruciali negli ambienti multi-cloud, la visibilità sul livello di sicurezza dei carichi di lavoro e il controllo della superficie di attacco sono fondamentali per proteggere i dati e non causare interruzioni delle operation.

Molti team aziendali, come IT Ops e SecOps, sono parti interessate chiave per quanto riguarda le prestazioni, la disponibilità e la sicurezza dei carichi di lavoro nel cloud. Un altro fattore di successo è la capacità di creare allineamento e non frammentazione tra i componenti dei team.

Questo white paper analizza le principali sfide che i team aziendali hanno dovuto affrontare per proteggere i carichi di lavoro nel cloud e illustra come superarle utilizzando l'approccio con sicurezza intrinseca di VMware, che si avvale di VMware Carbon Black Cloud™, VMware vSphere® e VMware NSX®. Questo documento esamina inoltre come il cloud imponga un nuovo modo di pensare ai rischi, che riunisce le parti interessate dei diversi team piuttosto che mantenere il divario digitale. Include infine una checklist di valutazione della piattaforma di protezione dei carichi di lavoro nel cloud per permettere alle organizzazioni di valutare le soluzioni disponibili senza dimenticare i requisiti chiave da soddisfare.

La sfide per la sicurezza con private cloud, public cloud e hybrid cloud

Distribuire e gestire carichi di lavoro e app in ambienti di private cloud, public cloud e hybrid cloud sono attività che richiedono il coinvolgimento di tantissime figure. Quella che un tempo era considerata attività esclusiva del reparto IT è ora un lavoro di squadra. IT Ops, DevOps e SecOps ora lavorano insieme per distribuire e proteggere le app e i servizi dal cloud.

1. Flexera, “Flexera 2020 State of the Cloud Report”, aprile 2020

Come si evince dalla Tabella 1, la mancanza di un coordinamento tra i diversi team e l'assenza di un piano per gestire gli elementi specifici dei carichi di lavoro nel cloud possono portare a un aumento dei rischi.

	OPERATION DELL'HYBRID CLOUD	SFIDE LEGATE ALLA SICUREZZA	OPERATION IT TRADIZIONALI	LACUNE NELLA SICUREZZA IT TRADIZIONALE
Architettura di progettazione	Servizi interconnessi	• Nessuna visibilità sul modo in cui i carichi di lavoro comunicano e sono collegati • Le reti non strutturate e non segmentate aumentano i rischi	Monolitiche e isolate	• I software antivirus (AV) tradizionali non sono creati per operare nel contesto dei carichi di lavoro nel cloud • Il monitoraggio incentrato sul data center non offre una base di confronto per comprendere quale sia il normale comportamento della rete
Modello operativo	Proprietà e gestione distribuite	• IT Ops è responsabile del livello di sicurezza, della gestione e della disponibilità dei carichi di lavoro, ma non è in grado di individuarne le vulnerabilità • I silos dei processi e della tecnologia contribuiscono a creare configurazioni non corrette o non sicure e a introdurre altri errori umani	Centralizzate	• L'aggiunta di prodotti mirati per la sicurezza richiede l'installazione di agenti aggiuntivi, che però rallentano le prestazioni del sistema e rendono le operation più complicate • La mancanza di visibilità unificata dei carichi di lavoro e tra i carichi di lavoro e i cloud complica il coordinamento tra i team
Scalabilità	Altamente dinamiche, automatiche	• Il mancato controllo dei cambiamenti determina errori di configurazione, come storage dei dati non sicuro, riconoscimento di un numero eccessivo di autorizzazioni, impostazioni di configurazioni e credenziali predefinite, nonché disattivazione dei controlli di sicurezza • L'incapacità di standardizzare le policy di sicurezza dei carichi di lavoro tra private cloud e public cloud aumenta il rischio	Statiche, manuali	• La scansione tradizionale non è progettata per rilevare gli errori di configurazione del cloud più diffusi (la causa principale delle violazioni dei dati basate su cloud)[2] • Distribuire soluzioni di sicurezza mirate per ciascun ambiente cloud complica la gestione della governance e delle policy secondo necessità

TABELLA 1. Le sfide per la sicurezza con i carichi di lavoro nell'hybrid cloud derivano dall'incapacità di riconoscere le differenze fondamentali tra cloud computing e IT tradizionale.

2. Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven Deep Dive", settembre 2020.

IT Ops, DevOps e SecOps condividono tutti la responsabilità di preservare la sicurezza e la disponibilità dei carichi di lavoro cruciali nel cloud.

Tre azioni per ridefinire il rischio

Il modo migliore per sfruttare appieno le possibilità della digital transformation è accettare la necessità di adottare un nuovo approccio. I vecchi modelli di gestione dei rischi non sono più applicabili quando il cambiamento è una costante e nel pollaio sono troppi i galli a cantare.

Quando si parla di sicurezza dei carichi di lavoro nel cloud, i team devono:

1. Aumentare la visibilità, ovvero identificare i rischi non noti o non rilevati nei carichi di lavoro.
2. Velocizzare il ripristino, ovvero accelerare il ripristino creando resilienza nei carichi di lavoro nel cloud.
3. Semplificare la sicurezza, ovvero unificare la mitigazione dei rischi tra carichi di lavoro, endpoint e container.

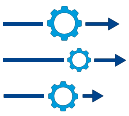
Fase 1: aumentare la visibilità - Identificare i rischi non noti o non rilevati nei carichi di lavoro

- **Perché questa è una sfida:** non è possibile gestire rischi di cui non si è a conoscenza. Sfortunatamente, la maggior parte degli amministratori di macchine virtuali (VM) non sa in che misura le app e i carichi di lavoro in esecuzione sulle VM sono potenzialmente vulnerabili ad attacchi. Se per chi attacca è sufficiente individuare e sfruttare una sola vulnerabilità per ottenere accesso non autorizzato, chi difende deve invece conoscere tutti i modi in cui una vulnerabilità può essere sfruttata per chiudere tutte le falle della sicurezza. Inoltre, una volta identificate le vulnerabilità, non è semplice per IT Ops e SecOps trovare un accordo su quali sono le più impellenti da risolvere, perché e quando.
- **Esempio:** Gianni è il Site Reliability Engineer (SRE) di una grande azienda di servizi per il settore sanitario ed è responsabile della gestione dell'infrastruttura del private cloud, che include server, carichi di lavoro e app che elaborano dati sanitari sensibili. Gianni sa che deve identificare e mitigare tutte le vulnerabilità che possono avere un impatto sulla compliance o compromettere la riservatezza dei dati dei pazienti. Partendo da questi presupposti, le prestazioni, la disponibilità e la continuità operativa sono le priorità fondamentali per Gianni e gli altri SRE nel suo team. Dopotutto, l'assistenza ai pazienti è mission critical.

  Al momento, Gianni si aspetta che Sara, analista della sicurezza, gli comunichi quando una scansione programmata del sistema rileva una vulnerabilità grave da mitigare. Spesso non sono d'accordo sulle azioni da intraprendere perché ognuno di loro utilizza strumenti diversi. Senza un sistema di record comune, è difficile raggiungere un accordo su queste problematiche cruciali: Quali vulnerabilità hanno la priorità? I controlli di compensazione sono sufficienti? Qual è l'obiettivo degli hacker? Come si muovono? e così via.
- **Cosa serve: individuazione dei rischi tra i domini:** individuare tutti i rischi dei carichi di lavoro nel cloud, da tutti i punti di vista e vettori di attacco, e utilizzare un sistema di registrazione comune per gestirli. Se non è possibile implementare una patch perché sussiste il rischio di downtime, è necessario raggiungere un accordo su un controllo di compensazione oppure definire una watchlist per rilevare quando la vulnerabilità è l'obiettivo di un attacco.

Fase 2: velocizzare il ripristino - Accelerare il ripristino creando resilienza nei carichi di lavoro nel cloud

- **Perché questa è una sfida:** per la maggior parte delle aziende, le violazioni dei dati non sono più una questione di "se", ma "quando". Durante una violazione, conoscere l'entità o il raggio d'azione dell'esposizione è fondamentale per prevenire violazioni simili in futuro. Inoltre, queste informazioni approfondite sono importanti per assicurare un ripristino rapido e completo. Questa sfida vede un conflitto di priorità. La priorità per i team DevOps e IT Ops è ripristinare i servizi il più presto possibile, anche se ciò significa distruggere evidenze legali e artefatti necessari al team SecOps per identificare e scoprire l'origine e la portata dell'attacco.
- **Esempio:** il ripristino dopo un attacco con ransomware in un ambiente cloud può essere costoso e complicato e richiedere un uso intensivo di manodopera. Questi attacchi possono passare dai carichi di lavoro ai server che li ospitano e raggiungere perfino gli endpoint utilizzati dai dipendenti per accedere a questi carichi di lavoro. L'obiettivo è ridurre la superficie di attacco in caso di attacco con ransomware contrastando le fasi iniziali dell'attacco stesso, ovvero l'esecuzione del codice nello stesso carico di lavoro, prima della distribuzione completa degli strumenti o della configurazione delle connessioni delle funzionalità di comando e controllo (C2) per esfiltrare o crittografare i dati per il riscatto.



- **Cosa serve: resilienza ai rischi:** il rapido ripristino dei servizi dopo una violazione o un attacco con malware e la conservazione dei dati necessari per effettuare le indagini legali è possibile nel cloud, ma sempre che si disponga della giusta piattaforma di sicurezza dei carichi di lavoro. Colmare questa lacuna è un aspetto fondamentale della creazione di una vera resilienza ai rischi nei carichi di lavoro nel cloud. Gestire la sicurezza degli endpoint e dei carichi di lavoro dalla stessa piattaforma permette ai team di identificare i rischi in questi punti di controllo e di perseguire una strategia di ripristino più resiliente.

Fase 3: semplificare la sicurezza - Unificare la mitigazione dei rischi tra carichi di lavoro, endpoint e container

- **Perché questa è una sfida:** gestire il rischio nei carichi di lavoro nel cloud utilizzando soluzioni mirate tradizionali porta a processi in silos, fattore che aumenta le spese generali e il rischio composito. L'utilizzo di strumenti di sicurezza diversi basati sul public cloud provider, sul SO dell'host o sul tipo di cloud (private o public) impedisce in pratica di adottare una strategia di mitigazione dei rischi coerente. Dopotutto, quando non esiste una SSOT (Single Source of Truth) per la sicurezza, i team non riescono ad accordarsi su come prevenire gli attacchi con malware, individuare e correggere le configurazioni errate o contenere le minacce che si muovono rapidamente.
- **Esempio:** per ottimizzare la resilienza operativa, alcuni team IT Ops scelgono di utilizzare più cloud provider o di utilizzare in modo congiunto l'infrastruttura di private cloud e public cloud. Senza una policy di sicurezza realmente indipendente, che trascenda da questi ambienti, i team avranno solo dei controlli eterogenei oppure rimarranno vincolati a un solo cloud service provider o a un'unica architettura cloud (private o public).
- **Cosa serve: sicurezza unificata:** l'obiettivo è distribuire sicurezza unificata progettata per il cloud e applicata in modo uniforme, indipendentemente dall'ubicazione del carico di lavoro (public cloud o private cloud). Utilizzando una singola gestione del ciclo di vita in tutti i cloud, carichi di lavoro e container, è possibile avere una strategia per le policy di sicurezza e la mitigazione dei rischi coerente e di ampia portata. L'utilizzo, ad esempio, di una singola piattaforma per la gestione delle vulnerabilità, gli audit e le correzioni e il rilevamento e la risposta degli endpoint (EDR) semplifica la sicurezza dei carichi di lavoro e crea collaborazione tra IT Ops, SecOps e DevOps.

Sicurezza intrinseca per i carichi di lavoro nel cloud

Come mostrato in questo white paper, l'adozione di tecnologie diverse per gestire i carichi di lavoro nel cloud complica i rischi e, in ultima analisi, non è scalabile. Al contempo, è fondamentale permettere a ogni team, IT Ops, DevOps e SecOps, di utilizzare la propria console. Questo non vuol dire che la migrazione al cloud richieda l'adozione di un processo completamente nuovo, di una nuova UI o di una console di gestione. Del resto, questi team hanno già abbastanza di cui occuparsi.

L'approccio con sicurezza intrinseca di VMware include il monitoraggio profondo e l'analisi del comportamento in ogni punto di controllo, ovvero cloud, carico di lavoro, endpoint, rete e identità, che sono poi unificati per offrire piena consapevolezza del contesto. Come una videocamera che registra ogni movimento in ciascun punto di controllo, la sicurezza intrinseca rende possibile la piena consapevolezza del contesto. Poiché non è necessario unire manualmente la telemetria da punti di controllo diversi, i team possono rintracciare rapidamente le minacce dal punto di accesso e in tutti i passaggi intermedi.

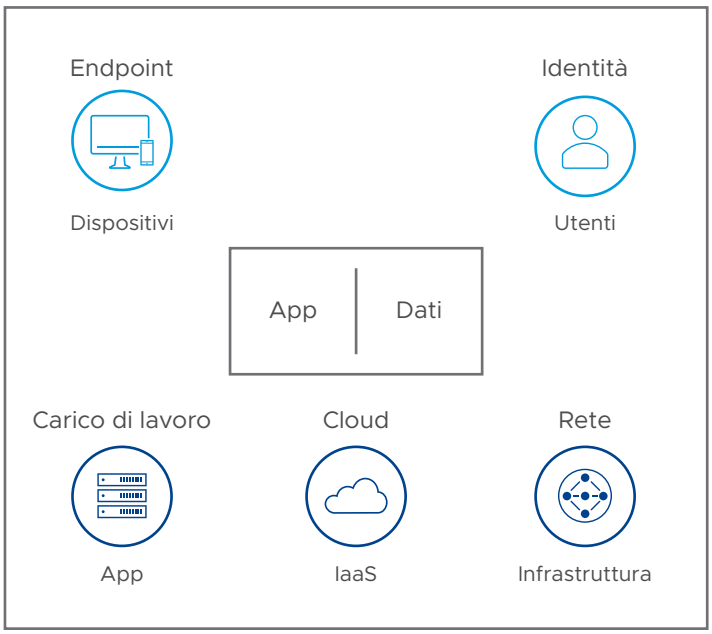


FIGURA 1. I CINQUE PUNTI DI CONTROLLO DELLA SICUREZZA INTRINSECA

Protezione scalabile dei carichi di lavoro nel cloud

VMware Carbon Black Cloud offre tutte le funzionalità per una protezione scalabile dei carichi di lavoro nel cloud e si integra in modo nativo con vSphere e NSX. Grazie a questa stretta integrazione, gli amministratori vSphere e gli amministratori NSX possono accedere a tutti i dati delle minacce rilevanti nel contesto dei loro rispettivi domini e nella stessa console ottimizzata per i loro ruoli.

Oltre a fornire consapevolezza completa del contesto all'interno di uno stesso cloud e tra cloud, carichi di lavoro, endpoint, reti e identità, VMware Carbon Black Cloud offre il sistema di record comune per IT Ops, DevOps e SecOps per prevenire, rilevare e correggere le minacce che hanno un impatto su app e carichi di lavoro cruciali.

I componenti fondamentali della sicurezza intrinseca sono:

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

VMware Carbon Black Cloud è una piattaforma di protezione dei carichi di lavoro nativa per il cloud che unisce il rafforzamento dei sistemi e la prevenzione dei comportamenti intelligenti necessari per tenere a bada le minacce emergenti, utilizzando una singola gestione del ciclo di vita e una console semplice da utilizzare.

VMware vSphere

vSphere è la piattaforma di compute virtualization leader del settore che è stata riarchitettata con *Kubernetes* nativo per permettere ai clienti di modernizzare i carichi di lavoro eseguiti su vSphere.

VMware NSX Advanced Threat Prevention™

Basato su un algoritmo di apprendimento automatico, VMware NSX Service-defined Firewall™ offre funzionalità di analisi del traffico sulla rete, rilevamento e prevenzione delle intrusioni e analisi avanzata del malware con funzionalità complete di rilevamento e risposta della rete.

Protezione dei carichi di lavoro nel cloud VMware: come funziona

L'approccio con sicurezza intrinseca di VMware consente alle aziende di proteggere i carichi di lavoro nel cloud utilizzando l'infrastruttura esistente per identificare i rischi in modo proattivo, impedire exploit ed esposizioni e rilevare e rispondere rapidamente a minacce nuove ed emergenti.

Il processo in tre fasi funziona come mostrato di seguito ed è supportato da controlli di sicurezza essenziali.

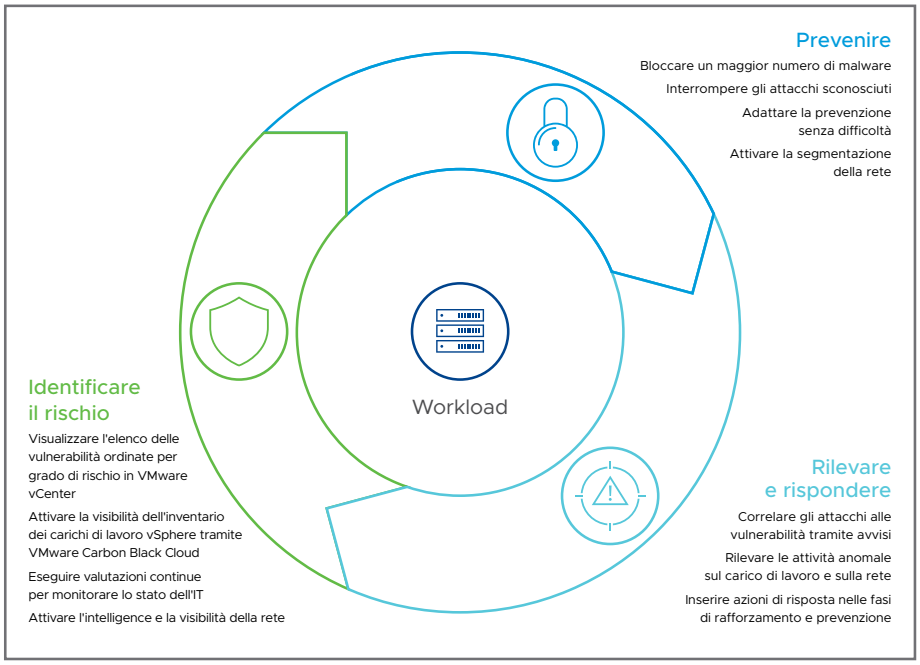


FIGURA 2. La sicurezza intrinseca per i carichi di lavoro nel cloud assicura una protezione completa per i carichi di lavoro vSphere.

Fase 1: identificare il rischio

- **Controllo dell'integrità dello stato iniziale:** VMware Carbon Black Cloud controlla l'integrità dello stato iniziale per confermare che il sistema in cui viene installato il carico di lavoro è pulito, compliant e appropriato per il tipo di carico di lavoro. Inoltre, acquisisce e analizza i livelli delle patch del SO, valuta le vulnerabilità e le configurazioni non corrette e determina se è necessario un ulteriore rafforzamento.
- **Visibilità continua dello stato del sistema:** VMware Carbon Black Cloud identifica lo scostamento della configurazione, la presenza di applicazioni sconosciute o non autorizzate, le vulnerabilità e altre attività dinamiche che aumentano la superficie di attacco dell'ambiente. Ad esempio, è in grado di:
  - Monitorare qualsiasi cambiamento che indica la presenza di attività pericolose (azzeramento delle password, modifiche della configurazione BitLocker)
  - Controllare e correggere interrogando 1.500 artefatti per ogni carico di lavoro ed endpoint in private cloud e public cloud
  - Consentire agli amministratori di eseguire query SQL personalizzate per analizzare attività o comportamenti pericolosi specifici
- **Visibilità continua delle vulnerabilità e dell'attività della rete:** VMware Carbon Black Cloud consente agli amministratori vSphere di visualizzare le vulnerabilità dei carichi di lavoro più rischiose in VMware vCenter® ed esegue periodicamente valutazioni delle vulnerabilità senza scansione nei carichi di lavoro. NSX fornisce un firewall distribuito integrato, in modo che i team IT Ops possano monitorare la comunicazione dei carichi di lavoro tra private cloud e public cloud, determinare quali carichi di lavoro fanno parte di un'app e capire come segmentare i carichi di lavoro non collegati.

Fase 2: prevenire l'escalation dei rischi

- **Prevenire gli exploit sul carico di lavoro:** VMware Carbon Black Cloud distribuisce software antivirus di nuova generazione (NGAV) per una protezione che va oltre gli indicatori dei punti temporali per malware, ransomware, attacchi zero-day, varianti rapide, file sospetti e processi potenzialmente indesiderati (PUP) specifici per i carichi di lavoro in private cloud e public cloud. La piattaforma VMware include file nascosti per individuare i ransomware, analisi dinamiche e apprendimento automatico per assicurare un'analisi continua capace di prevenire l'esecuzione di file sospetti.
- **Prevenire gli attacchi senza malware:** oltre a bloccare gli attacchi con malware, VMware Carbon Black Cloud protegge contro i più recenti attacchi persistenti che utilizzano malware senza file e tattiche basate sulla memoria e LotL (living-off-the-land). Questi attacchi pericolosi sfruttano software esistenti, app consentite (ad esempio, PowerShell) e protocolli autorizzati per eseguire le attività illecite. Diversamente dagli approcci legacy basati solo sulle minacce note, la piattaforma VMware è in grado di identificare nuove varianti ed exploit zero-day mettendo insieme comportamenti connessi.
- **Prevenire gli attacchi basati sulla rete:** NSX Service-defined Firewall protegge i carichi di lavoro contenendo gli spostamenti laterali e bloccando gli exploit in ingresso di servizi e app vulnerabili. Con questo livello di visibilità, è possibile comprendere in che modo gli attacchi LotL si spostano sulla rete, identificare gli indicatori di compromissione (IOC) e bloccare queste connessioni di rete per isolare i carichi di lavoro dall'azione degli hacker.
- **Personalizzare la prevenzione:** ogni ambiente ha limiti operativi diversi e spesso contrastanti. VMware offre ai clienti la possibilità di trovare un equilibrio tra sicurezza e rischi operativi con una granularità precisa. Con il motore delle policy VMware, è possibile scegliere come mitigare le minacce sulla base del tipo specifico di carico di lavoro, della sua funzione, della criticità e della vicinanza ad altri carichi di lavoro cruciali. Ad esempio, per isolare un carico di lavoro mission critical, un amministratore di sistema può impedire che PowerShell effettui lo scraping della memoria di un altro processo o richiami un'applicazione non affidabile.

Fase 3: rilevare e rispondere ai rischi continui

- **Sapere quando e dove iniziare un'analisi (dettaglio):** è possibile utilizzare la funzione di rilevamento delle minacce VMware pronta all'uso tramite l'intelligence sulle minacce aggiornata di VMware Threat Analysis Unit™ per identificare i sistemi interessati e isolarli in modo da correggerli. Le API VMware consentono di integrare feed e watchlist di terze parti e di arricchire la condivisione collaborativa delle informazioni sulle minacce grazie all'efficace User Exchange di VMware.
- **Vedere l'intero ambito e le tempistiche dell'attacco (generale):** la piattaforma VMware consente a chi effettua le indagini di riavvolgere il nastro e capire come è avvenuto un attacco, quali sistemi ha colpito e come è proseguito nel tempo. Poiché VMware acquisisce tutti i dati (ad esempio, attività dettagliate del processo, interazione tra processo e processo, rapporti tra i processi padre-figlio, ecc.), la creazione di una linea temporale dettagliata senza punti ciechi dopo l'evento permette di dare una risposta agli incidenti, consentendo ai team legali di arrivare alla verità.
- **Workflow rapido dal rilevamento alla prevenzione:** in questi tre semplici passaggi, VMware Carbon Black Cloud consente di tradurre il rilevamento delle minacce in una policy di prevenzione standardizzata tra i carichi di lavoro. È innanzitutto necessario applicare policy automatiche basate su rilevamenti personalizzati per i propri carichi di lavoro. Quindi è possibile visualizzare in anteprima gli effetti a valle della policy di prevenzione prima che venga applicata. Infine, con un solo clic, distribuire la policy aggiornata ai carichi di lavoro in qualsiasi ambiente.

La protezione dei carichi di lavoro nel cloud contro un'ampia gamma di minacce richiede un approccio su più fronti, con una visibilità granulare e, al tempo stesso, unificata di tutti gli aspetti dell'ambiente di elaborazione. IT Ops, DevOps e SecOps devono lavorare in sinergia per condividere la responsabilità della protezione dei carichi di lavoro cruciali nel cloud. Le aziende che tentano di utilizzare gli approcci tradizionali per proteggere gli hybrid cloud devono affrontare molte sfide, come la mancanza di visibilità della connessione tra i carichi di lavoro, processi frammentati e configurazioni non corrette. Come discusso in questo white paper, migliorare la visibilità, velocizzare il ripristino e semplificare la sicurezza sono le tre strategie chiave che i team aziendali devono adottare per contenere i rischi.

VMware è l'unica azienda in grado di proteggere i carichi di lavoro negli hybrid cloud. In particolare, le soluzioni VMware consentono ai team di identificare in modo preciso i rischi emergenti per i carichi di lavoro, impedendone l'escalation e contenendo le violazioni rapidamente senza interrompere le operation. Mentre altri prodotti per la sicurezza degli endpoint e dei carichi di lavoro raccolgono solo un set di dati relativo agli hacker noti, VMware Carbon Black Cloud raccoglie continuamente dati completi sulla rete, gli endpoint e i carichi di lavoro e analizza le modalità di comportamento degli hacker per bloccare in modo proattivo gli attacchi prima che possano verificarsi. Questo più alto grado di visibilità operativa semplifica la sicurezza e accelera il ripristino del sistema.

Sono molti i vendor che offrono prodotti per la protezione dei carichi di lavoro nel cloud, ma non tutte le soluzioni sono uguali. Le aziende devono considerare i requisiti chiave, come l'architettura di progettazione, i modelli operativi e la scalabilità e porsi le domande giuste per stabilire in che misura la piattaforma risponde alle loro esigenze. La checklist della Tabella 2 è un utile strumento di analisi nella scelta delle piattaforme di protezione dei carichi di lavoro nel cloud. Con 100 punti da assegnare, dare un punteggio per ogni domanda rispetto alla situazione della propria organizzazione. Il valore totale della colonna Valore ponderato deve essere 100. Completando questa checklist, sarà possibile capire meglio quali sono le priorità e le considerazioni principali.

Checklist di valutazione della piattaforma di protezione dei carichi di lavoro nel cloud

	REQUISITI CHIAVE	DOMANDE CHIAVE	VALORE PONDERATO
Architettura di progettazione	Descrivere in che modo la piattaforma di protezione dei carichi di lavoro visualizza le comunicazioni e le connessioni tra i carichi di lavoro.	È in grado di consolidare i dati di telemetria tra cloud, carichi di lavoro, reti ed endpoint?	
		Supporta qualsiasi applicazione indipendentemente dal sistema operativo, dalla configurazione e dal cloud oppure dipende da tutti questi elementi?	
		Può riconoscere un comportamento normale all'interno di un carico di lavoro o tra carichi di lavoro diversi?	
		Quali modelli di comportamento distribuisce per rilevare attacchi malware e non malware (senza file) all'interno di carichi di lavoro e tra carichi di lavoro?	
Modello operativo	Descrivere in che modo la piattaforma di protezione dei carichi di lavoro nel cloud supporta l'allineamento e la coordinazione senza attriti tra IT Ops, DevOps e SecOps per ridurre il rischio, semplificare la compliance e aumentare la resilienza.	Quanti agenti è necessario installare su ciascun carico di lavoro, container o sistema operativo?	
		I team IT Ops, DevOps e SecOps sono in grado di utilizzare lo stesso set di dati durante il monitoraggio e la risposta agli incidenti?	
		Quali framework di governance supporta la piattaforma (ad esempio, NIST 800-53)?	
		Qual è un normale workflow tra IT Ops, DevOps e SecOps dopo l'identificazione di una minaccia, una vulnerabilità o un errore di configurazione?	
Scalabilità	Descrivere in che modo la piattaforma di protezione dei carichi di lavoro supporta programmi sicuri ma rapidi per il controllo delle modifiche per migliorare la standardizzazione delle policy di sicurezza e ridurre il rischio di errori di configurazione e altri errori umani secondo necessità.	Qual è il consumo medio della CPU per ciascun agente di protezione dei carichi di lavoro nel cloud?	
		È in grado di consolidare più funzionalità di sicurezza, come EDR, NGAV e gestione delle vulnerabilità, in un singolo agente e un'unica console di gestione?	
		La piattaforma di protezione dei carichi di lavoro nel cloud è in grado di applicare e generare report su una policy di sicurezza standardizzata e coerente negli ambienti di private cloud, public cloud e hybrid cloud?	
		In che modo analizza periodicamente le vulnerabilità senza compromettere la disponibilità e le prestazioni?	

TABELLA 2. Checklist di valutazione della piattaforma di protezione dei carichi di lavoro nel cloud

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc. - Via Spadolini 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.com/it