Metti in sicurezza il tuo ambiente con la Invisible Security di Nutanix

Proteggi applicazioni e dati per impedire la diffusione del malware nei cloud ibridi

PRINCIPALI VANTAGGI

Proteggi i dati e previeni le violazioni

- Crittografa i dati a riposo
- Controlla e limita l'accesso ai dati sensibili
- Analizza e verifica le configurazioni di sicurezza
- Proteggi i tuoi cloud ibridi
- Previeni la diffusione del ransomware

Segmenta e proteggi le reti

- Implementa la microsegmentazione e l'ispezione della rete in pochi minuti
- Separa gli ambienti regolamentati tramite controlli software automatizzati

Semplifica le attività per la regolamentazione e la conformità

- Automatizza la configurazione della baseline di sicurezza delle piattaforme
- Convalida la conformità rispetto alle policy normative (HIPAA, PCI, NIST, ecc.)

LA SICUREZZA DEL CLOUD IBRIDO INIZIA DA UNA SOLIDA BASE INFRASTRUTTURALE

Sono tante le ragioni che rendono difficile garantire la sicurezza negli ambienti moderni. Molti stack infrastrutturali tradizionali includono prodotti svincolati dallo stack venduti da vendor differenti, e la conseguenza di questa eterogeneità è un controllo ristretto e limitato della sicurezza: validare e garantire una security baseline tramite aggiornamenti continui del software richiede non solo molto tempo, ma spesso anche interventi manuali soggetti a errori — il tutto a discapito dell'innovazione e della produttività.

Nell'era del cloud, la sicurezza deve essere radicata nella cultura aziendale e deve essere parte essenziale del processo decisionale, in modo da soddisfare i requisiti stringenti di conformità normativa e poter affrontare con successo le sfide imposte dalla continua evoluzione del panorama delle minacce informatiche. Le aziende devono impegnarsi a integrare l'automazione nei processi che permettono di garantire la sicurezza dell'infrastruttura se vogliono evitare gli errori umani e raggiungere la perfetta scalabilità senza però compromettere la sicurezza in un ambiente in continua evoluzione.

RIPENSARE LA SICUREZZA PER UN FUTURO DI CLOUD IBRIDO

La sicurezza del cloud ibrido inizia da una solida base infrastrutturale. La soluzione leader di settore di Nutanix fornisce non solo valore operativo e finanziario, ma permette anche di migliorare il livello di sicurezza generale e prevenire la violazione dei dati applicando una strategia di difesa in profondità per la sicurezza del cloud ibrido.

Platform Security

Application and Network Security

SecOps and Compliance

NUTANIX

STANDARD E CERTIFICAZIONI

Nutanix adotta molteplici standard di sicurezza e programmi di convalida e rispetta i più severi standard internazionali — inclusi numerosi standard ISO, SOC, e FIPS — per garantire i risultati attesi e il perfetto funzionamento dei prodotti Nutanix con la tecnologia esistente a governi e aziende di tutto il mondo.

Visita nutanix.com/trust per conoscere tutti i dettagli

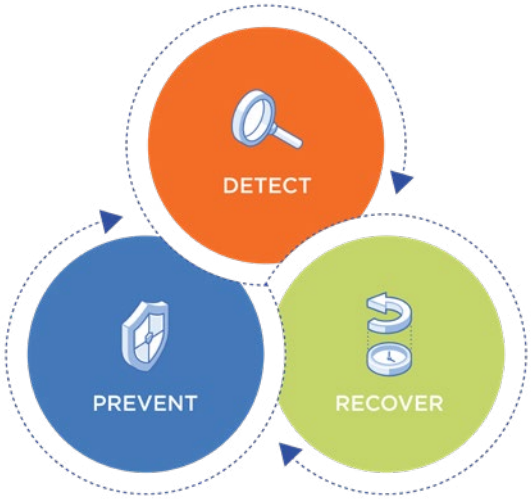
DIFESA A OGNI LIVELLO

Sicurezza della piattaforma: la sicurezza è un aspetto fondamentale della progettazione dei prodotti Nutanix a cominciare dalle pratiche di hardening integrate nella piattaforma Enterprise Cloud (crittografia dei dati a riposo, controlli completi degli accessi, e così via). Le best practice del settore e gli standard governativi sono parte di un processo automatizzato di monitoraggio delle configurazioni e di riparazione automatica che permette di soddisfare gli obiettivi di conformità. Il rischio di violazioni dei dati è ridotto al minimo grazie a test rigorosi per le vulnerabilità più diffuse e a patching frequenti. Le incongruenze vengono registrate e la baseline di sicurezza viene ripristinata, garantendo così una configurazione coerente della sicurezza.

Sicurezza delle applicazioni e delle reti: Nutanix Flow offre sicurezza di rete avanzata nel datacenter garantendo visibilità sulle applicazioni e bloccando la diffusione di minacce informatiche come il ransomware. Reti e applicazioni possono essere facilmente segmentate tramite una policy definita dal software, il tutto senza bisogno di hardware aggiuntivo o configurazioni di rete complesse. La funzionalità nativa di microsegmentazione della rete semplifica e automatizza l'applicazione di policy di rete granulari grazie al suo modello di rilevamento, visualizzazione e applicazione di policy tra le VM.

SecOps, conformità e auditing: Flow Security Central offre visibilità sul livello di sicurezza generale del cloud ibrido, assistenza nella gestione delle policy, controlli delle configurazioni e convalida della conformità per l'HCI Nutanix. Security Central utilizza una serie di controlli di sicurezza automatizzati per rilevare e correggere le vulnerabilità di sicurezza dell'infrastruttura e gli errori di configurazione. Gli amministratori addetti alla sicurezza possono creare criteri automatici per porre rimedio alle vulnerabilità in tempo reale. Security Central, inoltre, aiuta a convalidare il livello di conformità rispetto a linee guida quali PCI-DSS, HIPAA, NIST e altre ancora, offrendo una soluzione sempre attiva per la conformità di sicurezza.

Prevenzione, rilevamento e ripristino: non esiste un'azione, una soluzione software o un controllo di sicurezza specifico capace di mettere la tua organizzazione totalmente al riparo dalle minacce del malware e del ransomware. La soluzione migliore consiste in un approccio a più livelli, comunemente definito come strategia di "difesa in profondità". Insieme ai controlli e alle protezioni già presenti nel datacenter, un piano completo per la sicurezza dovrebbe includere tutte le funzionalità integrate di Nutanix per ridurre al minimo la spesa operativa e finanziaria.



NUTANIX

AFFIDATI A NUTANIX PER LA TUA STRATEGIA DI DIFESA INFORMATICA

Piattaforma HCI

- Configurazione della baseline di sicurezza con riparazione automatica
- Snapshot dello storage e punti di ripristino
- Automazione della data protection, delle repliche e dei runbook
- Crittografia dei dati a riposo con convalida FIPS 140-2
- Segmentazione del piano dei dati e del piano di controllo
- Virtualizzazione nativa — progettata per la sicurezza

Applicazione di patch e aggiornamenti

- Patching delle CVE, aggiornamenti della piattaforma e gestione del ciclo di vita “one-click”
- Gestione dell'aggiornamento di firmware e BIOS

Gestione e automazione

- Controllo degli accessi basato sui ruoli (RBAC)
- Gestione dell'identità e degli accessi
- Analitiche delle risorse, insight, e rilevamento delle anomalie
- Automazione senza bisogno di codice e trigger basati su eventi
- Automazione e blueprint delle applicazioni per garantire un'esecuzione organica delle policy

Networking e sicurezza

- Segmentazione della rete e delle applicazioni
- Visibilità sulle applicazioni e sulla rete
- Ispezione approfondita dei pacchetti e integrazioni dei partner per l'analisi delle minacce
- Logging delle policy e degli eventi
- Strumenti per la conformità di sicurezza e per l'auditing

Servizi di storage

- Policy di blocco dei file in base alla loro tipologia
- Rilevamento delle anomalie nelle attività dei file
- Supporto del protocollo ICAP per l'integrazione con antivirus
- Supporto delle policy WORM immutabili

Backup, business continuity e disaster recovery

- Replica e data protection native
- Soluzioni di archiviazione e backup per lo storage secondario
- Disaster Recovery-as-a-Service nel cloud

NUTANIX™
YOUR ENTERPRISE CLOUD

Tel. Milano +390287259332 | Tel. Roma +390679251100
info-italy@nutanix.com | www.nutanix.it | @NutanixItaly