APPLIANCE DELL EMC VXRAIL - PROGETTATI PER LA SICUREZZA COMPLETA

Abstract

L'appliance VxRail™, la piattaforma ideale per l'infrastruttura IT e la trasformazione della sicurezza, offre più livelli di protezione per i dati e le applicazioni aziendali. Solo le aziende del gruppo Dell Technologies sono in grado di offrire tutte le soluzioni end-to-end necessarie per stare al passo con un panorama di minacce in continua evoluzione. Questa guida tratta funzionalità di protezione integrate e opzionali, best practice e tecniche comprovate per la protezione del VxRail dal core all'edge, fino al cloud.

Marzo 2020

Sommario

Sommario 2
INTRODUZIONE 4
LA TRASFORMAZIONE DELLA SICUREZZA INIZIA CON DELL TECHNOLOGIES 5
Un ponte verso il futuro digitale 7
CREAZIONE DI FIDUCIA CON I PROGRAMMI DELL EMC PRODUCT SECURITY 7
Secure Development LifeCycle (SDL) 7
Sviluppo sicuro 8
Risposta alle vulnerabilità di Dell EMC 9
Risk management della supply chain 9
Collaborazione nel settore per migliorare la sicurezza dei prodotti 10
Partecipazione a gruppi di sicurezza dei prodotti del settore 11
VxRail: la base per la modernizzazione del data center e la trasformazione dell'IT 12
Dell EMC VxRail HCI System Software 13
VMware vSphere 14
VMware vCenter Server 15
Hypervisor VMware ESXi 15
Rete virtuale VMware 15
VMware vSAN 15
Storage Policy Based Management (SPBM) 16
VMware vRealize Log Insight 17
VMware Cloud Foundation (VCF) con NSX 17
Funzionalità di sicurezza VxRail 18
SICUREZZA DEI DATI 18
Riservatezza 18
Integrità 20
Disponibilità 21
SICUREZZA DEL SISTEMA 23
Framework AAA (Authentication, Authorization and Accounting - Autenticazione, Autorizzazione e Contabilità) di VxRail 23
Sicurezza della posizione fisica di VxRail 24
Automazione 24
VxRail STIG Hardening Package 25
Sicurezza integrata in VxRail ACE 25
Panoramica sulla sicurezza di VxRail ACE 26
Data collection di VxRail ACE 26
Dati di VxRail ACE in transito verso Dell 26

Dati at-rest di VxRail ACE 27
Controllo degli accessi ai dati di VxRail ACE 27
Accesso a VxRail ACE per gli utenti finali 27
Accesso amministrativo all'infrastruttura VxRail ACE gestita dall'IT di Dell EMC 28
Standard e certificazioni compatibili 28
NIST Cybersecurity Framework e VxRail 30
Soluzioni e partner per la sicurezza di VxRail 31
Gestione delle identità e degli accessi 31
Gestione di incidenti ed eventi di sicurezza 31
Server di gestione delle chiavi 32
Altri partner per la sicurezza 32
Conclusioni 33

INTRODUZIONE

Le organizzazioni di tutti i settori stanno modernizzando e trasformando il modo in cui operano e offrono prodotti e servizi differenziati. L'importanza del luogo in cui si trovano i dati, del modo in cui vi si accede e del numero di dispositivi, dal core all'edge, fino al cloud, cresce a un ritmo esponenziale. La sicurezza sarà sempre una parte dell'IT, con particolare attenzione all'autenticazione, ai firewall, alla conformità e ai criminali informatici. La sicurezza non è più una serie di progetti, ma un ciclo di vita continuo che richiede un'analisi e una revisione costanti. Dell Technologies ritiene che la sicurezza non rallenti ma, al contrario, acceleri l'innovazione, permettendo alle aziende di pensare in nuovi modi strategici e di cogliere l'opportunità.

Dell EMC VxRail offre il percorso più semplice e rapido per questa trasformazione della sicurezza, dal core all'edge, fino al cloud. VxRail fornisce un'infrastruttura agile con un'integrità full-stack e una gestione end-to-end del ciclo di vita per aumentare l'efficienza operativa, ridurre i rischi e consentire ai team di concentrarsi sull'attività aziendale. L'adozione dei sistemi VxRail, che eliminano i silo operativi e favoriscono l'innovazione continua attraverso il rapido provisioning e deployment dei carichi di lavoro, determina un notevole risparmio sui costi e un'elevata efficienza operativa, consentendo alle organizzazioni di IT di promuovere le opportunità di business anziché limitarsi a supportare le operazioni aziendali. Creato per VMware, con VMware e per migliorare VMware, VxRail è il primo e unico sistema HCI progettato congiuntamente con VMware per eliminare la complessità operativa di deployment, provisioning, gestione, monitoraggio e aggiornamento dell'infrastruttura iperconvergente VxRail.

VxRail è dotato di una sicurezza incorporata in tutti i livelli dello stack tecnologico integrato, a partire da ogni processore e server PowerEdge fino a VxRail HCI System Software, incluso il software VMware incorporato. La protezione di core, edge e cloud assicura disponibilità, integrità e sicurezza per ogni carico di lavoro, sia tradizionale che nativo per il cloud.

LA TRASFORMAZIONE DELLA SICUREZZA INIZIA CON DELL TECHNOLOGIES

In Dell Technologies trasformazione della sicurezza significa ripensare la protezione e accelerare l'innovazione. Dell Technologies si concentra sulla sicurezza a tutti i livelli, dalle collaborazioni tra le sue società fino al prodotto sviluppato e rilasciato. VxRail non fa eccezione, è realizzato con i massimi livelli di garanzia di sicurezza dei prodotti e fornisce funzionalità di sicurezza completamente integrate che possono essere utilizzate dall'organizzazione per ottimizzare la resilienza della sicurezza informatica dal core all'edge (vedere la figura seguente), fino al cloud per accelerare l'innovazione.

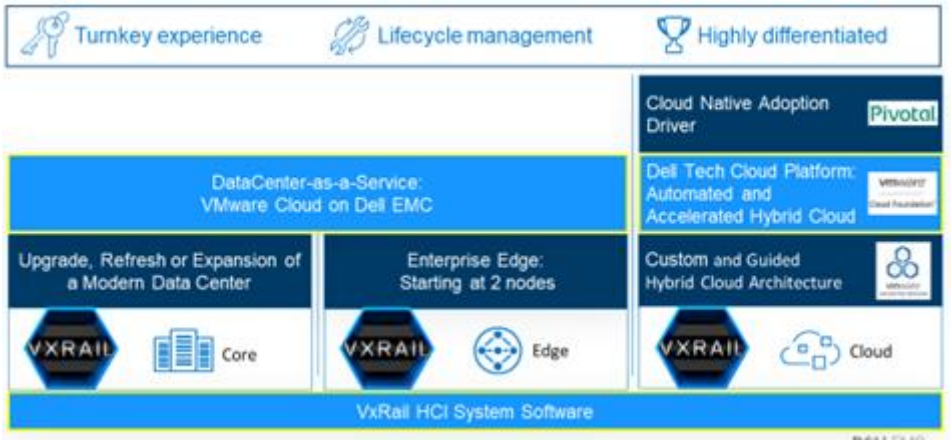

Figura 1: dal core all'edge fino a cloud

Riportato da Forbes; in base a un recente studio sulla sicurezza basata sul rischio, 2019 MidYear QuickView Data Breach Report, nei primi sei mesi del 2019 si sono verificate oltre 3.800 violazioni, con l'esposizione dell'incredibile numero di 4,1 miliardi di record. In base a questi numeri, le violazioni potrebbero superare i 6.515 eventi di compromissione dei dati che erano stati segnalati nel 2018 dalla stessa azienda.

Dell Technologies può garantire che le tue strategie di sicurezza rimangano al passo con le tue iniziative di modernizzazione per ridurre il rischio aziendale.

1. Unificare i programmi di sicurezza con il rischio aziendale complessivo per sapere quali rischi valga la pena correre.
2. Implementare operazioni di sicurezza avanzate che si adattino al panorama mutevole delle minacce per poter rispondere con efficacia alle minacce stesse.
3. Creare una moderna infrastruttura resiliente che protegga endpoint, rete, applicazioni e dati.
4. Avvalersi di servizi di consulenza affidabili per progettare e implementare il proprio programma di trasformazione della sicurezza. Dell Technologies si trova in una posizione unica per aiutarti a gestire tutte queste aree.

Se, da una parte, è necessario implementare una difesa stratificata con più livelli di sicurezza, è altrettanto importante che questi elementi interagiscano tra loro. La trasformazione della sicurezza inizia da una moderna infrastruttura cyber-resiliente come VxRail, progettata e realizzata pensando alla sicurezza.

L'attuale panorama delle minacce in evoluzione richiede un cambiamento nell'approccio finalizzato a prevenire o mitigare queste minacce. Un'infrastruttura obsoleta è difficile da difendere. Inoltre, l'utilizzo di diversi prodotti di più fornitori aggiunge complessità e aumenta il rischio di vulnerabilità che possono essere sfruttate. Questo livello di complessità offre diversi punti di ingresso agli aspiranti criminali.

È inoltre necessario prendere in considerazione gli standard di sicurezza e la conformità. Sono spesso previste ingenti sanzioni giuridiche e pecuniarie per la mancata conformità. Per quanto onerose, queste sanzioni hanno un impatto minore rispetto agli effetti che una violazione può provocare sulla reputazione di un'azienda. In generale, tutti sono meno propensi a fare affari con un'azienda che ha subito una violazione.

- Payment Card Industry Data Security Standard (PCI DSS): protezioni per i titolari di carta di credito
- General Data Protection Regulation (GDPR): normativa dell'Unione europea sulla privacy dei dati
- Bundesdatenschutzgesetz (BDSG) tedesca: disciplina dettagliata della protezione dei dati
- Sarbanes-Oxley Act (SOX): protezione dei dati sensibili in relazione al reporting finanziario nelle società pubbliche
- Gramm-Leach-Bliley Act (GLBA): protezione dei dati personali non pubblici (NPPI) nel settore dei servizi finanziari
- Health Insurance Portability & Accountability Act (HIPAA): protezione di informazioni e dati sanitari dei pazienti in formato elettronico
- California Consumer Privacy Act (CCPA): perfezionamento dei diritti sulla privacy e della tutela dei consumatori per i residenti della California (convertito in legge il 28/06/2018)

Dell Technologies ritiene che la trasformazione della sicurezza preveda la disponibilità di un partner di fiducia, un partner che contribuisca a gestire il rischio digitale, fornisca servizi di sicurezza gestiti, apporti competenze, servizi, soluzioni e prodotti a protezione di tutto lo stack (dall'infrastruttura alle applicazioni) e che semplifichi le operazioni rendendo la sicurezza una parte essenziale della strategia aziendale.

Dell Technologies è un partner affidabile per la trasformazione della sicurezza. Che si tratti di endpoint, data center, sviluppatori, identità, operazioni di sicurezza, cloud o virtualizzazione, la sicurezza oggi deve essere end-to-end e Dell Technologies può essere di aiuto. Siamo in grado di aiutare nella gestione del rischio aziendale e correlato alla sicurezza, nella gestione delle violazioni della sicurezza, nel ripristino da un attacco ransomware e nella creazione di applicazioni sicure. La sicurezza ha notevoli implicazioni, positive e negative, per molte persone. In un caso o nell'altro, Dell Technologies desidera accompagnare le organizzazioni in questo percorso.

Un ponte verso il futuro digitale

Ci troviamo in un momento in cui l'IT viene utilizzato più che mai per risolvere i problemi aziendali. A questo scopo, le organizzazioni implementano analisi dei dati, intelligenza artificiale, nuove applicazioni e dispositivi smart per generare enormi quantità di dati. Questi dati consentono di ottenere informazioni strategiche e vantaggi esclusivi sulla concorrenza. Nonostante ciò, molte organizzazioni non dispongono ancora di una chiara visione e strategia digitale; utilizzano tecnologie obsolete che creano vincoli e una cultura resistente al cambiamento. Senza un piano adeguato, queste organizzazioni finiscono spesso per pensare ai rischi e alla sicurezza solo in un secondo momento oppure questi aspetti semplicemente non fanno parte della più ampia discussione sulla strategia. A questo punto cruciale della tecnologia, questo modo reattivo di fare business non può più esistere. Per accelerare l'innovazione e realizzare il potenziale del futuro digitale, le organizzazioni devono ripensare il modo in cui si approcciano alla sicurezza.

Nel mondo dell'IT, la sicurezza è in genere considerata più un ostacolo che un acceleratore di cambiamenti positivi. Nella quotidianità, la gestione di questo aspetto può essere un compito ingrato e il management ha difficoltà a intravedere un ritorno sull'investimento. Il personale che si occupa di sicurezza deve gestire minacce crescenti e sistemi complicati e mantenere una conoscenza approfondita di un panorama in continua evoluzione. Le numerose notizie che sembrano arrivarci ogni giorno sugli attacchi informatici peggiorano solo questo stress, esattamente come la preoccupante sensazione che tutto ciò che l'organizzazione possiede possa andare perduto in un secondo. La sicurezza non deve essere tuttavia così caratterizzata da paura e frustrazione. La sicurezza ha sempre cercato di essere più positiva e proattiva, ma ciò è possibile solo con la giusta mentalità e tecnologia. Non possiamo continuare a pensare alla sicurezza e al rischio come in passato. Per porre questo cambiamento nella giusta prospettiva, pensiamo ai freni di un'automobile. Inizialmente si potrebbe pensare che i freni servano solo a rallentare, mentre consentono anche di andare più veloce. Offrono la sicurezza per accelerare mettendo in condizione di affrontare gli ostacoli e la strada che si hanno di fronte. Anche la sicurezza e il rischio devono essere considerati acceleratori delle organizzazioni e non un vincolo che le rallenta.

CREAZIONE DI FIDUCIA CON I PROGRAMMI DELL EMC PRODUCT SECURITY

Dell EMC ha iniziato a formulare le policy di sicurezza dei prodotti nel 2002, quando l'azienda è passata dall'essere principalmente un fornitore di hardware di storage all'essere un fornitore di software di livello aziendale. La società ha implementato il proprio programma di risposta alle vulnerabilità nel 2004 e ha stabilito una policy di sicurezza dei prodotti a livello aziendale nel 2005. La policy adotta standard di sicurezza ampi ma chiari che abbracciano la gamma completa di prodotti Dell EMC. Questa policy è stata continuamente aggiornata e nel 2007 è stata integrata nel nuovo SDL (Security Development Lifecycle) dell'azienda. SDL ha instillato una serie di prassi di sicurezza misurabili e ripetibili in ogni fase dello sviluppo e del deployment dei prodotti. Nel 2012, l'azienda ha inoltre formalizzato un programma di risk management della supply chain per estendere le prassi di sicurezza ai fornitori di componenti di Dell EMC. Dell EMC continua a perfezionare i propri programmi di sicurezza dei prodotti, all'avanguardia negli standard e nei processi del settore.

Con VxRail, Dell EMC prosegue l'impegno verso la sicurezza. Il ciclo di vita dello sviluppo di VxRail segue l'abbinamento tra processo di sviluppo Dell EMC Product Security e Security Development Lifecycle. Il Dell EMC Security Development Lifecycle segue un approccio rigoroso per rendere sicuro lo sviluppo dei prodotti e prevede un risk management a livello executive prima dell'introduzione dei prodotti nel mercato. Inoltre, VMware vSphere è una parte significativa dell'infrastruttura iperconvergente VxRail, sviluppato anch'esso con un Security Development Lifecycle simile.

Secure Development LifeCycle (SDL)

Il Dell EMC Security Development Lifecycle descrive l'insieme di attività necessarie per tutto il ciclo di vita del prodotto, al fine di creare resilienza della sicurezza e funzionalità di sicurezza coerenti nei prodotti, oltre a rispondere tempestivamente a vulnerabilità di sicurezza segnalate all'esterno. In linea con le best practice del settore, Dell EMC si basa su una serie di controlli implementati dalle organizzazioni di R&S dei prodotti. La figura 2 mostra alcune delle attività tipiche svolte nell'ambito del processo SDL.

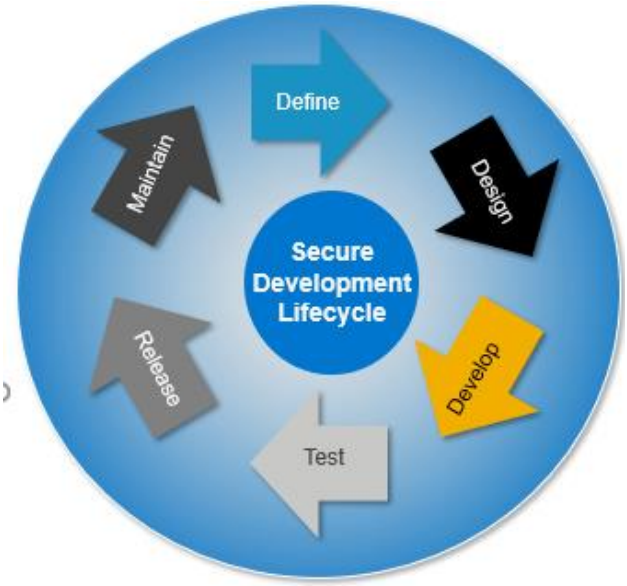

Figura 2: attività SDL di Dell EMC

L'implementazione e la convalida di questi controlli sono guidate da esperti della sicurezza all'interno delle organizzazioni di R&S che operano in stretta collaborazione con i consulenti della sicurezza del Product Security Office (PSO). La figura 3 illustra il modo in cui questo processo SDL si riflette su un tipico ciclo di vita agile.

Agile Development Activity		SDL Activity
High Level Planning	Requirements	• Formalize security requirements in PRD/PCD • Product Security Training
	Architecture	• **Threat Modeling** • **Security Testing** (test planning)
Sprint 1..*n*	Design	• Update **threat model**
	Develop	• **Static Analysis**
	Test	• **Security Testing**
	Release	• **Security Scanning** • **Security Configuration Guide** • Inventory of Embedded Components
General Availability	Assure	• Perform Code Signing
	Assess	• Finalize and **submit scorecard** • Have a plan for mitigating any "critical" and/or "high" issues
Post-GA	Respond	• Respond to vulnerabilities following EMC's vulnerability response policy

Figura 3: SDL e un tipico ciclo di vita agile

La scorecard è un meccanismo utilizzato in tutta l'azienda Dell EMC per acquisire le caratteristiche di sicurezza di un prodotto/una soluzione quando raggiunge la data di Directed Availability/General Availability (DA/GA).

Sviluppo sicuro

L'approccio completo di Dell EMC allo sviluppo sicuro è incentrato sul minimizzare il rischio di vulnerabilità del software e i punti deboli di progettazione nei prodotti.

Questo approccio completo per lo sviluppo sicuro del software passa attraverso policy, persone, processi e tecnologie e include quanto segue:

- La policy Dell EMC Product Security è un riferimento comune che consente alle organizzazioni dei prodotti di Dell EMC di confrontare la sicurezza dei prodotti con le aspettative del mercato e le best practice del settore.
- I team di progettazione di Dell EMC rappresentano una community di progettazione ben consapevole degli aspetti correlati alla sicurezza. Tutti i tecnici seguono un programma di progettazione della sicurezza basato su ruoli per ottenere una formazione sulle specifiche best practice di sicurezza e sull'uso delle risorse pertinenti. Dell EMC si impegna a creare una cultura consapevole della sicurezza nell'intera community di progettazione.
- Il processo di sviluppo di Dell EMC è sicuro e ripetibile. SDL abbina i processi di sviluppo standard per ottenere un livello elevato di conformità alla policy Dell EMC Product Security.
- I team di sviluppo di Dell EMC si basano sulle tecnologie di sicurezza migliori della categoria. Dell EMC ha sviluppato un set di software, standard, specifiche e progetti per elementi comuni della sicurezza del software come autenticazione, autorizzazione, audit e responsabilità, crittografia e gestione delle chiavi con la tecnologia RSA all'avanguardia. Ove opportuno, vengono utilizzate interfacce aperte che consentono l'integrazione con le architetture di sicurezza esistenti dei clienti.
- SDL di Dell EMC abbina la sicurezza ai processi di sviluppo standard per ottenere un livello elevato di conformità alla policy Dell EMC Product Security. SDL di Dell EMC segue un approccio rigoroso per rendere sicuro lo sviluppo dei prodotti e prevede un risk management a livello executive prima dell'introduzione dei prodotti nel mercato.
- SDL è parte di una serie più ampia di processi esistenti all'interno dello standard di progettazione sicura, che rappresenta il punto di riferimento per creare sicurezza nei prodotti Dell EMC. Lo standard si applica alla sicurezza di tutte le funzionalità dei prodotti e descrive le funzionalità di sicurezza obbligatorie che devono essere integrate in qualsiasi prodotto fornito da Dell EMC ai clienti. Con questo standard, i prodotti di Dell EMC:
    - Soddisfano i rigorosi requisiti di sicurezza dei clienti.
    - Aiutano i clienti a soddisfare i requisiti richiesti dalle normative vigenti come PCI, HIPPA e così via.
    - Riducono al minimo i rischi correlati alle vulnerabilità per i prodotti Dell EMC e gli ambienti dei clienti.
    - La protezione del codice sorgente definisce come proteggere correttamente i sistemi di progettazione di Dell EMC che contengono codice sorgente rispetto alla proprietà intellettuale correlata ai prodotti e garantisce l'integrità dei prodotti installati negli ambienti dei clienti.

Risposta alle vulnerabilità di Dell EMC

Le vulnerabilità di sicurezza in qualsiasi componente dei sistemi possono essere utilizzate da utenti malintenzionati per infiltrarsi e compromettere l'intera infrastruttura IT. Il tempo che intercorre tra il rilevamento iniziale delle vulnerabilità e la disponibilità di una correzione diventa una gara tra attacco e difesa. La massima priorità per Dell EMC è ridurre al minimo questo intervallo di tempo per ridurre i rischi.

Il Dell Product Security Incident Response Team (PSIRT) coordina la risposta e la divulgazione di tutte le vulnerabilità dei prodotti Dell EMC identificate esternamente. Il team PSIRT fornisce tempestivamente ai clienti informazioni, linee guida e strategie di mitigazione per risolvere le minacce provenienti dalle vulnerabilità.

Chiunque può comunicare a Dell le potenziali falle di sicurezza dei suoi prodotti tramite il sito web dell'azienda o per e-mail. Tutte le notifiche vengono esaminate, convalidate, evase e segnalate in base alle linee guida del settore.

Dell rilascia le informazioni sulle vulnerabilità dei prodotti a tutti i clienti contemporaneamente. I consulenti dell'azienda identificano la gravità delle vulnerabilità e diffondono le informazioni utilizzando più sistemi di reporting standardizzati. Come per le altre prassi di sicurezza dei prodotti, la policy di divulgazione di Dell si basa sulle best practice del settore.

Risk management della supply chain

I programmi di successo per la sicurezza dei prodotti sono completi e si estendono a componenti e software in outsourcing. I test di integrità all'interno della supply chain rappresentano una componente essenziale della creazione e del mantenimento della fiducia.

Dell Technologies dispone di un programma formale di risk management della supply chain che garantisce che i componenti hardware utilizzati nei prodotti dell'azienda provengano da fonti accuratamente valutate.

La sicurezza della supply chain è definita come la prassi e l'applicazione di misure preventive e di controllo a protezione di asset fisici, inventario, informazioni, proprietà intellettuale e persone. La gestione della sicurezza fisica, delle informazioni e del personale contribuisce a fornire la garanzia della supply chain, riducendo le opportunità di introduzione malevola di malware e componenti contraffatti nella supply chain.

Il framework di risk management della supply chain di Dell (di seguito) rispecchia il framework complessivo di gestione dei rischi del National Infrastructure Protection Plan (NIPP), che delinea le modalità in cui la pubblica amministrazione e il settore privato possono collaborare per ridurre i rischi e soddisfare gli obiettivi di sicurezza. Il framework di Dell include un ciclo di feedback aperto che consente un miglioramento continuo. I piani di riduzione dei rischi vengono classificati per priorità e implementati nelle modalità opportune durante l'intero ciclo di vita della soluzione. La figura 4 illustra il processo di risk management della supply chain.

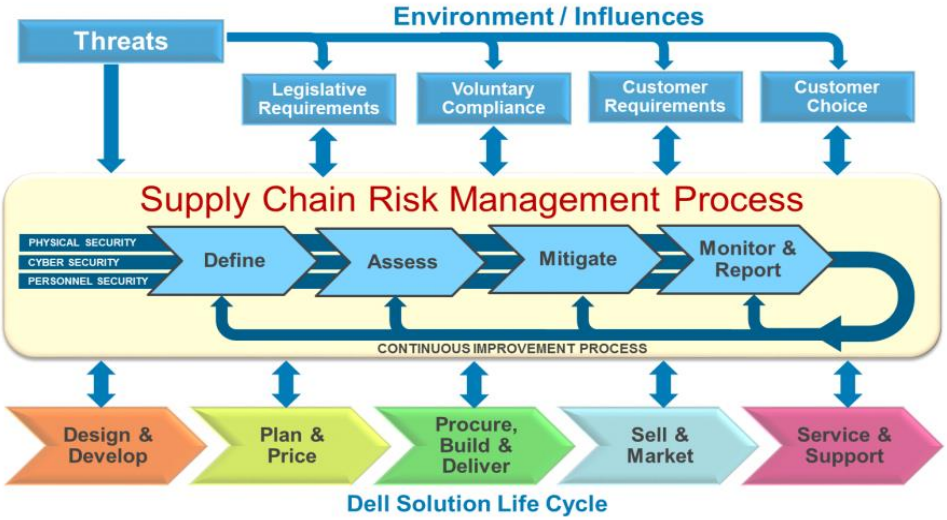

Figura 4: processo di risk management della supply chain di Dell

Collaborazione nel settore per migliorare la sicurezza dei prodotti

Dell Technologies ritiene che un approccio collaborativo sia il modo più efficiente ed efficace per affrontare le minacce alla sicurezza che emergono costantemente e che possono diffondersi rapidamente tra le organizzazioni attraverso gli attuali sistemi a elevata interconnessione.

Considerando i maggiori rischi, i fornitori di tecnologia devono mettere da parte i propri obiettivi di competitività sul mercato quando si tratta di sicurezza dei prodotti. Nessun singolo fornitore può risolvere da solo tutti i problemi di sicurezza dei prodotti IT. La sicurezza dell'IT è un'impresa collettiva e collaborativa. Dell Technologies ritiene che la collaborazione con altre aziende sia essenziale per garantire che il mercato rimanga un luogo in cui tutti possano prosperare.

Il fatto di essersi occupata di sicurezza dei prodotti per decenni ha consentito a Dell Technologies di accumulare una ricca storia di miglioramenti e informazioni strategiche di successo e l'azienda condivide apertamente ciò che ha appreso con i propri clienti, colleghi e partner. Dell Technologies comprende che il sistema IT di un cliente non si fonda esclusivamente sui prodotti di Dell Technologies, quindi ci impegniamo a migliorare la sicurezza dell'ecosistema ovunque vi sia un prodotto. Ciò significa partecipare attivamente e contribuire positivamente all'intero settore.

Il lungo impegno di Dell Technologies nel continuo perfezionamento della sicurezza dei prodotti ha creato l'obbligo di assistere e incentivare i nuovi operatori del settore. I responsabili della sicurezza dei prodotti dell'azienda agevolano lo scambio aperto di idee in occasione di conferenze, tramite post di blog e in altri contesti sociali e formali.

Partecipazione a gruppi di sicurezza dei prodotti del settore

Dell Technologies è attiva nei gruppi di sicurezza dei prodotti, dove apprende e insegna best practice innovative e coltiva un senso di responsabilità comune per la sicurezza dei prodotti. Le affiliazioni di Dell Technologies nel settore includono:

BSIMM: Building Security in Maturity Model valuta le iniziative di sicurezza software del settore in modo che le organizzazioni possano avere un riscontro sui propri sforzi nella sicurezza e suggerimenti su come migliorarli.

The Open Group: questo consorzio di 400 membri gestisce programmi di certificazione, tenuti in alta considerazione nel settore, per il personale IT, i prodotti e i servizi al fine di progettare e migliorare gli standard IT. L'obiettivo di The Open Group è comprendere i requisiti IT attuali ed emergenti e definire o condividere best practice per soddisfarli.

SAFECode: Software Assurance Forum for Excellence in Code, cofondata da Dell EMC, rappresenta un impegno del settore volto a identificare e promuovere le best practice al fine di fornire software, hardware e servizi più affidabili e sicuri.

CSA: Cloud Security Alliance è l'organizzazione leader a livello mondiale dedicata alla definizione e alla sensibilizzazione per le best practice al fine di offrire un ambiente di cloud computing sicuro.

FIRST: il Forum of Incident Response and Security Teams è un leader mondiale riconosciuto nella risposta agli incidenti. Dell PSIRT è membro di FIRSTVxRailteam.

VxRail: la base per la modernizzazione del data center e la trasformazione dell'IT

Per vincere la gara contro il panorama delle minacce alla sicurezza in continua evoluzione, VxRail ha l'adattabilità necessaria per difendere dalle minacce attuali e future. VxRail si basa sull'attuale generazione di server Dell PowerEdge e sulle più recenti tecnologie di processori che offrono una piattaforma sicura e opzioni di configurazione flessibili. vSphere fornisce la virtualizzazione di storage e server. VxRail è facilmente scalabile con la crescita dei requisiti dei carichi di lavoro. Con la modifica delle normative, le opzioni di configurazione flessibili di VxRail consentono all'IT di adattarsi rapidamente.

VxRail può aiutare la tua organizzazione a ottimizzare la cyber-resilienza, gestire i rischi e soddisfare i requisiti di conformità indipendentemente dal settore di attività. VxRail è l'unico appliance di infrastruttura iperconvergente completamente integrato, preconfigurato e testato con tecnologia VMware vSAN. A prescindere che sia implementato nel data center, nell'edge o nell'ambito di una soluzione di cloud ibrido, VxRail fornisce una distribuzione migliore, più semplice e sicura di applicazioni business-critical, VDI e infrastruttura remota. VxRail consente a Dell EMC di fornire al cliente le funzionalità necessarie per ottimizzare la cyber-resilienza nell'intero deployment. La figura 5 seguente illustra la sicurezza integrata in VxRail.

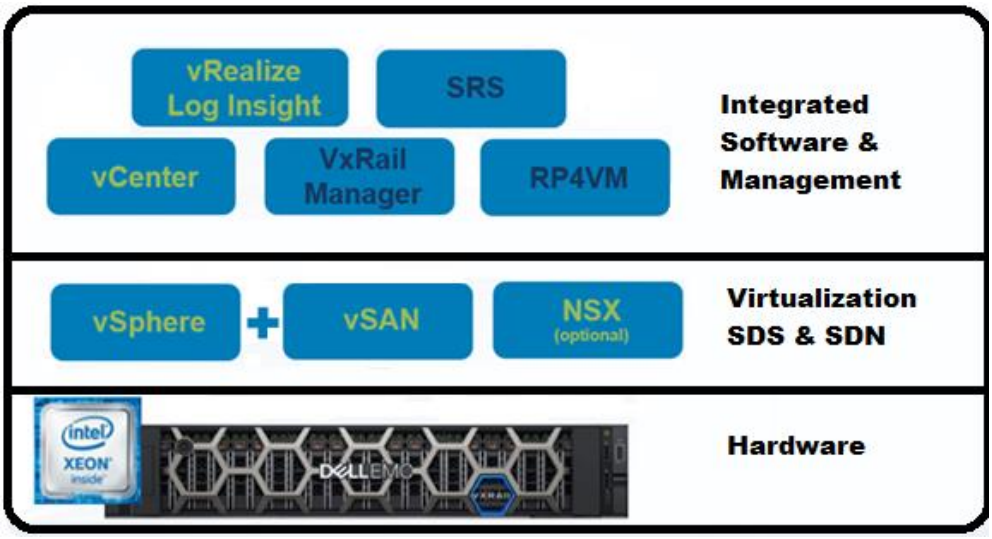

Figura 5: sicurezza integrata in VxRail

Server Dell EMC PowerEdge

VxRail si basa sulla piattaforma server Dell PowerEdge con funzionalità di protezione hardware e di sistema integrate per proteggere l'infrastruttura con livelli di difesa. Le violazioni vengono rilevate rapidamente, consentendo al sistema di eseguire il ripristino a una situazione di base affidabile. Le funzionalità di protezione differenziate nei server PowerEdge includono:

- Blocco del sistema per evitare modifiche non autorizzate o involontarie. Questa funzione innovativa impedisce le modifiche alla configurazione che creano vulnerabilità di sicurezza ed espongono dati sensibili.
- L'architettura cyber-resiliente con funzioni come l'avvio protetto UEFI, le funzionalità di ripristino del BIOS e il firmware con firma assicura una protezione avanzata contro gli attacchi.
- La funzione System Erase a livello di server assicura la privacy cancellando in modo rapido e sicuro tutti i dati degli utenti dall'unità e tutta la memoria non volatile al momento del ritiro di un server.

I server Dell EMC PowerEdge rappresentano l'hardware critico che costituisce i nodi di un cluster VxRail. Le risorse della CPU, della memoria e del disco in ciascun nodo forniscono le risorse in pool per il cluster, mentre le interfacce di rete forniscono la connettività. I server Dell EMC PowerEdge sicuri rappresentano pertanto la base della sicurezza di VxRail.

I server PowerEdge dispongono di un controller di accesso remoto integrato denominato iDRAC. iDRAC utilizza comunicazione sicura, autenticazione e controlli degli accessi in base al ruolo per consentire la gestione remota e la configurazione sicura del sistema fisico. Grazie agli avvisi configurabili, iDRAC è in grado di inviare informazioni sugli eventi al sistema SIEM (Security Incident and Event Management) ogni volta che si accede all'hardware o che la configurazione viene modificata. Il rilevamento e il reporting di modifiche non autorizzate proteggono l'integrità di un VxRail. Per ulteriori informazioni, consulta Cyber Resilient Security in 14th Generation of Dell EMC PowerEdge.

I server PowerEdge utilizzano un firmware verificato e con firma crittografica per creare un sistema di affidabilità, sfruttando le tecnologie di sicurezza integrate direttamente nel silicio. Funzionalità come la Trusted Execution Technology (TXT) di Intel verificano che il server esegua solo la versione prevista del firmware, del BIOS e dell'hypervisor, impedendo al tempo stesso l'introduzione non rilevata di malware. La figura 6 di seguito illustra la root of trust hardware.

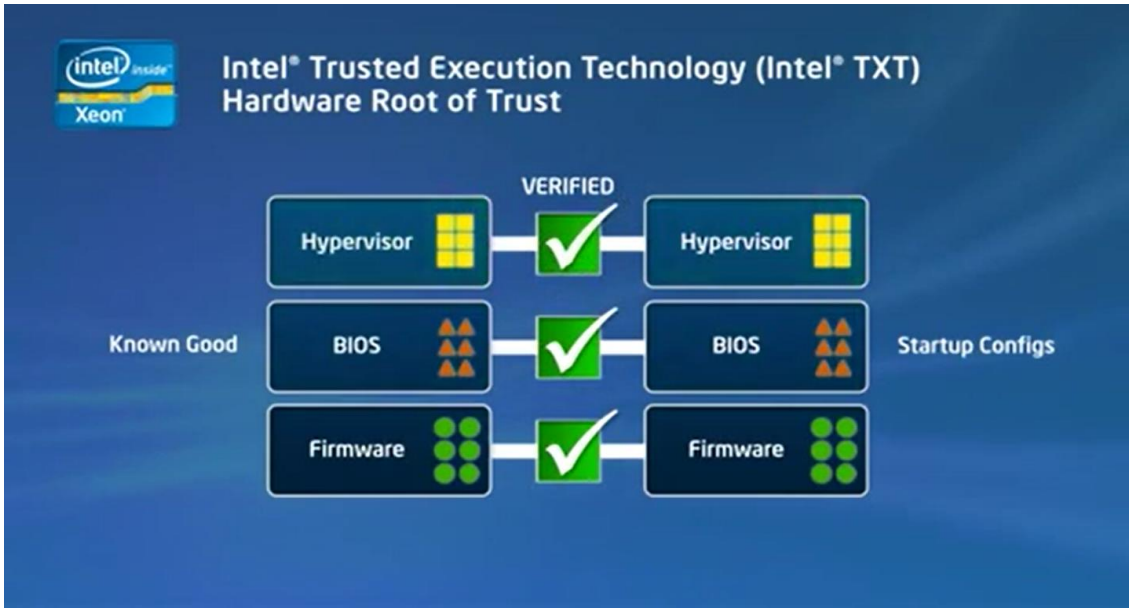

Figura 6: root of trust hardware

VxRail è in grado di ottenere livelli di protezione ancora più elevati per l'integrità del server mediante la configurazione dei nodi con un modulo TPM (Trusted Platform Management) opzionale (TPM v1.2 e v2.0). TPM è uno standard internazionale per i cryptoprocessor sicuri, ovvero un microcontroller dedicato progettati per fornire una sicurezza elevata per le chiavi di crittografia, ed è un'opzione per tutti i nodi VxRail.

Dell EMC VxRail HCI System Software

VxRail HCI System Software costituisce la base delle esclusive funzionalità di VxRail. Dal punto di vista dello stack dell'infrastruttura, si tratta del software di gestione che viene eseguito sul software VMware e sul server PowerEdge per consentire a VxRail di fungere da sistema unificato.

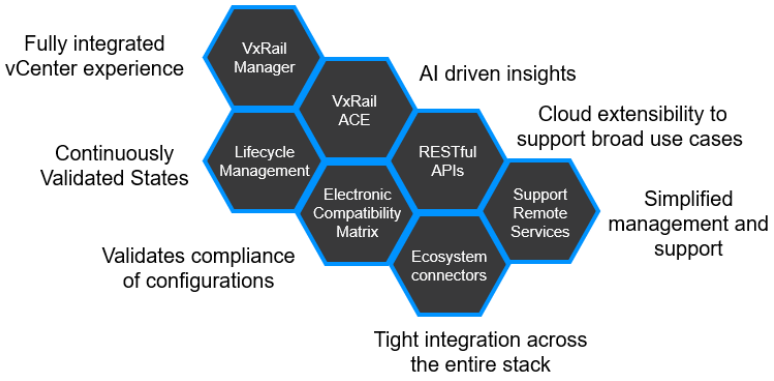

Figura 7: VxRail HCI System Software

Stati continuamente convalidati: VxRail viene eseguito su software e firmware pretestati e convalidati per l'intero stack VxRail, compresi i componenti del software VMware e del server PowerEdge. Le funzionalità di gestione del ciclo di vita di VxRail assicurano che i cluster VxRail siano in esecuzione in questo stato di integrità noto per l'intero ciclo di vita, mentre il cluster viene sottoposto a continue modifiche per sfruttare le più recenti innovazioni del software VMware, correzioni di sicurezza o bug fix. L'espressione "stati continuamente convalidati" racchiude la stabilità della configurazione fornita dai cluster VxRail.

Matrice di compatibilità elettronica: con tutti questi diversi componenti software e hardware nello stack, il team di VxRail testa e convalida costantemente l'intero stack in modo che qualsiasi stato desiderato l'utente determini dalla matrice di compatibilità VMware sia stato confermato come stato continuamente convalidato. Inoltre, VxRail fa riferimento a questa matrice per assicurare che la configurazione del cluster rimanga conforme. Questi vantaggi riducono drasticamente l'impegno e le risorse di test che un cliente dovrebbe investire, offrendo al cliente stesso la tranquillità necessaria per far evolvere i cluster VxRail in modo prevedibile e sicuro senza compromettere i carichi di lavoro delle applicazioni.

Connettori per l'ecosistema: per creare una matrice di compatibilità elettronica completa, VxRail deve essere in grado di comunicare con i membri dell'ecosistema nello stack, tra cui vSphere, vSAN, vCenter, il server PowerEdge e i diversi componenti hardware all'interno. I connettori consentono a VxRail di rilevare le versioni del software e del firmware in esecuzione in ciascun componente e di gestire il ciclo di vita di tali componenti. Le funzionalità di automazione e orchestration consentono di gestire VxRail come un unico sistema unificato.

VxRail Manager: l'interfaccia utente di gestione principale per VxRail è il plug-in vCenter denominato VxRail Manager. Gli utenti di VxRail possono eseguire qualsiasi attività VxRail tramite questa interfaccia, tra cui la configurazione iniziale del cluster, il monitoraggio dei componenti hardware, l'esecuzione di un arresto del cluster, l'espansione del cluster con l'aggiunta di nodi e l'aggiornamento di VxRail HCI System Software. VxRail Manager offre un'esperienza vCenter completamente integrata.

VxRail ACE (Analytical Consulting Engine): poiché i miglioramenti vengono realizzati per ottimizzare l'esperienza di gestione del ciclo di vita di VxRail, molto dipende dalle funzionalità di elaborazione analitica di VxRail ACE. ACE è l'acronimo di Analytical Consulting Engine. Tramite la telemetria avanzata raccolta da HCI System Software sui cluster VxRail, ACE viene utilizzato per fornire informazioni strategiche basate sull'intelligenza artificiale che consentiranno agli utenti di gestire in modo proattivo i cluster al fine di migliorare le prestazioni e la disponibilità. Le informazioni strategiche basate sull'intelligenza artificiale consentono inoltre funzionalità di gestione multi-cluster più attive in ACE, un'area per la quale gli utenti di HCI avranno un interesse crescente quando espandono il footprint di HCI e la gestione su scala diventa una necessità.

API REST: grazie ai vantaggi per la gestione del ciclo di vita, VxRail si posiziona idealmente come piattaforma di infrastruttura di scelta, in quanto l'attenzione alla semplificazione delle operazioni di IT ha un ruolo fondamentale nel consentire ai team di IT di concentrarsi sui modelli di erogazione dei servizi basati sul cloud. Rendere la piattaforma VxRail estensibile tramite API consente ai clienti di sfruttare soluzioni di infrastructure-as-a-service. Le API permettono inoltre la gestione su vasta scala, vantaggiosa per i clienti con un numero elevato di cluster VxRail installati in varie sedi e che hanno scelto soluzioni di script in-house per la gestione su vasta scala.

Servizi remoti di assistenza: anche l'esperienza dell'assistenza può essere un fattore critico nella scelta della soluzione HCI corretta. VxRail offre assistenza da parte di un unico fornitore per il software VMware, il server PowerEdge e il software VxRail tramite il supporto tecnico Dell. L'assistenza per VxRail include Dell EMC Secure Remote Services per la funzionalità "call-home" e la connessione remota proattiva bidirezionale per il monitoraggio, la diagnosi e la riparazione in remoto durante l'intero di ciclo di vita per assicurare la massima disponibilità.

VMware vSphere

La suite software VMware vSphere offre a VxRail un'infrastruttura virtualizzata altamente disponibile, resiliente e on-demand. ESXi, vSAN e vCenter Server sono componenti principali di vSphere. ESXi è un hypervisor installato in fabbrica su un nodo di server fisico VxRail che consente a un unico server fisico di ospitare più server logici o VM. vSAN è il software-defined storage utilizzato dalle VM, mentre VMware vCenter Server è l'applicazione di gestione per host ESXi, vSAN e VM.

vSphere Platinum è una soluzione di sicurezza progettata appositamente per proteggere le applicazioni, l'infrastruttura, i dati e l'accesso. Unisce due prodotti comprovati: vSphere per proteggere l'infrastruttura, i dati e l'accesso e AppDefense per proteggere le applicazioni in esecuzione sulle VM. AppDefense protegge l'integrità delle applicazioni in esecuzione su vSphere utilizzando l'apprendimento automatico per comprendere lo stato e il comportamento previsti dell'applicazione e del computer al fine di rilevare e prevenire le minacce. I clienti di VxRail che hanno acquistato licenze Platinum (inclusi gli abbonamenti) di VMware hanno diritto a utilizzare la licenza Platinum su VxRail con vSphere Enterprise Plus. È importante ricordare che l'LCM della parte AppDefense di vSphere Platinum è responsabilità del cliente

Come Dell EMC, VMware segue un rigoroso processo del ciclo di vita di sviluppo software sicuro e dispone di un Security Response Center. VxRail è sviluppato e supportato congiuntamente con VMware per garantire che tutti i componenti inclusi nella soluzione siano progettati, costruiti, testati e installati con la massima priorità per la sicurezza. Ulteriori informazioni sulla sicurezza dei prodotti VMware

VMware vCenter Server

vCenter Server è il principale punto di gestione per virtualizzazione dei server e storage vSAN. Una singola istanza di vCenter può essere scalata a livelli aziendali, con il supporto di centinaia di nodi VxRail e migliaia di VM. VxRail può utilizzare un'istanza di vCenter installata all'interno del cluster VxRail o un'istanza di vCenter esistente.

vCenter fornisce una gerarchia logica di data center, cluster e host. Questa gerarchia agevola la segmentazione delle risorse in base a casi di utilizzo o linee di attività e consente di spostare le risorse in modo dinamico in funzione delle esigenze. Tutto questo avviene con una singola interfaccia intuitiva.

vCenter Server fornisce servizi per VM e risorse, ad esempio il servizio di inventario, la pianificazione delle attività, la registrazione delle statistiche, la gestione degli avvisi e degli eventi, nonché il provisioning e la configurazione delle VM. vCenter Server offre inoltre funzionalità di disponibilità avanzate, tra cui:

- vSphere vMotion: consente la migrazione in tempo reale dei carichi di lavoro delle VM con zero downtime
- vSphere Distributed Resource Scheduler (DRS): bilancia e ottimizza continuamente l'allocazione delle risorse di elaborazione delle VM tra i nodi del cluster
- vSphere High Availability (HA): offre funzionalità di failover e riavvio delle VM

Hypervisor VMware ESXi

In VxRail, l'hypervisor ESXi ospita la VM nei nodi del cluster. Le VM sono sicure e portatili e ogni VM è un sistema completo con processori, memoria, rete, storage e BIOS. Le VM sono isolate l'una dall'altra, pertanto in caso di errore di un sistema operativo guest in esecuzione su una VM, le altre VM sullo stesso host fisico non saranno interessate dall'evento e continueranno a essere eseguite. Le VM condividono l'accesso alle CPU ed ESXi è responsabile della pianificazione delle CPU stesse. ESXi assegna inoltre alle VM un'area di memoria utilizzabile e gestisce l'accesso condiviso alle schede di rete fisiche e ai controller dei dischi associati all'host fisico. Sono supportati tutti i sistemi operativi basati su x86 e le VM sullo stesso hardware di server fisico possono eseguire sistemi operativi e applicazioni differenti.

Rete virtuale VMware

Un requisito di sicurezza fondamentale consiste nell'isolare il traffico di rete. Su VxRail, le funzionalità di rete virtuale di vSphere offrono connettività e isolamento flessibili. Le VM di VxRail comunicano tra loro utilizzando il VMware Virtual Distributed Switch (VDS) che funziona come un unico switch logico che si estende su più nodi nello stesso cluster. VDS utilizza protocolli di rete standard e implementazioni VLAN e inoltra i frame a livello di collegamento dati.

VDS è configurato in vCenter Server a livello di data center, mantenendo una configurazione di rete sicura e coerente nella migrazione delle VM tra più host. L'appliance VxRail si basa su VDS per il traffico degli appliance, mentre vSAN si basa su VDS per l'accesso alla rete.

VxRail può inoltre essere configurato con NSX per fornire una sicurezza di rete software-defined e un controllo degli accessi più accurato grazie alla micro-segmentazione.

VMware vSAN

Gli appliance VxRail si basano su VMware vSAN per il software-defined storage di livello aziendale. vSAN aggrega i dischi degli host in locale in un cluster vSphere per creare un pool di storage condiviso distribuito. La capacità è scalabile verso l'alto con l'aggiunta di ulteriori dischi al cluster e scalabile in orizzontale con l'aggiunta di ulteriori nodi VxRail. vSAN è completamente integrato con vSphere e funziona perfettamente con altre funzionalità vSphere.

vSAN è noto per l'efficienza e le prestazioni. È dotato di ottimizzazione automatica e bilancia le allocazioni in base al carico di lavoro, all'utilizzo e alla disponibilità delle risorse. vSAN offre una HCI a prestazioni elevate ottimizzata per flash adatta a una vasta gamma di carichi di lavoro. Le funzionalità di storage di livello aziendale comprendono:

- Efficiente tecnologia di riduzione dei dati, tra cui deduplica e compressione, nonché codifica di cancellazione
- Policy QoS per il controllo del consumo dei carichi di lavoro in base ai limiti definiti dall'utente
- Tecnologia di integrità e protezione dei dati, tra cui checksum software e domini di errore
- Maggiore sicurezza con crittografia dei dati at-rest vSAN

Con vSAN, i dischi su ciascun nodo VxRail vengono organizzati automaticamente in gruppi di dischi con un'unica unità cache e una o più unità di capacità. Questi gruppi di dischi vengono utilizzati per creare un unico datastore vSAN accessibile su tutti i nodi di un cluster VxRail.

VxRail offre due diverse opzioni di configurazione dello storage di nodo vSAN: una configurazione ibrida che utilizza sia unità SSD flash che dischi rigidi meccanici e una configurazione SSD all-flash. La configurazione ibrida utilizza unità SSD flash per la memorizzazione nella cache e dischi rigidi meccanici per la capacità e lo storage dei dati persistente. La configurazione all-flash utilizza unità SSD flash per la memorizzazione nella cache e la capacità. La figura 7 illustra i concetti di base di vSAN.

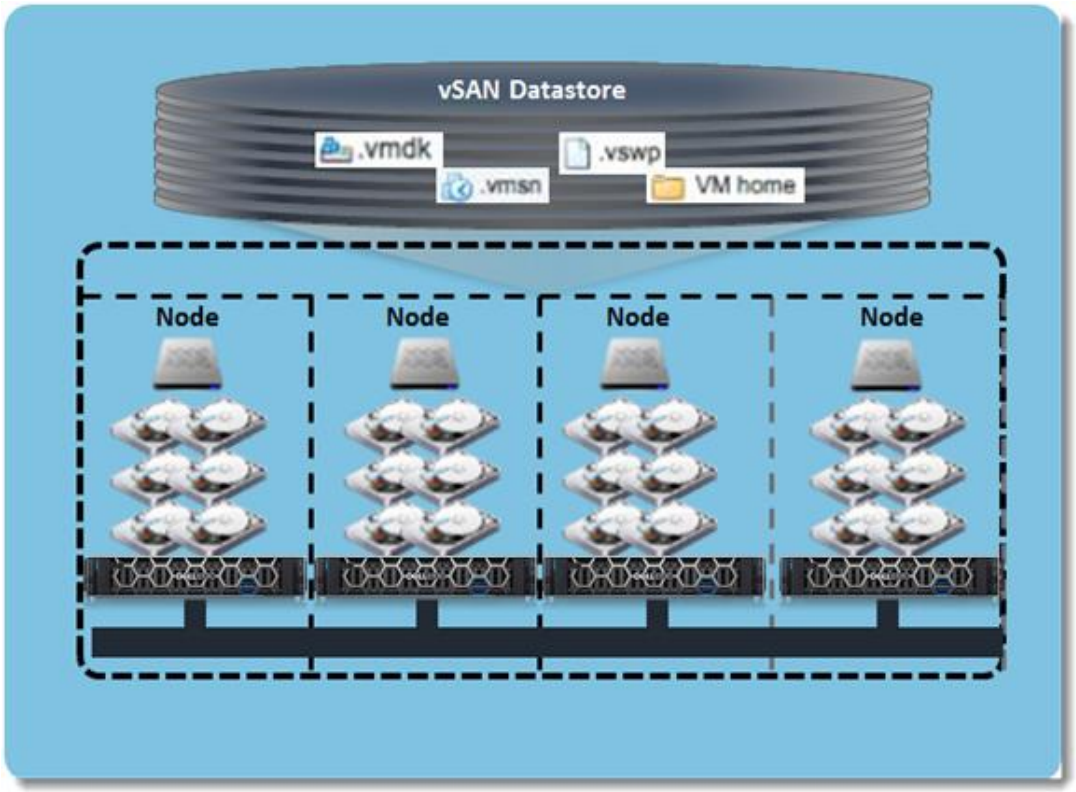

Figura 8: concetti di base di vSAN

vSAN viene configurato quando il cluster VxRail viene inizializzato per la prima volta ed è gestito tramite vCenter. Durante il processo di inizializzazione dell'appliance VxRail, vSAN crea un datastore condiviso distribuito dai dischi collegati in locale su ciascun nodo ESXi. La quantità di storage nel datastore è un aggregato di tutte le unità di capacità del cluster. La quantità di storage utilizzabile dipende dal livello di protezione utilizzato. La configurazione e la verifica vSAN orchestrate, eseguite nell'ambito dell'inizializzazione del sistema, garantiscono prestazioni coerenti e prevedibili e una configurazione di sistema che segue le best practice.

Storage Policy Based Management (SPBM)

vSAN è basato su policy e progettato per semplificare il provisioning e la gestione dello storage. Le policy di storage vSAN si basano su set di regole che definiscono i requisiti di storage per le VM. Gli amministratori possono modificare in modo dinamico la policy di storage di una VM in caso di variazione dei requisiti. Esempi di regole SPBM sono il numero di errori da tollerare, la tecnica di protezione dei dati da utilizzare e se sono abilitati i checksum a livello di storage.

VMware vRealize Log Insight

In dotazione con VxRail, VMware vRealize Log Insight monitora gli eventi di sistema e fornisce notifiche olistiche continue sullo stato dell'ambiente virtuale e dell'hardware degli appliance. vRealize Log Insight offre la gestione automatizzata dei registri in tempo reale per l'appliance VxRail con monitoraggio dei registri, raggruppamento intelligente e analisi per semplificare la risoluzione dei problemi su vasta scala in ambienti VxRail fisici, virtuali e cloud. La registrazione centralizzata è un requisito fondamentale dell'infrastruttura sicura. Per i clienti che dispongono già di una struttura di registrazione o di un SIEM, VxRail si integra facilmente utilizzando il protocollo syslog standard del settore.

VMware Cloud Foundation (VCF) con NSX

VMware Cloud Foundation su VxRail è una soluzione integrata progettata congiuntamente da Dell EMC e VMware con funzionalità che semplificano e automatizzano le operazioni dell'intero Software-Defined Datacenter (SDDC) dal giorno 0 al giorno 2. La nuova piattaforma offre una serie di servizi software-defined per l'elaborazione (con vSphere e vCenter), lo storage (con vSAN), la connettività di rete (con NSX), la sicurezza e la gestione cloud (con vRealize Suite) negli ambienti privati e pubblici, dando vita all'hub operativo per l'hybrid cloud.

VMware Cloud Foundation su VxRail offre il percorso più semplice per l'hybrid cloud attraverso una piattaforma di hybrid cloud completamente integrata che sfrutta le funzionalità hardware e software VxRail native e altre integrazioni VxRail esclusive (come i plug-in vCenter e Dell EMC Networking). Questi componenti interagiscono per ottenere una nuova esperienza utente di hybrid cloud pronto all'uso con l'integrazione full-stack. Con l'integrazione full-stack, i clienti ottengono il livello dell'infrastruttura HCI e lo stack del software cloud in una singola esperienza completa di ciclo di vita automatizzato pronta all'uso.

VMware NSX Data Center è la piattaforma di virtualizzazione e sicurezza di rete che abilita la rete cloud virtuale. Si tratta di un approccio software-defined alla connettività di rete che si estende a diversi data center, cloud, endpoint e posizioni edge. Con NSX Data Center, le funzioni di rete, tra cui switching, routing, firewalling e bilanciamento del carico, vengono avvicinate all'applicazione e distribuite in tutto l'ambiente. Analogamente al modello operativo delle VM, è possibile eseguire il provisioning e la gestione delle reti indipendentemente dall'hardware sottostante.

NSX Data Center riproduce l'intero modello di rete nel software, consentendo in pochi secondi la creazione e il provisioning di qualsiasi topologia di rete, dalle reti semplici a quelle complesse a più livelli. Gli utenti possono creare più reti virtuali con requisiti diversi, sfruttando una combinazione dei servizi offerti tramite NSX, inclusa la micro-segmentazione, o da un ampio ecosistema di integrazioni di terze parti che spaziano dai firewall di nuova generazione alle soluzioni di gestione delle prestazioni per creare ambienti più agili e sicuri. Questi servizi possono essere quindi estesi a una serie di endpoint all'interno di un cloud e tra cloud. Per ulteriori informazioni, consulta la VMware Cloud Foundation on VxRail Architecture Guide

Funzionalità di sicurezza VxRail

Le funzionalità di sicurezza sono suddivise in due sezioni: sicurezza dei dati e sicurezza dei sistemi. La seguente configurazione e gestione sicura dei sistemi di VxRail segue i principi della triade Confidentiality-Integrity-Availability (CIA).

VxRail offre uno stack completamente preconfigurato e testato per tutte le funzionalità di sicurezza. Queste funzionalità di sicurezza sono integrate e incluse nell'appliance.

SICUREZZA DEI DATI

La sicurezza dei dati segue la triade CIA per assicurare che i dati siano disponibili solo per account autorizzati e/o specifici e che vengano soddisfatte conformità e specifiche. Ciò include l'accesso ai dati a livello fisico e utente.

Riservatezza

Impedire che le informazioni sensibili raggiungano le persone sbagliate, assicurando al contempo l'accesso adeguato e autorizzato ai dati di un'azienda, è un problema fondamentale che si riassume con i termini "riservatezza" o "privacy". VxRail affronta il problema della riservatezza dei dati in uso, dei dati in movimento e dei dati at-rest in diversi modi.

Crittografia

La crittografia protegge la riservatezza delle informazioni mediante la codifica affinché siano indecifrabili per i destinatari non autorizzati. Con VxRail, i datastore possono essere crittografati utilizzando la tecnologia D@RE di vSAN, che fornisce protezione convalidata FIPS 140-2 Level 1. Le singole VM possono essere crittografate utilizzando la crittografia vSphere, mentre le VM in movimento possono essere crittografate utilizzando la crittografia vMotion. È possibile configurare livelli aggiuntivi di crittografia in base ai requisiti delle applicazioni.

La crittografia vSAN è il modo più semplice e flessibile per crittografare i dati at-rest, poiché l'intero datastore vSAN viene crittografato con un'unica impostazione. Questa è una crittografia a livello di cluster per tutte le virtual machine che utilizzano il datastore. In genere, i dati crittografati non traggono vantaggio da tecniche di riduzione dello spazio, come la deduplica o la compressione. Con vSAN, tuttavia, la crittografia viene eseguita dopo la deduplica e la compressione, quindi viene preservato il pieno vantaggio di queste tecniche di riduzione dello spazio.

La crittografia delle VM offre la flessibilità necessaria per abilitare la crittografia VM per VM, il che significa che un singolo cluster può disporre di VM crittografate e non crittografate. La crittografia delle VM segue la VM ovunque sia ospitata. La VM rimarrebbe quindi crittografata anche se venisse trasferita in un datastore al di fuori del VxRail.

Inoltre, la crittografia delle VM può essere attivata e disattivata. Per le VM che vengono crittografate, la migrazione con vSphere vMotion utilizzerà sempre vSphere vMotion crittografato. Per le VM non crittografate è possibile selezionare l'opzione di crittografia Disabled, Opportunistic e Required quando si utilizza vMotion. L'opzione Opportunistic viene utilizzata per impostazione predefinita su VM non crittografate durante l'uso di vMotion. La figura 8 riportata di seguito riassume la differenza tra crittografia delle VM e crittografia vSAN

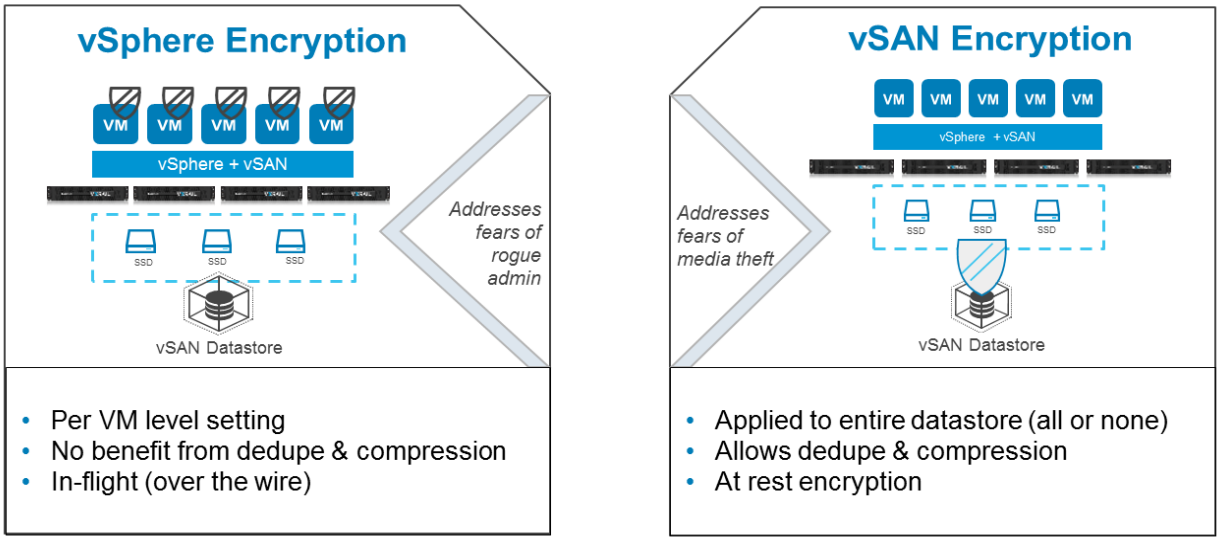

Figura 9: crittografia delle VM rispetto a crittografia vSAN

Inoltre, VxRail supporta vMotion crittografato, in cui le VM vengono crittografate quando vengono trasferite tra gli host. Ciò include le migrazioni vMotion all'interno di un VxRail, nonché migrazioni vMotion da o verso un cluster VxRail all'interno di un'istanza di vCenter. vMotion crittografato può essere utilizzato con la crittografia vSAN per ottenere la crittografia dei dati at-rest e la crittografia dei dati in volo. vMotion crittografato viene applicato per le VM con crittografia vSphere abilitata.

Fatta eccezione per la crittografia vMotion, dove vSphere fornisce le chiavi temporanee utilizzate per crittografare i dati in movimento, è necessario un Key Management Server (KMS) per la generazione, lo storage e la distribuzione sicuri delle chiavi di crittografia. Quando la crittografia è abilitata, vCenter stabilisce una relazione di trust con il KMS, quindi passa le informazioni sulla connessione KMS agli host ESXi. Gli host ESXi richiedono chiavi di crittografia direttamente dal KMS ed eseguono la crittografia e la decrittografia dei dati. La connettività vCenter è necessaria solo per la configurazione iniziale.

Poiché il KMS è un componente critico dell'infrastruttura di sicurezza, deve avere lo stesso livello di ridondanza e protezione in genere applicato ad altri componenti di infrastruttura critici, come DNS, NTP e Active Directory. È importante ricordare che il KMS deve essere eseguito fisicamente separato dagli elementi crittografati. Durante l'avvio, gli host ESXi richiederanno le chiavi al KMS. Se il KMS non è disponibile, il sistema non sarà in grado di completare l'avvio.

VxRail e VMware supportano KMS compatibili con KMIP (Key Management Interoperability Protocol) versione 1.1 o superiore, ad esempio Dell EMC CloudLink. VMware mantiene una guida alla compatibilità di KMS convalidata con vSphere.

All'interno di vSphere, la crittografia viene gestita da un insieme comune di moduli con convalida FIPS 140-2. Questi moduli comuni sono progettati, implementati e convalidati dal Secure Development Lifecycle di VMware. Disporre di una serie di moduli comuni per la crittografia consente a VxRail di semplificare l'implementazione, la gestione e il supporto della crittografia stessa.

La crittografia viene abilitata su VxRail tramite una semplice impostazione di configurazione in vCenter. I controlli degli accessi assicurano che solo gli utenti autorizzati possano abilitare o disabilitare la crittografia. Un ruolo denominato "No Cryptography Administrator" consente all'amministratore di svolgere attività di gestione normali, ma senza l'autorità di modificare le impostazioni di crittografia.

Software-defined networking VxRail con NSX opzionale

L'ambiente virtuale dinamico, ad esempio VxRail, trae spesso vantaggio dalla flessibilità offerta dai servizi SDN (Software Defined Network). Il modo più semplice per fornire servizi SDN su VxRail è con VMware NSX, una licenza software opzionale non inclusa in VxRail. NSX è una piattaforma completa di sicurezza e virtualizzazione della rete che consente agli amministratori di creare intere reti virtuali tra cui router, firewall e bilanciatori del carico puramente nel software. Dal momento che questo software-defined networking è disaccoppiato dall'infrastruttura di rete fisica sottostante, non dipende dal fatto che VxRail sia collegato a un particolare fornitore di switch.

NSX con VxRail è una soluzione di sicurezza integrata che riduce la necessità di installare componenti di sicurezza hardware o software aggiuntivi. Con NSX, gli amministratori di VxRail configurano la microsegmentazione per proteggere e isolare diversi carichi di lavoro dei tenant, controllare l'ingresso e l'uscita e fornire una maggiore sicurezza per tutti i carichi di lavoro, tra cui le applicazioni multi-tier tradizionali e le VM per scopi generici, nonché gli ambienti VDI. Alcuni dei vantaggi derivanti dall'utilizzo di NSX con VxRail includono:

- Possibilità di applicare le policy di sicurezza più in prossimità del carico di lavoro. Le policy di sicurezza vengono applicate nel software e i controlli di sicurezza si muovono con il carico di lavoro tra gli host del cluster.
- La gestione semplificata con la sicurezza è integrata nello stack vSphere e gestita in modo centralizzato tramite vSphere HTML5 Web Client e il plug-in NSX Manager.
- Controlli di sicurezza uniformi e automatici con gruppi e policy. I carichi di lavoro vengono automaticamente identificati e dinamicamente posizionati nella corretta configurazione di sicurezza.
- L'implementazione efficiente dei controlli di sicurezza a livello di hypervisor riduce la latenza delle applicazioni e il consumo di larghezza di banda rispetto ai controlli di sicurezza esterni o perimetrali.
- Isolamento a livello DMZ per controllare l'ingresso e l'uscita Internet per i client interni ed esterni con l'uso di regole appropriate di autorizzazione e rifiuto per controllare il traffico.
- Rilevamento e blocco di indirizzi IP di VM contraffatti grazie alla funzione SpoofGuard. Per ulteriori informazioni su questa funzionalità, consulta la documentazione Using SpoofGuard di VMware.
- Firewall di identità che consente a un amministratore di NSX di creare regole DFW basate sull'utente di Active Directory. Per ulteriori informazioni su questa funzionalità, consulta la documentazione di VMware NSX.
- Si integra con i servizi di sicurezza di terze parti, come rilevamento delle intrusioni e prevenzione delle intrusioni (IDS/IDP).

NSX migliora le caratteristiche di sicurezza di un ambiente ed è conforme alle certificazioni e agli standard seguenti:

- Certificazione Common Criteria - EAL 2+
- Firewall certificato ICSA Labs
- FIPS 140-2
- Soddisfazione di tutte le raccomandazioni NIST per la sicurezza informatica relative alla protezione dei carichi di lavoro virtualizzati

I firewall e le policy di sicurezza sono integrati grazie alla piattaforma VMware NSX opzionale per la sicurezza con VxRail. Si ottiene così un appliance davvero convergente rispetto alla sicurezza collocata all'esterno sul perimetro. L'installazione di NSX con VxRail consente di ridurre ulteriormente il tempo necessario per il deployment di nuove iniziative di applicazioni: i controlli di sicurezza diventano parte dell'appliance anziché aggiungere ulteriori componenti hardware o software.

Modalità blocco

Per gli ambienti che necessitano di una sicurezza ancora maggiore con la flessibilità, è possibile configurare la modalità di blocco per ESXi. Nella modalità di blocco, la possibilità di eseguire operazioni di gestione su singoli host è limitata, dettando il completamento delle attività di gestione tramite vCenter.

Il blocco in modalità "Normal" consente di inserire un gruppo selezionato di utenti in una whitelist, consentendo loro di gestire i server a livello locale anziché tramite vCenter. Questa whitelist deve includere determinati account di gestione VxRail.

Nella modalità di blocco "Strict", nessun utente può gestire i server in locale. Il blocco in modalità "Strict" non è supportato da VxRail.

Gestione sicura con HTTPS

Il traffico di gestione non protetto rappresenta un notevole rischio per la sicurezza. Per questo motivo, VxRail utilizza interfacce di gestione protette con Transport Layer Security "TLS 1.2". vCenter, iDRAC e HCI System Software disabilitano tutti l'interfaccia HTTP di testo in chiaro e richiedono l'utilizzo di HTTPS che usa TLS 1.2. Inoltre, l'accesso alla riga di comando dei server ESXi deve usare SSH. L'utilizzo di SSH e HTTPS è una parte fondamentale del comando e del controllo sicuri per un VxRail.

Integrità

L'integrità dei dati di un'azienda è un requisito fondamentale per le operazioni aziendali. VxRail assicura l'integrità dei dati mantenendone la coerenza, l'accuratezza e l'affidabilità durante il ciclo di vita, controllando l'accesso degli utenti e le funzioni incorporate di integrità come i checksum dei dati

Segmentazione della rete

La segmentazione della rete viene utilizzata per isolare il traffico di rete privato dal traffico pubblico al fine di ridurre la superficie di attacco. Rappresenta inoltre un efficace controllo di sicurezza per limitare i movimenti degli utenti malintenzionati tra le reti.

VxRail è progettato con più livelli di segmentazione della rete, tra cui la segmentazione fisica della rete di gestione hardware, la segmentazione virtuale delle reti di applicazioni e infrastrutture e la micro-segmentazione a livello di VM e applicazioni con il software NSX opzionale di VMware. Grazie alla segmentazione, la visibilità degli strumenti di amministrazione critici è limitata, impedendo agli utenti malintenzionati di utilizzarli contro un sistema. Per impostazione predefinita, la segmentazione di rete appropriata viene configurata automaticamente nell'ambito dell'inizializzazione del sistema e l'amministratore dispone della flessibilità necessaria per definire ulteriori livelli di segmentazione eventualmente necessari per l'ambiente delle applicazioni. Le best practice per la configurazione di rete sono presentate nella Dell EMC VxRail Network Planning Guide.

VxRail utilizza gli switch virtuali distribuiti VMware che segmentano il traffico per impostazione predefinita utilizzando VLAN separate per gestione, vSAN, vMotion e traffico delle applicazioni. Le reti vSAN e vMotion sono reti private e non instradabili. A seconda delle applicazioni supportate da una rete VxRail, il traffico potrebbe essere ulteriormente segmentato in base a diverse applicazioni, traffico di produzione e di non produzione o altri requisiti.

Gli switch virtuali distribuiti su un VxRail vengono configurati per impostazione predefinita con vSphere Network I/O Control (NIOC). NIOC consente l'allocazione della larghezza di banda fisica per le diverse VLAN. Alcuni attacchi informatici, come il Denial of Service e i worm, possono comportare un utilizzo eccessivo delle risorse. Ciò può causare una negazione delle risorse ad altri servizi che non sono direttamente sotto attacco. NIOC è in grado di garantire che i servizi dispongano della larghezza di banda di rete di cui necessitano per mantenere l'integrità in caso di attacco ad altri servizi. Le impostazioni di NIOC vengono configurate automaticamente secondo le best practice consigliate durante l'inizializzazione del sistema. La Dell EMC VxRail Network Planning Guide include i dettagli delle impostazioni di NIOC per le VLAN VxRail predefinite.

Ogni nodo VxRail dispone di una porta Ethernet fisica separata per l'interfaccia di gestione hardware iDRAC. La segmentazione fisica di questa rete rende difficile l'accesso alla gestione dell'hardware da parte degli utenti malintenzionati. In caso di attacchi Denial of Service distribuiti, la rete fisicamente segmentata non sarà interessata, limitando l'ambito di un potenziale attacco.

Avvio protetto UEFI

L'avvio protetto UEFI protegge il sistema operativo dagli attacchi di danneggiamento e rootkit e verifica che firmware, boot loader e VMkernel siano tutti firmati in formato digitale da un'autorità affidabile. Inoltre, l'avvio protetto UEFI per ESXi verifica che i pacchetti VIB (VMware Install Bundle) siano firmati in modo crittografato. In questo modo, lo stack di avvio del server esegue solo software autentico e che non sia stato modificato.

Checksum software

Una parte fondamentale dell'integrità dei dati consiste nel convalidare che i dati recuperati dallo storage non siano stati modificati dal momento in cui sono stati scritti. VxRail utilizza per impostazione predefinita il checksum di integrità dei dati end-to-end a livello di blocco. Il checksum viene creato alla scrittura dei dati e viene quindi verificato in lettura; se mostra modifiche rispetto al momento della scrittura, i dati vengono ricostruiti da altri membri del gruppo RAID. vSAN utilizza inoltre un meccanismo scrubber proattivo per rilevare e correggere potenziali danneggiamenti dei dati, anche per i dati a cui si accede raramente.

Disponibilità

Aggiornare costantemente il sistema IT, garantire il corretto funzionamento dell'hardware e la presenza di una larghezza di banda adeguata sono tutti elementi fondamentali per assicurare che i dati di un'azienda siano disponibili per gli utenti autorizzati. La gestione del ciclo di vita del software VxRail, le funzioni di disponibilità vSphere, il monitoraggio proattivo e il ripristino integrato, nonché la sicurezza fisica dell'hardware e la configurazione sicura del sistema garantiscono la massima availability del sistema stesso.

Gestione del ciclo di vita del software VxRail

Una delle azioni più importanti che un'organizzazione possa intraprendere per mantenere la sicurezza dell'infrastruttura IT consiste nell'avere sempre a disposizione gli aggiornamenti e le patch più recenti. Gli aggiornamenti e le patch non si limitano a migliorare le prestazioni o a risolvere problemi che potrebbero potenzialmente causare downtime, ma spesso riparano vulnerabilità della sicurezza. La community della sicurezza è caratterizzata da una straordinaria collaborazione. Grazie alla collaborazione tra VxRail e VMware, veniamo prontamente coinvolti nei piani per le correzioni di sicurezza, pertanto il team di VxRail può convalidare e preparare rapidamente patch di sicurezza prequalificate. Ma non tutti sono dalla stessa parte ed è una gara tra i difensori che lavorano per mitigare e correggere le minacce e gli aggressori il cui obiettivo è sfruttare le vulnerabilità. Grazie alla collaborazione tra VxRail e VMware, veniamo prontamente coinvolti nei piani per le correzioni di sicurezza, pertanto il team di VxRail può convalidare e preparare rapidamente patch di sicurezza prequalificate.

La gestione del ciclo di vita del software VxRail rende facili e sicure l'installazione e l'implementazione di aggiornamenti potenzialmente complessi e rischiosi. Il sistema HCI VxRail è l'unico sistema in cui tutti i componenti software sono progettati, testati e rilasciati come pacchetto. I pacchetti software VxRail possono includere aggiornamenti di BIOS, firmware, hypervisor, vSphere o di qualsiasi componente di gestione incluso. Se e quando vengono rilevate vulnerabilità, le correzioni vengono rapidamente sviluppate per mitigare le minacce indipendentemente dalla loro ubicazione. I pacchetti di aggiornamento vengono testati in modo approfondito sulla piattaforma hardware VxRail e sull'intero stack software VxRail prima del rilascio ai clienti.

Quando sono disponibili aggiornamenti, gli amministratori ricevono notifiche tramite HCI System Software. L'amministratore può quindi scaricare direttamente il pacchetto di aggiornamento e avviare o pianificare un processo di aggiornamento orchestrato. Gli aggiornamenti vengono eseguiti come processi graduali, mentre il sistema rimane online al servizio dell'azienda. Se è necessario un riavvio, le VM vengono automaticamente trasferite ad altri nodi del cluster prima di continuare.

La gestione del ciclo di vita di HCI System Software non solo riduce la complessità, ma rende l'infrastruttura più sicura, riducendo i tempi e le difficoltà correlati all'applicazione di patch per i sistemi e alla rimozione del rischio.

Funzioni di disponibilità di vSphere per VxRail

VxRail sfrutta le funzioni di disponibilità di vSphere integrate, tra cui VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS) e gli stretched cluster VMware. Queste funzionalità supportano il software automatizzato VxRail e forniscono la disponibilità continua dei servizi in hosting su VxRail. Si consiglia pertanto ai clienti di utilizzare versioni di vSphere che includano queste funzionalità.

VMware HA monitora le VM in esecuzione in un cluster VxRail. In caso di errore di una VM o di un nodo, HA viene riavviato su un altro nodo in un altro punto del cluster. Gli errori delle VM possono verificarsi per una serie di motivi, tra cui un attacco informatico, un guasto dell'hardware sottostante o un software danneggiato. Anche se VMware HA non impedisce le interruzioni, riduce al minimo il tempo necessario per il ripristino dei servizi.

VMware DRS distribuisce il carico di lavoro delle VM tra tutti gli host del cluster. Con la variazione della necessità di risorse delle VM, DRS esegue la migrazione dei carichi di lavoro delle VM ad altri host all'interno del cluster utilizzando vSphere vMotion. Gli attacchi informatici possono causare problemi di risorse per le VM non interessate dall'attacco. Gli attacchi informatici spesso causano un utilizzo intensivo delle risorse da parte della VM sotto attacco e quindi un utilizzo intensivo delle risorse a livello di host, con un impatto sulle risorse disponibili per altre VM presenti su quell'host. DRS protegge le VM trasferendole dagli host con risorse limitate, consentendo alle VM stesse di continuare a fornire servizi.

Lo stretched cluster VMware estende il cluster VxRail da un unico sito a due siti per un livello di disponibilità più elevato. È presente una sola istanza di una VM, tuttavia le copie complete dei suoi dati vengono mantenute in entrambi i siti. Se il sito corrente in cui è in esecuzione la VM non è più disponibile, la VM verrà riavviata nell'altro sito.

Protezione dei dati

Le forti difese per la sicurezza sono fondamentali, ma un piano di ripristino solido e affidabile è altrettanto importante. Il backup e le repliche sono i capisaldi del ripristino dopo una violazione. Al fine di agevolare il ripristino, HCI System Software include il backup e il ripristino basati su file. Tutti gli appliance VxRail incorporano uno starter pack per Dell EMC RecoverPoint for VM (RP4VM), che offre replica locale e remota di livello superiore e ripristino granulare.

Il backup e il ripristino basati su file di HCI System Software proteggono dall'eliminazione accidentale dell'appliance virtuale o dal danneggiamento interno dell'appliance. I backup possono essere configurati per essere eseguiti regolarmente o in base alle esigenze. Si tratta di una funzione all-inclusive che esegue il backup dei file all'interno del datastore vSAN in modo che non siano necessari hardware e software aggiuntivi.

Con RP4VM, se ad esempio una VM è compromessa o i dati vengono danneggiati o sequestrati, la VM e il dataset tornano rapidamente al momento precedente all'attacco, consentendo all'azienda un ripristino rapido. Installato direttamente da VxRail Manager, RP4VM viene distribuito rapidamente e il monitoraggio giornaliero avviene tramite il noto plug-in vCenter. Il ripristino è semplice ed eseguito utilizzando un'interfaccia vSphere nota.

Per le organizzazioni che necessitano di funzionalità di protezione dei dati avanzate e complete, VxRail supporta opzioni tra cui Dell EMC Data Protection Suite for VMware, Dell EMC Power Protect e Dell EMC Data Domain Virtual Edition.

I backup basati su file di VxRail HCI System Software contribuiscono a garantire la continuità aziendale nel raro caso in cui la VM VxRail debba essere creata nuovamente.

SICUREZZA DEL SISTEMA

Framework AAA (Authentication, Authorization and Accounting - Autenticazione, Autorizzazione e Contabilità) di VxRail

Framework AAA (Authentication, Authorization, and Accounting - Autenticazione, Autorizzazione e Contabilità) integrato. Il sistema AAA è progettato per controllare l'accesso, assicurando che sia l'utente corretto a utilizzare il sistema, per fornire il livello di accesso necessario e per registrare l'attività al fine di tenere conto di quanto è stato fatto e da chi.

AUTENTICAZIONE

L'autenticazione a HCI System Software è gestita da SSO tramite il plug-in vCenter. VxRail vCenter supporta il sistema di gestione delle identità centralizzato dell'organizzazione secondo le policy di sicurezza dell'autenticazione.

Le organizzazioni spesso centralizzano la gestione delle identità utilizzando i servizi di directory, ad esempio Microsoft Active Directory (AD) con LDAP. Se VxRail è un ambiente standalone e non fa parte di un dominio, è possibile gestire utenti e password localmente in vSphere e iDRAC. Dal punto di vista delle best practice è consigliabile utilizzare l'autenticazione centralizzata.

Spesso ci possono essere soggetti diversi responsabili dei server fisici, della gestione del ciclo di vita di VxRail e della gestione dell'ambiente di virtualizzazione di server, storage e rete. VxRail utilizza pertanto controlli degli accessi accurati basati sui ruoli per iDRAC, HCI System Software e vSphere.

AUTORIZZAZIONE

Utilizzando il "principio del privilegio minimo" (POLP), a un utente vengono concessi i diritti richiesti per svolgere il proprio ruolo, ma non più di quanto sia necessario. vSphere include diversi ruoli predefiniti che vengono utilizzati per la concessione di privilegi appropriati. Ad esempio, a un utente potrebbe essere concesso il ruolo di vSphere Administrator, HCIA Management o entrambi. Il ruolo HCIA Management concede all'utente un privilegio per l'esecuzione delle attività di gestione del ciclo di vita di VxRail dal plug-in di gestione VxRail all'interno di vCenter. vSphere Administrator concede il privilegio di eseguire le attività di amministratore in vCenter. Inoltre, vSphere consente un livello di controllo degli accessi ancora più preciso grazie alla creazione di ruoli personalizzati. Ad esempio, a un utente con privilegi può essere concessa la possibilità di confermare un allarme o di creare un profilo di storage, ma non di installare le VM.

I ruoli sono associati a utenti e gruppi e a oggetti specifici, in cui un oggetto è un elemento o un gruppo di elementi. Ad esempio, un utente o un gruppo potrebbe essere autorizzato a riconoscere gli avvisi per una particolare VM o porta, ma non per altri oggetti. È inoltre possibile assegnare agli utenti ruoli restrittivi come "No Access", impedendo loro di visualizzare aree specifiche all'interno di vCenter. È possibile concedere a più utenti o gruppi gli stessi o diversi livelli di accesso allo stesso oggetto. Le autorizzazioni concesse a un oggetto figlio possono essere utilizzate per eseguire l'override delle autorizzazioni ereditate da un oggetto principale.

Il controllo degli accessi basato sui ruoli di vSphere supporta i principi di sicurezza granulare di "minor privilegio" e "separazione della responsabilità" e consente al Security Administrator di migliorare la sicurezza stessa definendo autorizzazioni precise basate sulla struttura di gestione dei sistemi di un'organizzazione.

CONTABILITÀ

La comprensione delle modifiche apportate alla configurazione e allo stato dei componenti è fondamentale per proteggere i sistemi e renderli disponibili. Le modifiche possono essere il risultato di una correzione temporanea che causa un configuration drift. In alternativa, queste modifiche potrebbero indicare un'eventuale intrusione. Il monitoraggio proattivo dell'infrastruttura è un'importante attività di sicurezza.

Il rilevamento tempestivo quando si verifica un'intrusione può fare la differenza tra una breve interruzione in cui l'aggressore non è in grado di compromettere i sistemi critici e un'intrusione che persiste per mesi, con la compromissione di più sistemi critici. L'assenza di un sistema di audit log potrebbe non fornire informazioni adeguate sull'attacco per determinarne la gravità. Secondo il 2019 Trustwave Global Security Report (registrazione richiesta), il 57% degli incidenti esaminati ha coinvolto le reti aziendali e interne (fino al 50% nel 2017).

Il configuration drift è una sfida che interessa tutti i sistemi. I sistemi possono partire da una configurazione sicura, ma nel corso del tempo possono verificarsi modifiche che potrebbero lasciare il sistema vulnerabile. Queste modifiche possono verificarsi per una serie di motivi, tra cui una modifica temporanea durante la risoluzione dei problemi o una modifica approvata che deve entrare a far parte della configurazione di base. Senza il monitoraggio, il rilevamento di queste modifiche diventa molto complesso.

La sfida con il monitoraggio delle informazioni risiede nel fatto che provengono da molte fonti diverse: una singola VM, un server fisico, l'infrastruttura di virtualizzazione, la rete, i componenti di sicurezza o le applicazioni stesse. Per dare un senso a queste informazioni è necessaria una visione consolidata delle attività e delle modifiche. VxRail include vRealize Log Insight. Log Insight compila log VMware che includono server, dispositivi di rete, storage e applicazioni. Come illustrato di seguito, Log Insight crea un dashboard con grafici basati sui dati nei log. Ciò consente all'amministratore di risalire rapidamente e facilmente alla root cause del problema. La figura 10 di seguito mostra il dashboard di vRealize Log Insight.

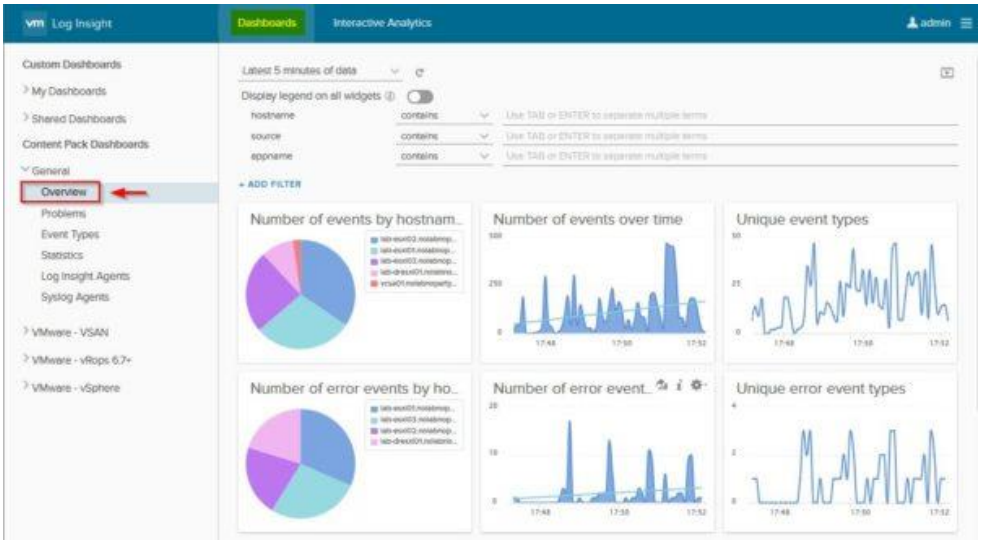

Figura 10: vRealize Log Insight

La correlazione di tutte queste informazioni è uno dei tanti motivi per cui VxRail utilizza il protocollo NTP (Network Time Protocol) standard del settore per garantire la sincronizzazione di tutti gli orologi dei componenti.

Per le organizzazioni che dispongono già di un sistema di gestione dei registri o di un sistema SIEM (Security Incident and Event Management), VxRail si integra facilmente utilizzando il protocollo syslog standard.

Sicurezza della posizione fisica di VxRail

La sicurezza fisica è una parte importante di una soluzione di sicurezza completa. Poiché VxRail può essere distribuito all'esterno di un data center tradizionale, la sicurezza fisica può assumere un'importanza ancora maggiore. Per evitare che il malware o il software infetto venga introdotto tramite un'unità USB, le porte USB su un VxRail possono essere disabilitate e quindi abilitate solo quando necessario.

I nodi VxRail monitorano anche altri eventi come aperture dello chassis, guasti o sostituzione dei componenti, modifiche al firmware e avvisi sulla temperatura. Queste informazioni vengono registrate nel Lifecycle Log di iDRAC. In molti casi non è necessario aprire uno chassis dopo la messa in produzione e il rilevamento di tale attività potrebbe essere l'indicatore di un tentativo di compromissione del sistema.

Automazione

Una parte importante della preservazione della sicurezza è assicurare che tutti gli elementi di configurazione della sicurezza pertinenti vengano implementati su tutti gli oggetti presenti in un ambiente. Un singolo cluster VxRail può disporre di un massimo di 64 nodi fisici e più cluster VxRail possono essere gestiti da un unico vCenter, supportando così migliaia di VM. Anche una semplice modifica, se deve essere configurata su tutte le VM, potrebbe richiedere un notevole lasso di tempo per la messa in atto. Inoltre, quando si eseguono attività ripetitive, le persone sono inclini a commettere errori. È qui che l'automazione diventa fondamentale.

L'automazione consente a un ambiente di avere meno errori di configurazione e una configurazione più coerente, aumentando al contempo l'efficienza e riducendo il tempo che intercorre tra una decisione e la sua implementazione, aumentando il time to value di tali decisioni.

Gli strumenti compatibili come vRealize Automation consentono l'automazione di vSphere e vSAN. Questi strumenti possono essere utilizzati per automatizzare le operazioni quotidiane standard, ad esempio la creazione di macchine virtuali o di criteri di storage. vRealize Automation può anche essere utilizzato per verificare che la configurazione di sicurezza non si sia discostata dalle impostazioni corrette. Se la configurazione è stata modificata, vRealize Automation è in grado di riconfigurare i server ESXi, vCenter o le singole VM in modo da soddisfare nuovamente la configurazione di sicurezza richiesta. Inoltre, poiché vRealize Automation è uno strumento VMware standard, molti team di virtualizzazione IT sanno già utilizzare vRealize Automation e hanno creato profili che funzionano con un cluster VxRail.

VxRail STIG Hardening Package

La configurazione della sicurezza può essere un processo complesso e soggetto a errori che presenta molti di quegli stessi rischi che tenta di mitigare. Tre diversi elementi semplificano il processo di protezione dell'infrastruttura VxRail. In primo luogo, vSphere dispone di un approccio "sicuro per impostazione predefinita" alla configurazione. In secondo luogo, le Security Technical Implementation Guides della Defense Information Systems Agency (DISA STIG) forniscono un modello per l'hardening della sicurezza e una vasta gamma di strumenti di automazione consente di verificare e definire il monitoraggio e la configurazione di parametri di sicurezza secondo le esigenze. In questo modo è possibile configurare il profilo di rischio appropriato in base alle esigenze aziendali. Infine, la possibilità di automatizzare il ripristino della configurazione a uno stato sicuro noto quando si verificano modifiche impreviste è una parte fondamentale della sicurezza di VxRail.

A partire da vSphere 6.0, VMware ha avviato un'iniziativa per rendere la sicurezza l'impostazione predefinita per vSphere. VxRail nasce quindi già più sicuro. Nell'ambito di questa iniziativa, la maggior parte delle impostazioni di sicurezza consigliate è stata classificata come specifica del sito oppure modificata su un valore predefinito di impostazione sicura. Le impostazioni che in precedenza dovevano essere modificate dopo l'installazione sono state aggiornate in modo che l'impostazione sicura sia quella predefinita.

Le impostazioni di configurazione classificate come specifiche del sito non possono essere configurate per impostazione predefinita, ad esempio il nome host di un server syslog o NTP remoto. Con VxRail, molte delle impostazioni classificate da VMware come specifiche del sito vengono configurate da HCI System Software durante l'installazione.

Molte organizzazioni utilizzano le STIG come base per l'hardening dei propri sistemi. Queste STIG forniscono un elenco di controllo sia in formato PDF leggibile che in uno script automatizzato. Ciò consente agli strumenti di automazione di leggere la STIG e configurare l'ambiente in modo che corrisponda alla configurazione consigliata con un intervento manuale minimo. Mentre le STIG VMware esistenti coprono i componenti di VxRail, tra cui vSphere, ESXi e vSAN semplificano al massimo l'implementazione. Dell VxRail Appliance con il software VxRail Appliance v4.5.x o 4.7.x è conforme ai requisiti delle Security Technical Implementation Guidelines (STIG) della DISA.

Nel corso del tempo, le configurazioni possono virare verso posizioni meno sicure. Per questo motivo è importante non solo monitorare la configurazione, ma anche automatizzare il ripristino dell'ambiente allo stato di sicurezza iniziale. VxRail supporta più opzioni diverse a seconda del livello di automazione richiesto. VxRail dispone di strumenti di hardening automatici che verificano la configurazione corrente a fronte di una STIG e, se la configurazione è cambiata, ripristinano la configurazione stessa allo stato sicuro noto. Se è necessario uno strumento di automazione più completo, VMware vRealize Suite interagisce con gli ambienti VxRail per automatizzare la gestione della configurazione, mantenendo al contempo il controllo e la governance. VMware offre inoltre AppDefense, uno strumento più orientato alle applicazioni che utilizza l'apprendimento automatico per raccogliere informazioni su uno stato noto corretto per le VM e le applicazioni supportate. Con questo strumento, l'amministratore riceverà una notifica quando viene rilevata una variazione rispetto allo stato noto corretto; la risposta può essere automatizzata da una libreria di routine di risposta agli incidenti.

Sicurezza integrata in VxRail ACE

VxRail Analytical Consulting Engine (ACE) integra la semplicità operativa tipica di Dell EMC VxRail con l'intelligenza operativa per i cluster VxRail, e offre una combinazione di semplicità operativa e intelligenza operativa con sicurezza intrinseca, consentendo alle aziende di perseguire la trasformazione dell'infrastruttura IT.

VxRail ACE viene eseguito su una piattaforma cloud gestita dall'IT di Dell EMC. Come soluzione SaaS basata sul cloud, VxRail ACE offre la flessibilità necessaria per fornire nuove funzionalità di frequente e senza interruzioni, assicurando al cliente un'esperienza eccezionale. La sua rete neurale per l'apprendimento approfondito migliorerà continuamente le funzionalità predittive grazie all'acquisizione dell'enorme quantità di metadati che VxRail può raccogliere sui cluster.

Gli utenti di VxRail possono accedere a VxRail ACE all'indirizzo https://vxrailace.emc.com utilizzando le credenziali del supporto Dell EMC.

Panoramica sulla sicurezza di VxRail ACE

VxRail ACE raccoglie i dati telemetrici dai nodi VxRail nei cluster VxRail dell'organizzazione e trasmette questi dati in modo sicuro a una soluzione SaaS gestita dall'IT di Dell EMC come mostrato nella figura 11.

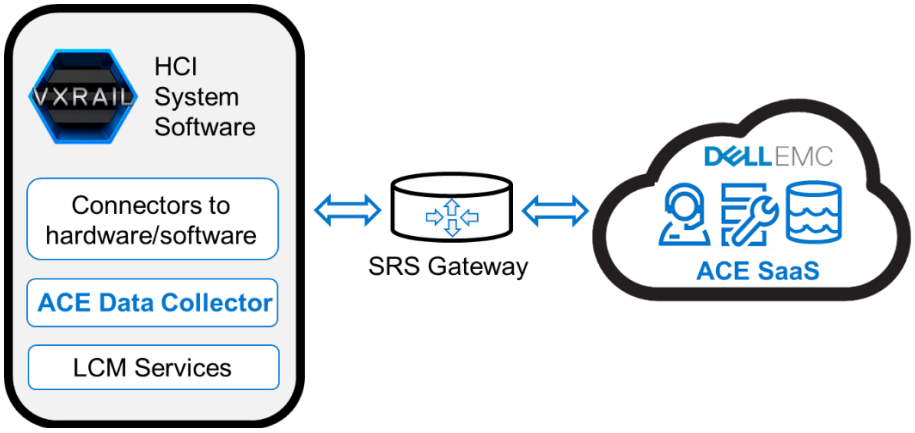

Figura 11: diagramma dell'architettura di alto livello di VxRail ACE

Dell EMC comprende le preoccupazioni dei clienti in merito al mantenimento della sicurezza dei propri dati. La sicurezza è intrinseca a VxRail ACE, dalla data collection fino ai dati in transito e at-rest. Inoltre, VxRail ACE è stato sviluppato in modo sicuro utilizzando i controlli architetturali nell'ambito del Dell EMC Security Development Lifecycle. Questo standard definisce le attività incentrate sulla sicurezza che i team dei prodotti di Dell EMC devono seguire per la creazione e il rilascio dei prodotti, al fine di consentire ai prodotti di Dell EMC di ridurre al minimo il rischio di vulnerabilità per i nostri prodotti e gli ambienti dei clienti.

Data collection di VxRail ACE

Su ciascun cluster VxRail viene eseguito un ADC (Adaptive Data Collector) che recupera i dati di telemetria da HCI System Software tramite i connettori hardware e software di VxRail. L'ADC non raccoglie informazioni di identificazione personale (PII). I dati di telemetria raccolti dall'ADC sono illustrati nella tabella 1.

Telemetria di base (topologia HW: appliance, unità, firmware, PSU)	**Dati sulle prestazioni**	**Allarmi**	**Dati dei sensori hardware**
• Informazioni sul cluster • Informazioni sull'appliance	• Cluster (CPU, memoria, disco) • VM (CPU, memoria, disco) • vSAN (disco, rete)	• vCenter • VxRail	• Tipo di sensore • Stato • Nome • Lettura corrente

Table 1 Dati di telemetria di VxRail raccolti da ACE

I dati di telemetria raccolti dall'ADC non vengono archiviati localmente, vengono trasmessi in modo sicuro sul gateway Secure Remote Support (SRS) di Dell EMC.

Dati di VxRail ACE in transito verso Dell

Solo i dati raccolti dall'Adaptive Data Collector (ADC) vengono inviati al backend Dell EMC sul gateway Secure Remote Service (SRS) di Dell EMC. VxRail ACE sottoscrive le notifiche di arrivo dei dati del sistema HCI tramite il gateway SRS. I clienti di VxRail ACE definiscono i sistemi che inviano i dati del sistema HCI sul gateway. Tutti i dati trasmessi sul gateway SRS di Dell EMC sono protetti in transito da best practice standard del settore. Il gateway SRS viene autenticato in modo bidirezionale utilizzando i certificati digitali RSA® in associazione alle policy di accesso controllate dal cliente e a un audit log dettagliato. La comunicazione point-to-point viene stabilita mediante l'utilizzo della crittografia AES (Advanced Encryption Standard) a 256 bit, che garantisce che tutti i dati vengano

trasportati in modo sicuro nell'infrastruttura gestita dall'IT di Dell EMC. Inoltre, SRS fornisce la VPN dedicata e l'autenticazione a più fattori. Una volta che i dati arrivano a Dell, VxRail ACE esegue la crittografia e l'archiviazione dei dati ACE nella propria infrastruttura gestita dall'IT di Dell EMC.

Dati at-rest di VxRail ACE

I dati del sistema HCI ricevuti dai sistemi gestiti di VxRail ACE vengono crittografati e archiviati nell'infrastruttura gestita dall'IT di Dell EMC.

L'infrastruttura IT di Dell EMC:

- Fornisce una piattaforma sicura che garantisce l'isolamento dei dati telemetrici di ogni cliente.
- Offre alta disponibilità, tolleranza di errore e ripristino di emergenza.
- Individua i dati telemetrici del cliente (inclusi i backup) negli Stati Uniti.
- Mantiene indefinitamente i dati cronologici per i sistemi che vengono monitorati attivamente da ACE, incluse le informazioni strategiche derivate da ACE.
- Consente a ciascun cliente di accedere a un portale indipendente e sicuro dal quale ciascun utente può visualizzare in VxRail ACE solo i sistemi che fanno parte dell'accesso al sito dell'utente, in base a quanto definito in Dell EMC MyService360.

Il Security and Resiliency Office (SRO) di Dell Technologies, diretto dal Chief Security Officer di Dell, è responsabile della sicurezza e della protezione dell'infrastruttura informatica di Dell EMC che ospita la soluzione SaaS VxRail ACE. Questa operazione viene eseguita tramite procedure e policy di sicurezza consolidate, nonché con l'applicazione dei controlli di sicurezza delle informazioni, che includono misure come firewall multi-layer, sistemi di rilevamento delle intrusioni, antivirus leader del settore e protezione da malware. Il team di sicurezza informatica di Dell EMC esegue continue scansioni di vulnerabilità continue sull'applicazione e sull'ambiente sottostante. Tutte le correzioni richieste vengono gestite mediante un programma continuo di risoluzione dei problemi di vulnerabilità, che prevede ad esempio aggiornamenti software, patch o modifiche alla configurazione.

Tutti i dati inviati a VxRail ACE vengono memorizzati su un'infrastruttura in hosting nel data center di Dell EMC. La policy di sicurezza delle informazioni garantisce che tutte le informazioni e le risorse di Dell EMC siano adeguatamente protette; i proprietari delle informazioni devono assicurarsi che vengano prese in considerazione tutte le risorse e che ciascuna risorsa disponga di un responsabile designato. Tutti i componenti dell'infrastruttura si trovano nella rete enclave protetta da firewall di Dell EMC, che non è esposta all'accesso esterno. Non sono consentiti singoli accessi diretti al database server e al database, ad eccezione dei membri dei team di amministrazione di sistema e del database. Gli account delle applicazioni di database vengono gestiti utilizzando l'autenticazione basata su password di database standard. Dell EMC ha implementato un processo di gestione delle modifiche best practice del settore per assicurare che l'hardware dell'infrastruttura Dell EMC sia stabile, controllato e protetto. La gestione delle modifiche fornisce le policy, le procedure e gli strumenti necessari per gestire tali modifiche, per assicurare che vengano sottoposte alle adeguate revisioni e approvazioni e che vengano comunicate efficacemente agli utenti.

Controllo degli accessi ai dati di VxRail ACE

L'accesso ai dati di VxRail ACE può essere suddiviso in due categorie:

- Accesso a VxRail ACE da parte dei clienti per la visualizzazione dei dati dei sistemi e delle informazioni strategiche derivate da ACE.
- Accesso da parte delle figure interne di amministratore di sistema e amministratore di database dell'IT di Dell EMC all'infrastruttura VxRail ACE gestita da Dell EMC.

Le sottosezioni di seguito descrivono come l'accesso ai dati sia controllato da queste due categorie di utenti.

Accesso a VxRail ACE per gli utenti finali

I clienti utilizzano il proprio account di supporto esistente per effettuare l'accesso a VxRail ACE. L'accesso ai dati di VxRail ACE dal portale di VxRail ACE richiede che ciascun utente finale disponga di un account di supporto Dell EMC valido. L'autenticazione è gestita dall'infrastruttura SSO (Single-Sign-On) di Dell EMC. VxRail ACE utilizza il profilo utente per clienti Dell EMC MyService360 per il controllo degli accessi. Il profilo utente viene creato e associato a un profilo cliente valido quando l'utente effettua la registrazione per un account con Dell EMC. VxRail ACE fornisce a ciascun cliente una vista sicura indipendente dei propri sistemi e assicura che i clienti siano in grado di visualizzare solo i propri dati tramite VxRail ACE. In VxRail ACE, ogni utente può visualizzare solo i sistemi che fanno parte del proprio accesso al sito, in base alla configurazione di tale utente in Dell EMC MyService360.

Accesso amministrativo all'infrastruttura VxRail ACE gestita dall'IT di Dell EMC

Dell EMC attribuisce molta importanza alla protezione delle informazioni riservate e proprietarie dei clienti. A tal fine, tutti i dipendenti di Dell EMC sono tenuti a sottoscrivere un contratto che include disposizioni riguardanti tutte le informazioni dei clienti. Gli obblighi di questo contratto si estendono a tutti i dati archiviati nei computer, in qualsiasi modalità o formato, individuati durante i servizi di manutenzione e rimangono in vigore anche dopo la cessazione del rapporto di lavoro con Dell EMC.

Standard e certificazioni compatibili

VxRail è un'infrastruttura iperconvergente solida e flessibile che può essere configurata per consentire alle organizzazioni di soddisfare le normative in materia di conformità. Sebbene alcuni fornitori di HCI possano asserire la compatibilità, Dell EMC persegue attivamente la certificazione completa per gli standard di sicurezza importanti per i nostri clienti. Contatta il tuo rappresentante Dell EMC per scoprire come VxRail soddisfi anche i requisiti di business e richiesti dalle normative vigenti più rigorosi. Di seguito è riportato un elenco di alcuni degli standard e delle certificazioni applicabili a VxRail.

Crittografia dei dati at-rest FIPS140-2: la Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) stabilisce i requisiti e gli standard per i componenti hardware e software dei moduli di crittografia. FIPS 140-2 è richiesto dal governo degli Stati Uniti e da altri settori regolamentati, come gli istituti finanziari e sanitari, che raccolgono, archiviano, trasferiscono, condividono e diffondono informazioni sensibili ma non classificate. I server PowerEdge utilizzati da VxRail sono stati convalidati.

Common Criteria EAL 2+: Common Criteria for Information Technology Security Evaluation è uno standard internazionale (ISO/IEC 15408) per la certificazione di sicurezza dei computer. Le valutazioni Common Criteria vengono eseguite su sistemi e prodotti per la sicurezza dei computer al fine di valutare le funzionalità di protezione dei sistemi e fornire un livello di confidenza per le funzionalità di protezione del prodotto mediante SAR (Security Assurance Requirement) o EAL (Evaluation Assurance Level). La certificazione Common Criteria non può garantire la sicurezza, ma può garantire che le dichiarazioni sugli attributi di sicurezza siano verificate in modo indipendente. I server PowerEdge e i componenti vSphere utilizzati da VxRail dispongono attualmente della piena certificazione.

NIST Cybersecurity Framework: il framework NIST per il miglioramento dell'infrastruttura critica è una guida volontaria sviluppata per aiutare le organizzazioni a migliorare la sicurezza informatica, il risk management e la resilienza dei sistemi. Il NIST si è consultato per oltre un anno con un'ampia gamma di partner governativi, industriali e accademici al fine di creare una serie di linee guida e pratiche valide basate sul consenso. La pubblicazione speciale 800-131A presenta le raccomandazioni per la lunghezza delle chiavi di crittografia.

NSA Suite B: Suite B è un insieme di algoritmi crittografici promulgati dalla National Security Agency nell'ambito del Cryptographic Modernization Program. Le versioni correnti di ESXi e vCenter utilizzante con VxRail supportano NSA Suite B.

Section 508 VPAT: gli standard Access Board Section 508 degli Stati Uniti si applicano alle tecnologie elettroniche e informatiche acquisite dal governo federale e definiscono i requisiti di accesso per le persone con disabilità fisiche, sensoriali o cognitive. I componenti software dei server PowerEdge e di vSphere utilizzati da VxRail sono conformi alla Section 508 VPAT.

Trade Adjustment Assistance (TAA): il programma Trade Adjustment Assistance è un programma federale che fornisce un percorso per la crescita dell'occupazione e le opportunità attraverso aiuti ai lavoratori statunitensi che hanno perso il lavoro a causa del commercio estero. Quando è venduto come sistema, VxRail è conforme a TAA.

DISA-STIG: la Defense Information Systems Agency (DISA) del Department of Defense (DOD) degli Stati Uniti sviluppa standard di configurazione noti come Security Technical Implementation Guides (STIG) come uno dei modi per mantenere la sicurezza dell'infrastruttura IT del DOD. Queste guide forniscono istruzioni tecniche per bloccare i sistemi informativi e/o il software che potrebbero altrimenti essere vulnerabili a un attacco. Dell EMC fornisce procedure manuali e automatizzate per la configurazione dell'appliance VxRail affinché sia conforme ai requisiti DISA STIG della rete informatica del DOD.

IPv6: IPv6 è il protocollo di nuova generazione utilizzato da Internet. Oltre a risolvere i limiti di indirizzamento di IPv4, IPv6 offre una serie di vantaggi in termini di sicurezza e molti ambienti si stanno muovendo verso l'adozione di IPv6. VxRail ha superato i test di interoperabilità USGv6 per IPv6 in modalità dual stack, nonché lo standard più elevato per il test IPv6 Ready.

Trusted Platform Module: il Trusted Computing Group definisce la specifica per il Trusted Platform Module (TPM). TPM 1.2 e 2.0 sono disponibili come opzione con VxRail. Entrambi sono certificati con i requisiti di sicurezza FIPS 140-2, TCG e Common Criteria. vSphere supporta TPM 1.2 e TPM 2.0

NIST Cybersecurity Framework e VxRail

Il NIST Cybersecurity Framework (NIST CSF) fornisce un framework di policy per la sicurezza dei computer che indica il modo in cui le organizzazioni del settore privato possono valutare e migliorare la capacità di prevenire, rilevare e rispondere agli attacchi informatici. Questo framework volontario è costituito da standard, linee guida e best practice per gestire i rischi correlati alla sicurezza informatica. L'approccio prioritizzato, flessibile e conveniente del Cybersecurity Framework contribuisce a promuovere la protezione e la resilienza dell'infrastruttura critica.

Il materiale "centrale" del NIST CSF è organizzato in cinque "funzioni", suddivise a loro volta in categorie come illustrato nella figura 12 di seguito.

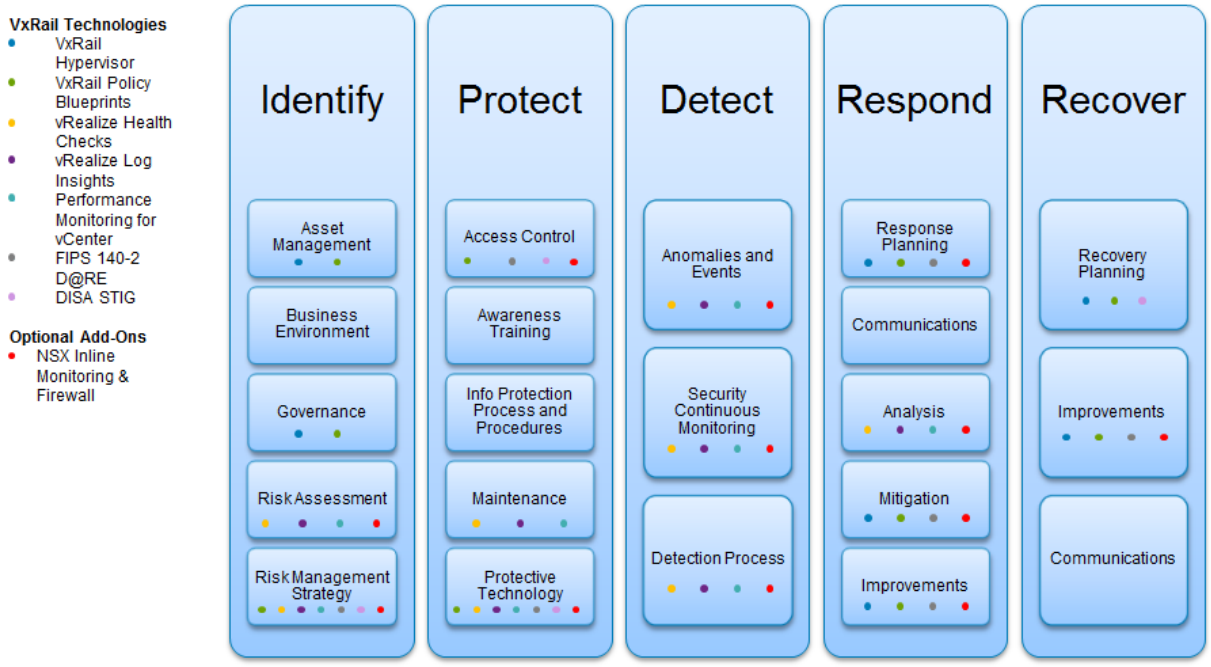

Figura 12: National Institute of Standards and Technology, Cybersecurity Framework

Per ulteriori informazioni sul NIST CSF, visita il sito web NIST. Per ulteriori informazioni sulle modalità di allineamento di VxRail con il NIST CSF, consulta il documento VxRail Features Supporting NIST Cyber Security Framework disponibile qui (framework di sicurezza).

Soluzioni e partner per la sicurezza di VxRail

VxRail è progettato per la sicurezza integrata e implementato secondo le best practice di sicurezza. Gli utenti vengono autenticati e autorizzati con il livello di accesso appropriato. I cluster VxRail sono facilmente configurabili con la crittografia dei dati at-rest per salvaguardare la riservatezza delle informazioni contenute, il traffico dei segmenti di configurazione di rete predefiniti e gli strumenti come RecoverPoint for VM, assicurando che le applicazioni e i servizi possano essere rapidamente ripristinati in caso di compromissione dell'integrità dei dati. Queste funzionalità di protezione sono fondamentali e inerenti all'appliance VxRail.

Tuttavia, la protezione di un ambiente dalle minacce attuali richiede una "difesa in profondità" con più livelli di sicurezza. Le reti che collegano applicazioni e servizi eseguiti sull'appliance VxRail agli utenti che li utilizzano devono essere protette, così come le applicazioni e i servizi stessi. Firewall, sistemi di prevenzione e rilevamento delle intrusioni, antivirus/antimalware, protezione degli endpoint e operazioni e gestione della sicurezza fanno tutti parte di una difesa multilayer. Solo Dell Technologies dispone di una gamma completa di tecnologie e servizi che contribuiscono a proteggere l'intero ambiente.

Le dimensioni dell'organizzazione e il punto in cui l'organizzazione si trova nel percorso di trasformazione dell'IT determinano l'approccio corretto. Alcuni ambienti possono funzionare all'interno dei framework di sicurezza esistenti, mentre altri possono trarre vantaggio dall'opportunità di trasformare le proprie operazioni di sicurezza insieme alla trasformazione dell'infrastruttura IT. Le organizzazioni si affidano spesso a molti fornitori diversi nell'ambito del proprio programma di sicurezza, incrementando una complessità che aumenta i rischi. La famiglia di Dell Technologies include RSA e SecureWorks; entrambi contribuiscono a gestire il rischio e proteggere le risorse digitali. Solo Dell Technologies è in grado di offrire una relazione con un unico fornitore, con un'esperienza di sicurezza completa e un ecosistema di migliaia di partner. La figura 13 di seguito illustra la potenza di Dell nell'aiutarti a gestire il rischio e proteggere i dati.

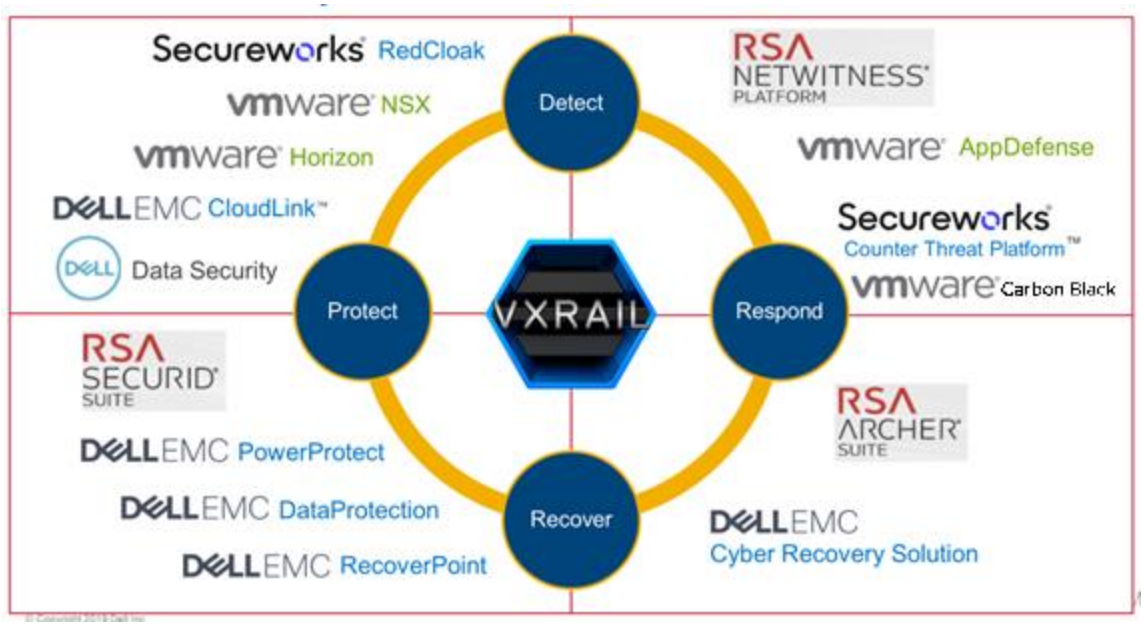

Figura 13: potenza di Dell nell'aiutarti a gestire il rischio e proteggere i dati

Gestione delle identità e degli accessi

VxRail supporta gli account utente locali, l'integrazione LDAP e Single Sign-On. Sebbene sia possibile disporre di un VxRail standalone, la maggior parte degli ambienti si integra con i sistemi IAM (Identity and Access Management) aziendali che utilizzano servizi di directory come Microsoft Active Directory.

Gestione di incidenti ed eventi di sicurezza

L'appliance VxRail include vRealize Log Insight per centralizzare la gestione dei registri per il sistema. Per le organizzazioni che già dispongono di un sistema di gestione dei registri centralizzato, ad esempio Splunk, oppure di un sistema SIEM (Security Incident and

Event Management), VxRail si integra facilmente con l'interfaccia syslog standard del settore. RSA NetWitness Suite fornisce la raccolta dei registri, l'analisi e molte altre funzionalità di protezione che migliorano le funzionalità di sicurezza di VxRail.

Per i clienti che non desiderano gestire autonomamente gli eventi di sicurezza, SecureWorks fornisce servizi di gestione dei registri per VxRail e praticamente qualsiasi risorsa di informazioni cruciali o tecnologia di sicurezza. SecureWorks raccoglie e monitora le informazioni di sicurezza necessarie per proteggere l'azienda. Aspetto ancora più importante, gli esperti di sicurezza di SecureWorks altamente qualificati, che operano nei centri integrati di contrasto alle minacce, indagano e rispondono immediatamente a qualsiasi attività malevola 24 ore al giorno, 7 giorni su 7.

Server di gestione delle chiavi

La crittografia è uno strumento potente per proteggere la riservatezza delle informazioni e VxRail è dotato di funzionalità di crittografia per proteggere i dati in uso, in movimento e at-rest. Tuttavia, la sicurezza dei dati fornita dalla crittografia è valida solo in funzione della generazione, della protezione e della gestione delle chiavi utilizzate nel processo di crittografia.

Le chiavi di crittografia devono essere disponibili quando sono necessarie e l'accesso alle chiavi durante le attività di decrittografia deve essere mantenuto per l'intero ciclo di vita dei dati. Pertanto, la corretta gestione delle chiavi di crittografia è essenziale per l'uso efficace della crittografia stessa. Molte organizzazioni centralizzano la gestione delle chiavi in tutta l'azienda per semplificare la gestione, applicare le policy e fornire reporting e verifica per la conformità.

VxRail e vSphere supportano il Key Management Interoperability Protocol (KMIP) che consente all'IT di lavorare con molti sistemi di gestione delle chiavi aziendali. Dell EMC CloudLink offre una gestione delle chiavi conforme a KMIP, nonché la crittografia per public, private e hybrid cloud. Per le organizzazioni che dispongono di servizi esistenti per la gestione delle chiavi, VxRail e vSphere si integrano facilmente e offrono un unico punto di gestione delle chiavi in tutta l'azienda. VMware offre un elenco di server di gestione delle chiavi compatibili.

Altri partner per la sicurezza

La protezione dell'infrastruttura IT e delle risorse digitali attuali è un'impresa complessa. Un'unica soluzione non è in grado di offrire una difesa sufficientemente solida. Per questo motivo, Dell Technologies offre un ecosistema di partner che collaborano per affrontare i rischi e le vulnerabilità specifici del proprio ambiente. Comprendiamo che l'intero settore deve collaborare per aiutare i clienti a raggiungere i propri obiettivi di sicurezza informatica.

L'appliance Dell EMC VxRail e VMware vSphere supportano gli standard di sicurezza aperti e i partner giocano un ruolo fondamentale nell'aiutare i clienti a passare a un mondo IT sicuro, virtuale e multi-cloud.

Il white paper "VMware Integrated Partner Solutions for Networking and Security" con link disponibile nell'appendice A include un elenco di alcune soluzioni dei partner per rete, sicurezza e conformità integrate con VMware vSphere®, vCenter™, vShield Endpoint™ e vCloud® Networking and Security™ e riporta la serie completa di applicazioni e software supportati da vSphere. Oltre alle API EPSEC per la protezione antivirus/antimalware fornite da vShield Endpoint, VMware vCloud Ecosystem Framework offre l'inserimento di servizi a livello di vNIC ed edge virtuale. La VMware Compatibility Guide semplifica l'individuazione del componente giusto.

Conclusioni

La trasformazione della sicurezza inizia con un'infrastruttura IT sicura. VxRail fornisce un'infrastruttura moderna e sicura dal core all'edge, fino al cloud. Si tratta di un'infrastruttura iperconvergente progettata, realizzata, costruita e gestita come un unico prodotto per limitare la possibile superficie di attacco, riducendo il numero di componenti coinvolti nell'infrastruttura. I pacchetti compositi del ciclo di vita del software VxRail possono includere aggiornamenti per BIOS, firmware, hypervisor, vSphere o qualsiasi componente di gestione incluso per semplificare notevolmente l'aggiornamento dello stack software completo, riducendo così la vulnerabilità agli attacchi.

La protezione di un ambiente dalle minacce attuali richiede una "difesa in profondità" con più livelli di sicurezza. Le reti che collegano applicazioni e servizi eseguiti sull'appliance VxRail agli utenti che li utilizzano devono essere protette, così come le applicazioni e i servizi stessi. Firewall, sistemi di prevenzione e rilevamento delle intrusioni, antivirus/antimalware, protezione degli endpoint e operazioni e gestione della sicurezza fanno tutti parte di una difesa multilayer.

Dell Technologies conosce la sicurezza e dispone di esperti in tutto il mondo che possono aiutarti a valutare l'ambiente e progettare un piano di sicurezza che soddisfi le tue esigenze specifiche. Per ulteriori informazioni, contatta un agente di Dell Technologies.

Appendice A: riferimenti

Di seguito sono riportati tutti i collegamenti e i riferimenti citati nel white paper.

Asset	URL
Sicurezza basata sul rischio:	https://www.riskbasedsecurity.com/2019/02/13/over-6500-data-breaches-and-more-than-5-billion-records-exposed-in-2018/
Sicurezza dei prodotti EMC:	https://www.dellemc.com/it-it/products/security/index.htm
Dell EMC Security Development Lifecycle:	https://www.dellemc.com/it-it/products/security/index.htm#tab0=2
Dell Product Security Incident Response Team (PSIRT):	https://www.dell.com/support/contents/it/it/19/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy
Sicurezza cyber-resiliente nei server Dell EMC PowerEdge di 14a generazione:	http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download
AppDefense:	https://www.vmware.com/products/appdefense.html
VMware Cloud Foundation on VxRail Architecture Guide:	https://www.dellemc.com/resources/it-it/asset/technical-guides-support-information/products/converged-infrastructure/vmware_cloud_foundation_on_vxrail_architecture_guide.pdf
Sicurezza dei prodotti VMware:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf
Dell EMC VxRail Network Guide:	https://www.dellemc.com/resources/en-us/asset/technical-guides-support-information/products/converged-infrastructure/h15300-VxRail-network-guide.pdf
Guida "Using SpoofGuard" di VMware:	https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-06047822-8572-4711-8401-BE16C274EFD3.html
Documentazione di VMware NSX:	https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-B5C70003-8194-4EC3-AB36-54C848508818.html
Security for Hyper-Converged Solutions:	https://communities.vmware.com/servlet/JiveServlet/download/36084-3-183512/Security for Hyper-Converged Solutions_NSX.pdf
2019 Trustwave Global Security Report:	https://www.trustwave.com/Resources/Library/Documents/2019-Trustwave-Global-Security-Report/
*1 2017 Data Breach Investigation Report.	http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
*2 "20thCEO Survey" di PWC condotta su 5.351 cittadini in 22 Paesi.	https://www.pwc.com/jg/en/publications/pwc-ceo-report-2017%20(2).pdf
NIST Cyber Security Framework:	https://www.nist.gov/cyberframework
Elenco dei server di gestione delle chiavi compatibili:	https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&details=1&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

Soluzioni partner VMware integrate per rete e sicurezza:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vcns/vmware-integrated-partner-solutions-networking-security.pdf
VMware Compatibility Guide:	https://www.vmware.com/resources/compatibility/search.php
Techbook di VxRail	https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf
Security Features of the integrated Dell Remote Access Controller (iDRAC):	http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download
Documentazione su vSAN:	https://docs.vmware.com/en/VMware-vSAN/index.html
Four business transformations:	https://www.youtube.com/watch?v=TcKJ39_4Rwc
Certificazioni della crittografia VMware:	https://www.vmware.com/security/certifications/fips.html
VMware vRealize Log Insight:	https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vrealize-log-insight/vrealize-log-insight-datasheet.pdf
Certificazioni NIST per FIPs 140-2. Cercare Dell EMC e VMware nel campo "Vendor":	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
VMware Secure Development Lifecycle:	https://www.vmware.com/security/sdl.html
Gestione delle chiavi VMware:	https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
vSphere 6.5 Security Guide:	https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-security-guide.pdf
Creazione di fiducia con i programmi DELL EMC Product Security:	https://www.emc.com/products/security/index.htm
	Risorse ACE
Demo video con panoramica di ACE	https://vxrail.is/acedemo
Demo video di preparazione dei pacchetti di aggiornamento intelligenti	https://vxrail.is/aceupdates
Panoramica della soluzione	https://www.dellemc.com/resources/it-it/asset/offering-overview-documents/products/converged-infrastructure/vxrail-ace-solution-brief.pdf
Panoramica di MyService360 di Dell Technologies	https://www.delltechnologies.com/en-us/services/support-deployment-technologies/my-service-360.htm
VxRail Comprehensive Security by Design (white paper)	https://www.dellemc.com/resources/it-it/asset/white-papers/products/converged-infrastructure/VxRail_Comprehensive_Security_by_Design.pdf
Prassi di sicurezza dei prodotti di Dell Technologies	https://www.delltechnologies.com/it-it/products/security/index.htm
	YouTube - Risorse sulla sicurezza
Youtube - VxRail Security Overview	https://www.youtube.com/watch?v=ZTNmYBgJv4s
Youtube - VxRail Security Hardening and Compliance	https://www.youtube.com/watch?v=ZjhfCE5nq6U