DIGITALIZZAZIONE DEA I E II LIVELLO

INFRASTRUTTURE ICT

PIATTAFORMA DI VIRTUALIZZAZIONE

Piattaforma di Virtualizzazione - PNRR

Data 25/01/2023

Sommario

1. Premessa

I data center tradizionali non sono in grado di tenere il passo con la velocità delle richieste delle amministrazioni. Mentre i data center tipici di oggi forniscono servizi affidabili e conformi all'interno delle loro organizzazioni. I team IT hanno sempre più difficoltà a tenere il passo con le nuove esigenze i sistemi e processi obsoleti stanno limitando la capacità degli IT di rispondere alle esigenze e alle richieste aziendali.

2. Infrastruttura Sanitaria Regionale Federata

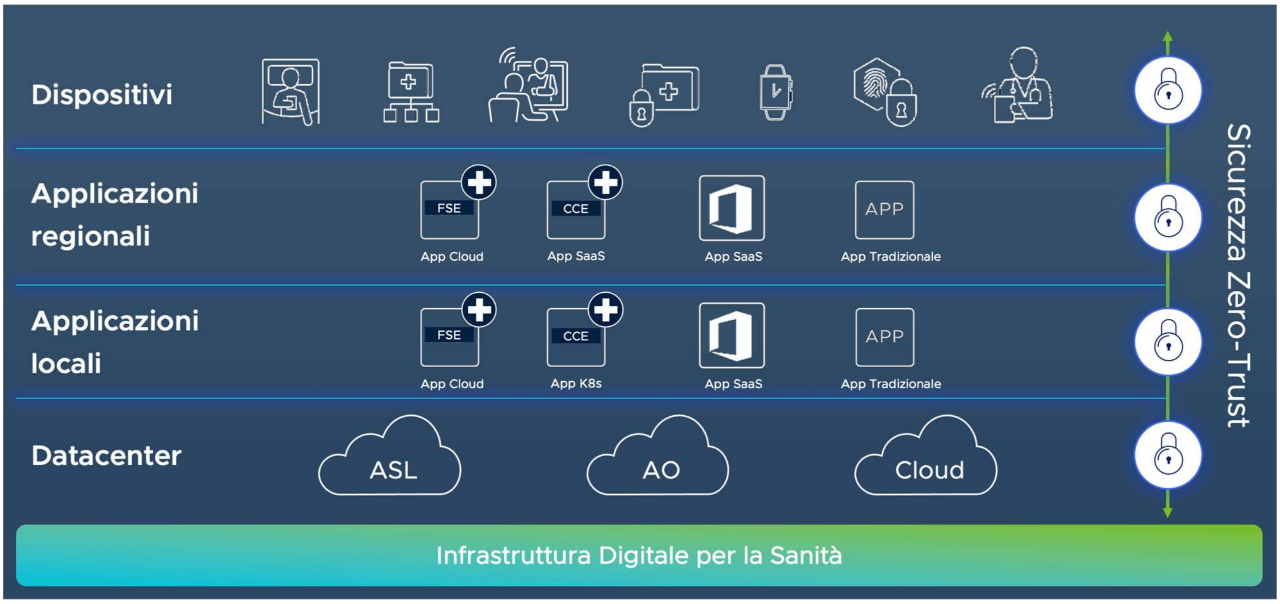
2.1. Panoramica

La proposta per l'Infrastruttura Sanitaria Regionale si fonda sulla implementazione di siti autoconsistenti basati su tecnologia VMware Cloud Foundation (VCF) e, a corredo, tutti gli strumenti per garantire una soluzione che abbia le caratteristiche di:

- Robustezza;
- Sicurezza;
- Alta Affidabilità;
- Gestione automatizzata del ciclo-vita.

Questo renderà possibile un approccio a più livelli:

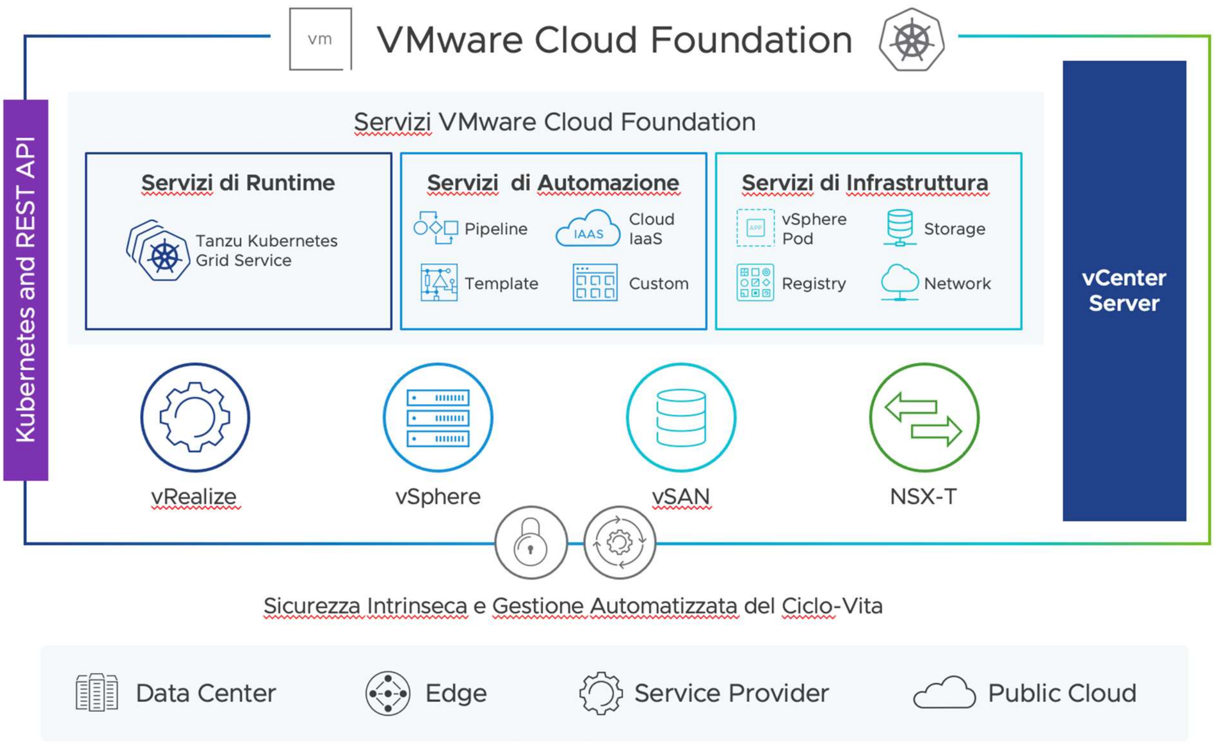
- **Livello Locale:** il singolo sito potrà erogare i servizi localmente in alta affidabilità, sia basati su Virtual Machine che su Container (Kubernetes).
- **Livello Regionale:** la piattaforma comune (VCF) permetterà di realizzare una federazione tra i siti facenti parte del gruppo per la realizzazione di servizi distribuiti, come ad esempio:
  - Applicazione basata su container in alta affidabilità (e.s. Cartella Clinica Elettronica);
  - Disaster Recovery centralizzato, tra siti o in cloud;
  - Monitoraggio centralizzato delle capacità e delle risorse disponibili.



2.2. VMware Cloud Foundation (VCF)

VMware Cloud Foundation è una piattaforma cloud ibrida che unisce l'infrastruttura cloud (elaborazione, archiviazione, rete e sicurezza) e servizi di gestione del cloud, consentendo di eseguire applicazioni aziendali tradizionali e moderne sia in ambienti cloud privati (on-premise) che pubblici. Consente di evolvere verso un modello operativo cloud indipendentemente da dove risiede il workload, fornendo infrastruttura, policy di sicurezza, gestione e operazioni coerenti. Gli amministratori IT possono distribuire rapidamente servizi IT standardizzati ai propri clienti interni, che si tratti di macchine virtuali o workload in container, su un'unica piattaforma, accelerando l'innovazione e guidando l'impatto sul business.

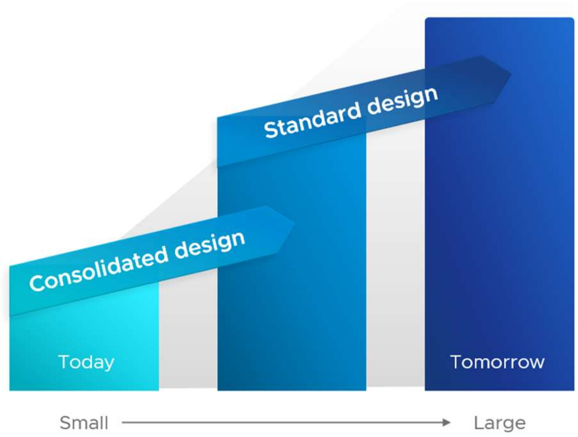
Si tratta di un'infrastruttura cloud unificata che combina le funzionalità essenziali per tutti gli scenari di cloud ibrido in una singola soluzione integrata (o attraverso componenti modulari e interoperabili), a supporto del Data Center che già si utilizza, per preservare gli investimenti. In questo senso, come riconosce anche Gartner, Cloud Foundation offre un'esperienza Software-Defined Data Center (SDDC) completa – grazie alla vasta serie di servizi software-defined per Elaborazione, Storage, Networking, Security e Cloud Management.



2.3. Scalabilità

La soluzione è pensata per essere modulare e scalabile in maniera semplice in base alle esigenze attuali e future. In quest'ottica l'approccio iperconvergente permette di identificare nel server l'elemento base sia per la componente computazionale (CPU, RAM) sia per quella dello spazio disco (HDD/SSD interni) e permette di costruire i cluster in base alle esigenze puntuali, sapendo a priori come andranno ad aumentare le risorse e quali workload sarà possibile ospitare al loro interno.

Nell'architettura ipotizzata la componente di management e i workload di produzione saranno ospitati sulla stessa infrastruttura andando a realizzare quella che viene definita una "Architettura Consolidata". Questo tipo di architettura potrà evolvere semplicemente in una di tipo "Standard" dove un cluster è dedicato al management e i restanti specializzati per il tipo di servizio che dovranno ospitare (VDI, Kubernetes, ecc)



2.4. Modernizzare l'infrastruttura in base alle proprie esigenze

Dal punto di vista squisitamente tecnologico, VMware Cloud Foundation rappresenta l'evoluzione della virtualizzazione del server VMware vSphere, ovviamente per quanto riguarda l'ampliamento delle potenzialità dell'hypervisor principale con funzionalità di Software-Defined Storage, networking e sicurezza integrate, che possono essere utilizzate in modo flessibile on-premise o come servizio nel public cloud. Ma ancora di più Cloud Foundation rappresenta di fatto il "core" dei data center e, grazie alle funzionalità di management integrate, permette quindi di poter sfruttare in modo completo la piattaforma di cloud ibrido generata estesa tra ambienti pubblici e privati, quindi con la libertà di eseguire applicazioni ovunque senza i costi, la complessità o il rischio di "refactoring" delle applicazioni stesse.

Si qualifica quindi come offerta di infrastruttura iperconvergente ottimizzata per tutte le applicazioni, quelle che girano su macchine virtuali, quelle containerizzate, quindi le applicazioni pacchettizzate e Open Source. Lo stack unificato (calcolo, storage, networking e gestione) consente altresì di modernizzare l'infrastruttura del Data Center esistente, ma anche gestire con maggiore efficienza gli ambienti on-premise e passare al cloud senza difficoltà gestendo l'intero cloud ibrido con un unico modello operativo. Sono oltre 60 i cloud provider globali che utilizzano Cloud Foundation come base per i propri servizi cloud.

Con VMware Cloud Foundation è possibile gestire l'inventario dei servizi infrastrutturali, ed eseguire il provisioning degli ambienti mantenendo la piena visibilità sulle risorse in modo da risolvere eventuali problemi anche in modo proattivo su tutti i cloud, ma si possono anche automatizzare le modalità di distribuzione dei workload in ogni ambiente.

Unico resta il modello di Disaster Recovery e Business Continuity, unica la visibilità dettagliata sui costi di ogni ambiente. L'approccio "unificato" si riverbera, come già accennato, anche per quanto riguarda la gestione delle applicazioni, dal cloud all'edge, con la possibilità di distribuire le app, applicare policy, pensare alla strategia di Disaster Recovery, garantendosi la possibilità di sfruttare lo stesso ambiente per test e sviluppo e quindi poi in produzione e per la migrazione sul cloud più favorevole.

2.5. Funzionalità e Benefici principali

VMware Cloud Foundation semplifica notevolmente il passaggio a un autentico cloud ibrido, migliorando al contempo la produttività degli amministratori e riducendo il TCO generale. I clienti che distribuiscono VMware Cloud Foundation possono ottenere i seguenti vantaggi rispetto agli Hardware-Defined Data Center legacy.

- **Stack integrato:** Cloud Foundation è una soluzione ingegnerizzata che integra l'intero stack Software-Defined con interoperabilità garantita, in questo modo non sarà più necessario preoccuparsi di gestire complesse matrici di interoperabilità
- **Architettura standardizzata:** basata sull'architettura VMware Validated Design standard, la soluzione garantisce distribuzioni rapide e ripetibili, eliminando il rischio di errori di configurazione
- **Gestione automatizzata del ciclo di vita:** la piattaforma include servizi esclusivi per la gestione del ciclo di vita in grado di automatizzare le operations iniziali e successive, dall'implementazione alla configurazione e al provisioning delle risorse, fino all'installazione di patch o upgrade
- **Percorso semplificato verso il cloud ibrido:** semplifica notevolmente il passaggio al cloud ibrido offrendo una piattaforma comune per cloud privati e pubblici e garantendo un'esperienza operativa comune che si avvale del personale, degli strumenti e dei processi esistenti
- **Ampio ecosistema:** la piattaforma può essere distribuita in modo flessibile on-site su componenti hardware certificati offerti dai principali vendor OEM o eseguita come servizio da VMware Cloud on AWS oppure da selezionati VMware Cloud Provider.

3. Gestione e Automazione centralizzata

3.1. Cloud Management Platform (CMP)

La piattaforma di Cloud Management (CMP) vRealize offre una base digitale coerente e dinamica per la distribuzione delle applicazioni in ambienti multi-cloud, favorendo così l'innovazione aziendale.

Rappresenta, inoltre, la soluzione più completa del settore per la creazione e la gestione di ambienti di cloud ibrido multi-vendor. vRealize Suite aiuta le aziende a distribuire le seguenti funzionalità di gestione delle operation:

- **Operation delle applicazioni:** consente agli sviluppatori di distribuire rapidamente le applicazioni cloud basate su microservizi e altamente distribuite, ottimizzandone le prestazioni e risolvendone eventuali problemi. Tutto in tempo reale.
- **Provisioning programmabile:** aiuta gli sviluppatori e l'IT ad accedere facilmente alle risorse applicative e di infrastruttura su qualsiasi cloud tramite API, catalogo o CLI con gestione completa del ciclo di vita.
- **Operation automatizzate:** aiuta l'IT a ottimizzare in modo continuo la capacità e le prestazioni in funzione degli obiettivi aziendali e operativi. vRealize Suite consente inoltre alle aziende di gestire i suddetti casi d'uso per comprendere il costo delle opzioni di infrastruttura e l'utilizzo delle risorse da parte degli utenti finali, al fine di ottimizzare i costi di capitale.

3.2. Funzionalità e Benefici principali

Le funzionalità si possono riassumere in:

- **Industrializzazione del cloud privato (SDDC):** con vRealize Suite il cloud privato diventa semplice da gestire e utilizzare come il cloud pubblico, grazie a gestione del ciclo di vita e operation automatizzate in grado di assicurare alta disponibilità e SLA (accordo sui livelli di servizio) con una quantità minima di errori a costi ridotti.
- **Infrastruttura adatta agli sviluppatori:** la piattaforma CMP consente all'IT e ai provider di servizi di offrire un'ampia scelta agli sviluppatori supportando più modelli di sandbox per la richiesta dei servizi e offrendo agli sviluppatori la libertà di utilizzare gli strumenti preferiti, incrementandone in tal modo la produttività.
- **Approccio comune per cloud ibrido e multi-cloud:** vRealize Suite consente all'IT e ai provider di servizi di mettere gli sviluppatori in condizioni di creare applicazioni basate su VM e container in modo semplice, rapido e sicuro in qualsiasi cloud privato, pubblico o ibrido con governance semplificata.
- **Integrazione ottimale:** grazie all'integrazione nativa con altre soluzioni SDDC di VMware, la piattaforma CMP consente di definire una policy di sicurezza tramite un blueprint di provisioning automatizzato all'inizio del ciclo di vita delle applicazioni, facendo sì che lo stato di sicurezza possa seguire un'app attraverso l'intero ciclo di vita, dalla creazione di istanze alla dismissione.

I vantaggi che scaturiscono da questo approccio sono:

- **Agilità:** velocizza la distribuzione dei servizi IT per consentire all'IT di soddisfare appieno le aspettative degli sviluppatori
- **Controllo:** offre il giusto livello di controllo per supportare le esigenze dei team IT tramite l'equilibrio degli obiettivi di agilità, rischio e costi

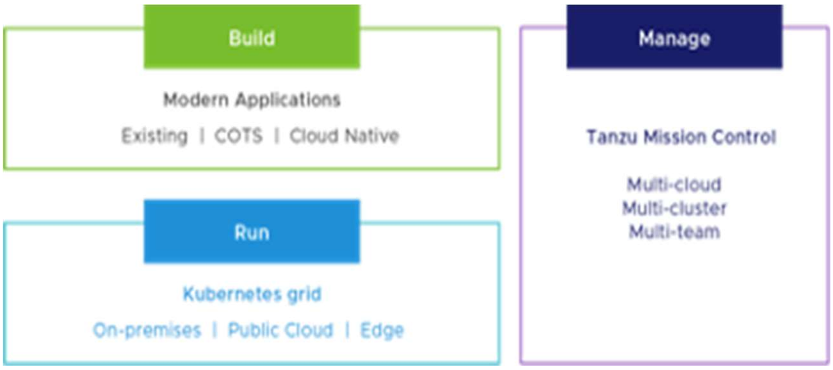
- **Efficienza:** aumenta l'efficienza del personale IT e l'utilizzo delle risorse del cloud privato e pubblico, riducendo OpEx e CapEx
- **Libertà di scelta:** consente agli sviluppatori di utilizzare le risorse tramite API, CLI e cataloghi, nonché gli strumenti dedicati che preferiscono

4. Applicazioni Moderne

VMware Cloud Foundation offre un'infrastruttura standardizzata basata su software in grado di rispondere in modo dinamico a ciò di cui l'azienda e gli sviluppatori hanno bisogno. Le amministrazioni possono, quindi, offrire la stessa esperienza on-premise che i loro sviluppatori di applicazioni ricevono dal cloud.

4.1. VMware Tanzu

VMware Tanzu è una piattaforma applicativa modulare per le applicazioni moderne che consente ai team operativi e di sviluppo di fornire valore aziendale in modo più rapido e sicuro a qualsiasi cloud, nonché di gestire app su larga scala tra i cloud. Utilizzando VMware Tanzu, è possibile ridurre la complessità di creazione, distribuzione e gestione delle applicazioni moderne basata su micro-servizi in un mondo multi-cloud.



- **Tanzu Build:** Strumenti che supportano la creazione, la gestione e la governance automatizzate dei container su scala aziendale. Inoltre, fornisce tool di sviluppo semplificato ed un catalogo costantemente aggiornato di componenti e applicazioni open source
- **Tanzu Run:** Standard open source, Kubernetes. Un framework che include la gestione completa del ciclo di vita di cluster kubernetes su qualsiasi cloud-privato, pubblico e periferico.
- **Tanzu Manage:** Control-plane Kubernetes che fornisce un unico punto di governance e controllo. Fornisce un meccanismo per riunire tutti i cluster, indipendentemente dall'ambiente di runtime, dalla gestione delle policy e della configurazione e fornisce agli sviluppatori funzionalità self-service.

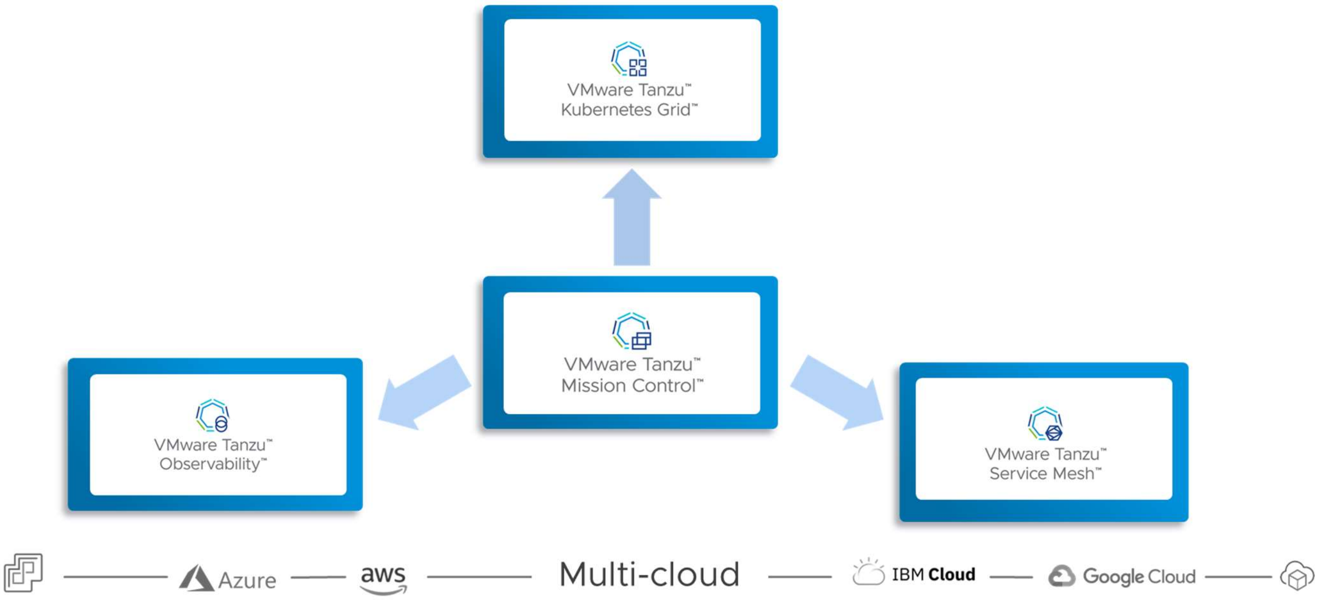
L'obiettivo di Tanzu è quello di supportare l'intero ciclo di modernizzazione del proprio parco applicativo fornendo tutti gli strumenti adeguati a semplificare l'esperienza dello sviluppatore e garantire una semplificazione delle IT operations con particolare attenzione agli aspetti di sicurezza.

4.2. Considerazioni Gestionali

Con l'aiuto di Tanzu Manage sarà possibile governare centralmente ambienti applicativi e piattaforme distribuite potenzialmente in contesti eterogenei tipici di modelli hybrid/multi-cloud.

Tanzu Mission Control, grazie alle sue forti integrazioni con la parte Tanzu Run e con gli strumenti di Observability e Service Meshing risulta essere un elemento essenziale quando l'ambiente "scala" in termini di numero di cluster K8s da gestire, quantità e complessità delle applicazioni e numero di "utenti" che vanno governati nell'accesso alla piattaforma.

Tanzu Manage non dimentica di coprire i temi di Operations più "tradizionali" quali la Data Protection centralizzata, il controllo costante della compliance infrastrutturale e l'automazione dei servizi di networking necessari alla dinamicità intrinseca delle applicazioni Cloud Native.



4.3. Funzionalità e Benefici principali

- **Integrazione nativa con VMware vSphere:** integrazione nativa con l'hypervisor vSphere di VMware, in modo da poter gestire con un unico control plane (vCenter) sia le VM che i container
- **Gestione ciclo di vita di Kubernetes:** la piattaforma Tanzu consente l'erogazione di "K8s as a Service" occupandosi del provisioning, del patching e dell'**upgrade di versione di Kubernetes in pochi semplici passaggi** utilizzando Tanzu Kubernetes Grid per vSphere. Queste funzionalità possono essere esposte tramite un catalogo di servizi tramite la suite VMware vRealize Automation in un contesto di private Cloud .
- **Integrazione nativa con VMware NSX-T e AVI Advanced Load Balancer:** Tanzu integra tecnologie di Node Networking, Automatic Routing, Load Balancing, K8s Ingress Controller services in un'unica soluzione supportata da VMware.

- **Integrazione nativa con Kubernetes storage:** qualsiasi soluzione storage supportata da vSphere è direttamente consumabile da K8s sotto forma di Persistent Volumes tramite un unico CSI driver, anche in R/W per VMware vSAN.
- **OS supportati:** VMware Tanzu fornisce una “command-line interface” (CLI) per il deploy e la gestione dei cluster kubernetes i cui binari (eseguibili) sono disponibili su sistema operativi Linux, macOS e Windows.

Come possibile evoluzione a supporto delle applicazioni moderne sarà possibile considerare anche:

- **Service Mesh:** il service meshing e’ un servizio fondamentale per le architetture containerizzate. **Tanzu Service Mesh** consente il service meshing in contesti **multi-cluster** astraendo in un unico management plane la connettività tra microservizi distribuiti geograficamente in diversi datacenters e/o in topologie ibride e multicloud. Il concetto di Global Namespaces consente la federazione di mesh distribuiti, la gestione della risoluzione nomi DNS cross-cluster, la cifratura end-to-end delle comunicazioni e il Distributed Tracing con piena visibilità di parametri fondamentali come latenze, request per seconds, error rate. Sulla base di queste metriche è possibile effettuare autoscaling e failover dei microservizi in alta affidabilità così come il debugging intelligente e abilitare scenari di patching/upgrading applicativo tramite canary deployment.
- **Observability:** VMware Tanzu integra strumentazioni di monitoring Open Source come Prometheus e Grafana ma anche soluzioni di Observability avanzata a più ampio spettro che mediante centinaia di integrazioni con i più comuni strumenti provvede ad una correlazione di eventi, metriche e tracce che provengono dall’infrastruttura HW, attraversano il layer di virtualizzazione e containerizzazione e si spingono fino a livello dell’**Application Performance Monitoring (APM).**
- **Data Management platform:** la piattaforma VMware Tanzu include una serie di soluzioni supportate per la gestione dei dati che risultano indispensabili per sviluppare applicazioni moderne. Il portafoglio Tanzu include database molto popolari come **MySQL, PostgreSQL e GreenPlum che sono supportati direttamente da VMware**. Oltre ai DB VMware supporta anche **RabbitMQ** (message-broker software), **Gemfire** (in-memory, key-value database).
- **PaaS con sicurezza integrata:** VMware Tanzu offre strumenti per garantire un ciclo di produzione del software intrinsecamente sicuro nelle sue componenti di OS, librerie e dipendenze supportando i più comuni linguaggi e framework di programmazione (Java con Spring, .NET con Steeltoe ma anche Python, Ruby, NodeJS ed altri). Tanzu fornisce altresì un catalogo curato di componenti OpenSource quali runtimes, messaging systems, databases che consentono di garantire la messa in produzione di tali componenti altamente customizzati e **sicurizzati** secondo un approccio **DevSecOps.**

5. Disaster Recovery

Per aumentare la robustezza dell'architettura è stata prevista la possibilità di attivare una soluzione di Disaster Recovery tra i siti facenti parte della federazione per proteggere le VM e le applicazioni critiche; con questa soluzione sarà possibile, infatti, far ripartire velocemente i servizi, locali o distribuiti, su un sito attivo a seguito di un "disastro" naturale o di altra natura occorso in uno degli altri siti.

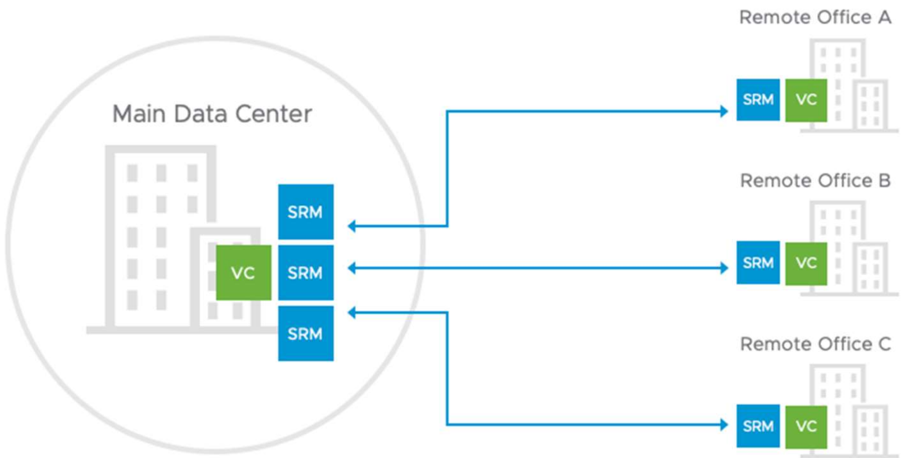
5.1. Site Recovery Manager

VMware Site Recovery Manager (SRM), un software di automazione che si integra con una tecnologia di replica sottostante per offrire gestione basata su policy, test senza interruzioni di servizio e orchestrazione automatizzata dei piani di ripristino, è destinato alle macchine virtuali e offre la necessaria scalabilità per gestire tutte le applicazioni in un ambiente VMware vSphere. Per garantire flessibilità e libertà di scelta, si integra in modo nativo con vSphere Replication oltre a supportare un'ampia gamma di soluzioni di replica basata su array (offerte da tutti i più importanti partner di storage VMware).

La soluzione consente di sfruttare in modo nativo i vantaggi di VMware vSphere e di utilizzare l'architettura SDDC (Software-Defined Data Center) integrandosi con altre soluzioni VMware, come VMware NSX (virtualizzazione della rete) e VMware vSAN (software alla base delle soluzioni di infrastruttura iperconvergente).

Site Recovery Manager può essere utilizzato in diversi scenari di failover a seconda dei requisiti, dei vincoli e degli obiettivi finali; di seguito una lista delle topologie possibili:

- **Attivo-Passivo:** un sito di produzione che esegue applicazioni e servizi e un sito secondario o di ripristino inattivo finché non è necessario per il ripristino
- **Attivo-Attivo:** una configurazione in cui i carichi di lavoro a bassa priorità come test e sviluppo vengono eseguiti nel sito di ripristino e vengono disattivati come parte del piano di ripristino. Ciò consente l'utilizzo delle risorse del sito di ripristino e una capacità sufficiente per i sistemi critici in caso di emergenza
- **Bi-direzionale:** le applicazioni di produzione sono attive in entrambi i siti (ad es. macchine virtuali nel sito A protette nel sito B e macchine virtuali nel sito B protette nel sito A)
- **Multi sito:** più siti remoti sono protetti da un unico sito di ripristino oppure un singolo sito esegue il failover di alcune applicazioni/macchine virtuali su un sito remoto e altri su uno o più siti remoti aggiuntivi



5.2. Funzionalità e Benefici principali

Di seguito le caratteristiche più rilevanti della soluzione:

- **Test di ripristino senza interruzioni di servizio:** è possibile eseguire test di failover automatizzati con la frequenza richiesta in una rete isolata per evitare conseguenze sulle applicazioni di produzione e garantire la compliance normativa attraverso report dettagliati
- **Workflow di orchestrazione automatizzata:** è possibile eseguire un failover di DR o una migrazione pianificata, quindi il failback al sito originario delle macchine virtuali ripristinate. Il tutto eseguendo lo stesso piano di ripristino con un solo clic.
- **Ripristino automatizzato delle impostazioni di rete e sicurezza:** Site Recovery Manager si integra con VMware NSX, eliminando la necessità di riconfigurare gli indirizzi IP sulle macchine virtuali ripristinate. Vengono anche conservate le policy di sicurezza, riducendo così ulteriormente le operazioni di configurazione post-ripristino
- **Estensibilità per l'automazione personalizzata:** è possibile utilizzare il plug-in VMware vRealize Orchestrator per Site Recovery Manager per sviluppare workflow di automazione personalizzati. I workflow pre-integrati semplificano il processo per avviare la creazione dei workflow personalizzati
- **Spostamento orchestrato con vMotion tra più istanze di vCenter:** i piani di ripristino consentono di orchestrare operation di spostamento con vMotion tra più istanze di vCenter, secondo necessità, in caso di utilizzo di storage esteso. Inoltre, è possibile eseguire la prevenzione dei disastri e le migrazioni dei data center senza downtime
- **Piani di ripristino centralizzati:** è possibile creare e gestire piani di ripristino per migliaia di macchine virtuali direttamente dall'intuitivo vSphere Web Client basato su un'interfaccia utente HTML5
- **Gestione basata su policy:** i gruppi di protezione dei "profili di storage" identificano i datastore protetti e automatizzano il processo di attivazione e disattivazione della protezione per le macchine virtuali, oltre a quello di aggiunta e rimozione dei datastore dai gruppi di protezione.

- **Mappature di rete automatizzate:** è possibile utilizzare gli switch logici VMware NSX per mappare automaticamente le impostazioni di rete sui due siti
- **Provisioning self-service:** i tenant delle applicazioni possono eseguire il provisioning della soluzione di protezione con Disaster Recovery utilizzando i blueprint disponibili in VMware vRealize Automation
- **Operation intelligenti:** è possibile risolvere le problematiche legate al monitoraggio grazie alla visibilità globale dell'ambiente assicurata da Management Pack per vRealize Operations

6. Accesso Agile e Sicuro

Nel processo di trasformazione digitale delle aziende sanitarie di ARES, un fattore fondamentale è quello di garantire l'accesso sicuro alle applicazioni e ai dati aziendali, per tutto il personale sanitario e i collaboratori esterni, ovunque essi si trovino.

6.1. Panoramica

La soluzione VMware Workspace ONE mette a disposizione tutti gli strumenti necessari per indirizzare le varie tipologie di utenti presenti nel contesto sanitario, avendo i seguenti obiettivi fondamentali:

- **Facile per l'Utente:** a partire dall'on-boarding guidato dei nuovi utenti, l'obiettivo è quello di rendere l'accesso alle applicazioni e dati aziendali il più semplice possibile, limitando dove possibile l'inserimento di password in favore di soluzioni più vicine alle possibilità della gran parte dei dispositivi moderni (es. accesso con sensori biometrici, Single-Sign On, ecc.)
- **Sicuro per l'Azienda:** la possibilità di accedere ad applicazioni e dati aziendali in qualsiasi contesto richiede il cambio di paradigma per quello che riguarda la sicurezza, andando a sfruttare soluzioni che verifichino costantemente la postura del dispositivo attraverso un approccio Zero-Trust

6.2. Workspace One

Workspace ONE è l'unica piattaforma di Digital Workspace basata sull'intelligence che consente di distribuire e gestire in modo semplice e sicuro qualsiasi app su qualunque dispositivo, integrando funzionalità di controllo dell'accesso, gestione delle applicazioni e gestione degli endpoint multipiattaforma.

La soluzione offre innanzitutto accesso Single Sign-on con semplicità di livello consumer sia al mobile app sia alle app cloud, web e Windows in un catalogo unificato, oltre a includere strumenti di collaborazione avanzati per e-mail, calendario, file e social media destinati ai dipendenti. Di conseguenza, questi ultimi hanno un maggiore controllo sulla scelta dei dispositivi da utilizzare (personali o forniti dal datore di lavoro), con la possibilità per i team IT di applicare policy di accesso condizionale granulari e basate sul rischio che tengano anche conto delle informazioni sulla compliance dei dispositivi.

Workspace ONE automatizza le tradizionali attività di integrazione e configurazione di laptop e dispositivi, oltre a consentire la gestione in tempo reale del ciclo di vita delle applicazioni, facendo quindi da tramite tra le app aziendali client-server legacy e l'era del mobile-cloud.

6.3. Horizon

VMware Horizon è una piattaforma moderna per la distribuzione sicura di desktop e app virtuali nel cloud ibrido. Sfruttando le migliori capacità di gestione e integrazioni profonde con l'ecosistema tecnologico VMware, la piattaforma Horizon offre un approccio moderno per la gestione di desktop e app che si estende da on-premise all'ibrido e multi-cloud. Il risultato è una distribuzione di applicazioni e desktop virtuali rapida e semplice che estende la modalità di accesso agile e sicuro a tutte le applicazioni.

I virtual desktop conservano la personalizzazione dell'utente da una sessione all'altra e possono essere distrutti al logout, un approccio di provisioning agile che può distribuire rapidamente immagini e app aggiornate al successivo accesso. Il provisioning uno-a-molti e la completa estensibilità API della piattaforma Horizon semplificano e automatizzano la gestione ordinaria di immagini, app, profili e policy. L'IT può trarre vantaggio da questo approccio moderno e leggero che semplifica la gestione, fa risparmiare tempo e riduce i costi, ma non a scapito della personalizzazione dell'utente.

6.4. Funzionalità e Benefici principali

Workspace ONE permette di migliorare drasticamente le esperienze e le attività che in precedenza erano caratterizzate da costi elevati, notevole dispendio di tempo e utilizzo elevato delle risorse.

Di seguito le principali funzionalità:

- **Accesso con semplicità di livello consumer sia alle app cloud, web, Windows e Mac sia al mobile app:** l'onboarding di nuove app e nuovi dipendenti non è mai stata così facile. Una volta eseguita l'autenticazione tramite l'app VMware Workspace ONE, i dipendenti avranno accesso immediato al catalogo delle app aziendali personalizzato che consente la sottoscrizione di qualsiasi mobile app, app Windows e Mac. Workspace ONE semplifica la gestione di applicazioni e accessi offrendo funzionalità Single Sign-on (SSO) e supporto dell'autenticazione a più fattori.

- **Possibilità di utilizzare qualsiasi dispositivo, BYOD o aziendale:** L'architettura distribuita nel presente deve essere compatibile con i nuovi dispositivi che verranno in futuro. Dai dispositivi indossabili alle workstation per la grafica 3D, per assicurare la produttività dei dipendenti è necessario rendere disponibili le app necessarie sempre e ovunque. Alcuni dispositivi appartengono all'azienda e devono essere configurati e gestiti dai team IT per tutto il ciclo di vita, mentre molti altri sono di proprietà dei dipendenti. VMware Workspace ONE con gestione adattiva offre ai dipendenti la libertà di scegliere il livello di praticità, accesso, sicurezza e gestione più appropriato al proprio stile di lavoro, agevolando l'adozione dei programmi BYOD senza alcun coinvolgimento dell'IT.
- **App sicure per la produttività: posta, calendario, documenti e social:** Workspace ONE include gli strumenti per la gestione di e-mail, calendario, contatti, documenti, chat e social media aziendali richiesti dai dipendenti, mentre misure di sicurezza invisibili proteggono l'azienda da eventuali perdite di dati, limitando le modalità di modifica e condivisone di allegati e file. A differenza degli ambienti chiusi (i cosiddetti "walled garden"), nelle applicazioni e negli strumenti già in uso è possibile integrare chat per team, discussioni aziendali, sessioni di domande e risposte, accesso ai contenuti e altri strumenti social che consentono ai dipendenti di collaborare in tempo reale per garantire non solo la produttività, ma anche un reale coinvolgimento.
- **Sicurezza dei dati e compliance degli endpoint con accesso condizionale:** Per proteggere le informazioni più sensibili, Workspace ONE combina la gestione delle identità e dei dispositivi per applicare decisioni di accesso basate su una serie di condizioni, come il livello di autenticazione, la rete, la posizione e la compliance del dispositivo.
- **Distribuzione e automazione delle app in tempo reale:** Workspace ONE sfrutta al meglio le nuove funzionalità di Windows e la tecnologia Workspace ONE UEM, leader del settore, per consentire agli amministratori dei desktop di automatizzare la distribuzione delle applicazioni e gli aggiornamenti in tempo reale. Combinata con la tecnologia di virtualizzazione Horizon all'avanguardia, l'automazione del processo di distribuzione delle applicazioni consente di migliorare la sicurezza e la compliance. Workspace ONE semplifica il passaggio alla gestione moderna di Windows 10 con funzionalità di gestione congiunta per Microsoft System Center Configuration Manager (SCCM).
- **Sicurezza End-to-End:** Horizon offre un accesso remoto sicuro alle risorse aziendali da dispositivi personali o aziendali e desktop e app ospitati centralmente. La sicurezza intrinseca integrata nella tua infrastruttura VMware aiuta a fornire una sicurezza completa dal dispositivo, attraverso la rete, nel Data Center e nel cloud. Il portale di accesso aziendale stabilisce e verifica l'identità dell'utente finale con l'autenticazione a più fattori e funge da base per l'accesso condizionale e le policy di micro-segmentazione di rete per desktop e app virtuali. Questi elementi intrinseci aiutano a fornire un modello di sicurezza dell'accesso Zero Trust tra utenti, app ed endpoint dando la possibilità agli utenti di utilizzare le risorse aziendali in qualsiasi momento senza sacrificare la sicurezza.

- **Esperienza "Digital Workspace" completa:** Fornendo l'accesso ai desktop virtuali e alle app di Horizon tramite Workspace ONE, l'IT può estendere ulteriormente l'esperienza di "Digital Workspace" a tutte le app e i casi d'uso. Le funzionalità di Horizon includono single sign-on, collaborazione di sessione e supporto per centinaia di periferiche. I desktop personalizzati offrono prestazioni ottimali e un'esperienza utente coinvolgente e ricca di funzionalità su dispositivi, posizioni, media e connessioni di rete. I lavoratori remoti e mobili godono di prestazioni di classe workstation e grafica 2D e 3D con il protocollo Blast Extreme, che offre ottimizzazione dinamica in condizioni di rete non ideali, ad alta latenza e con larghezza di banda ridotta.

7. Sicurezza Intrinseca

7.1. Panoramica

La sicurezza intrinseca è un approccio fondamentalmente diverso per proteggere i dati e le applicazioni. Non è un prodotto, uno strumento o un pacchetto, è una strategia per sfruttare l'infrastruttura e i punti di controllo in modi nuovi. La capacità di passare da una posizione di sicurezza reattiva a una posizione di forza richiede la capacità di farlo in tempo reale, su qualsiasi app, cloud o dispositivo.

La sicurezza intrinseca consiste nell'utilizzare l'infrastruttura in modo da poter unificare i team di sicurezza e IT e dare loro a disposizione un contesto approfondito che accelera il modo in cui vengono identificati i rischi e prevenute, rilevate e gestite le minacce.

Questo approccio strategico si fonda su tre caratteristiche fondamentali:

Integrato: massimizza i controlli di sicurezza integrati direttamente nell'infrastruttura, invece di affidarsi a prodotti standalone. Alla base c'è l'intenzione di reinventare le funzionalità di sicurezza (es. distributed firewall) e creare tali controlli direttamente nella tua infrastruttura, piuttosto che "trasformare" un firewall hardware e riconfezionarlo come appliance virtuale mantenendo, però, gli stessi limiti e vincoli di uno fisico.

La sicurezza intrinseca è integrata direttamente nel software. Sfruttando il livello virtuale, è possibile utilizzare l'infrastruttura esistente in nuovi modi per proteggere endpoint e workload, reti, spazi di lavoro e cloud, ottenendo al contempo maggiore visibilità e controllo sulle policy che proteggono l'azienda.

Unificato: riunisce strumenti e team consentendo ai professionisti della sicurezza di utilizzare dati ed eventi provenienti dall'IT e dalle operazioni per controllare in modo più efficace minacce e policy. Questo approccio unificato sfrutta l'infrastruttura cloud, delle applicazioni e dei dispositivi per fornire informazioni dettagliate sulle applicazioni e sull'infrastruttura.

Riunendo la tecnologia e le informazioni dettagliate utilizzate dai team di sicurezza e IT, il personale può collaborare di più e aumentare la propria agilità per rispondere a nuove vulnerabilità e minacce attive.

Contestualizzato: fornire un contesto completo non solo sulle minacce, ma anche su ciò che stai proteggendo: endpoint e workload, reti, spazi di lavoro e cloud.

Sicurezza incentrata sul contesto significa conoscere i comportamenti e le azioni previste, inclusi dati, utenti, punti di accesso e configurazioni. Ti fornisce una potente intelligenza che ti consente di comprendere rapidamente:

- Quali workload compongono le applicazioni?
- Come comunicano?
- Quali servizi di rete consumano?
- Quali utenti e dispositivi si connettono a tali applicazioni?
- Qual è la postura di questi dispositivi?

Questa comprensione incentrata sul contesto consente di agire più rapidamente per prevenire o rispondere a nuove minacce.

7.2. Il modello Zero-Trust

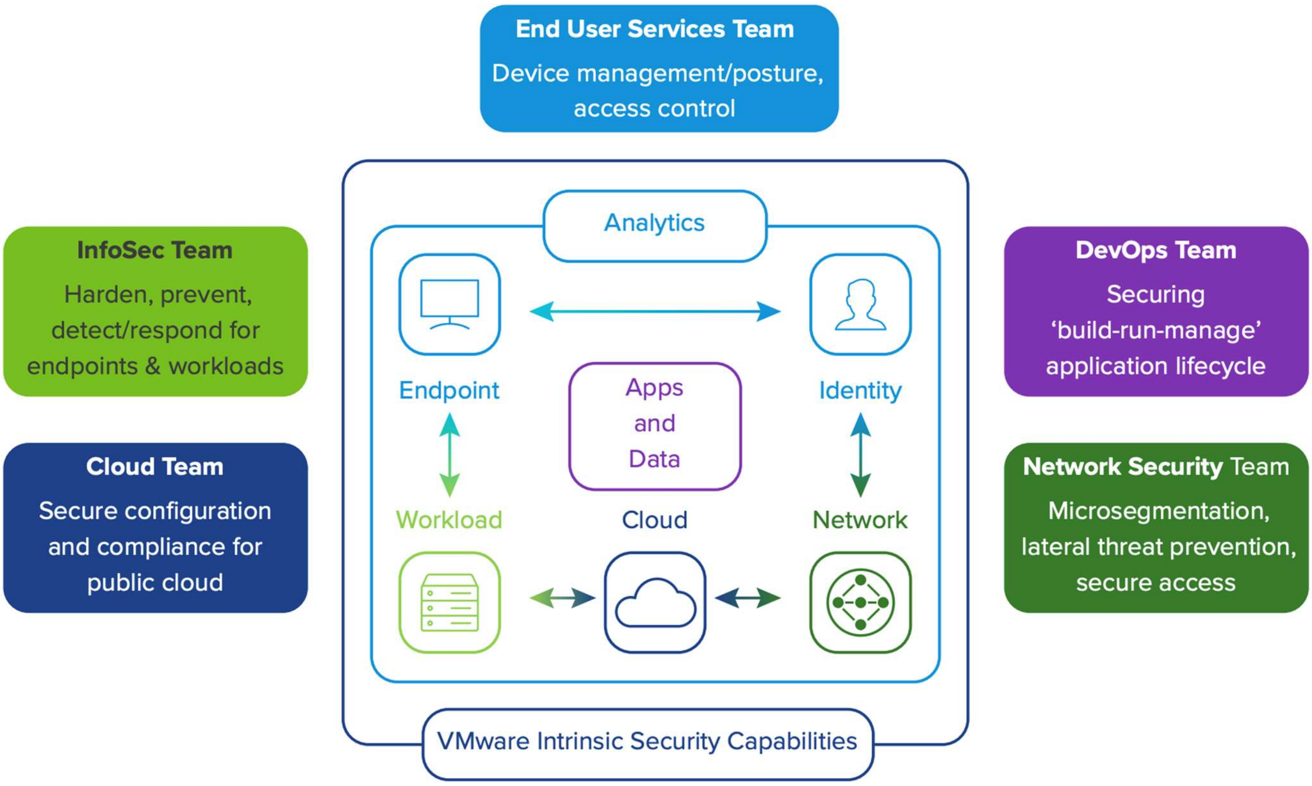
Zero-trust è il nome di un approccio alla sicurezza IT che presuppone l'assenza di un perimetro di rete affidabile e in base al quale ogni transazione di rete deve essere autenticata prima che possa concretizzarsi.

Il modello zero-trust si basa sul principio “non fidarsi mai, verificare sempre” e fa affidamento su altre metodologie di sicurezza della rete, quali la segmentazione della rete e controlli di accesso rigorosi. Una rete zero-trust definisce una “superficie protetta” che include dati, risorse, applicazioni e servizi critici. La superficie protetta è di solito notevolmente più piccola dell'intera superficie di attacco, poiché sono incluse solo le risorse critiche.

La sicurezza zero-trust ha sostituito i vecchi presupposti secondo cui le risorse all'interno del perimetro della rete aziendale devono essere ritenute affidabili e considera la fiducia come una vulnerabilità, dal momento che gli utenti di una rete “affidabile” potevano spostarsi all'interno della rete o causare l'esfiltrazione di tutti i dati ai quali avevano legittimamente accesso.

Poiché la forza lavoro è geograficamente dispersa e remota, il modello zero-trust non dipende da una particolare posizione. Le risorse e gli utenti possono risiedere ovunque: on-premise, in uno o più cloud o sull’edge, a casa dei dipendenti o come dispositivi IoT.

L'approccio alla sicurezza intrinseca di VMware sfrutta l'infrastruttura VMware esistente come punti di controllo della sicurezza fornendo visibilità su reti, endpoint, identità degli utenti, infrastruttura cloud e workload. Utilizzando un approccio integrato, gli strumenti e i team possono essere unificati riducendo complessità e costi. La migliore visibilità tra i team può aiutare l'IT e la sicurezza a lavorare insieme supportando un approccio collaborativo a Zero Trust.



Di seguito alcuni esempi di come l'approccio alla sicurezza intrinseca VMware si declina nei vari elementi tipici che costituiscono il Data Center, le applicazioni e l'accesso a quest'ultime.

7.3. Dati

Ogni accesso ai dati viene verificato con autenticazione e autorizzazione a livello di dispositivo e rete. Le soluzioni di storage di VMware forniscono la crittografia integrata per i dati inattivi.

7.4. Utenti e Dispositivi

Le soluzioni VMware uniscono la gestione unificata dei dispositivi, l'accesso condizionato e le funzionalità di intelligence per stabilire l'autenticazione continua e l'applicazione delle policy di accesso. Gli amministratori possono consentire l'accesso solo da dispositivi compatibili consentiti. Una volta stabilita la conformità del dispositivo, è possibile impostare una serie di criteri di accesso che utilizzano la posizione, l'applicazione e l'analisi del rischio mentre gli utenti finali si autenticano senza problemi tramite una gamma di diversi metodi di autenticazione moderni per l'accesso sicuro alle applicazioni e ai dati. Inoltre, la protezione degli endpoint nativa del cloud combina il rilevamento delle minacce e la protezione comportamentale per rafforzare ulteriormente la sicurezza.

7.5. Workload

Per i workload, VMware fornisce:

- visibilità e analisi di configurazione, stato e vulnerabilità utili per la messa in sicurezza
- meccanismi di prevenzione contro malware, ransomware e attacchi non malware/file-less;

- rilevamento e meccanismi di risposta agli attacchi che aggirano sia tali processi che controlli.

I workload sono protetti sia in cloud privati che pubblici, sia su macchine virtuali tradizionali che per container Kubernetes. Il loro approccio può sfruttare anche alcune integrazioni uniche con il tessuto virtuale che gli consentono di essere agentless su vSphere (e un unico sensore leggero in altri ambienti) e integrato con vCenter, fornendo un'unica sorgente della verità sia ai team di sicurezza che a quelli dell'infrastruttura. Ciò consente una migliore collaborazione tra sicurezza e IT, e un'operatività più efficace della sicurezza del workload attraverso il team dell'infrastruttura.

Combinato con la tecnologia di micro-segmentazione NSX, può applicare un modello Zero Trust sia dal punto di vista del workload che della rete, entrambi allineati alle applicazioni.

7.6. Reti

L'approccio distribuito di VMware al firewall va dalla macro alla micro-segmentazione offrendo controlli L7 con stato e prevenzione avanzata delle minacce. La sua esclusiva architettura distribuita non richiede modifiche alla rete.

Presente nell'hypervisor, la piattaforma firewall distribuita ha visibilità completa sulla topologia dell'applicazione e automaticamente formula policy di micro-segmentazione. Un'unica soluzione fornisce policy coerenti tra workload containerizzati e bare-metal che si estendono in ambienti cloud pubblici e privati.

7.7. Analytics

Le soluzioni VMware includono analisi integrate per fornire visibilità e avvisi completi agli operatori della sicurezza. Oltre all'analisi integrata, VMware Threat Analysis Unit (TAU), un team centrale di ricercatori sulle minacce e data scientist, sfrutta la telemetria del prodotto, i feed dei partner e le tecniche di intelligenza artificiale per garantire che le piattaforme siano alimentate con la migliore intelligence sulle minacce e algoritmi aggiornati.

7.8. Orchestrazione e Automazione

Le soluzioni VMware offrono opzioni di orchestrazione tra workload, dispositivo e rete. Una panoramica dettagliata sui flussi di lavoro può essere costruita per automatizzare le attività, tra cui la distribuzione del workload, la segmentazione della rete, la configurazione dei dispositivi e l'isolamento delle minacce.

8. Carbon Black

Carbon Black Cloud è una piattaforma di protezione di endpoint e datacenter che consente di identificare i rischi e prevenire, rilevare e rispondere agli attacchi più recenti e complessi. Utilizzando i moduli della piattaforma, è possibile cercare in modo proattivo attività anomale utilizzando informazioni sulle minacce e watchlist personalizzabili. Le funzionalità di risposta in tempo reale, come l'isolamento e la rimozione di file dannosi, consentono all'IT di rispondere più rapidamente quando vengono identificati gli attacchi.

8.1. Funzionalità e Benefici principali

Di seguito le principali funzionalità:

- **Proteggere i workload nel datacenter:** I team del Security Operation Center (SOC) possono prevenire, rilevare e rispondere alle minacce che prendono di mira le risorse più critiche dell'organizzazione con antivirus di nuova generazione (NGAV) certificati per sostituire gli antivirus legacy, combinati con funzionalità di rilevamento e risposta leader del settore. Gli amministratori di vSphere possono attivare facilmente la protezione del workload come funzionalità direttamente dal client vSphere, con l'abilitazione in blocco e la gestione del ciclo di vita per l'inventario delle macchine virtuali. VMware Carbon Black offre una visibilità più profonda e senza precedenti nell'ambiente per ridurre i rischi e rafforzare i workload, aiutando nel contempo a semplificare e rendere operativa la sicurezza.
- **Gestione dei rischi e messa in sicurezza dei workload:** aiuta i team di sicurezza e infrastruttura a ridurre la superficie di attacco dell'azienda con la messa in sicurezza dei workload, i rapporti sulla compliance e la definizione delle priorità delle vulnerabilità. Incorporando la sicurezza nell'infrastruttura, è possibile controllare facilmente lo stato attuale del sistema per tenere traccia dello stato di sicurezza e mettere in sicurezza i workload, consentendo al contempo una collaborazione più semplice con gli amministratori dell'infrastruttura e del cloud per affrontare le vulnerabilità critiche.
- **Prevenire, identificare e rispondere agli attacchi:** Enterprise EDR è una soluzione avanzata di threat hunting e risposta agli attacchi che offre visibilità continua ai principali centri operativi di sicurezza (SOC) e ai team di risposta agli incidenti (IR). Enterprise EDR viene fornito tramite una piattaforma di protezione degli endpoint di nuova generazione che consolida la sicurezza nel cloud utilizzando un unico agente, console e set di dati.
- **Semplificare le operazioni per i team IT e di sicurezza:** grazie all'approccio di sicurezza intrinseca possiamo eliminare il compromesso tra sicurezza e semplicità operativa fornendo un'unica fonte di verità per i team di infrastruttura e sicurezza per accelerare la risposta a vulnerabilità e attacchi critici, consentendo al contempo la collaborazione e riducendo gli attriti.

8.2. NSX Distributed Firewall

VMware NSX Distributed Firewall è un firewall di livello 7 definito dal software, creato appositamente per proteggere il traffico tra workload virtualizzati. Con una visibilità completa su applicazioni e flussi, NSX Distributed Firewall offre una sicurezza superiore con l'automazione delle policy collegata al ciclo di vita del workload. A differenza dei firewall tradizionali che richiedono la riprogettazione della rete e il blocco del traffico, NSX Distributed Firewall distribuisce il firewall a ciascun host, semplificando radicalmente l'architettura di sicurezza. Ciò consente ai team di sicurezza di segmentare facilmente la rete, fermare il movimento laterale degli attacchi e automatizzare le policy in un modello operativo molto più semplice.

8.3. Funzionalità e Benefici principali

Di seguito le principali funzionalità e benefici:

- **Semplificare la segmentazione della rete:** visibilità sul traffico e creazione facilitata di segmentazioni di rete o zone di sicurezza virtuali in pochi minuti, senza modifiche alla rete esistente, definendole interamente nel software
- **Implementare la micro-segmentazione per l'approccio zero trust:** generare automaticamente suggerimenti sulle policy in base a criteri intrinseci e di comprensione della topologia dell'applicazione. Ciò consente di creare, applicare e gestire facilmente policy di micro-segmentazione granulari e sfruttare il modello di policy basato su oggetti per l'automazione.
- **Nessuna modifica alla rete:** semplifica radicalmente l'implementazione e le operazioni del firewall eliminando le modifiche alla rete ed evitando gli hair-pinning del traffico.
- **Nessun punto cieco:** copertura completa per la sicurezza della rete su tutti i flussi con l'unico firewall L7 distribuito via software nell'hypervisor in un'architettura distribuita a ogni workload. Visibilità e contesto del workload per identificare e bloccare le minacce rimanendo isolati dalla superficie di attacco.
- **Sicurezza come codice:** offri "sicurezza come codice" con un modello basato su oggetti basato su API che fornisce consigli sulle policy, automatizza la mobilità delle policy e garantisce che i nuovi workload ricevano automaticamente le policy di sicurezza appropriate.
- **Orchestrazione dinamica delle policy:** ottieni una sicurezza agile tramite policy firewall coerenti su più livelli ambienti. Assicurati che i workload mantengano le loro policy di sicurezza durante tutto il loro ciclo di vita, indipendentemente da dove il workload si trova o si sposta. Scrivi la tua polizza una volta e applicala automaticamente ovunque.

8.4. Workspace One Access

VMware Workspace ONE Access è il portale aziendale dove mettere a disposizione all'utente finale tutte le risorse aziendali da qualsiasi dispositivo, siano esse applicazioni virtualizzate, SaaS, siti web intranet o VDI. Funge anche da Identity Manager offrendo autenticazione a più fattori (MFA), accesso condizionato e Single Sign-On (SSO) per le applicazioni fornite da VMware Workspace ONE. Agendo come broker per altri identity provider, Workspace ONE Access consente di implementare in modo rapido e sicuro strategie di applicazioni e dispositivi che offrono un accesso uniforme a livello aziendale ad applicazioni e dati da qualsiasi dispositivo in qualsiasi luogo.

8.5. Funzionalità e Benefici principali

Di seguito le principali funzionalità e benefici:

- **Broker di accesso:** si integra con i provider di identità cloud e locali esistenti per ridurre i tempi di implementazione e consentire un accesso più sicuro a qualsiasi applicazione, migliorando al contempo l'esperienza utente

- **MFA e SSO integrate:** fornisce Multi-Factor Authentication (MFA) nativa o si integra con provider MFA esistenti e fornisce Single Sign-On (SSO) a Web, SaaS, app mobili e legacy attraverso l'integrazione con Workspace ONE Intelligent Hub
- **Accesso condizionato:** utilizza dozzine di combinazioni di criteri di accesso che sfruttano la registrazione dei dispositivi, la rete, l'SSO, la riparazione automatizzata dei dispositivi e le informazioni di terze parti per stabilire livelli di affidabilità, consentendo decisioni di accesso intelligenti
- **Portale SaaS:** riduce drasticamente i tempi di implementazione e i costi di manutenzione; permette di sbloccare nuove funzionalità come i Workspace ONE Hub e la gestione degli aggiornamenti e del ciclo-vita sono inclusi.