Cloud & Business

n.81
Maggio 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

COVER STORY

CLOUD FIRST, NOT CLOUD ONLY È LA CHIAVE PER LA TRASFORMAZIONE DIGITALE

di Giuseppe Saccardi

La piattaforma cloud di VEM Sistemi raccoglie i parametri di produzione, calcola efficienza, OEE di produzione del singolo lotto e si propone come strumento estremamente flessibile e completo di supporto alle decisioni del manifatturiero

Marco Bubani -Direttore innovazione di VEM sistemi

Reportec Cloud&Business - Numero 81 - Maggio 2019 - Registrazione al tribunale n°574 del 5 Novembre 2010 -
Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (**www.reportec.it**) - Direttore responsabile: Giuseppe Saccardi
In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

Cloud e Innovazione hanno molto in comune. Nella nuvola il ritmo con cui vengono ideati, sviluppati e rilasciati nuovi servizi è mozzafiato. Il tasso di innovazione interno alle principali organizzazioni che forniscono servizi di cloud pubblico è elevatissimo e questa onda di innovazione ne genera un'altra: quella di tutte le organizzazioni che, attraverso le tecnologie digitali, stanno cercando nuove strade per aumentare la loro competitività, cambiare il loro modello di business oppure individuare orizzonti completamente nuovi.

Queste aziende sempre di più trovano nel cloud la loro "cassetta degli attrezzi dell'innovazione". Semilavorati innovativi che abilitano nuovi servizi altrettanto innovativi. Innovazione che abilita innovazione.

È sfruttando queste leve che il gruppo VEM all'inizio del 2017 ha cominciato un percorso di Open Innovation che l'ha portata ad affrontare progetti digitali in una modalità del tutto nuova rispetto al passato.

VEM Sistemi è una società fondata a Forlì nel 1986 che si è sempre occupata di progettare e realizzare infrastrutture ICT come reti di comunicazione, data center, sistemi di sicurezza informatica.

Puntando su qualità e avanzati servizi di gestione delle soluzioni realizzate, VEM ha consolidato la sua posizione di mercato diventando un gruppo che oggi genera circa 50M di euro di fatturato, 250 dipendenti e sei sedi operative dislocate in tutto il centro e nord Italia.

La caratteristica di operare su infrastrutture come la rete o i sistemi computazionali, non aveva portato VEM a realizzare soluzioni ICT direttamente connesse al processo di business dei propri clienti fino al 2017, quando il

neonato team di innovazione ha cominciato un percorso nuovo. Sposando i concetti della Open Innovation sono stati avviati una serie di progetti di esplorazione mettendo al centro il cliente, le sue esigenze ed il suo processo di business per comprendere come le tecnologie digitali potessero effettivamente aprire nuove opportunità,

Vediamo due esempi concreti che ha illustrato **Marco Bubani,** Direttore innovazione di VEM sistemi.

Il cloud per la filiera alimentare

Un primo progetto è stato realizzato nella filiera alimentare, in particolare con un produttore di carni avicole e ci si è concentrati sull'area zoo-mangimistica, oggi scarsamente digitalizzata.

Dopo una serie di workshop condotti con tutti gli stakeholder del processo di allevamento sono stati individuati una serie di parametri fondamentali da monitorare per il benessere animale, che oggi vengono gestiti in maniera empirica dal singolo allevatore. L'obiettivo che ci si è posti è stato quello di raccogliere questi parametri in modo strutturato per po-

terli storicizzare, confrontare, ed analizzare in modo molto più profondo al fine di migliorare il processo di allevamento. Fornire quindi a tutti gli attori che orbitano attorno al processo di allevamento uno strumento molto più flessibile e completo che li supporti e li agevoli nelle decisioni.

Il cloud è stato il veicolo per riuscire a realizzare una piattaforma IIoT in tempi brevi che potesse rispondere alle esigenze emerse dai workshop. Il team di VEM sfruttando tool e servizi resi disponibile dal public cloud ha creato una piattaforma composta sostanzialmente da due macro componenti: un modulo edge software di raccolta e prima elaborazione dati dal campo (da sensori e automazioni presenti o aggiunte in allevamento) e una componente cloud che riceve in modo sicuro dalla componente edge i dati raccolti e li archivia in modo nativo. La piattaforma consente quindi l'applicazione di algoritmi per l'individuazione di situazioni anomale o migliorative per il processo e la generazione di allarmi singoli o correlati fra più grandezze. Il tutto è restituito agli stakeholder mediante dashboard web e app utilizzabili da smartphone.

È stato possibile realizzare questa piattaforma in tempi rapidi e con costi relativamente contenuti grazie al cloud. E sempre grazie al cloud, se il progetto si amplierà, sarà possibile scalare senza nessuna frizione e sarà possibile attingere a funzionalità di gestione ed elaborazione dati più avanzati come algoritmi di machine learning o computer vision in modo estremamente rapido ed efficace.

Il cloud per il packaging

Mutuando l'esperienza fatta con gli allevamenti e replicando la logica edge-cloud, in un distretto industriale completamente diverso, abbiamo realizzato una piattaforma di raccolta dati delle macchine automatiche per un Machine Builder del settore packaging. Con questa piattaforma cloud il gruppo VEM attraverso la consociata MyDev, è in grado di raccogliere tutti i parametri di produzione generati dalla macchina, associarli al lotto di produzione e alla ricetta di macchina, e calcolare parametri di efficienza l'OEE di produzione del singolo lotto, la velocità e la qualità di produzione, le cause di fermo e molto altro, agevolando così la compatibilità della macchina al piano impresa 4.0.

Questi, ha osservato Bubani, sono solo due esempi di come il cloud sia ormai elemento fondamentale per supportare ed accelerare la trasformazione digitale. Cloud First, not Cloud Only.

Chi è VEM sistemi

Da 33 anni VEM sistemi è uno degli ICT player italiani più innovativi e attento a intercettare le nuove tendenze del settore, rendendole funzionali alle esigenze dei clienti. Dalle sei sedi dislocate nei poli manifatturieri dove il "made in Italy" ha le sue radici – Forlì, Milano, Modena, Padova, Roma e Senigallia - offre servizi di integrazione delle tecnologie di networking basate su IP, con una visione olistica che va dalla cybersecurity, alla mobility, dalla collaboration, al data cen-ter, fino all'automazione dell'edificio e al custom application development del software, per consentire ai propri clienti di cogliere il meglio dalla tecnologia in completa sicurezza. http://vem.com/

LA PROTEZIONE DELL'ASSET AZIENDALE INIZIA DAGLI UTENTI PRIVILEGIATI

Le soluzioni di CyberArk per la sicurezza degli accessi privilegiati garantiscono l'individuazione e la protezione continua dai rischi nel cloud

CyberArk, società leader a livello mondiale nello sviluppo di soluzioni per la sicurezza degli accessi privilegiati degli utenti umani e non-umani, ha annunciato l'espansione delle sue soluzioni con nuove funzionalità volte a semplificare l'individuazione dei rischi e ad assicurare in ambienti cloud la protezione continua degli accessi privilegiati.

In particolare, l'ultima release - la v10.8 - della soluzione "Privileged Access Security" di CyberArk, evidenzia l'azienda, è la prima nel suo genere per quanto concerne l'automazione del processo di individuazione di rischi, di alert e di risposta ai rischi per account Amazon Web Services (AWS) non gestiti e potenzialmente a rischio. La versione dispone in particolare di nuove funzionalità Just-in-Time che sono volte a garantire un accesso flessibile per l'utente ai sistemi Windows, sia che questi siano basati su cloud che di tipo on-premise.

In pratica, con la nuova release di Privileged Access Security Solution, l'azienda si è proposta di definire un vero e proprio nuovo standard e di abilitare un approccio ampiamente esaustivo e al top del settore per quanto concerne la sicurezza e l'efficienza operativa che deve essere garantita nel cloud.

- L'obiettivo postosi da CyberArk è stato perseguito tramite funzionalità che permettono la:
- Identificazione continua degli account privilegiati: identifica gli account privilegiati in AWS, come gli utenti IAM (Identity and Access Management) non gestiti, e le istanze e gli account EC2. Le organizzazioni possono, in pratica, tracciare le credenziali di AWS ovunque siano create e indipendentemente da come sono create, e accelerare il processo di on-boarding degli account non gestiti.
- Rilevazione e risposta automatica agli exploit: permette di inviare avvisi prioritari inerenti comportamenti potenzialmente rischiosi, quali ad esempio attività che bypassano il vaulting, il furto della chiave di accesso o una inadeguata gestione. La soluzione di CyberArk è anche in grado di assumere

il controllo su questi account e attivare una nuova chiave di accesso o una sua rotazione automatica per mitigare il rischio.

- Installazione semplificata in ambienti AWS: estende le funzionalità già esistenti per la protezione dell'infrastruttura cloud. Diventa possibile ad esempio semplificare l'implementazione di CyberArk Privileged Access Security Solution in AWS con AMI per tutti i componenti principali, inclusi il vaulting, la gestione delle sessioni e l'analisi delle minacce.
- Accesso just-in-time con opzioni di provisioning flessibili: permette all'amministratore di configurare la durata concessa per l'accesso ai sistemi Windows, sia che si tratti di cloud o di apparati on-premise. L'obiettivo è di consentire alle organizzazioni di ridurre in modo significativo la problematica operativa per gli end-user e mitigare il rischio costituito da un accesso privilegiato senza restrizioni.

La nuova versione estende, ha spiegato CyberArk, la propria leadership tecnologica con una gamma molto ampia di opzioni utili nell'implementare e nel rafforzare i controlli sugli accessi privilegiati, dagli account protetti tramite accesso Just-in-Time a quelli completamente gestiti tramite audit, sia on-premise che nel cloud.

Le soluzioni CyberArk posizionate al top dagli analisti

La conferma più diretta che le soluzioni di CyberArk rispondono a reali e sempre più diffuse esigenze aziendali viene dalle società di ricerca e analisi di mercato presso gli utenti finali.

La società è stata di recente nominata leader assoluto per la gestione degli accessi privilegiati per il quarto anno consecutivo da parte di KuppingerCole Analysts nel suo rapporto per il 2019 "Leadership Compass: Privileged Access Management".

Il rapporto della società di analisi indipendente fornisce un'analisi dettagliata del mercato relativa alla gestione degli accessi privilegiati e si propone di essere di ausilio per i responsabili della sicurezza e dell'Identity& Access Management (IAM) nell'identificare le soluzioni che hanno il maggiore impatto positivo sui loro programmi di sicurezza informatica. CyberArk risulta essere il fornitore preferito per le organizzazioni globali che cercano una soluzione di gestione degli accessi privilegiati e leader del mercato per requisiti complessi.

Delle 20 società valutate nel report, solo CyberArk, ha notato la società, è stata riconosciuta come leader in tutti i segmenti a motivo del suo "focus sulla costante innovazione" ed è stata identificata come "il più importante fornitore" sul mercato.

In particolare, tra le venti società analizzate, la soluzione per la sicurezza degli accessi privilegiati di CyberArk ha ricevuto il punteggio più alto possibile in tutte le categorie di valutazione del prodotto ed è stata riconosciuta per la qualità della sua progettazione per quanto concerne l'intuitività e la robustezza dell'interfaccia utente; l'efficacia del supporto DevOps e l'ampio supporto per quanto concerne applicazioni e infrastrutture cloud.

CyberArk è stata posizionata tra i leader nel Privileged Identity Management anche in una ricerca indipendente realizzata dalla società di analisi Forrester Research nel suo "The Forrester Wave: Privileged Identity Management, Q4 2018" – un report che ha analizzato gli 11 fornitori più quotati del settore, tra i quali, ha evidenziato la società, CyberArk è stata riconosciuta leader.

Il report è di di alto valore per le organizzazioni globali che necessitano di una guida che le aiuti nel decidere cosa acquistare e le supporti nel definire la loro strategia per quanto concerne gli account privilegiati on premise o nel cloud.

L'importanza della scelta della corretta strategia e di relativi prodotti è strettamente dipendente

dal fatto che a seguito dei crescenti investimenti effettuati nella migrazione al cloud, nel DevOps e nell'Internet of Things (IoT), nonché in altre aree emergenti a livello industriale come la automazione basata su processi robotici, la superficie di attacco si sta espandendo esponenzialmente.
In questo complesso e variegato processo di digitalizzazione, la gestione oculata e sicura delle identità privilegiate, mette in guardia CyberArk, diventa cruciale al fine di rafforzare la postura aziendale e organizzativa per quanto concerne la sicurezza e migliorare la gestione del rischio.
Secondo il report, CyberArk dispone di una gestione delle password sicura, di gestione delle sessioni, di analitiche privilegiate dei rischi, nonché del più ampio supporto DevOps di qualsiasi altro dei produttori valutati da Forrester Wave.
In particolare, osserva l'azienda, CyberArk si posiziona al top nelle categorie quali il portfolio di soluzioni e la presenza sul mercato ed ha ottenuto il massimo punteggio possibile, tra altre voci, per quanto concerne la customer satisfaction, il cloud, il supporto DevOps e dei Container.

BASTA CENTRALINI CON IL CLOUD PBX DI NFON

Aperta la filiale italiana del gruppo paneuropeo. Modello economico semplice: "un servizio una tariffa" e una user experience lineare su qualsiasi dispositivo

Marco Pasculli - Managing Director di Nfon

NFON è sbarcato in Italia con l'obiettivo di portare un approccio dirompente nel mercato della telefonia in cloud, superando il concetto di centralino o PBX e proponendo un modello economico lineare: una singola tariffa per utente (8,80 euro mese) con un numero unico sempre disponibile su fino a nove dispositivi, fissi o mobili.
Altra semplificazione economica riguarda il risparmio che l'azienda stima essere pari al 50% del costo di possesso, nessuna tariffa aggiuntiva per le chiamate in tutta Europa e stesse condizioni per qualsiasi filiale in tutto il Vecchio Continente. Quella italiana, peraltro, è la quattordicesima filiale inaugurata in Europa dal gruppo tedesco, che intende ampliare la presenza internazionale.
A dar peso alle aspettative di NFON sono soprattutto i risultati sin qui dimostrati, con una crescita costante a partire dalla nascita della società a Monaco di Baviera nel 2007, per arrivare

oggi a oltre 30mila aziende clienti.
Responsabile della filiale italiana: è Marco Pasculli, volto noto nel settore della telefonia in Italia, visti i suoi trascorsi presso Nortel Networks, Avaya, Huawei Enterprise Division e Alcatel-Lucent Enterprise.
«Vogliamo la libertà della comunicazione cioè: una sola tariffa, lo stesso piano per tutte le imprese europee, tutti i servizi inclusi e la possibilità di scindere il contratto ogni mese», ha sottolineato Pasculli.
Il cloud abilita questo modello, grazie a due data center in Europa, geo-ridondanti e conformi alle normative internazionali, GDPR incluso, ovviamente,
Più in dettaglio, il modello di Nfon prevede l'assegnazione di un numero d'interno a ciascun utente, ma non c'è la connessione fisica al centralino, poiché il Cloud PABX virtualizza il collegamento. Il numero è una sorta di identificativo, al quale possono essere abbinati fino a 9 nove dispositivi, attivabili dall'utente. Per esempio è possibile indirizzare le chiamate che arrivano al fisso sulla scrivania in ufficio verso il cellulare in modo che se si è in vacanza nessuno potrà accorgersi che non si stia rispondendo dall'ufficio,
A questo modello si aggiunge la strategia di Nfon che «non si limita alla vendita di telefonia a una qualsiasi azienda italiana, ma sviluppa soluzioni che, svolgono un ruolo essenziale nella modernizzazione delle esigenze di comunicazione all'interno di interi comparti industriali», aggiunge Pasculli.
Nhospitality e Ncontactcenter e Neorecording sono alcune delle prime soluzioni offerte da Nfon al 100% attraverso il canale indiretto.
Più in dettaglio, Nhospitality è pensata per soddisfare le esigenze di comunicazione delle strutture alberghiere, circa 33mila hotel e 22mila agriturismo in Italia.
Ncontactcenter permette alle tante imprese che raggiungono la clientela attraverso il telefono di configurare le risorse in maniera dinamica, fronteggiando la scalabilità con un semplice clic per aumentare o diminuire le linee attive.
Neorecording soddisfa le esigenze delle aziende che chiudono le vendite al telefono attraverso la registrazione vocale del contratto. Il servizio è conforme alle stringenti normative sia tecniche sia legali, per la registrazione, fornendo capacità di indicizzazione e archiviazione permanente in storage protetti.
Le potenzialità per Nfon appaiono elevate. Secondo la società di ricerca MZA i numeri di telefono in cloud erano 13 milioni nel 2017 e raddoppieranno entro il 2022. Inoltre, Marcus Krammer, vice president New Product, Merge & Acquisitions di Nfon, sottolinea che in Europa ci sono 439 milioni di abitanti, 135 milioni di telefoni fissi, 143 milioni di dipendenti nelle piccole e medie imprese e altri 67 milioni nelle medio grandi e grandi aziende. Numeri che colpiscono e che si abbinano a un momento di trasformazione del mercato che va in direzione del cloud, mentre il tasso di adozione del centralino in cloud in Italia è ancora molto basso.

NUTANIX AMPLIA LA PROPRIA OFFERTA DI SOLUZIONI MULTI-CLOUD

Nuove funzioni del portfolio Nutanix semplificano l'accesso ai desktop virtuali tramite cloud, migliorano il disaster recovery e proteggono applicazioni e desktop

Nutanix, ha ampliato la propria offerta in ambito cloud pubblico e privato estendendo la soluzione desktop-as-a-service Xi Frame dal cloud pubblico al cloud privato, evoluzione che consente la distribuzione di applicazioni e desktop in un ambiente cloud ibrido.

Ha rilasciato anche nuove funzionalità e ulteriori aree geografiche di disponibilità per Xi Leap, il suo servizio di disaster recovery (DR) basato su cloud.

In pratica,tramite Xi Frame possono accedere alle applicazioni e ai desktop virtuali direttamente tramite i più diffusi cloud pubblici, come AWS e Azure, utilizzando qualsiasi browser e dispositivo.

L'aggiornamento di Xi Frame in esecuzione sul proprio hypervisor AHV, ha approfondito l'azienda, permette ai clienti di estendere la distribuzione dei desktop al loro cloud privato Nutanix, integrando i servizi VDI (Virtual Desktop Infrastructure) nella piattaforma Nutanix Enterprise Cloud.

I desktop Xi Frame possono anche essere distribuiti simultaneamente tramite più cloud e gestiti da una singola consolle.

Oltre ad essere disponibile per gli utenti AWS e Azure, Xi Frame è disponibile a livello mondiale per i clienti con distribuzioni di cloud privato Nutanix che utilizzano la soluzione AHV.

Disaster recovery in cloud con Xi Leap

Se implementato correttamente, il disaster recovery basato su cloud è un approccio adatto e proficuo per aziende di qualsiasi dimensione che vogliono proteggere le loro applicazioni business-critical. Il problema è però far coesistere l'ambiente aziendale con quello in cloud.

Questo è quello che Nutanix si è proposta di fare con Xi Leap, che permette di estendere il data center aziendale al cloud, e ai team IT di armonizzare i cloud pubblici e privati in modo da garantire una maggiore disponibilità di applicazioni e dati critici. Il servizio include nuove funzionalità quali:

- Nuove cloud Region: Nutanix Xi Leap, attualmente erogato da centri negli Stati Uniti Occidentali e Orientali e in Inghilterra, sarà a breve reso disponibile in Italia tramite la partnership tra Nutanix e Sparkle, l'operatore del Gruppo Telecom Italia, oltre che in Germania e Giappone.
- Supporto per ESXi: da oggi, Xi Leap fornisce servizi di disaster recovery per i carichi di lavoro aziendali su cloud privati Nutanix, tramite VMware ESXi, semplificando ulteriormente la trasformazione delle applicazioni esistenti in un servizio ibrido.

«Con i sistemi di disaster recovery precedenti, non siamo riusciti a raggiungere le prestazioni desiderate per il ripristino delle macchine virtuali; inoltre, la gestione del disaster recovery come silo separato ha reso la nostra infrastruttura più comples-

sa - ha dichiarato **Patrick Sudderth**, Director of Technical Services di Lexipol -. Nutanix Xi Leap ci permette di configurare policy che automatizzano il workflow DR direttamente all'interno della console Prism ed effettuare il ripristino in pochi minuti».

Applicazione protette con Xi-Beam

Un altro aspetto critico nel cloud è la sicurezza. Nella distribuzione delle applicazioni in un'architettura multi-cloud è fondamentale garantirne la sicurezza, indipendentemente dall'infrastruttura cloud adottata. Sono ad esempio necessarie valutazioni di conformità atte a garantire la mobilità delle applicazioni tra i cloud.
Per assicurarla, Xi Beam, l'offerta SaaS di Nutanix per la governance del cloud, includerà un modulo di conformità alla sicurezza in tempo reale che ha progettato per identificare le vulnerabilità critiche dell'infrastruttura cloud e suggerire azioni di remediation specifiche.
«Il multi-cloud è la nuova realtà per l'IT e non è più oggetto di dibattito. I clienti hanno bisogno di soluzioni in grado di riunire l'intero mix piattaforme cloud pubbliche, private ed edge che presto costituiranno la loro infrastruttura critica senza farli naufragare in inutili complessità e costi incontrollati. Grazie alla continua integrazione di nuove funzionalità nel nostro portfolio, i clienti sono liberi di distribuire applicazioni e dati dal cloud più adatto al loro business», ha commentato **Sunil Potti**, Chief Product and Development Officer, Nutanix.

SAP GUIDA I CLIENTI VERSO IL CLOUD COL PROGETTO EMBRACE

I benefici previsti includono trattative commerciali più brevi, team semplificati e implementazioni più rapide e sicure

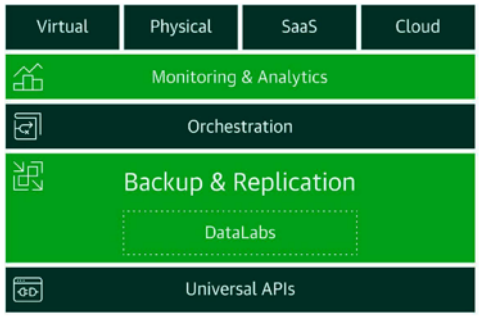
SAP ha dato il via al progetto "Embrace", un programma di collaborazione con Microsoft Azure, Amazon Web Services (AWS) e Google Cloud oltre ai partner per i servizi strategici globali (GSSP).
"Embrace" si propone di aiutare il passaggio a SAP S/4HANA in cloud nel linguaggio e contesto del settore di riferimento dei clienti, evidenziando i benefici della piattaforma, del software, dei servizi e dell'infrastruttura di SAP, insieme ai principali hyperscaler e partner di servizio.
Il passaggio a SAP S/4HANA in cloud è definito da practice consolidate dal mercato, architetture di riferimento e modi di accesso ai servizi tecnologici di base necessari alle aziende per ottenere migliori risultati di business. La collaborazione con hyperscaler e GSSP punta nella sua essenza a fornire alle aziende un unico progetto atto a supportare la transizione e il percorso verso un'impresa intelligente.
«I nostri clienti sono molto chiari rispetto ai risultati di business che si aspettano di ottenere migrando al cloud, e questo include eccellenza operativa e innovazione - ha affermato **Jennifer Morgan**, president of Cloud Business Group and executive board member di SAP -. Lavorando insieme agli hyperscaler e ai partner per i servizi strategici globali, siamo in una posizione privilegiata per definire con i nostri

clienti i percorsi migliori per diventare imprese intelligenti».
I benefici previsti includono trattative commerciali più brevi, team semplificati e implementazioni più rapide e sicure. In particolare, ha osservato l'azienda, "Embrace" punta a includere i seguenti elementi:

- Soluzioni: un set di servizi di base disponibili su SAP Cloud Platform per abilitare l'integrazione, l'orchestrazione e l'estensione di sistemi SAP e applicazioni di terzi per ambienti cloud o on-premise.
- Architettura di riferimento: un progetto tecnico sviluppato congiuntamente che incorpora i componenti SAP e hyperscaler necessari per eseguire le applicazioni del cliente.
- Practice consolidate dal mercato: una road map creata congiuntamente e validata dal mercato per SAP S/4HANA per i diversi settori, realizzata con hyperscaler e partner di servizi strategici globali.
- Nuovi servizi SAP MaxAttention e servizi SAP ActiveAttention: un set di servizi appena lanciato per supportare i clienti che utilizzano un'infrastruttura cloud o ibrida di un hyperscaler.

IL CLOUD DATA MANAGEMENT DI VEEAM SUPPORTA TXT NELL'INNOVAZIONE

In una critica fase di ristrutturazione dell'intera architettura IT, TXT e-solutions ha scelto di affidarsi a Veeam per il backup del suo ambiente VMWare



TXT e-solutions è un'azienda che opera in mercati che richiedono una elevata specializzazione e pari capacità di innovazione. Dispone di due data center on-premises e un'infrastruttura cloud e di circa cento macchine virtuali dedicate a sviluppo e test di applicazioni dei clienti.
Cessioni di rami di azienda e acquisizioni hanno però lasciato in eredità un ambiente IT estremamente eterogeneo, un ambiente che oltretutto richiedeva di essere messo in sicurezza e reso conforme alle nuove normative GDPR in tempi molto rapidi.

Pr mettersi al passo TXT e-solutions ha dato vita ad una serie di investimenti in tecnologie che portassero a una semplificazione delle architetture e alla compliance e nell'arco di dieci mesi, partendo da un ambiente complesso ed eterogeneo, è passata a un'architettura totalmente virtualizzata e basata su cloud, un'infrastruttura affidabile che. osserva, le ha consentito, tra le altre cose, di ottenere la certificazione ISO 9100.
Nella critica fase di ristrutturazione dell'intera architettura IT, TXT e-solutions ha scelto di affidarsi a Veeam per il backup del suo ambiente VMWare.

Dopo una prima fase di test per verificare l'adattabilità delle soluzioni all'architettura appena rivoluzionata, il team IT di TXT e-solutions ha implementato la soluzione Veeam in dieci giorni dalla sua squadra interna, con un aiuto per il fine tuning da parte del personale Veeam.
In sostanza, TXT e-solutions ha messo in sicurezza i dati contenuti nei due data center on-premise (presso le sedi di Milano e Berlino), nella replica dei sistemi in cloud e anche nei personal computer di tutta la prima linea di manager.
Inoltre, ha spiegato TXT, se con la vecchia architettura e con la soluzione di backup proprietaria riusciva ad eseguire il backup di circa il 50% dei sistemi, con Veeam arriva al 100%, una mole di dati di circa 70 TB se si considerano i due data center.
Veeam Backup & Replication è poi integrata nell'ambiente ibrido on-premises/cloud che sta creando, cosa che le permetterà di crescere anche nell'infrastruttura multicloud quando a Microsoft Azure affiancherà AWS o altri fornitori.
Nel prossimo futuro, TXT e-solutions vede l'adozione delle soluzioni di backup anche per gli strumenti Sharepoint e Onedrive in ambiente Microsoft 365 e Microsoft Exchange.

CRESCE L'ADOZIONE DI SOLUZIONI PAAS NELLE AZIENDE

La società di ricerca Gartner evidenzia quali sono i trend in corso nel 2019 nell'ambito della Platform as a Service e Platform Architecture

Per fornire una guida nel mercato in forte crescita dei servizi Paas (Platform as a Service), Gartner ha evidenziato in una sua ricerca (The Key Trends in PaaS and Platform Architecture, 2019) quali sono le tendenze chiave che dovrebbero essere prese in considerazione quando si prendono decisioni che riguardano la tecnologia, il budget da spendere e l'organizzazione.
«Le tendenze che vediamo in ambito PaaS riflettono e guidano la tendenza nella trasformazione del cloud computing e del business digitale» ha dichiarato **Yefim Natis**, vice presidente della ricerca di Gartner, che ha sottolineato anche che: «Man mano che le organizzazioni adottano le piattaforme cloud si trovano di fronte a una varietà di cambiamenti».
Innanzitutto il primo trend che la società di analisi mette in evidenza è che a partire dal 2019, il mercato PaaS totale è rappresentato da più di 360 fornitori e offre oltre 550 servizi di piattaforma cloud suddivisi in 21 categorie.
Gartner si aspetta che dal 2018 al 2022 il mercato raddoppierà le sue dimensioni e che il modello di distribuzione PaaS sarà quello prevalente in futuro. «Tutti i segmenti PaaS mostrano buoni tassi di crescita. Tuttavia, il mercato rimane a corto di standardizzazione, pratiche consolidate e leadership sostenute. I venditori devono affrontare queste problematiche in modo tempestivo per incoraggiare l'adozione da parte delle organizzazioni più avverse al rischio» ha commentato Natis.
Un altro trend evidenziato da Gartner è il fatto che oltre alle funzionalità dei servizi Paas a supporto della cloud platform, anche gli altri servizi

cloud tra cui l'infrastructure as a service (IaaS) e il software as a service (SaaS) possono essere fattori chiave per una piattaforma. In pratica quello che Gartner sottolinea è che insieme, questi servizi, costituiscono il continuum della piattaforma cloud stessa. Riconoscere le opportunità di innovazione platform-based attraverso l'intero spettro di servizi cloud sarà presto parte di ogni strategia cloud.

Il terzo trend messo in risalto da Gartner riguarda il design native-cloud. A seguito della diffusione della tecnologia cloud stanno nascendo nuove architetture tecnologiche progettate per riflettere in modo nativo gli elementi essenziali dell'esperienza cloud: agilità, innovazione continua, delivery veloce. Esempi recenti di tecnologie cloud-native includono piattaforme serverless, macchine microvirtuali e offerte low-code.

«Il cloud computing si sta evolvendo per diventare solo computing, e il design cloud-native nei nuovi investimenti sta diventando pervasivo nelle organizzazioni, nei casi d'uso e nei modelli di implementazione» ha aggiunto Natis.

Infine, evidenzia Gartner, l'IT aziendale diventa un

fornitore di servizi per l'organizzazione aziendale. «Quello che vediamo è che l'IT fornisce all'organizzazione aziendale servizi di abilitazione come piattaforme, formazione, consulenza e supporto. Sono anche responsabili della governance generale - ha affermato Natis -. Questo sviluppo è guidato dall'impatto combinato di innovazioni come gli strumenti low-code, sviluppo basato sul machine learning e modelli di consumo self-service, che portano a una ridefinizione del ruolo dell'IT centrale, lontano dall'ottica di delivery della "fabbrica", ma più vicino a un approccio di fornitore di servizi».

IL NOVE PER CENTO DELLE VIOLAZIONI DI DATI AVVIENE NEL CLOUD. ECCO COSA FARE

Uno studio di Kaspersky Lab evidenzia come il 90% dei data breach avvenga nel cloud pubblico e sia causato dagli utilizzatori

Secondo il recente report di Kaspersky Lab – "Understanding security of the cloud: from adoption benefits to threats and concerns" - all'interno delle infrastrutture del cloud pubblico sono molto più probabili gli incidenti causati dai dipendenti dei vari clienti, piuttosto che quelli legati ad azioni dei cloud provider stessi.

Questo perché le aziende pensano che siano i provider ad essere responsabili dell'integrità dei dati archiviati all'interno delle piattaforme.

Al di là di questo più o meno opinabile punto di vista, circa il 90% delle violazioni di dati

aziendali nel cloud (l'88% per le PMI e il 91% per le grandi aziende) avviene grazie a tecniche di social engineering che prendono di mira i dipendenti dei clienti dei servizi stessi, non per problemi causati dai cloud provider.

L'adozione del cloud permette alle organizzazioni di beneficiare di processi aziendali più agili, di ridurre le spese normalmente impiegate per l'acquisto di asset durevoli e di poter contare su una fornitura IT più veloce, osserva l'azienda, ma nonostante questi appurati benefici le stesse organizzazioni si preoccupano della stabilità dell'infrastruttura cloud e della sicurezza dei propri dati.

Oltre un terzo delle PMI e delle realtà enterprise (35%) tra quelle coinvolte nello studio ha dichiarato di essere preoccupato in merito a possibili incidenti che possono colpire le infrastrutture ospitate da terze parti.

Ilo motivo è che ritengono che le conseguenze di un incidente di sicurezza IT potrebbero vanificare tutti i benefici ottenuti dall'adozione del cloud e portare, invece, a potenziali rischi dal punto di vista commerciale e reputazionale.

Attenti al vicino

Un aspetto evidenziato è che anche se le organizzazioni si preoccupano soprattutto per l'integrità delle piattaforme cloud esterne, è più probabile che vengano colpite da vulnerabilità che possono trovarsi vicino a loro.

Un terzo degli incidenti (33%) all'interno del cloud è causato da tecniche di social engineering che cercano di sfruttare il comportamento dei dipendenti, mentre solo l'11% può essere imputato ad azioni dei cloud provider.

L'indagine mostra che si può fare di più per garantire l'adozione di misure di cybersicurezza adeguate quando si ha a che fare con terze parti. Solo il 39% delle PMI e la metà (47%) delle realtà enterprise ha infatti adottato soluzioni di protezione su misura per il cloud.

Vari i fattori che hanno portato a tali percentuali. Ad esempio, alcune aziende scelgono di affidarsi direttamente al proprio cloud provider per quanto riguarda la sicurezza IT, altre che la protezione standard per gli endpoint possa funzionare senza problemi all'interno dell'ecosistema cloud.

«Nel momento della migrazione ad un cloud pubblico il primo passo per qualunque azienda è capire chi sia davvero responsabile dei dati aziendali e dei carichi di lavoro che li riguardano. I provider di servizi cloud dispongono normalmente di misure di cybersecurity dedicate per proteggere piattaforme e clienti, ma quando la minaccia riguarda il cliente in modo diretto, non è più una responsabilità del fornitore. La nostra ricerca dimostra che le aziende dovrebbero prestare più attenzione alla "cybersecurity hygiene" dei propri dipendenti e adottare misure che proteggano l'ambiente cloud a partire dall'interno», ha commentato **Maxim Frolov**, Vice President of Global Sales presso Kaspersky Lab.

I suggerimenti dei Lab

Che fare per contenere i rischi? Kaspersky Lab consiglia alle aziende l'adozione di misure di protezione specifiche per assicurarsi che i dati siano al sicuro all'interno del cloud:

- Spiegare ai dipendenti che anche loro possono diventare vittime di minacce informatiche. I dipendenti non devono cliccare su link o aprire allegati che arrivano da utenti sconosciuti.

- Per ridurre al minimo il rischio di un uso non approvato delle piattaforme cloud, è importante formare lo staff sui possibili effetti negativi del "Shadow IT" e definire, per ogni dipartimento, le corrette procedure di acquisto e uso dei servizi delle infrastrutture cloud.
- Utilizzare una soluzione di sicurezza per gli endpoint che blocchi eventuali vettori d'attacco basati sul social engineering. La soluzione dovrebbe comprendere la protezione per i server di posta elettronica, i client di posta e i browser.
- Dopo la migrazione, implementare il prima possibile una protezione per l'infrastruttura cloud tramite una soluzione di cybersicurezza fatta appositamente per l'ecosistema cloud, con una console di gestione unificata per gestire la sicurezza su tutte le piattaforme, supportare il rilevamento automatico degli host in-the-cloud, oltre alla scalabilità del roll out per ciascuna di esse.

Se non proprio eliminabili del tutto a questo punto i rischi sarebbero perlomeno fortemente contenuti, viene da concludere.

LA NUOVA FRONTIERA DELLA SICUREZZA LA SI TROVA NEI SERVIZI GESTITI

Uomo e macchina assieme in servizi gestiti garantiscono la sicurezza informatica. Lo spiega F-Secure, che con un report fa il punto anche sui rischi dell'IoT

Antonio Pusceddu - Country Sales Manager per l'Italia di F-Secure

La diffusione della digitalizzazione e delle smart technology stanno cambiando profondamente la natura stessa delle aziende, indipendentemente dal settore di appartenenza. E' una trasformazione in chiave digitale che ha mutato ogni azienda in una software company, e questo vale ancora di più per le aziende che vendono online.

In quanto tali dovrebbero preoccuparsi di proteggere al meglio i propri asset e le risorse digitali accedute da locale, remoto, via dispositivi mobili o nel cloud.

La realtà di cui va preso atto è che il panorama delle minacce a cui un ambiente IT o produttivo è sottoposto è profondamente mutato. Attacchi avanzati, spear phishing e violazioni di dati sono all'ordine del giorno, e non più l'eccezione. Serve quindi affrontare queste minacce con nuove tecnologie e crescenti investimenti in risorse di talento. Ma non sempre i budget lo consentono, osserva F-Secure, che da tre decenni è pio-

niera nello sviluppo di soluzioni di cyber security e le cui soluzioni difendono decine di migliaia di aziende e milioni di persone tramite tecnologie che combinano il machine learning con l'esperienza umana degli esperti dei suoi laboratori.
Il problema non è però solo di budget ma anche di competenze atte a contrastare le minacce. Le previsioni parlano di 3.5 milioni di posizioni nella sicurezza informatica che resteranno vacanti entro il 2021. Nel frattempo, oltre il 67% delle Enterprise globali ha subito una violazione di dati (Fonte: 2018 Thales Data Threat Report).
Cosa ancor più allarmante, è che molti di questi attacchi si basano su tattiche di attacco avanzato che sono impossibili da rilevare con soluzioni standard anti-malware o di protezione degli endpoint. Ne consegue che questo panorama minaccioso non può più essere ignorato.
In sostanza, il problema più grande da risolvere riguarda le risorse: non semplicemente i soldi, bensì il tempo e l'esperienza accumulata.
Ed è qui che interviene in aiuto il paradigma dei servizi, come quello sviluppato da F-Secure, L'idea che sta alla base dei servizi di sicurezza gestiti è semplice. La parola "gestiti" significa proprio questo: il servizio è completamente gestito da un partner esterno, che richiede pochissimo input dal team IT interno di un'organizzazione. "Rilevazione e risposta" (detection and response) si riferisce in un tale contesto come approccio al modo in cui funziona il servizio.
Tramite sensori sofisticati su endpoint e reti di un'azienda, una soluzione basata su un servizio abilita rapidamente una visibilità completa in un ambiente IT anche molto ampio e dai confine estesi al mobile e al multi cloud. Quello che ne risulta è una architettura, una soluzione che può rilevare le violazioni analizzando il comportamento, e non gli ovvi segnali di un'attività malevola.
Questo è quello che ha fatto F-Secure con lo sviluppo dei servizi di sicurezza gestiti MDR, che hanno l'obiettivo di consentire anche azioni di risposta rapide ed efficaci, supportate dall'automazione o dalle decisioni umane, o da un loro intimo e sinergico connubio

Il fattore uomo - macchina

Una cosa è evidente: nessun essere umano sarebbe in grado di rilevare da solo le minacce avanzate così come sono andate delineandosi. Queste minacce non danno chiari segnali che qualcosa non va. Gli allarmi del software di endpoint non li rilevano e, ad esempio la protezione della posta elettronica non cattura le e-mail di phishing sul gateway che le inoltra all'ignaro utente. L'unico modo per rilevare attacchi come questi, osserva F-Secure, è mediante una combinazione di uomo e macchina tramite l'unione di sensori che raccolgono dati rilevanti, l'intelligenza artificiale che processa questi dati e la competenza di risorse esperte che analizzano rilevazioni sospette di violazioni.
Questo è il messaggio di allarme che F-Secure lancia e che sta alla base della sua vision di servizio e di connubio uomo-macchina, e come il modo più efficace e rapido per contrastare le minacce tramite un nuovo servizio di rilevazione delle intrusioni e di risposta agli incidenti che permette di scoprire e bloccare al loro insorgere e in tempi utili le minacce presenti sulla rete aziendale.

Il fattore tempo

Il fattore "Tempo" è un punto chiave nella sicurezza. In media le violazioni di dati possono durare settimane, mesi o persino anni prima di essere rilevate. Le organizzazioni non riescono ad effettuare diagnosi precoci di una violazione, con oltre il 92% di violazioni che restano nascoste all'organizzazione che è stata colpita.
Inoltre, numerose sono ancora le aziende che si basano solamente sulla difesa perimetrale per proteggere sé stesse, che è sì importante ma solo come parte di una strategia di sicurezza informatica globale. In queste condizioni un

tentativo di attacco finisce quasi certamente col superare i controlli di sicurezza e penetrare nella rete.
La capacità nel riuscire a rilevare velocemente le intrusioni e a rispondere in modo immediato è quindi fondamentale ma non semplice da mettere in atto.
E' a questo vulnus temporale che pone rimedio un servizio gestito come quello sviluppato da F-Secure, che combina il meglio dell'uomo con l'intelligenza delle macchine, con la promessa di informare le aziende in soli 30 minuti dalla rilevazione di una minaccia.
Le aziende che si stanno rendendo conto che da sole fanno realmente fatica a rilevare intrusioni e a rispondere agli incidenti hanno con F-Secure, osserva la società, la possibilità di affidarsi a un team di esperti di sicurezza informatica, costruire un'infrastruttura di monitoraggio, e ottenere validi dati per un'efficace intelligence delle minacce.

Il servizio gestito di Rapid Detection&Response

«Per scenari del tipo analizzati, in F-Secure abbiamo sviluppato F-Secure Rapid Detection & Response Service (RDS), un servizio gestito di rilevamento e risposta ai cyber attacchi mirati», osserva **Antonio Pusceddu**, Country Sales Manager per l'Italia.
RDS include sensori leggeri per il rilevamento delle intrusioni per endpoint, reti e server esca distribuiti nell'intera infrastruttura IT. I sensori monitorano le attività avviate dagli attaccanti e trasmettono tutte le informazioni al cloud di F-Secure in tempo reale.
Il servizio basato su cloud ricerca eventuali anomalie nei dati utilizzando una combinazione di tecnologie avanzate, come l'analisi del comportamento in tempo reale, l'analisi dei Big Data e l'analisi della reputazione.
La ricerca delle anomalie procede in due direzioni: comportamenti malevoli noti e sconosciuti. Questo perché l'adozione di tipologie di analisi differenti garantisce il rilevamento degli attaccanti, anche se usano tattiche di evasione progettate per eludere metodi di rilevamento specifici.
Una volta rilevate, le anomalie riscontrate vengono segnalate al team di esperti di sicurezza del Rapid Detection & Response Center di F-Secure che ricercano minacce operando h24 per verificarle e filtrare i falsi positivi.
Il processo di alert è peraltro molto rapido. Quando viene confermato che un'anomalia costituisce una minaccia effettiva, il cliente riceve un avviso entro 30 minuti. Ma non è tutto. Gli esperti di F-Secure propongono contestualmente i passaggi necessari per contrastare e correggere la minaccia. E non ultimo, vengono anche fornite informazioni dettagliate sull'attacco, che possono essere anche utilizzate come prova nell'ambito di procedimenti forensi.
Nei casi più difficili o laddove le risorse IT del cliente non siano disponibili, è poi sempre possibile contare sull'assistenza del servizio di risposta agli incidenti on-site di F-Secure.

IoT sempre più a rischio

Conferma della necessità di nuovi approcci alla cyber security sono i dati di un report di F-Secure che rivela un aumento di attacchi e minacce che prendano di mira dispositivi IoT.
Il report evidenzia che le minacce e il numero di attacchi continuano a crescere, pur basandosi su punti deboli della sicurezza già noti, come software non aggiornati e password deboli.
Il report "IoT threats: same hacks, new devices", che usa dati raccolti e analizzati dai Laboratori di F-Secure, sottolinea che le minacce che prendono di mira i dispositivi connessi a Internet stanno iniziando a moltiplicarsi più rapidamente che in passato.
Il numero di minacce IoT osservato è pressoché raddoppiato nel corso dello scorso anno, passando dal 19 precedente a 38. Per fortuna, re-

lativamente parlando, molte di queste minacce usano ancora tecniche conosciute e prevedibili per compromettere i dispositivi.

Le minacce che prendono di mira credenziali deboli o quelle predefinite fornite dal produttore, oppure le vulnerabilità non risolte, o tutte queste insieme, hanno costituito l'87% delle minacce osservate.

Tom Gaffney, F-Secure Operator Consultant ha dichiarato in proposito che i maggiori produttori di dispositivi IoT o ad essi assimilabili stanno prestando più attenzione alla sicurezza che non in passato, ma c'è un gran numero di dispositivi di numerosi produttori che non offrono molto in termini di sicurezza e privacy agli utenti finali. «I grandi come Google e Amazon hanno fatto passi da gigante nei loro prodotti per la smart home grazie all'enorme sostegno di hacker etici come il nostro Mark Barnes, che ha eseguito il primo proof of concept per l'hacking di Echo nel 2017» ha spiegato Gaffney. «Ma per anni i produttori hanno rilasciato sul mercato prodotti senza pensare molto alla sicurezza, quindi molti dispositivi 'smart' in circolazione sono vulnerabili ad attacchi relativamente semplici.»

Le minacce IoT sono state riscontrate raramente prima del 2014, si spiega nel report. Ma ciò è cambiato con il rilascio del codice sorgente per Gafgyt - una minaccia che ha preso di mira una varietà di dispositivi IoT, inclusi i dispositivi BusyBox, le telecamere a circuito chiuso (CCTV) e molti registratori video digitali (DVR).

Nell'Ottobre 2016, Mirai, che è stato sviluppato dal codice di Gafgyt, è diventato il primo malware IoT a raggiungere notorietà a livello globale quando la sua massiccia botnet è stata utilizzata per lanciare uno dei più grandi attacchi denial-of-service distribuiti nella storia.

Il codice di Mirai è pubblico "per scopi di Ricerca/Sviluppo IoC" dal 2016. Originariamente, utilizzava 61 combinazioni univoche di credenziali utilizzate per le infezioni.

Nel giro di tre mesi, quel numero era proliferato a quasi i 500 ed è prevalente come famiglia di malware. Circa il 59% del traffico di attacco rilevato dai server honeypot di F-Secure nel 2018 ha preso di mira le porte Telnet esposte, con tentativi di Mirai di diffondersi.

Secondo **Jarno Niemela**, F-Secure Labs Principal Researcher, la causa principale di molti problemi IoT inizia con le supply chain dei produttori.

«La maggior parte dei vendor di dispositivi rilasciano kit di sviluppo software per i chipset che utilizzano nelle loro smart camera, smart appliance e altri dispositivi IoT. Ecco da dove vengono le vulnerabilità e altri problemi» spiega Niemela. «I produttori di dispositivi devono iniziare a chiedere di più in termini di sicurezza da questi fornitori e anche essere pronti a rilasciare aggiornamenti e patch non appena disponibili».

LA VISIBILITÀ DELL'IT E COME MANTENERLA NELL'ERA DEL CLOUD IBRIDO

Le aree grigie dell'IT aziendale spaziano dai dispositivi mobili alle workstation , dall'on-premise alla containerizzazione. I suggerimenti di Qualys per eliminare le aree grigie dell'IT

Emilio Turani, Qualys

Cloud, multi cloud, cloud ibrido, dispositivi mobili, workstation fisiche o virtuali, sono di certo strumenti e servizi che favoriscono la digital transformation, l'ottimizzazione di Capex e Opex e l'espansione del business. Con il crescere in azienda di architetture e dispositivi aumenta però il rischio per la sicurezza perché senza un approccio pragmatico e omni-comprensivo si perde visibilità e di controllo.

La visibilità, osserva **Marco Rottigni**, Chief Technical Security Officer EMEA di Qualys, non è l'unica sfida, ma costituisce indubbiamente lo step fondamentale per tutti i processi volti ad armonizzare l'IT, predisponendo quegli ambienti sicuri e conformi necessari all'interno di ogni realtà aziendale.

La risposta risiede nel comprendere cosa sta avvenendo nell'IT ma per farlo, osserva Rottigni, servono "occhi": sensori che potenzino la raccolta dei dati e che siano studiati appositamente per gli ambienti di elaborazione in cui vengono implementati, sia esso l'on-premise che il cloud ibrido.

Per i servizi on-premise dell'ambiente IT, ad esempio, la visibilità riguarda server, client, dispositivi di rete, dispositivi di sicurezza ed altri tipi di host, su piattaforme di più sistemi operativi.

La realtà è di certo già complessa ma andrebbero considerati, mette in guardia il manager, altri due fattori che contribuiscono ad aumentarla: il primo è l'Enterprise Mobility, il secondo è la containerizzazione.

Alle preoccupazioni che riguardano in termini di visibilità lo scenario on premise, si aggiungono poi altri due elementi critici: l'adozione del cloud e i DevOps.

Il cloud, sovente, comporta il disassemblaggio dell'infrastruttura tradizionale in parti più piccole: archiviazione, logica applicativa, funzioni, rete, logica di bilanciamento del carico, database, gestione di identità, di accesso e altro ancora.

Ne deriva l'esigenza di creare relazioni tra queste parti, ma, ci si può legittimamente chiedere, dove e quando sono state implementate queste parti e come si gestisce la loro sicurezza?

La soluzione a tutte queste sfide può basarsi, spiega Qualys, solo su un approccio strategico ed olistico che permetta di concentrarsi su aspetti quali:

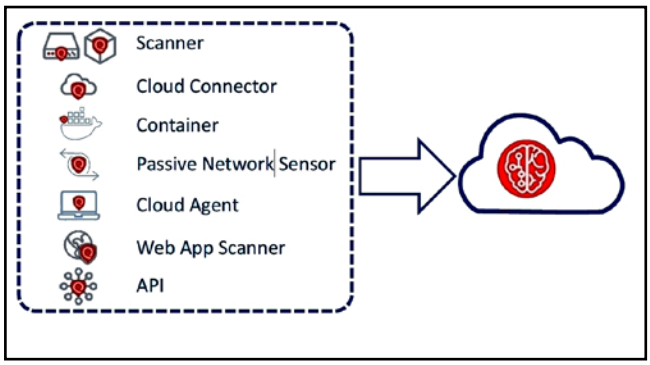
- La visibilità su tutto il panorama IT.
- L'accuratezza nel normalizzare i dati durante

lo screening.
- La scalabilità verso l'alto e verso il basso.
- L'immediatezza nel raggiungimento dei risultati.
- La consapevolezza dello stato dell'arte.

Queste cinque capacità, nella vision di Qualys, dovrebbero essere implementate o rafforzate da un punto di vista strategico, fondate su strumenti e tecniche adeguate per supportare le procedure basilari.

Un approccio pragmatico potrebbe focalizzarsi sull'analisi accurata del panorama IT che si possiede, cercando di comprendere i vari e differenti ambienti di cui si compone, e sulla relazione tra questi: ad esempio, se gli ambienti di produzione si espandono al cloud, o se il cloud viene utilizzato principalmente per lo sviluppo e area di controllo qualità.

"Per aiutare ad affrontare questi problemi abbiamo sviluppato una piattaforma olistica, evolvendo l'approccio di disaccoppiamento della raccolta dei dati, realizzato con sensori specializzati distribuiti in tutto il panorama IT, dall'elaborazione dei dati, eseguiti centralmente all'interno della nostra piattaforma cloud. Questo approccio offre la coerenza necessaria per visualizzare, riepilogare, approfondire e aggregare i dati per più profili utente; questo approccio fornisce la consapevolezza della situazione a supporto del processo decisionale e dei processi come SecOps», ha spiegato Rottigni.



Gli elementi IT di cui la piattaforma Qualys convoglia i dati osservati all'intelligenza centrale

Dall' on-premise al cloud ibrido

Se la visibilità atta a garantire la sicurezza informatica è già di per sé complessa in ambienti on-premise, il problema viene enfatizzato quando ad esso si aggiunge il cloud.

L'utilizzo di piattaforme cloud pubbliche, evidenzia in proposito **Emilio Turani**, Managing Director Italia, Spagna, Portogallo e Central Eastern Europe di Qualys, comporta sfide di security e compliance che, se non affrontate con i giusti strumenti e per mezzo di processi corretti, possono rivelarsi complesse e dal costo proibitivo.

Le criticità del cloud risiedono principalmente in due aree: la mancanza di visibilità degli asset e delle risorse cloud, e il modello di responsabilità di sicurezza condivisa disposto dai cloud provider. Spazi storage permeabili, non sicuri, gruppi di sicurezza mal configurati, e user policy errate sono tutte criticità che si possono riversare sull'end-user.

Man mano che si trasferiscono i carichi di lavoro sul cloud, i team di sicurezza perdono visibilità dell'infrastruttura al di fuori dal loro diretto controllo.

Il problema si complica ulteriormente se l'azienda sfrutta le piattaforme cloud di più fornitori. I responsabili della sicurezza IT devono sapere quali vulnerabilità esistono nei nuovi ambienti cloud che le loro business unit stanno sfruttando, e dare priorità alle minacce sulla base di veri e propri indicatori di criticità.

Ma non solo. Devono monitorare i regolamenti, i mandati di settore e le policy interne per essere certi che la propria azienda rispetti i requisiti. E, non ultimo,si devono stabilire dei processi risolutivi per affrontare l'elasticità degli ambienti cloud.

In sostanza, il punto chiave è comprendere le specifiche del modello di "responsabilità di sicurezza condivisa" tra il fornitore di servizi cloud e l'azienda che usufruisce dei servizi cloud. La demarcazione di responsabilità può ad esempio prevedere che ciò che accade all'interno delle virtual machi-

ne è responsabilità dell'azienda mentre l'hardware fisico, la virtualizzazione, e i servizi cloud sono gestiti e assicurati dal cloud provider.
Per concretizzare un tale approccio e assicurare la visibilità e la sicurezza dell'IT nel suo complesso Qualys ha sviluppato un set molto ampio di soluzioni di security e compliance per gli host e le istanze cloud che include vulnerability management, policy compliance, il monitoring dell'integrità dei file e la scansione delle applicazioni web. Nel loro insieme, evidenzia l'azienda, sono soluzioni che aiutano le imprese nel:

- Identificare, classificare, e monitorare tutti gli asset e le vulnerabilità riguardanti gli ambienti on-premises, cloud, endpoint o mobile
- Rispettare le policy interne ed esterne, così come quelle normate dal GDPR
- Rimediare alle vulnerabilità in base a prestabilite priorità
- Trovare e contrastare automaticamente i malware su tutti i siti e le app web
- Integrare ed automatizzare security e compliance di tutti i processi DevOps

Più sicurezza e meno vulnerabilità con il patch management

Un altro punto critico è costituito dalla gestione delle patch, che deve essere la più rapida ed esaustiva possibile.
Per abilitarla Qualys ha reso disponibile la Patch Management (PM), una cloud App dotata di funzionalità per distribuire in modalità automatica le patch. Consente di eseguire l'orchestrazione trasparente della gestione delle vulnerabilità per l'intero ciclo di vita dei sistemi operativi e dei software presenti in ambienti ibridi globali.
Tramite la PM App la Qualys Cloud Platform abilita il consolidamento dell'assessment delle vulnerabilità, la definizione delle priorità delle minacce e le attività di remediation. In sostanza, consente ai team IT e di sicurezza di gestire centralmente l'eliminazione delle vulnerabilità su sistemi operativi Windows, macOS e Linux oltre che su più di 300 applicazioni di terze parti.
Operativamente gli utenti sono in grado di affrontare rapidamente vulnerabilità e falle di sicurezza note senza consultare le indicazioni suggerite dai vendor, di distribuire le patch alle risorse locali, negli end-point o nel cloud e di verificare l'esito della remediation direttamente da un'unica console.
Qualys PM può essere attivata istantaneamente tramite lo stesso agente cloud di Qualys utilizzato per valutare le configurazioni e la presenza di vulnerabilità. L'agent invia costantemente al cloud dati sulle modifiche critiche e dettagli giustificativi e consente di abilitare l'installazione di patch su end-point remoti e in roaming all'esterno della rete.
Una volta attivata, la PM App raccoglie e trasmette alla Qualys Cloud Platform dati di telemetria relativi ai software installati, alle vulnerabilità aperte e alle patch mancanti. La visibilità sulle risorse e sul relativo stato di sicurezza mette a disposizione una serie di dati omogenei con cui analizzare, classificare, distribuire e verificare le patch in modo più efficiente.
Il supporto interessa i sistemi operativi Windows e oltre 55 applicazioni Windows e di terze parti. In futuro comprenderà i sistemi operativi Mac e Linux,i flussi di approvazione ampliati e un maggiore livello di automazione. Le prossime versioni saranno dotate anche di funzioni di reportistica e visibilità in tutte le fasi del processo di patching, con separazione dei compiti per attività specifiche.

Reportec

Resta aggiornato con REPORTEC!

Informati sulle nuove tecnologie
a supporto del business

seguici su

www.reportec.it

oppure abbonati alle nostre RIVISTE!

info@reportec.it