Cloud & Business

n.69
Marzo 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

PAG 01
- La protezione degli Account privilegiati nel cloud è da migliorare

PAG 04
- FortiGuard AI rileva le minacce in modo proattivo

PAG 05
- Il cloud di Qualys supporta nel garantire la sicurezza

PAG 07
- PA ed aziende verso un futuro sempre più digitale

PAG 08
Voli sicuri con i servizi di Cyber Security di F-Secure

PAG 10
- Artificial Intelligence senza limiti con AIRI di Pure Storage

PAG 12
- Le opportunità del cloud e come sfruttarle

PAG 13
- Red Hat Virtualization disponibile in SAP HANA

PAG 14
- Comune di Palermo e NetApp insieme per Palermo Smart City

PAG 15
- Tyco e Google assieme per la digital transformation del retail

PAG 16
- Retelit espande le sue rotte in Asia ed Europa

PAG 17
- Forcepoint si focalizza sulla cybersecurity human-centric

PAG 18
- Cloudian acquisisce Infinity e si rafforza nel software defined storage

COVER STORY

LA PROTEZIONE DEGLI ACCOUNT PRIVILEGIATI NEL CLOUD È DA MIGLIORARE

Un survey evidenzia che le aziende non garantiscono la protezione nel cloud e negli endpoint dei Privileged Accounts e delle loro credenziali

Il crescente ricorso al cloud evidenzia tra gli utilizzatori alcune lacune, e tra queste quella inerente la protezione degli account privilegiati. Secondo un recente survey (CyberArk Global Advanced Threat Landscape Report 2018), quasi la metà (per l'esattezza il 46%) dei professionisti per la sicurezza cambia raramente in modo sostanziale la propria strategia, persino dopo aver direttamente sperimentato e subito un attacco cibernetico.

E' anche questa inerzia nell'affrontare il problema della cyber security e nel non voler trarre insegnamento dagli insuccessi nel garantire la sicurezza che mette a rischio i dati sensibili, le infrastrutture e l'intero complesso degli asset IT aziendali.

Ma chi inerte non è, da

Adam Bosnian - CyberArK

Reportec Cloud&Business - Numero 69 - Marzo 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 -

Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

dove dovrebbe partire per migliorare la sicurezza complessiva? Un suggerimento lo propone CyberArk proprio a seguito dei risultati evidenziati dal survey, realizzato da Vanson Bourne e condotto con il coinvolgimento diretto di 1.300 IT security decision maker, sviluppatori DevOps e App e LoB manager nei principali sette paesi mondiali.
DIDA: Il 46% delle aziende non cambia strategia anche dopo aver subito un attacco

Partire dalla protezione dei Privileged Accounts

Il fatto che sia importante proteggere i privileged accounts è ampiamente riconosciuto. Una preponderante percentuale di professionisti IT nella sicurezza si dice convinta che la scurezza di un ambiente IT inizia dalla protezione degli utenti privilegiati.
Quasi il 90% ritiene infatti che sia l'infrastruttura IT che i dati sensibili non risultino adeguatamente protetti a meno che non lo siano anche gli utenti privilegiati, e che le loro credenziali e i privilegi siano messi al sicuro.
Se poi si scende nel particolare dl quale tipo di attacco ci si trova più di frequente a fronteggiare la situazione è la seguente:

- Phishing (56%)
- Threats interni (51%)
- Ransomware o malware (48%)
- Privileged accounts non sicuri (42%)
- Dati nel cloud non sicuri (41%)

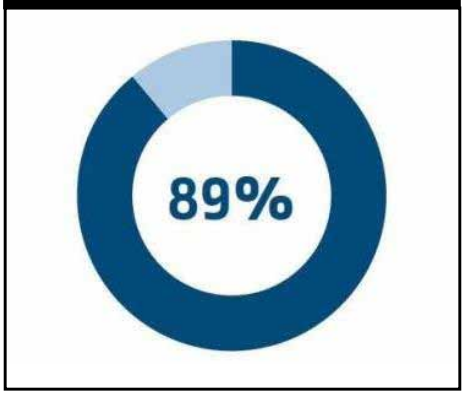
La situazione diventa ancor più critica per quanto concerne gli utenti privilegiati se si considera che secondo quanto riportato dai manager IT, il numero di utenti che dispongono di privilegi sul loro dispositivo endpoint è salito dal 62% nel 2016 a ben l'87% nel 2017, un incremento che richiede adeguate best practice e una maggiore sicurezza.

Dati compromessi

Cosa è possibile dedurre dai risultati dello studio? I risultati evidenziano che l'inerzia in fatto di sicurezza sembra permeare numerose organizzazioni, con una conseguente incapacità nell'affrontare e nel contrastare i cyber attacchi, con tutti i rischi che ne possono conseguire. In particolare:

- Il 46% afferma che la propria organizzazione non è in grado di prevenire attacchi portati alla rete aziendale interna.
- Il 36% evidenzia che le credenziali amministrative sono conservate in documenti Word o Excel su Pc aziendali.
- Il 50% ammette che la privacy dei clienti può essere a rischio perché i loro dati non sono adeguatamente protetti oltre il minimo legale.

L'89% ritiene le proprie infrastrutture non adeguatamente protette



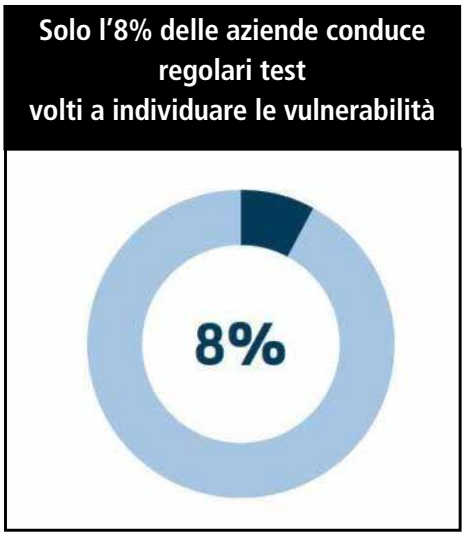
I rischi nel cloud

Se si passa al cloud la situazione non sembra migliore. L'automatizzazione dei processi inerenti cloud e DevOps ha come conseguenza il fatto, mette in guardia CyberArk, che privileged ac-

counts, credenziali e informazioni riservate sono generate con un elevato tasso di prolificità.
Se queste informazioni vengono compromesse , ciò può permettere ad un attaccante di fare il passo successivo e avere accesso a dati sensibili attraverso l'intera rete aziendale, ai dati, alle applicazioni, sino a poter fruire delle infrastrutture e delle risorse cloud per attività illecite di crypto mining.
Anche in questo caso si evidenzia una sostanziale differenza tra il dire e il fare. Le organizzazioni riconoscono sempre più la situazione di rischio e le sue possibili conseguenza , ma sembrano però mantenere un approccio rilassato nei confronti della sicurezza nel cloud:

- Il 49% delle organizzazioni non ha approntato una strategia per la sicurezza nel cloud dei privileged accounts.
- Il 68% demanda la sicurezza al fornitore del servizio facendo conto sulla sicurezza native del provider.
- Il 38% afferma semplicemente che il cloud provider non fornisce la protezione adeguata.

Solo l'8% delle aziende conduce regolari test volti a individuare le vulnerabilità



Cambiare la cultura per la sicurezza

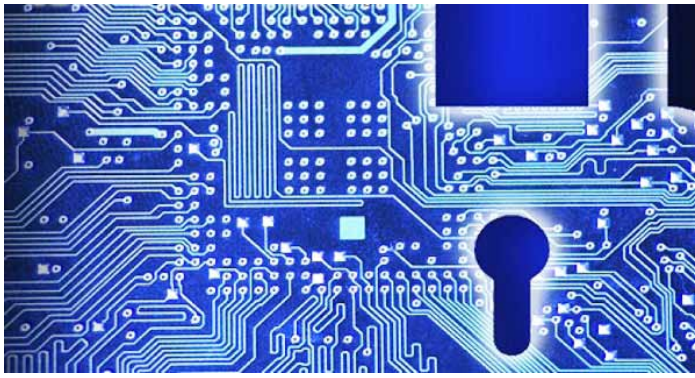
Per combattere l'inerzia nel campo della sicurezza cibernetica quello che serve, evidenzia CyberArk, è il farla diventare un punto centrale nella strategia e nel comportamento di una organizzazione e non un qualcosa che sia dettato esclusivamente dalle esigenze commerciali e competitive. Anche in questo caso i dati del survey sono molto espliciti:

- L'86% dei professionisti per la IT security ritengono che la sicurezza dovrebbe essere uno dei punti regolarmente affrontati a livello di board.
- Il 44% afferma di riconoscere e premiare i dipendenti che aiutano nel prevenire falle nella sicurezza.
- L'8% delle aziende conduce continuamente esercitazioni (Red Team) il cui obiettivo è individuare vulnerabilità critiche e identificare le contromisure da mettere in atto.

«Gli attaccanti continuano a far evolvere le proprie tattiche, ma le aziende devono fronteggiare una persistente inerzia per quanto concerne la sicurezza che è tutta a favore degli attaccanti», ha commentato Adam Bosnian, Executive Vice President, global business development di CyberArk. «Ci deve essere una maggior urgenza nell'incrementare la resilienza in fatto di cyber security nel confronto dei moderni attacchi. Questo inizia dall'identificare appieno l'ampiezza in continua espansione della superficie di attacco alla sicurezza degli account e come questo ponga seriamente a rischio l'intera organizzazione. Vincere l'inerzia richiede una forte leadership, misurabilità dei risultati, una strategia chiaramente definite e resa nota, nonché la capacità di adottare un approccio mentale del tutto simile a quello di un attaccante».

FORTIGUARD AI RILEVA LE MINACCE IN MODO PROATTIVO

FortiGuard AI automatizza analisi di threat intelligence e rilevamento delle minacce e aiuta nel contrastare uno scenario di attacchi in rapida espansione



Fortinet, società che sviluppa soluzioni di cyber security integrate e automatizzate, ha annunciato FortiGuard AI, una soluzione integrata nella piattaforma di servizi di threat intelligence di Fortinet che fornisce analisi automatizzata e rilevamento delle minacce che hanno l'obiettivo di garantire che le soluzioni Security Fabric siano continuamente aggiornate. In particolare, ha evidenziato l'azienda:

- Costituisce un sistema di rilevamento delle minacce auto-evolutivo che utilizza l'apprendimento automatico e la formazione continua per raccogliere, analizzare e classificare autonomamente le minacce alla velocità della macchina.
- E' integrato nella piattaforma di servizi di threat intelligence di Fortinet per potenziarne le funzionalità di rilevamento delle minacce che i servizi FortiGuard condividono attraverso il Security Fabric.
- Comprende funzionalità si User Entity and Behavioral Analysis (UEBA) e FortiGuard Threat Intelligence Service (TIS) come offerta di servizi enterprise.

L'obiettivo postosi da Fortinet con il rilascio della soluzione è dichiaratamente quello di potenziare i servizi di threat intelligence che forniscono aggiornamenti in tempo reale e protezioni proattive dalle minacce all'interno del Security Fabric. Come evidenziato, oltre al rilascio di FortiGuard AI, Fortinet ha annunciato anche gli aggiornamenti del FortiGuard Threat Intelligence Service (TIS) e l'aggiunta di nuove funzionalità di analisi comportamentale per FortiSIEM:

- FortiGuard TIS: è ora disponibile come servizio enterprise che fornisce metriche di threat intelligence basate su cloud e trend di attività specifici per l'eccezionale panorama delle minacce di un'organizzazione. Consente ai CISO di comprendere ciò che accade nel panorama delle minacce globale per assegnare priorità alle risorse e ottimizzare le policy di sicurezza.
- FortiSIEM User and Entity Behavior Analysis (UEBA): sono tecniche di machine learning che migliorano il rilevamento avanzato con le nuove funzionalità UEBA in FortiSIEM versione 5.0, che apprende modelli di comportamento tipico degli utenti come posizione, ora del giorno, dispositivi utilizzati e server specifici a cui si accede. Può ad esempio segnalare automaticamente attività anomale come accessi simultanei da postazioni separate o

accessi anomali ai server utilizzati raramente. «Sempre più spesso, i criminali informatici e le nazioni antagoniste sfruttano tecniche automatizzate e polimorfiche per aumentare la velocità e la portata delle loro attività malevole, evitando al contempo il rilevamento attraverso la creazione di centinaia di varianti zero-day ed eludendo le difese. Le aziende hanno bisogno di un modo per affrontare tali tecniche incidendo sui costi degli aggressori e riducendo al contempo le proprie spese operative. L'investimento quinquennale dei Fortinet Labs nell'analisi automatizzata e nel rilevamento di minacce polimorfiche ha portato a FortiGuard AI, un passo da gigante nel raggiungimento di questo obiettivo. FortiGuard AI analizza e identifica le minacce in maniera veloce, agile e accurata per fornire un rilevamento proattivo delle minacce a velocità e scalabilità della macchina. Ciò consente agli analisti delle minacce e agli operatori di rete di concentrarsi sulla ricerca di minacce critiche e su problemi superiori, riduce l'esposizione agli attacchi zero-day e abbassa al minimo il rischio per i clienti Fortinet aumentando invece i costi per l'aggressore», ha commentato Phil Quade, chief security security officer di Fortinet.

IL CLOUD DI QUALYS SUPPORTA NEL GARANTIRE LA SICUREZZA

La Qualys Cloud Platform fornisce la visibilità delle risorse IT e previene i rischi, mettendo in grado di soddisfare i requisiti imposti dal GDPR

Emilio Turati - Qualys

Qualys, società che fornisce soluzioni di sicurezza e compliance tramite la sua Cloud Platform, ha fatto il punto sulla sua presenza nel mercato nazionale e come si propone di supportare le aziende nel garantire la sicurezza, sgravarle del compito arduo del gestirla e rispondere a quanto stabilito dal GDPR.

Il nucleo portante della suo offerta, fruibile in cloud in modo che sia costantemente aggiornata, ha come pilastro portante il controllo dell'asset IT, la raccolta dei dati e la valutazione dei rischi, il tutto in aderenza ai requisiti imposti dal GDPR. La piattaforma consente anche la protezione costante dei dati personali gestiti negli ambienti IT globali e soprattutto con le terze parti.

Il nuovo Regolamento europeo sulla protezione dei dati, ha evidenziato la società, introduce un'unica legislazione in tutte le nazioni dell'Unione Europea. In Italia prenderà il posto dell'attuale Codice Privacy (Dlgs 196/2003) e le aziende dovranno adeguarsi alle nuove disposizioni, non solo per evitare sanzioni, ma anche per essere più competitive in un mercato unico digitale.

Diventa quindi prioritario per le organizzazioni poter tracciare e classificare gli asset IT che gestiscono i dati, adottando la piena governance e gli opportuni processi di sicurezza che consentano di

rispondere ai requisiti del GDPR.
«Il GDPR cambia radicalmente la cultura sul trattamento dati e dei processi interni da rispettare e rappresenta un'occasione importante per ripensare la propria azienda in ottica sicurezza. Indagini di mercato presentano però un quadro ancora allarmante. Dal nostro punto di vista i settori dove registriamo i migliori tassi di adeguamento al GDPR, sono attualmente quelli della PA e del Finance, mentre risultano ancora abbastanza indietro le aziende di Manufacturing e Servizi», ha sottolineato Emilio Turani, Managing Director Italia, Spagna e Portogallo.
Elemento saliente della piattaforma cloud di Qualys, ha invece illustrato Francesco Amando, Technical Account Manager, è che integra oltre dieci applicazioni e fornisce validi strumenti per assicurare la visibilità delle risorse e dei dati di clienti e fornitori, consentendo la revisione dei processi interni in modo da migliorare la sicurezza globale.
In pratica, se il GDPR chiede all'azienda di introdurre regole pratiche per regolare la gestione della sicurezza IT, Qualys ha risposto mettendo a disposizione via cloud un approccio semplice e molto ampio per rendere un'azienda conforme alle normative.
Quattro i punti chiave della piattaforma cloud per la sicurezza e corrispondenza normativa, ha illustrato **Luca Besana**, Channel Manager della società:

- Piattaforma di Asset Inventory/Monitoring per capire cosa è presente nel perimetro aziendale
- Soluzioni di gestione continua delle vulnerabilità per monitorare le debolezze applicative e consentire di sapere proattivamente dove ci potrebbero essere degli attacchi
- Soluzioni di Policy Compliance per permettere alle aziende di conoscere esattamente il loro livello di conformità rispetto alle normative (standard e custom).
- Security Assessment Questionnaire per automatizzare, centralizzare e ottimizzare il processo di gestione del rischio dei fornitori e delle terze parti.

Piattaforma predisposta per il cloud privato e ibrido

La piattaforma per la sicurezza è fruibile sia in modalità completamente su cloud che in modalità privare cloud per le aziende che desiderano mantenere i dati sulla sicurezza e sull'asset strettamente sotto controllo. In quest'ultima versione può poi essere fruita in diverse modalità, come server rack preconfigurato con capacità elaborativa e storage oppure come Virtual rack oppure, per lo small business, in versione appliance stand alone.
In tutte le versioni permette di assicurare il mantenimento locale dei dati sensibili conservati in versione criptata mentre la gestione è in ogni caso demandata a Qualys, che mantiene la proprietà e la completa responsabilità della soluzione. L'utente paga solamente un canone basato sul numero di dispositivi da mantenere sotto controllo e in funzione della configurazione.
Presenza qualificata sull'intero territorio nazionale
Attiva direttamente in Italia da due anni, ha illustrato Besana, Qualys ha alla data già oltre 100 clienti distribuiti nel finance, nella PA e nell'Industry ed opera attraverso una rete di partner di canale specializzati e integratori di sistema che coprono l'intero territorio nazionale.
E una struttura 1 tier che non fa uso di un distributore intermedio per l'alta preparazione tecnica e ingegneristica richiesta e che vede alcuni dei partner in grado a loro volta di costruire soluzione più complesse basate sui servizi cloud di Qualys per rispondere alle specifiche esigenze del cliente.

PA ED AZIENDE VERSO UN FUTURO SEMPRE PIÙ DIGITALE

SIAV ha annunciato un software di EIM che ottimizza i processi della PA e delle aziende tramite la gestione digitale di documenti e file multimediali

Il Mercato del "Digitale" italiano continua ad essere in espansione, con una forte attenzione al tema della Trasformazione abilitata dal Digitale, e quindi a tutte quelle aree che tramite l'IT permettono il recupero di competitività, come l'accesso multicanale alle informazioni, l'integrazione delle Informazioni e la loro valorizzazione e la gestione delle Informazioni tramite strumenti flessibili ed orientati al futuro, in primis il Cloud.

Tutto questo si è tradotto nel passaggio dal semplice gestionale o Document Management all'Enterprise Information Management. La differenza tra i due approcci risiede nel fatto che il Document Management è focalizzato sul documento, e sull'archiviazione, mentre l'Enterprise Information Management è incentrato sull'accessibilità, fruibilità e integrazione dell'informazione con i processi di business. Le aziende, sia private sia PA, osserva SIAV, azienda attiva nella fornitura di soluzioni in cloud e servizi informatici per la dematerializzazione e per il miglioramento dei processi digitali, sono tornate ad investire in questo settore, anche per restare al passo con la regolamentazione, , mirando a un approccio dinamico alla gestione del ciclo dell'informazione, e questo partendo dalla dematerializzazione.

Puntare sulla gestione digitale

Per favorire questa trasformazione che permette di semplificare e ottimizzare i processi

SIAV ha ideato Silloge, un software di Enterprise Information Management con cui si è prefissa di permettere di ottimizzare i processi e i procedimenti della PA e delle aziende attraverso la gestione digitale dei documenti, file multimediali ed informazioni.

La soluzione, ha spiegato, è basata su tecnologie Open Source e Cloud Native in modo che possa essere fruibile e accessibile da tutte le Imprese, incluse PMI e Enti pubblici, e costituire una soluzione adatta in termini di potenza dell'infrastruttura tecnologica disponibile e budget da dedicare alla digitalizzazione.

Per le aziende che vogliono esternalizzare la complessità dell'IT , le caratteristiche del prodotto, ha spiegato la società, ne permettono la fruizione tramite System Integrator che vogliono costruire con Siav una solida partnership tecnologica. Elemento chiave per questo approccio è l'utilizzo della tecnologia dei "docker", che consente l'attivazione progressiva delle funzionalità disponibili e programmabili via API e l'integrazione con i sistemi informativi aziendali (ERP, CRM, prodotti

per la Conservazione Digitale etc).

Ampie funzionalità

Nella sua essenza, la piattaforma Silloge permette di organizzare e gestire attività quali il workflow management, la collaborazione tra utenti, la PEC, le anagrafiche e la gestione dei fascicoli, ma è anche una soluzione che nell'intendimento di SIAV guarda al futuro, perché dispone di funzioni per lo smart working, la messaggistica istantanea, la metadatazione automatica, la clusterizzazione e il tagging automatici dei documenti, un sistema di ricerca federato e integra funzioni di process mining e social network analysis.

«Ci siamo impegnati per sviluppare un software in linea con le effettive esigenze delle imprese. Il risultato è una piattaforma di nostra proprietà con un'interfaccia unica sul mercato, capace di garantire integrabilità, interoperabilità e la sicurezza del sistema. Silloge si affianca oggi alla nostra offerta di soluzioni ECM e per la conservazione digitale, e apre una porta sul futuro a tutte le tipologie d'azienda, grandi o piccole, pubbliche o private», ha commentato Leonardo Bernardi, General Manager di SIAV.

VOLI SICURI CON I SERVIZI DI CYBER SECURITY DI F-SECURE

Un nuovo servizio di F-Secure combina l'esperienza nella cyber security e nell'aviazione per supportare le aziende del settore nel proteggere gli asset strategici

Hugo Teso - F-Secure

In volo ci si aspetta comprensibilmente di essere al sicuro, e non solo perché vada a buon fine, ma anche che i servizi erogati a bordo siano a prova di hacker. E un attacco che va a buon fine, fosse anche uno minimo che si limiti a prendere di mira un sistema di intrattenimento, potrebbe avere effetti negativi sulla fiducia in una compagnia aerea o persino sull'intera industria del settore.

Per evitarli F-Secure ha sviluppato un'offerta specializzata di Servizi di Cyber Security per l'Aviazione che è stata progettata per aiutare le compagnie aeree e organizzazioni simili a proteggere i loro aerei, le infrastrutture, i dati, e la loro reputazione.

L'offerta non giunge senza motivi. La cyber security, soprattutto quando ci sposta e viaggia, ha assunto un'importanza significativa per molte industrie, incluse proprio quelle che lavorano nell'aviazione. In un'indagine del 2015, l'85% dei CEO delle compagnie aeree ha identificato la cyber security come un rischio significativo.

Mentre molte industrie hanno a che fare con violazioni di dati e attacchi informatici da molti anni, Hugo Teso di F-Secure ha evidenziato come i cambiamenti nell'industria dell'aviazione stiano apportando nuovi rischi per le compagnie aeree. «Tecnologie standard di comunicazione stanno trovando il loro posto negli aerei, il che rende la sicurezza molto più complicata da gestire che in passato,» ha spiegato Teso, ex pilota e oggi a capo dei Servizi di Cyber Security per l'Aviazione di F-Secure. »Dato che queste tecnologie standard non sono state create necessariamente per rispondere ai rigorosi requisiti di safety delle compagnie aeree, l'industria dell'aviazione sta ponendo la cyber security come massima priorità. Ma serve un partner che possa comprendere sia la cyber security che i dettagli del funzionamento di una compagnia aerea, poiché parliamo di un'industria dove questi dettagli fanno una grossa differenza».

Servizi mirati, da terra al volo

I Servizi di Cyber Security per l'Aviazione di F-Secure sono stati progettati, come evidenziato, per aiutare le compagnie aeree e altre aziende che lavorano nel mondo dell'aviazione a proteggere le loro attività sui diversi aspetti coinvolti.

Includono valutazioni di sicurezza dell'avionica, di sistemi di terra e data link, scansioni delle vulnerabilità, monitoraggio della sicurezza, servizi di risposta agli incidenti, e formazione specializzata in cyber security per gli IT manager e per il personale di bordo e di cabina di pilotaggio, il tutto compreso in un unico pacchetto di offerta pensato per supportare le compagnie aeree nel rafforzamento delle attività di individuazione, prevenzione e blocco degli attacchi informatici.

In particolare, ha osservato F-Secure, Le valutazioni di sicurezza giocano un ruolo particolarmente importante nella cyber security nel settore dell'aviazione poiché possono segnalare potenziali problemi prima che le compagnie aeree o i produttori tentino di certificare dispositivi o servizi per l'uso.

Le valutazioni di sicurezza possono focalizzarsi su componenti individuali come pezzi specifici di hardware e software, o su problematiche più vaste, per esempio su come sistemi differenti interagiscono tra loro. «Aiutiamo le organizzazioni su una questione chiave che riguarda la protezione di sistemi critici di safety di un aereo dalla compromissione di quei sistemi che sono, in un certo senso, più esposti ma meno significativi per le funzionalità di un aereo,» ha commentato Andrea Barisani, Head of Hardware Security di F-Secure, «Una misura di protezione molto importante riguarda la separazione dei sistemi in differenti 'domini fidati', e il controllo di come sistemi in domini differenti possono interagire tra loro. Ciò previene che problematiche di sicurezza informatica in un dominio, come per esempio per un servizio Wi-Fi accessibile ai passeggeri, finiscano con l'infettare sistemi critici di safety, come i controlli di un aereo o i data link aria-terra».

ARTIFICIAL INTELLIGENCE SENZA LIMITI CON AIRI DI PURE STORAGE

Con la soluzione AI-ready e all-in-one AIRI, Pure Storage rende semplice l'uso dell'intelligenza artificiale

Pure Storage, società che sviluppa soluzioni tutte all-flash di storage di fascia alta ha annunciato la disponibilità di AIRI, una soluzione all-in-one sviluppata con NVIDIA, nel corso di una collaborazione strategica, ideata per chi necessita di infrastrutture IT di nuova generazione adatte ad applicazioni di intelligenza artificiale in un contesto di big data e dati strutturati e non strutturati.

La nuova architettura, ha illustrato Alfredo Nulli, Principal Systems Engineer EMEA della società, coniuga lo storage all-flash ad alta capacità e bassissima latenza fornito dalla tecnologa Flashblade di Pure Storage con le elevatissime capacità di calcolo parallelo delle GPU della piattaforma DGX di NVIDIA.

La combinazione ottimizzata delle due tecnologie in un'architettura in grado di supportare sia lo scale-out che lo scale-up apre la strada ad una forte evoluzione nel campo del computing e dell'intelligenza artificiale su larga scala per aziende di settori di punta e critici sia della PA che del mondo Industry nonché dei provider di servizi cloud, dove il fattore capacità elaborativa e velocità si coniuga con l'esigenza di contenere spazi e consumi energetici. Quello che ne è derivata, evidenzia Nulli, è una soluzione estremamente innovativa potente che concretizza il concetto di AI-in-a-box in grado di auto adattarsi alle esigenze di calcolo e a seguito di una architettura altamente ridondante rispondere alle necessità di applicazioni business o industry always-on.

Artificial Intelligence senza frontiere

L'esigenza di una architettura ideata per trarre il meglio dalle tecnologie ad alte prestazioni come quelle garantite da GPU a elevato calcolo parallelo e storage flash con bassissima latenza utilizzato in modo estensivo a livello 1 deriva dalla necessità espressa da aziende di vari settori (e.g. il finance dove il microsecondo nel piazzare un ordine fa la differenza, la genomica, l'automotive, il customer care, eccetera) di sfruttare appieno le opportunità create dall'intelligenza artificiale, opportunità che un'architettura IT convenzionale spesso impedisce di perseguire a causa degli incompatibili tempi di accesso a uno storage multi-layer, a processori con limitate capacità di I/O e a reti di interconnessione non in grado di smaltire l'elevato traffico intercorrente tra unità di calcolo e di storage di una applicazione di AI.

E' questa barriera all'utilizzo estensivo dell'Artificial Intelligence che Pure Storage si è proposta di rimuovere con lo sviluppo della soluzione AIRI, che racchiude in un unico rack tutte le componenti di storage all-flash, di GPU e di rete ad al-

Alfredo Nulli -
Pure Storage

tissime prestazioni ideate e costituenti un sistema pre-configurato e ottimizzato per il supporto di applicazioni che richiedono elevate velocità di calcolo e uno storage estensibile dell'ordine dalle decine alle centinaia di Terabyte (fino all'ordine del Petabyte).

Gli elementi chiave di AIRI

Due gli elementi chiave di AIRI, ha illustrato Nulli. Il primo è l'unità Flashblade, una soluzione ultra-compatta di storage flash che riesce ad erogare in un solo rack di 4U le prestazioni in termine di capacità dell'equivalente di dieci rack disco convenzionali, con capacità di I/O enormemente superiori e adatte alle esigenti necessità dl calcolo parallelo e dell'intelligenza artificiale.

Il secondo elemento sono i server NVIDIA DGX, che sono in grado secondo dati di targa di erogare la capacità elaborativa equivalente di 10 rack server convenzionali.

A parte i benefici derivanti dal disporre di storage e capacità di calcolo ad alto potenziale in grado di soddisfare le severe esigenze di applicazioni di AI, sono evidenti, osserva Nulli, i più che consistenti benefici derivanti dal consolidamento che viene reso possibile in termine di spazi occupati in un data center nonché la forte riduzione di necessità in termini di consumi energetici e di condizionamento che ne derivano, cose che da sole permettono di accelerare notevolmente il ritorno dell'investimento tecnologico. Va poi osservato che la tecnologica Flashblade di Pure Storage è stata ideata a livello di architettura specificatamente proprio per accelerare il trattamento di carichi di lavoro parallelo.

Lo storage Flashblade di AIRI

Tre sono gli elementi salienti della componente storage di AIRI. Il primo sono le blade (o lame, o schede) predisposte per una espansione di tipo scale-out. Si caratterizzano per una latenza ultra bassa e hanno una capacità di 8, 17 o 52 TB. Sono inseribili e sostituibili a caldo e una volta inserite nel rack sono gestite dal software di controllo in modo che i dati vengano ridistribuiti in modo omogeneo sulle diverse lame, cosa che ottimizza lo storage stesso e la latenza nelle operazioni di I/O da e verso l'unità GPU.

Il secondo elemento è il software. Costituisce la chiave di volta di un'architettura software driven, nell'implementare lo scale-out e la gestione ottimizzata dei dati, e fornisce i servizi e la gestione in locale e nel cloud, analisi predittiva e servizi di supporto e protezione dei dati.

L'architettura e il software di Flashblade sono anche la chiave che garantisce un massiccio calcolo parallelo, la gestione concorrente di decine di migliaia di utenti e di decine di milioni di oggetti e di file.

Il terzo elemento è la fabric che garantisce l'interconnessione di lame e rack. Comprende una rete built-in Ethernet in fibra ottica con connessioni multiple di sino a 40 Gb/s (espandibile a 100 Gb/s) che fornisce una capacità di banda complessiva per singolo chassis pari a 320Gb/s.

Un rack da 4 U completamente equipaggiato con 15 lame (che possono essere di 8, 17 o 52 TB) può arrivare dell'ordine dei Petabyte (considerando la compressione).

«Le caratteristiche tecniche e funzionali di AIRI ne fanno la soluzione adatta per le esigenze di AI nell'ambito del trading, del customer care, dell'analisi predittiva, nel manifatturiero, nella simulazione. E' una soluzione che rendiamo disponibile world wide tramite un selezionato e ristretto numero di operatori di canale con una consolidata esperienza nel campo delle GPU e in Italia la soluzione è disponibile tramite il nostro partner di canale PNY» ha commentato Nulli.

LE OPPORTUNITÀ DEL CLOUD E COME SFRUTTARLE

Un sondaggio su 164 partner di canale nell'area Emea fa emergere aree di business nel cloud e nella sua sicurezza che possono essere attivamente perseguite

Al crescere delle organizzazioni che abbracciano soluzioni di cloud ibrido, il canale ha innegabilmente un ruolo di primo piano da giocare in termini di educazione del clienti, in particolare quando si tratta di sicurezza.
Essendo la tecnologia cloud relativamente nuova, pur se oramai ampiamente accettata come concetto, molte organizzazioni non dispongono ancora e in numerosi casi non è nemmeno per loro conveniente, dotarsi delle competenze specialistiche nella sicurezza cloud al proprio interno, un gap spesso colmato e colmabile rivolgendosi ai servizi erogabili dai partner di canale.
Per farsi un'idea più precisa di come il canale stia aiutando le organizzazioni nel loro percorso verso il cloud, Barracuda, ha illustrato Chris Hill, Director Business Development for Public Cloud, EMEA della società, ha condotto un sondaggio su un campione di 164 partner di canale nell'area Emea, confrontando poi i risultati con quelli di analoghe ricerche condotte sugli utenti finali.
Quello che ne è risultato è che se in molte aree i risultati non sono troppo dissimili, il cloud è un aspetto in cui i partner non sembrano essere allineati con i loro clienti.

Chris Hill - Barracuda

La domanda che viene da porsi dunque è: i partner stanno sfruttando come potrebbero l'opportunità offerta dal cloud? Vediamo qualche dato e relative considerazioni del manager emerse:
Canale e utenti finali concordano sul fatto che le organizzazioni usano il cloud prevalentemente per il backup: il 56% degli utenti dichiara di usare il cloud principalmente per il data recovery.
Il futuro del cloud si prospetta del tutto positivo: l'86% dei partner dichiara infatti che i propri clienti oggi si fidano del cloud più che nei cinque anni passati e solo l'8% afferma che la fiducia è diminuita. Il dato conferma ricerche precedenti nelle quali il 64% dei decisori IT in Emea affermava che la fiducia nel cloud pubblico era cresciuta.
Vi sono aree di disaccordo. I partner di canale riferiscono di un 10-20% in media di clienti con un'infrastruttura di cloud pubblico, mentre parlando con le aziende la percentuale sale al 35%.
Il canale tende a sovrastimare la consapevolezza da parte delle organizzazioni del modello di sicurezza condivisa del cloud: solo il 55% pensa che i clienti non comprendano il modello, mentre il 64% degli utenti finali afferma di non avere nemmeno conoscenze di base del modello.
La discrepanza più grossa riguarda la sicurezza cloud. Mentre solo il 64% degli utenti finali afferma di avere un piano di cybersicurezza, solo il 27% del canale ritiene che i loro clienti abbiano

effettivamente un tale piano. Potrebbe essere che le organizzazioni abbiano piani di sicurezza datati che il canale ritiene siano superati? Quello che è certo è che c'è l'opportunità per i partner di canale di investigare quel 64% per capire quali aree siano coperte. Ciò potrebbe portare i partner a ritagliarsi un ruolo per aiutare i clienti a sviluppare un nuovo piano di sicurezza allo stato dell'arte adatto al cloud.
In generale e tirando le somme, osserva Hill, il canale sembra sottostimare l'uso del cloud da parte delle aziende e sovrastimare il livello di formazione, in particolare rispetto alla sicurezza, il che porta a pensare che il canale stia perdendo un'ottima opportunità di generare fatturato.
Ciò probabilmente accade più perché i clienti non ne parlano ai partner che per colpa dei partner che non chiedono. Ma i partner dovrebbero ricordarsene la prossima volta che discuteranno col cliente del suo approccio alla sicurezza.

RED HAT VIRTUALIZATION DISPONIBILE IN SAP HANA

La nota diffusa di virtualizzazione è stata certificata per workload SAP HANA e garantire le prestazioni necessarie nell'analisi dei big data

Red Hat ha annunciato che Red Hat Virtualization supporta SAP HANA, la piattaforma di sviluppo di dati e applicazioni in-memory per workload big data.
L'azienda si è così messa in grado di fornire un sistema operativo (Red Hat Enterprise Linux for SAP HANA) e hypervisor entrambi validati per l'utilizzo in ambienti SAP HANA e rispondere alle richieste di uno standard aperto da parte delle aziende che vogliono avere a livello di data center libertà di scelta in termini di soluzioni di virtuali, efficienza operativa e riduzione di costo.
Soluzione di virtualizzazione scalabile basata su KVM, Red Hat Virtualization, ha spiegato l'azienda, rappresenta una piattaforma aperta e sicura in grado di gestire numerosi workload, compresi quelli legati alle applicazioni e alle analisi dei big data, senza per questo richiedere modifiche significative o hardware personalizzato.
In pratica, la soluzione supporta le implementazioni SAP HAN e aiuta a consolidare l'hardware fisico al fine di ridurre la spesa IT senza perdere in funzionalità operativa. Non ultimo, può costituire una solida base per tecnologie innovative quali Linux container e cloud, pur conservando la possibilità di integrazione con ambienti IT esistenti.
«Red Hat è impegnata nell'offrire ai clienti scelta a tutti i livelli dello stack, dalle tecnologie di base come il sistema operativo e l'hypervisor fino alle soluzioni avanzate basate su Linux container e Open Stack. Red Hat Virtualization for SAP HANA conferma questo impegno offrendo una piattaforma aperta, flessibile e scalabile sulla quale gestire workload big data e relative applicazioni senza imporre il lock in software o hardware personalizzato», ha commentato il supporto di SAP HANA annunciato Gunnar Hellekson, senior director, Product Management Platforms Business in Red Hat.

COMUNE DI PALERMO E NETAPP INSIEME PER PALERMO SMART CITY

Il progetto si inserisce nell'ambito del percorso di trasformazione digitale intrapreso dal Comune siciliano

Si è svolta alla presenza del Sindaco di Palermo, Leoluca Orlando, del Rettore dell'Università degli Studi di Palermo, Fabrizio Micari, e di Marco Pozzoni, Country Manager di NetApp Italia, la firma di un protocollo di intesa per la realizzazione di servizi innovativi per le smart city, la formazione continua per la Pubblica Amministrazione e la costituzione di un Centro di Competenza per il trasferimento tecnologico e per la diffusione di progetti imprenditoriali innovativi.

L'iniziativa si inserisce nell'ambito del percorso di trasformazione digitale intrapreso dal Comune di Palermo, anche con riferimento al programma PON Metro, volto a realizzare gli obiettivi dell'Agenda digitale, una piattaforma informatica integrata attraverso cui gestire servizi digitali a favore di cittadini e imprese, in maniera snella ed efficiente. In particolare i servizi riguarderanno la mobilità sostenibile, l'efficienza energetica, l'inclusione sociale e, più in generale, l'e-government.

Nel complesso si tratta di un vero e proprio ecosistema tecnologico metropolitano costituito da un data center di nuova generazione, al quale forniranno un contributo rilevante le tecnologie per la gestione dei dati di NetApp, potenziato e ridisegnato per archiviare e gestire in sicurezza ed efficienza dati e informazioni, componenti IoT e servizi in cloud. Il servizio di archiviazione, fruibile in cloud, di tutte le informazioni e i servizi relativi alla Pubblica Amministrazione consentirà di renderli disponibili anche ai Comuni dell'hinterland coinvolti nel progetto PON Metro Città di Palermo, ai loro cittadini, alle imprese e ad altre PA, creando una vera e propria smart city interconnessa.

«Il Comune di Palermo intende proseguire sul cammino intrapreso da anni di innovazione dei servizi digitali a beneficio del territorio e dei cittadini. La sottoscrizione del presente Accordo è un'occasione per accelerare il processo di digitalizzazione della pubblica amministrazione, ma anche di stimolo all'insediamento sul territorio di nuove imprese e/o allo sviluppo di quelle già esistenti, grazie alle sinergie che potranno crearsi con l'Università di Palermo e con NetApp», ha dichiarato il Sindaco di Palermo, Leoluca Orlando.

Il progetto prevede inoltre lo sviluppo di competenze ICT e di sicurezza digitale del personale della Pubblica Amministrazione e la creazione, con il supporto del Comune, dell'Università degli Studi di Palermo, di Sispi e di NetApp, di un Centro di Competenza con laboratori aperti a personale specializzato, agli studenti universitari e alle imprese del territorio per lo sviluppo di nuove applicazioni e servizi per la PA.

«Siamo molto soddisfatti di essere, con le nostre soluzioni tecnologiche e competenze, al fianco del Comune di Palermo, dell'Università e di tutte le realtà coinvolte nella realizzazione di questo importante progetto di trasformazione digitale. L'innovazione tecnologica e la gestione dei dati che sempre più ricoprono un ruolo strategico, sono un asset fondamentale per migliorare la qualità dei servizi della PA e per lo sviluppo sociale ed economico di qualsiasi territorio», ha commentato Marco Pozzoni, Country Manager di NetApp Italia.

TYCO E GOOGLE ASSIEME PER LA DIGITAL TRANSFORMATION DEL RETAIL

Dalla collaborazione di Tyco e Google nasce una combinazione di dati, analitiche e infrastrutture per fornire reale valore di business al punto di vendita

Tyco Retail Solutions ha annunciato una collaborazione con Google Cloud volta a rafforzarne la presenza e nel mercato delle soluzioni di analisi in tempo reale, store execution e performance. L'adozione di Google Cloud Platform , un'infrastruttura scalabile, sicura e ad alte prestazioni, ha commentato Tyco, testimonia l'impegno nell'evoluzione delle proprie piattaforme in vista dello sviluppo e implementazione di soluzioni per il punto vendita e di analisi nel retail di prossima generazione.

La fase iniziale della partnership prevede l'integrazione delle informazioni in tempo reale e le funzionalità relative a inventario, loss prevention e traffico in store di Tyco nella Google Cloud Platform per assicurare ai retailer prestazioni coerenti, scalabili e in tempo reale in termini di visibilità sull'inventario, nonché dati e informazioni sul traffico nel punto vendita per consentire un migliore coinvolgimento del cliente.

Il nuovo servizio basato su Google Cloud per la gestione degli ammanchi in store ha l'obiettivo di permettere ai retailer di migliorare la produttività e aumentare l'affidabilità e le prestazioni dei sistemi EAS, il tutto favorendo lo sviluppo di una nuova generazione di soluzioni di loss prevention.

Gli utenti dell'applicazione potranno anche integrare dati esterni provenienti da Google Analytics e Tyco nella nuova piattaforma di analisi.

"Siamo entusiasti di collaborare con Google Cloud per offrire ai retailer soluzioni innovative - analisi predittiva compresa - sfruttando una tecnologia all'avanguardia come Google Cloud Platform", ha dichiarato Amin Shahidi, vice president strategy, Tyco Retail Solutions. "Combinando tecnologie, processi e personale di qualità siamo in grado di fornire informazioni estremamente dettagliate per garantire ai retailer risultati di business strategici".

Di Google Tyco si è anche proposto di sfruttare le soluzioni di machine learning e big data per dare vita a prodotti innovativi e supportare nuove soluzioni.

siamo in grado di fornire informazioni estremamente dettagliate per garantire ai retailer risultati di business strategici".

Di Google Tyco si è anche proposto di sfruttare le soluzioni di machine learning e big data per dare vita a prodotti innovativi e supportare nuove soluzioni.

RETELIT ESPANDE LE SUE ROTTE IN ASIA ED EUROPA

I nuovi collegamenti integrano la presenza internazionale già consolidata con la rotta del cavo sottomarino in fibra ottica AAE-1

Retelit, uno dei principali operatori italiani di servizi dati e infrastrutture operante nel mercato delle telecomunicazioni, ha espanso la sua rete internazionale con l'inserimento di nuove tratte di capacità in Asia e in Europa, pari a 160 Gbps. Le nuove rotte vanno ad aggiungersi a quelle già operative sul cavo sottomarino AAE-1, che con i suoi 25.000 km collega tre continenti (Asia, Africa, Europa) da Marsiglia a Hong Kong, e a quelle paneuropee.

L'operazione in particolare prevede l'apertura di nuove rotte diversificate per il Mediterraneo e il Far East. In pratica, Retelit rafforza la sua presenza in Asia con un nuovo collegamento diretto tra Singapore e Hong Kong diversificato rispetto alla corrispondente tratta già raggiunta tramite il cavo sottomarino AAE-1, nell'area del Mediterraneo con un anello tra la Sicilia e la Grecia e, infine, diversificando la tratta end-to-end dall'Italia al Far East, con un ulteriore collegamento diretto tra Palermo e Singapore.

La presenza internazionale di Retelit, sempre più capillare, ha l'obiettivo di permettere alle aziende, agli operatori e agli OTT (Over the Top) di collegarsi alle principali città europee, asiatiche e del Middle East ad alta velocità, in maniera sicura e, soprattutto, ridondata grazie alle soluzioni integrate che permettono di avere il restore e il backup dei dati tra le tratte raggiunte.

«La nostra infrastruttura e i nostri collegamenti nei tre continenti raggiunti – ha commentato Federico Protto, Amministratore Delegato e Direttore Generale di Retelit - permettono di connettere l'Europa, attraverso il Sud d'Italia, e le aree del mondo a più alto sviluppo demografico, industriale e tecnologico. In questo scenario, l'Italia è sempre di più un punto di snodo strategico dei flussi di traffico dati provenienti dai paesi del Far East, del Medio Oriente e dell'Africa verso l'Europa e viceversa. La vera sfida è rendere questi hub attrattivi con ritorni per l'indotto dell'intero Paese, attraverso la creazione delle condizioni, infrastrutturali e commerciali, che favoriscano gli investimenti dei soggetti che veicolano grandissime quantità di contenuti e traffico Internet, dai grandi Carrier Internazionali ai cosiddetti OTT».

Con l'annuncio, Retelit consolida ulteriormente la sua posizione di Carrier internazionale con un network che collega anche 70 data center tra i quali quattro in Asia (due a Singapore e due a Hong Kong) e, anche in virtù di partnership e accordi con operatori di telecomunicazioni internazionali, connette 10 paesi in Europa.

FORCEPOINT SI FOCALIZZA SULLA CYBERSECURITY HUMAN-CENTRIC

La cybersecurity human-centric è stato il tema centrale della Channel Conference EMEA, che ha visto premiare le italiane Project Informatica e D.G.S.

Neal Lillywhite - Forcepoint

Il produttore e fornitore mondiale di soluzioni per la sicurezza informatica Forcepoint ha annunciato i partner vincitori degli awards presentati durante la cena di gala che si è svolta alla Channel Conference EMEA a Lisbona, in Portogallo.

L'annuncio è stato dato in occasione dell'evento a cui hanno partecipato i principali partner di canale di tutta l'area, una conferenza di due giorni per esaminare la strategia di cybersecurity human-centric e sul portafoglio a valore Human Point System, nonché per celebrare la community dei partner mondiali e il contributo da essi dato all'organizzazione di Forcepoint.

Tra i premi assegnati, quello di Rising Star Award è andato a Project Informatica SRL e sempre ad un'italiana è andato il riconoscimento Southern Europe Partner of the Year, attribuito a D.G.S.

«Forcepoint con il suo approccio sta creando un vero e proprio punto di svolta nel settore della sicurezza informatica. L'approccio che l'industria ha utilizzato finora non è più efficace. È stato costruito per un tempo diverso, un ambiente IT diverso e più strettamente controllabile e un diverso panorama delle minacce. In Forcepoint, stiamo reinventando la sicurezza con il nostro approccio incentrato sull'individuo, offrendo sistemi adattivi che comprendono il comportamento e le motivazioni delle persone mentre interagiscono con dati e IP ovunque essi siano», ha affermato Neal Lillywhite, vice president of Channel, EMEA.

La Partner Conference EMEA ha visto i partner strategici di tutta l'area apprendere di più sul nuovo approccio di Forcepoint verso la cybersecurity e sulle opportunità di crescita per quest'anno e per i prossimi. Solo negli ultimi tre mesi Forcepoint è stata riconosciuta da CRN nella sua lista dei 20 migliori fornitori di Cloud Security, all'interno dei 2018 Cloud 100 e come prodotto dell'anno 2017 per quanto riguarda Forcepoint CASB. Flink inoltre, è stato inserito nella prestigiosa lista dei CRN 2018 Channel Chiefs.

La conferenza ha offerto ai partner EMEA approfondimenti su come l'attenzione di Forcepoint si stia spostando sempre più verso l'utente finale, abilitando la risk adaptive protection, la quale applica in modo dinamico le policy di controllo alle attività e attiva gli alert che rappresentano il rischio più elevato per un'impresa o un'organizzazione governativa, piuttosto che combattere una battaglia senza fine per fermare le minacce.

CLOUDIAN ACQUISISCE INFINITY E SI RAFFORZA NEL SOFTWARE DEFINED STORAGE

Tramite la tecnologia di Infinity, Cloudian semplifica la gestione dello storage ad oggetti e abilita l'evoluzione verso il software defined storage

Oltre l'80% dello storage installato è relativo alla conservazione dei dati. Solo il 20% richiede uno storage ad alta velocità per elaborazioni quali la in-memory computing o la gestione ultraveloce di transazioni, come avviene nel campo finanziario. E dell'80% una percentuale crescente serve per la memorizzazione di file in diversi ambienti operativi come ad esempio gli esami clinici o radiografie in ambiente medicali oppure, cambiando campo, per l'archiviazione di videoregistrazioni nell'ambito di infrastrutture per la sicurezza privata o di aree pubbliche.
Nei vari casi il comune denominatore e la tecnologia di archiviazione verso cui ci si sta spostando sempre più prepotentemente è quella ad oggetti, un approccio architetturale che abilita una organizzazione flessibile e un rapido retrieval delle informazioni quando servono e dove servono, sia che vengano archiviate su infrastrutture on-premise che nel cloud.
Il problema è che non è facile coniugare qualità dello storage e qualità delle applicazioni che vi risiedono che permettano l'archiviazione in modo sicuro, protetto e in ambienti operativi variegati di informazioni ad oggetti.
La cosa è ancor più complicata quando, in chiave di ottimizzazione e apertura delle infrastrutture, si decide di evolvere verso una architettura storage di tipo software defined, ovverosia una architettura che separa il piano hardware dal piano software e che in quanto tale permette di adeguare le caratteristiche dell'uno indipendentemente dall'altro, seppur entro i confini delle esigenze applicative tecnologiche.

Due tecnologie e know how che si fondono

Il problema evidenziato lo ha dovuto affrontare Cloudian, azienda con copertura mondiale che si è specializzata nello sviluppo di dispositivi storage e che era alla ricerca di un'azienda con cui entrare ancor più massicciamente nel settore in crescita dello storage ad oggetti e del software defined storage.
La risposta, ha spiegato Michael Tso, CEO di Cloudian, l'ha trovata in Infinity, azienda italiana attiva dalla fine degli anni '90 e guidata dalla sua fondatrice Caterina Falchi, che nel corso di due decenni ha accumulato una profonda esperienza nella gestione di file in diversi ambiti applicativi e di settore.
Dopo una approfondita analisi dell'esperienza e dei prodotti di Infnity, Cloudian ha deciso di fare di Infinity uno dei propri pilastri aziendali, con Caterina Falchi che ricoprirà la carica strategica di VP File Technology.

L'acquisizione di Infinity ha permesso a Cloudian di completare il proprio portfolio con soluzioni integrate di archiviazione di file e oggetti che danno la possibilità, ha spiegato Tso, di consolidare e archiviare praticamente qualsiasi tipo di dati non strutturati in un pool di risorse scalabile all'infinito. E di farlo in chiave software defined.

L'acquisizione di Infinity ha permesso a Cloudian di aggiungere alle proprie competenze la consistente esperienza di Infinity nel campo dei file system dedicati a storage WORM e le forti competenze sul kernel dei sistemi operativi, nonché quanto connesso allo sviluppo di soluzioni per la gestione dei vari tipi di storage per dati legali e di lunga durata, dove necessita un accesso trasparente ma sicuro alle applicazioni di utente.

Ne consegue, ha osservato Cloudian, una gestione più semplice dello storage che permette di ridurre il TCO anche di oltre il 70% rispetto ai tradizionali sistemi NAS multi-silo.

Una collaborazione iniziata nel mondo NAS

L'acquisizione, ha spiegato Falchi, che coniuga una solida esperienza manageriale ad una scientifica, non è però giunta all'improvviso. Come tutti i matrimoni meglio riusciti è stata preceduta da una convivenza che ha permesso alle due società di verificare una comunità di intenti e di vision del mercato. L'acquisizione sopraggiunta rappresenta in sostanza l'ultimo passo quasi naturale di una partnership da tempo esistente.

Le due aziende hanno infatti in precedenza collaborato alla realizzazione del controller NAS Cloudian HyperFile, una piattaforma che rende disponibili file service di livello Enterprise su Cloudian HyperStore. Cloudian HyperFile è una soluzione che comprende in pratica tutte quelle funzionalità NAS essenziali per le applicazioni enterprise, incluso il supporto di SMB(CIFS)/NFS, snapshot, WORM, failover non distruttivo, scalabilità orizzontale, conformità POSIX e integrazione con Active Directory.

«Per oltre dieci anni, il software Infinity Storage ha aiutato i grandi clienti a semplificare la gestione dei file con funzioni di classe enterprise volte a offrire un front-end trasparente verso le applicazioni utente per l'archiviazione di dati su tutti i tipi di storage di nuova generazione», ha commentato Caterina Falchi, VP File Technology di Cloudian.

Il merge delle tecnologie delle due società apre ora concrete prospettive di ottimizzazione di ambienti storage e applicativi, nonché dei costi, va aggiunto. Tramite l'alta scalabilità delle soluzioni di archiviazione di classe Enterprise di Cloudian HyperStore, con HyperFile le organizzazioni vengono in pratica a disporre di nuove opzioni per gestire localmente una quantità elevata di dati non strutturati, dati che, probabilmente in modo conservativo, si stima avranno ogni anno una crescita di oltre il 50%.

«L'acquisizione accelera ulteriormente l'impegno di Cloudian nel ridurre i carichi di lavoro IT mediante file system facilmente scalabili e dotati di sistemi di autoprotezione che, secondo gli analisti, sono di estrema importanza per la gestione storage di nuova generazione», ha affermato Tso.