Cloud & Business

n.84
Agosto-Settembre 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

Il cloud diventa multi-cloud e richiede maggiori competenze e migliori infrastrutture

Il cloud computing è un paradigma affermato come mezzo per intraprendere proficuamente il percorso verso la digital transformation e la razionalizzazione della propria infrastruttura ICT, indipendentemente dalle dimensioni della propria azienda e dal settore di business in cui si opera.

L'accettazione crescente da parte degli utilizzatori e delle aziende di questo approccio nel modo di fruire delle risorse informatiche ai fini del business è conseguenza della semplificazione che apporta all'organizzazione interna, alla possibilità di esternalizzare la complessità dell'ICT, ai benefici derivanti dal disporre di tecnologie e applicazioni senza doversi preoccupare di licenze e nuove versioni. Non ultimo, e proprio nello spirito del Cloud, il beneficio di far corrispondere in modo

Giuseppe Saccardi - Reportec

Reportec Cloud&Business - Numero 84 - Agosto-Settembre 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

lineare gli investimenti in Capex e Opex ai risultati economici e alle esigenze di business.
Quello del Cloud, e delle sue varianti ibride o multi-cloud, è uno scenario complesso che interessa ogni settore dell'ICT: dalla pura infrastruttura di rete, server e storage e alle relative applicazioni di virtualizzazione, Backup e di Data Recovery, alle applicazioni più complesse necessarie per elaborare i Big Data o per gestire una nuova branca dell'ICT, l'IoT.
Quando dal concetto si passa però alla pratica, la scelta della soluzione e del partner con cui intraprendere la strada del Cloud e la esternalizzazione dell'ICT, può non essere semplice. Pur trattandosi di soluzioni idealmente aperte, una volta intrapresa la strada del cloud presenta indubbie criticità.
Sono tutti aspetti che vengono esaminati negli articoli seguenti, dove aziende primarie attive in settori che vanno dall'IaaS al SaaS esprimono la loro posizione e suggeriscono come far fronte alle diverse esigenze della trasformazione digitale in atto, dall'IaaS al PaaS sino al SaaS.

Come efficientare l'IT con flash storage virtuale on-premise e nel multi-cloud

La tecnologia flash storage e la movimentazione dei dati nel multi-cloud richiedono progetti e un approccio flessibile alla digital transformation

Alfredo Nulli - EMEA Cloud Architect di PureStorage

Lo storage è uno degli elementi chiave del cloud assieme a server, reti e applicazioni. Esso costituisce storicamente nell'ambito infrastrutturale del cloud, sia privato che pubblico, l'elemento che è stato alla base della sua iniziale formulazione e costante diffusione, nonché l'elemento che, negli ultimi anni, ha subìto la maggior evoluzione tecnologica e architetturale. Per approfondire cosa rappresenta oggi e come aziende come Pure Storage (www.purestorage.com/it) stanno rispondendo alle necessità tecniche ed economiche delle aziende impegnate nella trasformazione digitale, e analizzare quali sono i problemi a cui devono porre attenzione, è utile partire dall'analisi delle loro esigenze.

Nell'evoluzione dello storage esistono due distinti livelli: uno relativo all'evoluzione e gestione del dato, ed uno inerente all'evoluzione dello storage come punto di memorizzazione.

Il mondo della gestione dei dati si è rivelato particolarmente complesso perché ha sofferto negli anni di problemi dovuti ad esigenze di segmentazione, derivanti dall'utilizzo di silos indipendenti, richiesti dalla necessità di adottare tecnologie diverse atte a supportare le disparate tipologie di dati.

È un modello che è andato avanti per anni con tecnologie quali ad esempio NAS, SAN e DAS, e su questo si sono costruiti dei silos applicativi separati.

La prima evoluzione che si è andata evidenziando, e a cui ci siamo prefissati di rispondere, è la necessità dei clienti di avere un unico livello di "Data Service": in sostanza, un livello di gestione dei dati che fornisca varie interfacce che possano essere fruite dalle applicazioni senza doversi preoccupare della tipologia di implementazione tecnologica, senza isole tecniche e con un livello di servizio comune che possa essere esportato facilmente verso le applicazioni.

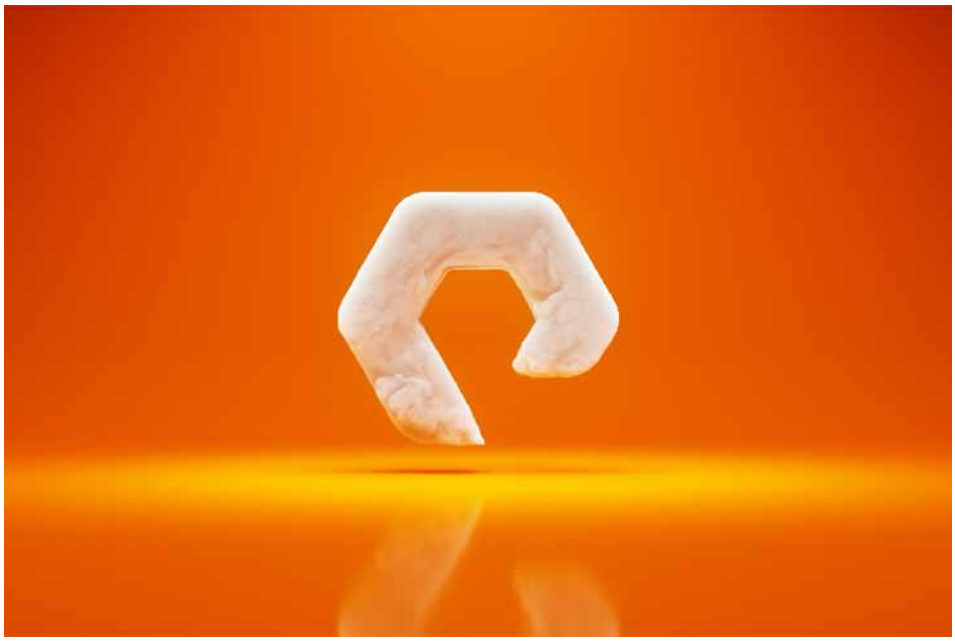
Per ottenere il massimo della flessibilità, questo livello di data service deve necessariamente essere indipendente dall'hardware sottostante, sia che si utilizzi un ambiente on-premise, cloud pri-

vato o un cloud provider.
Questo modello rappresenta la prima profonda cesura rispetto al passato per quanto concerne lo storage.
La seconda cesura, che ha interessato le applicazioni aziendali e il livello tecnologico di base, è rappresentata dall'introduzione nel mercato della tecnologia Flash. Pure Storage ha reso disponibili soluzioni "All Flash", che permettono di utilizzare questa tecnologia a 360°, anche laddove, inizialmente, gli hard disk erano economicamente più vantaggiosi.
Questa possibilità, che permette di semplificare l'intero panorama delle infrastrutture IT aziendali o di un provider, è in parte dovuta alla capacità, da parte dei produttori, di realizzare dispositivi in grado di memorizzare più informazioni nel medesimo spazio fisico, cosa che ha favorito l'adozione della tecnologia flash con la conseguente riduzione di costi per unità di informazione. Questo consente di utilizzare il flash per tutta la catena applicativa.
Se si mettono a fattor comune l'esigenza di un data service che risulti omogeneo dall'Enterprise al Cloud, l'evoluzione tecnologica che semplifica la sottostante componente tecnica, e l'economicità della tecnologia all flash che aumenta la competizione con i dischi, ne emerge che il mondo dello storage va evolvendo verso un modello semplificato che non inficia le prestazioni, la semplicità d'uso e la flessibilità.
Ciò permette alle aziende, soprattutto come conseguenza della diffusione del cloud, di poter considerare lo storage come un elemento infinito, e cioè una sorta di immenso data hub dove è possibile continuare ad aggiungere capacità senza creare criticità o impattare sulle applicazioni di business.
Quindi l'evoluzione del mondo storage, così come la vediamo in Pure Storage, ha l'obiettivo di aiutare le aziende a semplificare tendendo verso l'adozione di un data service unico, con un livello tecnologico comune, operando come se lo storage a disposizione fosse "infinito". In sostanza, l'innovazione sta nel non dover accettare compromessi nell'usare questa tecnologia ed essere aperti al mondo degli standard senza risultare vincolati ad una particolare evoluzione tecnologica. Inoltre, la "openess", ossia l'apertura agli standard, è estremamente importante perché assicura un ampio grado di libertà sia all'azienda che progetta lo storage sia al cliente nelle sue scelte future.
La "openess" da sola, però, non basta. Il lavoro che ha fatto Pure negli ultimi anni è stato volto anche alla semplificazione della fruizione dello storage operando su due distinti livelli: il data service e il livello della tecnologia di base.
Congiuntamente, le due cose permettono alle aziende di disporre di un grado di libertà che fa emergere il valore dello storage e di gestione dei dati e non quello della semplice memorizzazione degli stessi.
Perseguire un tale obiettivo ha richiesto un notevole lavoro, non solo tecnologico e di sviluppo di prodotti, ma anche di formazione e diffusione di questa nuova cultura presso le aziende e i loro tecnici.

Lo storage nel cloud e nel multi-cloud

Il tema del multi-cloud e dei relativi problemi gestionali è molto attuale nelle aziende che lo stanno adottando, le quali, oltre ai benefici, riscontrano al contempo problemi che coinvolgono dal financial officer alll'ufficio acquisti.
Per affrontare il tema del cloud, e le sue relative implicazioni, si deve però segmentare il suo utilizzo, e analizzarlo a partire dal cloud fruito come IaaS, quindi a livello di infrastruttura, diversamente dal "Software as a Service".
Semplificando, il livello IaaS si potrebbe paragonare al modello "Ikea", dove si acquistano e poi si assemblano personalmente i mobili desiderati. Trasposto nel cloud, ciò significa che se si costru-

isce l'IT sulla base di questo modello, il manager deve trasformarsi in "assemblatore".
Una prima domanda da porsi è: si è culturalmente pronti a ridiventare assemblatori?
La seconda domanda è: anche se si avesse la capacità per diventare assemblatori, si hanno a disposizione il tempo e il budget necessari?
Per evitare di dover incorrere in queste scelte si stanno affacciando sul mercato del cloud una serie di soluzioni che utilizzano i cloud provider come elementi basici e, similmente ad una fabbrica, a partire dai componenti di base, assemblano per il cliente un prodotto finito. Si tratta di soluzioni proposte da grandi vendor che utilizzano i cloud provider per poter armonizzare il data service e proporlo poi all'azienda cliente.
Sotto il profilo di fruizione questo significa per un'azienda poter disporre di soluzioni di data service omogenee e interoperabili, sia che siano acquisite da un produttore come Pure Storage sia da un provider come Amazon AWS o Microsoft Azure. In pratica, significa disporre di un ambiente multi-cloud in cui i dati, a differenza di una complessa migrazione, possono essere spostati automaticamente e in modo semplice verso un provider, e da un provider all'altro, perché il livello di data service è in ogni caso il medesimo.
Naturalmente si tratta di servizi a pagamento, che permettono tuttavia di ottenere una "data efficiency" e un'ottimizzazione del volume di storage che, assieme alla forte semplificazione gestionale che ne deriva, permettono di impattare profondamente sul piano sia dell'Opex sia del Capex.



Come intraprendere la migrazione al cloud?

Nel percorso verso il cloud un aspetto critico è la scelta del provider. Dal punto di vista della gestione dati esistono due distinti modi per farlo.
Il primo consiste nell'acquisire servizi di infrastruttura da un cloud provider.
E' il modello più difficoltoso perché richiede forti competenze specifiche, formazione sui servizi erogati dal cloud provider selezionato e la conseguente verifica della corrispondenza alle proprie esigenze di business attuali e future.
Questo è un punto fondamentale e, se si pensa a come si acquisiva l'IT in passato, rappresenta un'inversione di rotta: prima i corsi sulla tecnologia del fornitore venivano fruiti in una fase successiva all'acquisto, mentre ora con i cloud provider la formazione deve avvenire in una fase antecedente alla decisione in quanto la correttezza di quest'ultima è influenzata a sua volta dal livello di formazione a cui si è sottoposto il team IT.
Il secondo modo consiste nell'acquisire dei servizi di piattaforma, ossia dei servizi che già esprimono dei comportamenti e quindi non

necessitano di conoscenze infrastrutturali: ad esempio, un servizio di database, o di "storage as a service", di file storage, eccetera.
Ovviamente la scelta del provider dipende anche dalla ampiezza dei servizi del suo portfolio in corrispondenza dei bisogni aziendali.

Pure Storage e multi-cloud

In un momento in cui le aziende perseguono l'obiettivo della trasformazione digitale, Pure Storage ha intrapreso due percorsi atti a favorirla.
Il primo è consistito nell'espandere nel cloud e nel multi-cloud il portfolio di soluzioni fornito alle aziende che hanno acquisito storage tradizionale, in modo da minimizzarne l'impatto in termini di formazione del personale tecnico o di migrazione dei dati se si decide di passare da un cloud provider ad un altro. Per farlo, Pure lavora con provider quali Amazon, Azure e Google. Sono provider che propongono soluzioni infrastrutturali riferite come soluzioni di piattaforma (PaaS), come ad esempio un Data Base as a Service o un File Service.
Si tratta di soluzioni che permettono di uniformare l'accesso ai dati e risultano del tutto uguali a quelle che fornisce alle aziende sotto forma di hardware.
In pratica, le aziende hanno a disposizione un modello di acquisto unificato che permette loro di spostare in corso d'opera quantità notevoli di dati da un tradizionale on-premise a un cloud provider o, nel ciclo di vita della soluzione, anche ad un altro cloud provider che risulti più conveniente a livello economico o di prestazioni.
Il secondo percorso che Pure Storage persegue è la collaborazione con service provider locali, ad esempio le Telecom, al fine di creare soluzioni storage verticali che spaziano dall'healthcare alla video sorveglianza, dall'intelligenza artificiale al machine learning, sino a quelle tipiche per i settori pubblici.
Il punto fermo della strategia nei confronti delle aziende o dei provider è che la tecnologia non cambia, quello che muta è la proposizione della stessa in modalità diverse con l'estensione delle funzionalità all'utilizzo del cloud come piattaforma di base.
L'ampia accettazione sul mercato dell'approccio adottato, basato sul sistema operativo Purity che fornisce alle aziende e ai provider un data layer universale, è la conferma che le scelte strategiche fatte oltre otto anni fa si sono rivelate stabili nel tempo alla luce dell'evoluzione della tecnologia Flash e del mercato Cloud, mentre per altri fornitori ciò si è rivelato una sorta di terremoto che ha richiesto una loro riorganizzazione aziendale molto critica che ha avuto profondi impatti sulle aziende clienti.

Chi ne beneficia?

Quello che cambia nel cloud e con il cloud è anche la segmentazione delle aziende che possono trarne beneficio. Le aziende vanno, a tal proposito, suddivise non tanto in base alle loro dimensioni ma tra quelle che sono "cloud mature" e quelle che sono in viaggio verso il cloud.
Le soluzioni del portfolio Pure Storage hanno come target ottimale le aziende cloud mature, e cioè quelle aziende che hanno già multi tera o peta byte nel cloud e che si sono poste come obiettivo una ottimizzazione di secondo livello al fine di ottenere ulteriori benefici operativi ed economici.
Ottimizzarne il volume anche del 25-30%, come possibile con le soluzioni Pure Storage, vuol dire ottenere sostanziali benefici economici.
Per chi ha appena intrapreso il viaggio verso il cloud e con una quantità limitata di dati, i benefici, pur esistenti, sono più contenuti.

La sicurezza di utenti privilegiati in ambienti SaaS, SAP e Multi-Cloud

La CyberArk Privileged Session Manager for Cloud estende la protezione degli account privilegiati oltre il perimetro aziendale e nel cloud

David Higgins - EMEA Technical Director di CyberArk

Oggigiorno le organizzazioni fanno affidamento su sistemi informativi complessi che hanno fatto propri paradigmi come il cloud, la mobility, l'Artificial Intelligence e i servizi forniti da operatori e provider qualificati.
Questi sistemi condividono lo scopo primario di permettere ai dati e alle applicazioni di essere sempre raggiungibili e di costituire una potente leva per il business e garantire un flusso ininterrotto e sicuro delle informazioni.
In questo scenario i fornitori di tecnologie e i provider di servizi ricoprono un ruolo primario per quanto concerne l'infrastruttura di base, ma sono però le applicazioni che rappresentano il vero fulcro di un sistema informativo e che abilitano l'operatività funzionale e lo svolgimento dei compiti precipui delle diverse entità aziendali.
In tutto questo, osserva CyberArk (www.cyberark.com), società leader a livello mondiale nello sviluppo e commercializzazione di soluzioni per la sicurezza degli accessi privilegiati, SAP ricopre un ruolo essenziale.
Il motivo risiede nel fatto che SAP fornisce il software di Enterprise Management che necessita alle aziende per condurre il proprio business.
Ma come per ogni medaglia, anche in questo caso esiste un rovescio.
Il successo e la diffusione di SAP ha finito con l'attrarre l'attenzione di hacker e di chi può essere interessato a penetrare nel mondo SAP ed impossessarsi di dati aziendali critici, sia che essi siano conservati on-premise che nel cloud o nel multi-cloud.
In proposito ai rischi per il business derivanti da un fuori servizio di applicazioni critiche, conseguenza di malfunzionamenti o di attacchi informatici, CyberArk ha realizzato un sondaggio condotto coinvolgendo decision maker sia IT che di altre divisioni aziendali.
Quasi sei su dieci dei manager hanno risposto che persino un breve e non pianificato fuori servizio avrebbe avuto un effetto traumatico sul business aziendale. Quasi i tre quarti hanno invece dichiarato che la loro vita lavorativa sarebbe divenuta più difficile se applicazioni critiche si fossero interrotte per un periodo di tempo significativo.

Per i due terzi, infine, le ordinarie operazioni sarebbero divenute addirittura impossibili da condurre nel caso di non funzionamento di applicazioni cruciali.
Tralasciando quanto derivante da eventi naturali o malfunzionamenti applicativi e concentrandosi su possibili attacchi di malintenzionati, il rischio in cui si può incorrere è poi enfatizzato dal fatto che in molti casi i criteri di autenticazione forte posti in essere per proteggere le informazioni sensibili distribuite sui vari ambiti IT da cui può dipendere il corretto funzionamento delle applicazioni di business critiche sono condivisi tra più dipendenti di una medesima divisione o ufficio. E non ultimo, le password finiscono con l'essere ampiamente conosciute nell'ambito dell'organizzazione.
Seppur SAP disponga di misure di sicurezza ideate per il proprio ambiente, il dover garantire un accesso sicuro a utenti privilegiati, o farlo nel cloud, e ancor più nel multi-cloud, può costituire una complessità operativa addizionale che spesso porta a mancare gli obiettivi mandatori di sicurezza e di corrispondenza alle normative.

La protezione nel cloud delle sessioni privilegiate

Per estendere la protezione degli account privilegiati, e i dati a cui questi hanno accesso, ad ambienti esterni al perimetro aziendale fisico, CyberArk ha sviluppato una specifica applicazione, la CyberArk Privileged Session Manager for Cloud. Il punto chiave dell'approccio adottato nel suo sviluppo, ha osservato David Higgins, è che mediante una user experience trasparente l'applicazione estende la protezione per le sessioni di accesso privilegiate e il monitoraggio delle attività oltre che il loro controllo, alle più comuni applicazioni web, nel cloud e sui social media, come ad esempio AWS, Azure o SalesForce.
Privileged Session Manager for Cloud fa inoltre leva sulle capacità delle piattaforme di sicurezza CyberArk di individuare e allertare su attività connesse agli utenti privilegiati.
Numerose le possibilità offerte dalla soluzione atte a migliorare la sicurezza in ambienti cloud ibridi per la protezione degli utenti privilegiati.
Per quanto concerne le piattaforme cloud e web sono ad esempio supportate dalla soluzione le principali piattaforme cloud IaaS e PaaS, SaaS e social media, compreso Amazon Web Services (AWS), Red Hat OpenShift, Salesforce.com, nonché applicazioni social media quali Twitter, LinkedIn, Facebook e Instagram.
Un accesso utente che avviene in modalità trasparente permette di stabilire una connessione sicura verso le piattaforme cloud e le applicazioni web.
La sicurezza è ulteriormente garantita tramite l'isolamento reciproco delle sessioni, che prevede che gli utenti business privilegiati e le sessioni degli amministratori cloud avvengano in modo isolato, un approccio che permette di mantenere riservati dati critici e che gli stessi siano usati solo al fine di stabilire una connessione sicura.
Attenzione è stata dedicata anche a quanto concerne la gestione. In particolare, il monitoraggio delle sessioni permette di condurre attività di auditing dettagliate delle attività degli utenti privilegiati all'interno della piattaforma cloud e delle applicazioni web. In pratica è possibile accelerare le attività forensi e di investigazione sulla sicurezza, così come fornire il supporto per la corrispondenza ai numerosi regolamenti e normative industriali.
A questo si aggiungono funzionalità per la valutazione del rischio che permettono di disporre di una comprensione del rischio inerente le sessioni privilegiate e la visibilità dei rischi connessi ad operazioni condotte da singoli utenti privilegiati. Tramite questa funzionalità l'organizzazione ha la possibilità di essere allertata su attività ad

alto rischio in cui potrebbe incorrere, nonché di avviare in modo prioritario attività di auditing di tipo periodico e in base al rischio.
La valutazione è abilitata da una combinazione di strumenti statistici, algoritmi deterministici, machine learning e di analisi comportamentale.

Soluzioni SaaS per la protezione del Cloud ibrido

Oltre a quelle per ambienti SAP e di Cloud Provider, per proteggere gli accessi privilegiati CyberArk ha anche investito nello sviluppo di un ampio portfolio di soluzioni SaaS. Nel loro insieme, sono volte a facilitare l'utilizzo e la gestione dei sistemi di protezione degli accessi privilegiati, in particolare per aziende focalizzate su strategie cloud e per coloro che stanno effettuando un percorso di trasformazione digitale, soprattutto in ambienti di cloud ibrido o multicloud.
Obiettivo strategico di CyberArk è anche la definizione di un nuovo standard nella fornitura di soluzioni di sicurezza SaaS. Due gli aspetti salienti.
Il primo è costituito da un Accesso Zero Trust (che prevede che le minacce siano ovunque) basato su CyberArk Alero, una soluzione dinamica per la mitigazione dei rischi associati all'accesso remoto dei vendor ai sistemi critici tramite CyberArk. Ha l'obiettivo di migliorare l'efficienza operativa e la produttività, semplificare il provisioning e la gestione degli accessi remoti.
La soluzione SaaS fornisce un accesso Zero Trust a tutti i fornitori che si connettono da remoto alla soluzione di protezione degli accessi privilegiati di CyberArk e garantisce visibilità e un controllo esaustivo sulle attività privilegiate. In pratica, coniuga in una singola soluzione accesso Zero Trust, autenticazione biometrica e provisioning just-in-time senza l'utilizzo di VPN, agent o password. Operativamente, confrontata con soluzioni VPN tradizionali, CyberArk Alero riduce da ore a minuti il processo di on-boarding per i vendor remoti.
Il secondo aspetto della strategia SaaS di CyberArk è costituito da CyberArk Endpoint Privilege Manager, una soluzione volta a ridurre il rischio di accessi amministrativi non gestiti su endpoint Windows e Mac.
Tramite le capacità just-in-time di Endpoint Privilege Manager è possibile ad esempio mitigare i rischi e ridurre i contrasti operativi, e fornire accesso a livello admin su dispositivi Windows e Mac su richiesta, per un periodo specifico, con audit log e la possibilità di revocarlo se necessario.
In pratica, permette alle realtà di medie dimensioni di ottimizzare la capacità di individuare e gestire le credenziali privilegiate in azienda e di tenere traccia e verificare le sessioni privilegiate per rispettare i requisiti di conformità.

Dati sempre disponibili con il Multi-Cloud e il Cloud Data Management

Il Cloud Data Management, parte integrante dell'Intelligent Data Management, rende i dati sempre disponibili e gestiti centralmente

Albert Zammar - Vice President Southern EMEA Region di Veeam

Ci sono dei momenti che rappresentano un punto fermo per quanto concerne la fruizione ed il modo in cui si vede e si percepisce una tecnologia, e la sua utilità nel perseguire i propri obiettivi di business.

Il 2018 per il cloud computing è stato uno di quelli perché è entrato a far parte dell'Hype Cycle di Gartner. In quel momento il cloud ha smesso di costituire un argomento affrontato solamente da CIO e IT manager ed è diventato una tecnologia essenziale per qualsiasi tipologia di business, anche se solo in esame e non ancora implementata in azienda.

Va considerato che il modello Hype Cycle, termine anglosassone che è letteralmente traducibile in ciclo dell'esagerazione, è una metodologia sviluppata da Gartner per rappresentare graficamente il livello di maturità, di adozione e di applicazione di specifiche tecnologie.

Osservando l'Hype Cycle di Gartner per il data management si evidenziano una serie di tecnologie che sono caratterizzate da diversi livelli di conoscenza, rilevanza e importanza. Si parte dal DataOps e Machine Learning-Enabled Data Management, sino ad arrivare all'integrazione dei dati e all'archiviazione delle informazioni per proseguire verso quello che è riferito come il Plateau of Productivity.

E' uno scenario evolutivo in cui, mentre il cloud è ormai riconosciuto come uno standard per la realizzazione delle moderne infrastrutture IT, il data management sta tuttavia diventando sempre più importante per le aziende di qualsiasi settore e dimensione.

Questo perché le aziende hanno iniziato a comprendere appieno il valore dei dati in loro possesso. Il motivo è semplice e può essere sintetizzato nel fatto che poter accedere ai dati giusti nel momento giusto ed essere in grado di recuperarli quando vengono persi o sono danneggiati, può risultare determinante per il successo di un'azienda e il perseguimento dei suoi obiettivi di mercato e di business.

Il binomio Multi Cloud e Cloud Data Management

Se si osserva lo scenario del mercato globale quello che emerge è che si è in presenza di un'economia sempre più incentrata sul digitale e sui dati. E' un contesto in cui le aziende, indipendentemente dalla loro tipologia e dimensione, hanno bisogno di poter gestire i dati in ambienti multi-cloud e di poter garantire che siano protetti ovunque si trovino. La disponibilità dei dati è in sostanza fondamentale per consentire ai diversi team aziendali una gestione immediata e appropriata delle diverse situazione di business che via via si presentano.

E' a questo punto che interviene il Cloud Data Management, osserva Albert Zammar, Vice President Southern EMEA Region di Veeam. Tramite esso, come parte integrante dell'Intelligent Data Management, i dati possono essere sempre disponibili a livello di intera azienda, essere gestiti centralmente, nonché controllati e posizionati laddove possono costituire ed esprimere il massimo del loro reale valore.

Il Cloud Data Management report 2019 realizzato da Veeam, che ha coinvolto oltre 1.500 aziende leader a livello globale, ha in proposito evidenziato che quasi la metà (il 44% dei rispondenti) ritiene che la gestione dei dati sia fondamentale per il successo delle loro aziende nei prossimi due anni.

Tra le realtà che utilizzano il data management nel modo più efficiente emergono quattro elementi condivisi: il cloud, la consapevolezza, le capacità e la cultura. Vediamo in cosa si sostanziano questi condivisi e condivisibili elementi.

Cloud e scalabilità

Se si fa riferimento a statistiche della Commissione Europea emerge che oltre la metà delle aziende dell'Unione utilizza attualmente servizi avanzati di cloud computing per applicazioni software in ambito finanziario e contabile, per la gestione delle relazioni con i clienti tramite soluzioni di CRM o per applicazioni di classe Enterprise. E' una percentuale peraltro in aumento grazie alla stratificazione dei servizi a valore aggiunto che consente alle aziende di sfruttare l'intelligenza artificiale, l'apprendimento automatico, l'analisi dei big data, la ricerca vocale e di immagini per trarre il maggior valore commerciale possibile dai dati in loro possesso.

Questo concetto è sostanziato dal fatto che quasi i tre quarti (il 72%) delle aziende utilizzano il Cloud Data Management per consentire un utilizzo più intelligente dei dati all'interno di tutta l'azienda.

I business leader reputano poi che il data management permetta di ottenere benefici attraverso l'aumento della produttività, il mantenimento della stabilità aziendale e il miglioramento della capacità di prevedere e prendere le decisioni più adatte al contesto. La maggioranza ha anche dichiarato di utilizzare soluzioni Software as a Service (77%), citando l'affidabilità, la flessibilità e la sicurezza dei dati come i tre principali motivi.

Investimenti ponderati

Quello attuale è uno scenario che vede mutare la postura dei CIO all'interno dell'azienda e il loro status. I CIO devono ad esempio poter fare affidamento sull'infrastruttura IT e sulla sua capacità di aiutare le aziende ad essere reattive, pronte e in prima linea sul mercato. Ma incidenti come le interruzioni di servizio possono minare questa fiducia, ostacolare l'innovazione e danneggiare la percezione dell'azienda da parte dei clienti.

Quello che però emerge è che quasi tre quarti (il 73%) delle aziende dichiara di non essere in grado di rispondere alla richiesta degli utenti di avere un accesso ininterrotto alle applicazioni e ai dati. Questo spiega in parte perché solo il

25% dei business leader ha dichiarato di avere piena fiducia nella loro capacità di affrontare le sfide digitali.
Ma cosa è allora possibile fare al fine di consolidare e accrescere sia il proprio business che la fiducia in un'azienda da parte del mercato e dei clienti?
La risposta non può essere puramente tecnica ma bensì anche organizzativa e gestionale e quella che si evidenzia come una condizione sine qua non è investire in soluzioni affidabili, scalabili e flessibili atte a permettere di far fronte a problemi mission-critical quali il backup, il disaster recovery e la protezione dei dati.
A questo però serve integrare le giuste competenze e le capacità necessarie a gestire il patrimonio dati in modo corretto per l'implementazione di tecnologie in grado di creare un business più intelligente.

Fondere potenzialità tecnologiche e umane

Le aspettative di ciò che il data management può offrire all'azienda sono molto alte, così come lo sono la richiesta di un ritorno sull'investimento tecnologico. In sostanza, una volta implementate le nuove tecnologie, i business leader rispondenti al survey si aspettano di ottenere i primi benefici finanziari in nove mesi e quelli operativi in sette mesi.
La tecnologia, mette in guardia Zammar, è solo però una delle due facce della medaglia e di per sé non è sufficiente. Affinché i risultati possano essere visibili in un così breve tempo, le aziende devono anche assicurarsi di avere le competenze interne necessarie per potersi avvalere dei nuovi sistemi implementati.
La stragrande maggioranza (il 91%) delle aziende ritiene che le competenze digitali dei dipendenti siano vitali per il successo. Ma non è un obiettivo sempre facile da ottenere perché può richiedere a monte una trasformazione culturale, in particolare quando un'azienda sta cercando di stabilire dei processi decisionali che utilizzino i dati.

Una cultura basata sui dati e il cloud

Se si mettono a fattor comune i punti e le esigenze sopra analizzate, emerge che il cloud rappresenta un grande equilibratore per le aziende, un equilibratore in grado di eliminare il superfluo in termini tecnologici.
Nella maggior parte delle aziende, i dati sono generati ad una velocità enorme e come conseguenza c'è una grande attenzione su come questi dati devono essere gestiti, analizzati e utilizzati per facilitare il processo decisionale.
Un'azienda può produrre enormi quantità di dati, ma se il management stesso non adotta una cultura basata sui dati, può diventare un grave onere piuttosto che un vantaggio.
Più di due terzi (il 69%) dei business leader concorda ad esempio sul fatto che la cultura aziendale deve diventare più aperta e favorevole al cambiamento nel percorso di digital transformation, mentre il 93% è concorde sul fatto che anche l'atteggiamento della leadership dovrà cambiare.
Il Cloud Data Management rappresenta sotto questo aspetto una grande opportunità che deve essere però prima accettata ai livelli più alti dell'organizzazione per poi essere condivisa e implementata in tutta l'azienda.
In sintesi, costruire solide basi digitali incentrate sulla disponibilità dei dati è ritenuto essere vitale per il futuro di qualsiasi organizzazione.
Quello che ne consegue è che la tecnologia assume un ruolo estremamente importante per favorire il successo di un'azienda.
Solo combinando la tecnologia con una cultura aziendale basata sui dati, le aziende saranno in grado di massimizzare il valore derivante dai dati, così da permettere alla prossima generazione di innovatori del settore di scalare il mercato in modo sicuro.

I punti chiave delle reti del futuro

Reti virtualizzate e architetture evolute e overlay per il multi-cloud richiedono soluzioni innovative e una forte capacità progettuale

Luigi Meregalli - General Manager di CIE Telematica

Mentre il mondo del mobile si avvia verso il 5G, considerato a torto o a ragione come la panacea a tutti i problemi connessi ad applicazioni che richiedono sempre più capacità trasmissiva a causa della crescita esplosiva dei dati, è opportuno concentrarsi su quelle che sono le reti di comunicazione fisse e mobili che saranno alla base del cloud del futuro, come stanno evolvendo e quali sono le funzionalità e i dispositivi coinvolti affinché il servizio erogato soddisfi la qualità richiesta dagli utenti.

Il settore delle reti, spiega **Luigi Meregalli**, General Manager di CIE Telematica (www.cietelematica.it), è stato interessato negli anni recenti da un processo di profonda trasformazione. Le funzioni di rete si sono virtualizzate, così come i CPE (Customer Premises Equipment), le architetture sono evolute verso topologie di tipo Overlay, si è assistito alla separazione tra il livello di trasporto dei dati da quello della sua gestione, eccetera.

A questo si è sovrapposto il fattore IoT e la sua incarnazione industriale, IIoT, che ha aggiunto esigenze e problemi gestionali a una situazione già critica per i gestori alle prese con la trasformazione delle loro reti, o delle aziende in cui il ciclo di vita di quanto installato era oramai al termine, e in non pochi casi ben oltre.

Volendo essere pragmatici, tre sono i temi che possono essere considerati alla base delle infrastrutture di rete di nuova generazione, quelle per intenderci che abilitano virtualizzazione, Cloud, IIoT e nel complesso una ben programmata e soprattutto gestibile trasformazione digitale. Temi su cui in CIE abbiamo sviluppato una consolidata esperienza soprattutto in campi quali la Virtualizzazione delle funzioni di network, ICT e Iperconvergenza, Industrial IoT e sicurezza, performance monitoring e fiber monitoring, per citare i principali.

Esaminiamoli in dettaglio per capire meglio cosa implicano.

Industrial IoT e esigenze di sicurezza

L'importanza riconosciuta all'IIoT deriva da un semplice dato di fatto, abilita la digital transformation in diversi settori, dalle infrastrutture critiche alle città intelligenti, alle fabbriche. Il volume economico messo in moto è notevole e in costante crescita.

E' una vera e propria rivoluzione a livello sociale e nel mondo industriale che sta spostando l'at-

tenzione sulla maggiore efficienza, sulla sicurezza di reti e servizi, sui costi inferiori connessi all'utilizzo di dispositivi remoti intelligenti e su quanto reso possibile dall'analisi dei Big Data.
Le caratteristiche principali di una infrastruttura IIoT sono che si basa principalmente su trasporto di rete TCP/IP, fa ampio uso del Cloud, fruisce di Reti Multiservizio ed è Internet Enabled.
Per realizzare una infrastruttura IIoT servono quindi diversi apparati situati nei suoi punti critici, di raccolta dati, di convogliamento e di gestione, in grado di assicurare :

- Il supporto di Media Differenti quali Fibra, Rame, Radio, Microwave
- Il supporto di ambienti Legacy dal livello L1 a L3
- Il trasporto TDM, CE, MPLS, IP
- La gestione via NMS
- Una sicurezza che si esprima in profondità e che sia distribuita e globale

A livello di ingegneria, progettazione, installazione e supporto sono soluzioni, spiega Meregalli, che possono ad esempio essere realizzate tramite apparati di rete quali switch e router industriali SecFlow, piattaforme per reti multi servizio Megaplex , piattaforme di aggregazione, servizi di sicurezza e una gestione centralizzata tramite RADview. A questo si aggiungono per l'IIoT apparati di IIoT Backhaul con connettività sicura su base end-to-eEnd, di data usability basate su gateway IIoT, di cyber security e soluzioni atte a garantire la raggiungibilità del servizio. E' quindi una realtà complessa che richiede un approccio progettuale di alto livello.

La virtualizzazione delle funzioni di rete

Un secondo punto è costituito dalle reti di accesso fisse e mobili e della loro virtualizzazione funzionale in linea con le evoluzioni più recenti. " … il termine virtualizzazione si riferisce alla possibilità di astrarre le componenti hardware, cioè fisiche, degli elaboratori al fine di renderle disponibili al software in forma di risorsa virtuale" si legge su Wikipedia.
Tradotto nel pratico, vuol dire che tramite la virtualizzazione ci si aspetta di poter migliorare scalabilità e prestazioni di un ambiente ICT, accelerare il rilascio di nuovi servizi o il loro aggiornamento, ridurre costi e evitare il vendor lock-in e, non ultimo, abilitare nuove fonti di reddito e servizi gestiti.
Va detto che il concetto è vecchio come l'IT stesso perché i primi elaboratori IBM a cui si collegavano dispositivi su linee multi punto vi facevano ampiamente ricorso.
La novità dell'oggi e del domani è che ora il concetto si applica in modo distribuito in tutti o quasi gli ambiti dell'ICT, dallo smartphone ai router, dagli IP-PBX ai load balancer.
La cosa è resa possibile dall'apparire sul mercato di nuovi modelli di CPE in grado di fornire multiple funzioni virtualizzate su di una piattaforma hardware comune. E' quello che viene chiamato uCPE, ovverosia universal CPE, che semplifica la convergenza di Value Added Services Network e IT sullo stesso hardware di base.
Quattro sono gli elementi chiave che rendono possibile una tale soluzione: white Box (uCPE),il sistema operativo, Virtual Network Functions (VNFs), Domain Orchestrator.
Le soluzioni, e i relativi dispositivi, che si rivelano necessarie per mettere in campo reti altamente virtualizzate e gestirle devono permettere, osserva Meregalli, di realizzare ad esempio uno strato di accesso a dorsali SDH/RFI tramite un dispositivo centrale collegato all'anello a standard quali l'STM-1 e dispositivi periferici collegati ad un anello a 2 Mbit a cui deve essere possibile accedere con varie modalità.
Un altro esempio di reti coinvolte nella virtualizzazione delle funzioni consiste in una rete Wi Fi per Smart City dove si devono collegare cen-

tinaia di siti o migliaia di Access Point. Sono realizzazioni che richiedono l'utilizzo di switch di tipo industriale PoE e Media Converter, e dove ai loro dispositivi di accesso periferico si devono poter collegare, come sempre più e in modo diffuso avviene, videocamere per il controllo del territorio e accessi WiFi pubblici.

Il monitoraggio dei servizi

Un terzo punto è che la complessità delle attuali reti ad alta virtualizzazione funzionale e la distribuzione sul territorio dei punti di accesso, come nel caso di dispositivi IoT, ha fatto emergere e porre in primo piano da parte degli addetti tecnici anche il problema del loro monitoraggio centralizzato.

Tradotto in pratica, quello che serve sono strumenti che permettano di realizzare analisi in tempo reale, ridurre l'MTTR e i costi operativi e, non ultimo, servono protocolli standard per la verifica degli SLA.

Tipicamente una soluzione prevede 4 livelli di intervento:

- L3 e L3+: Monitoraggio a livello di rete (pacchetti) e a livello sicurezza (IPS/IDS)
- L2: Monitoraggio a livello di rete (pacchetti)
- L1: Monitoraggio a livello fisico (fibra ottica)

Sotto il profilo architetturale il monitoraggio avviene tramite una rete overlay che si cala su quella di cui si devono controllare i parametri funzionali e che opera a livello più alto dell'infrastruttura raccogliendo i dati necessari e inviandoli al centro di controllo.

Tramite le soluzioni disponibili sul mercato è possibile ad esempio realizzare il monitoraggio delle prestazioni su reti L2 e L3, il monitoraggio di specifici segmenti di rete, il monitoraggio di servizi di tipo Legacy su reti IP e servizi MEF e PM per applicazioni wholesale.

Le possibilità che si offrono sono indubbiamente molte, cosa che però non rende facile la scelta per chi non nutra nel campo una solida esperienza realizzativa.

Come proteggere reti aziendali e cloud da attacchi Bot

Il traffico Internet è costituito per il 52% da Bot. Radware BOT Manager supporta le aziende nella protezione delle applicazioni aziendali e dei dispositivi

Nicola Cavallina - Channel and Alliance manager Italia, Grecia e Malta di Radware

Nel processo di trasformazione digitale le applicazioni sono cruciali per il successo del business e devono di conseguenza essere sempre accessibili da parte dei clienti.

Il negare questo accesso è però quello che invece si prefiggono i malintenzionati che utilizzano attacchi di tipo Botnet, ovverossia una rete controllata da un hacker composta da dispositivi di proprietari ignari infettati da malware specializzato, detti Bot. Tramite i computer infettati possono essere avviati attacchi a siti web, noti come Distributed Denial of Service (DDoS), subissandoli di richieste che ne rallentano di molto i tempi di risposta , molto spesso confondendosi alle richieste lecite o simulandole .

L'importanza del contrastare efficacemente attacchi DDoS e Botnet sta nella analisi comportamentale basata su AI, Machine Learning, e Big Data, evidenzia Nicola Cavallina, Channel Manager and Alliance Manager Italy, Greece, Malta di Radware (www.radware.com), società di livello mondiale specializzata nelle soluzioni per la security di reti e applicazioni, il cui portfolio Soluzioni è stato inserito ed integrato anche nell'offerta della società americana CISCO.

I dati di una recente ricerca Forrester hanno ad esempio rivelato che il traffico su Internet è per il 52% costituito da Bot e solo per il 48% dovuto ad agenti umani. Non tutto il traffico Bot è malevolo, ma lo è circa il 26%, in pratica un quarto del traffico Internet. E in 4 casi su 5 il fornitore dei servizi non è in grado di identificare il traffico malevolo da quello legittimo.

Tra i tipi di attacchi Bot più comuni vi sono ad esempio quelli riferiti come Web Scraping (utilizzato per estrarre dati da un sito web), Denial of Inventory (utilizzato per bloccare la disponibilità di beni, presenti a magazzino, senza completarne l'acquisto), per arrivare all'Account Takeover (che permette all'attaccante di ottenere beni o servizi utilizzando l'account di un ignaro cliente).

Il rischio connesso a tali attacchi è enfatizzato dallo sviluppo stesso della tecnologia e dal fatto che possono fare leva sulla diffusione di siti web, di App mobile e di API

Ma cosa serve per rispondere efficacemente a questo aumento continuo delle minacce?

«Quello che serve - osserva Cavallina - è una soluzione che permetta di individuare e bloccare i diversi tipi di attacchi, provenienti dai diversi canali disponibili per un malintenzionato, ma che allo stesso tempo riduca al minimo i falsi positivi».

Radware BOT Manager

Una risposta alle esigenze sopra evidenziate è quella che ha dato Radware sviluppando Radware BOT Manager, una soluzione che permette di perseguire quattro obiettivi fondamentali nella protezione delle applicazioni aziendali e dei propri siti Web.
Il primo è la protezione da tutti gli attacchi provenienti dai diversi canali esistenti.
Il secondo è costituito dal blocco proattivo e automatizzato degli attacchi tramite modelli di analisi e apprendimento in profondità e di tipo "semi supervised" del loro comportamento.
Il terzo è l'allestimento di un ampio Database delle impronte di Bot mediante attività di intelligence realizzate con i dati raccolti da migliaia di sorgenti.
Infine, il quarto è costituito da opzioni di installazione delle difese di tipo non intrusivo attuate mediante API che non hanno impatto sullo stack di tecnologie installate.
L'approccio "semi supervised" descritto ha l'obiettivo di combinare il meglio delle caratteristiche delle tecnologie di machine learning supervisionate con quelle non supervisionate, e di ottenere una elevata precisione per quanto riguarda il rischio di incorrere in falsi positivi o negativi.
Peraltro, ha osservato Cavallina, un ulteriore obiettivo perseguito nello sviluppo della soluzione è stato la ampiezza delle possibilità a livello di sua installazione, che comprendono il Reverse Proxing, l'Out-of-Path e il Cloud Service.
Ma quelli che si evidenziano come punti di interesse sono anche altri. BOT Manager è stato progettato anche per operare congiuntamente con l'intero portfolio di soluzioni Radware per la sicurezza e in primis i servizi Cloud, tramite la sua integrazione con Cloud WAF (Web Application Firewall).
A questa interoperabilità si aggiunge quella con le soluzioni per mitigare gli attacchi tramite la condivisione e la sincronizzazione delle attività di intelligence.
Di particolare utilità pratica è l'integrazione con Cloud WAF, realizzata tramite dashboard e widget che evidenziano graficamente il traffico Bot in corso, i diversi tipi di Bot e la geo mappa dei Bot stessi.
Per le aziende che non dispongono di personale specializzato o che sono orientate ad esternalizzare il servizio di security è disponibile anche il servizio gestito di Cloud Security, un servizio di classe Enterprise che mira a proteggere da attacchi multi vettore ed a ottimizzare le prestazioni delle applicazioni.
Al rilascio della soluzione di Bot Manager ha fatto seguire quello di Bot Analyzer, un servizio di valutazione gratuita per ambienti business che possono essere soggetti ad attacchi Bot e per gli utilizzatori che desiderano disporre di una miglior comprensione dell'impatto che Bot di tipo malevolo possono avere sulla loro organizzazione.
Lo strumento è di ausilio in particolare nel dimostrare l'esigenza di disporre di una evoluta soluzione di Bot Manager che faccia leva su processi di analisi in grado di mettere a disposizione analisi dettagliate entro le 48 ore.

La network security di Trend Micro a portata di mano con il cloud

La soluzione fruibile tramite AWS supporta le aziende indirizzando le esigenze di sicurezza di rete quando si migrano le applicazioni sul cloud

Steve Quane - Trend Micro

Trend Micro, tra i principali attori nella cyber security, per rispondere alle sfide operative che le aziende sperimentano con le soluzioni attuali di network security, ha annunciato di aver esteso la propria protezione anche al cloud. Disponibile all'interno del marketplace Amazon Web Services (AWS), la soluzione sarà inizialmente disponibile per AWS Transit Gateway e più avanti saranno disponibili anche altri modelli di fruizione.

«La cloud security è la priorità maggiore per AWS e ci impegniamo per aiutare i nostri clienti a raggiungere i livelli più alti di sicurezza nel cloud. Nel momento in cui le aziende spostano l'infrastruttura nel cloud, hanno bisogno di inserire e gestire facilmente la security all'interno delle reti. Attraverso AWS Transit Gateway, la soluzioni di sicurezza Trend Micro è ora disponibile per i 230.000 clienti del marketplace AWS e consentirà di rispondere alle esigenze di sicurezza nel cloud», ha commentato **Dave Brown**, Vice President, EC2 Compute&Networking Services di Amazon Web Services.

La soluzione, ha spiegato l'azienda, è stata pensata per soddisfare le esigenze di chi deve estendere la security al cloud, utilizzando le caratteristiche di AWS Transit Gateway, che semplifica il routing tra Amazon Virtual Private Clouds (Amazon VPCs) e le reti on-premises. In pratica, agendo come un hub che controlla il routing del traffico.

«I clienti ci raccontano di scontrarsi con ostacoli operativi significativi, se consideriamo l'odierno approccio alla cloud network security basato su firewall - ha spiegato **Steve Quane**, executive vice president of network defense and hybrid cloud security di Trend Micro -. Questo approccio presenta complessità operative ed è inefficiente, a causa delle complesse richieste di networking nel cloud. La strategia di Trend Micro supera queste sfide operative. Grazie a un deployment trasparente nella fabric di rete, permette una security scalabile e una visibilità continua, eliminando la necessità di riprogettazione ed evitando la disruption delle applicazioni».

Come accennato la Trend Micro Cloud Network Protection è disponibile all'interno del marketplace AWS. La soluzione sfrutta peraltro il potenziale di Trend Micro Research, incluso il bug bounty program della Zero Day Initive (ZDI) che rileva gli attacchi mirati, le vulnerabilità e gli exploit, integrandosi facilmente con gli strumenti di sicurezza.

Con Sirti rete e security a misura di multi-cloud

Sirti consolida la posizione nelle reti e servizi Telco e rafforza il portfolio per la digital transformation e la cyber security con Wellcomm e progetti suggeriti dai dipendenti

Roberto Loiola - AD di Sirti

Quando si parla di Cloud ci si concentra sovente su quello che viene riferito come SaaS, e cioè il software fruito come servizio. Si dimentica così che l'accesso alle applicazioni deve avvenire rapidamente e in modo sicuro, soprattutto quando si tratta di interconnettere data center tra cui movimentare i dati, realizzare procedure di restore o di backup o semplicemente effettuare transazioni che presentino un elevato grado di riservatezza. E' questo il caso del mondo finance, della sanità o della difesa, senza poi trascurare quanto afferente ali dispositivi IoT e IIoT di aziende di servizi pubblici come nel caso dell'energia.

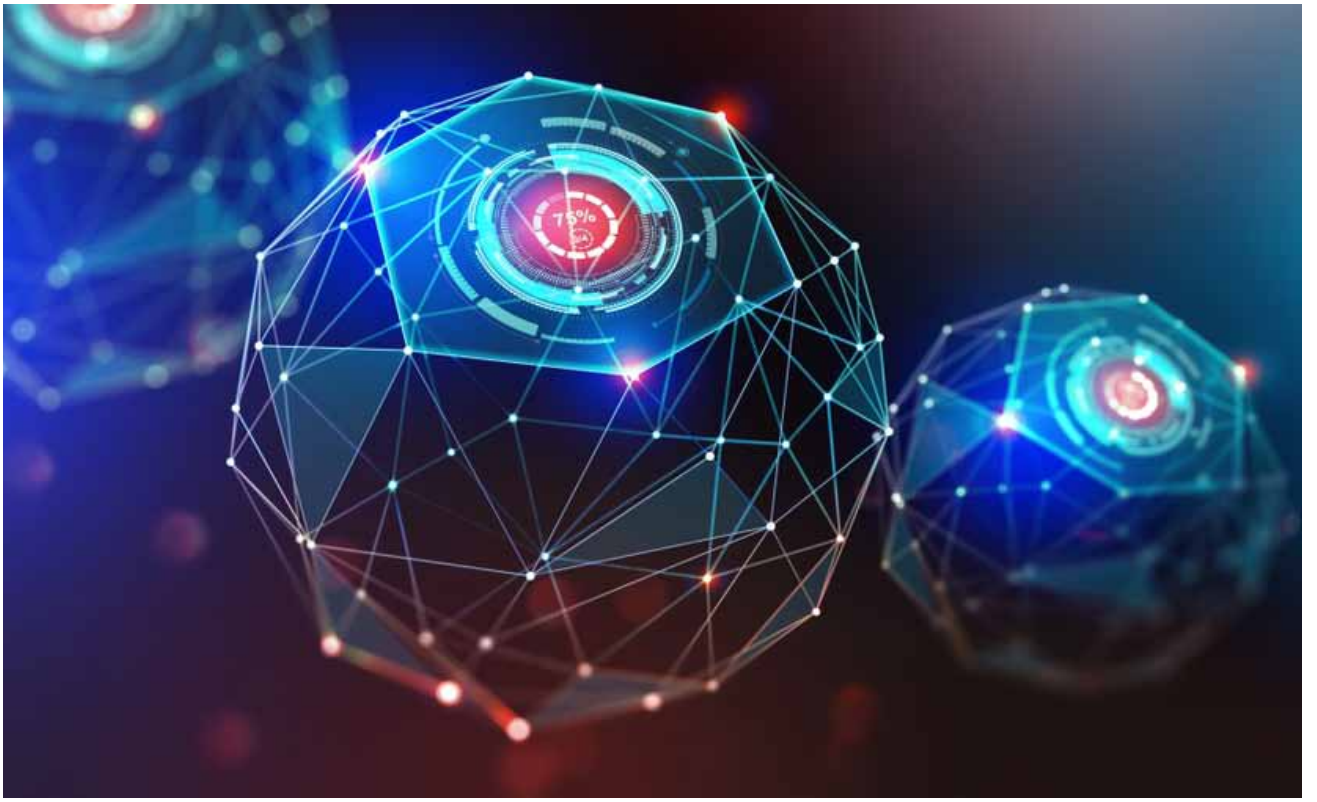
Quello delle reti ad alte prestazioni e con un elevato grado di sicurezza adatte per il supporto del nuovo modo di gestire i dati è uno dei settori su cui è impegnata Sirti, società che è stata una delle pioniere in Italia nella realizzazione delle infrastrutture di rete pubblica e privata, ora partecipata al 100% da Pillarstone e guidata da Roberto Loiola, e che, proprio per fornire infrastrutture altamente sicure, ha acquisito di recente Wellcomm Engineering, società specializzata nella cyber security e nelle soluzioni digitali.

L'acquisizione di Wellcomm è giunta dopo un anno, il 2018, che ha rappresentato per Sirti un anno di profonda trasformazione, con risultati in miglioramento rispetto al precedente esercizio nonostante i grandi cambiamenti strutturali e la forte competizione che da anni stanno interessando il mercato delle telecomunicazioni.

Se ha consolidato la propria posizione nel settore "Telco Infrastructures", con il coinvolgimento nella realizzazione della rete a Banda Ultralarga per Open Fiber e contratti pluriennali per la manutenzione e costruzione delle reti di accesso e di trasporto con operatori primari, è però nel settore digitale che ha maggiormente esteso il suo coinvolgimento, dove a consuntivo ha ottenuto nuovi ordini e ricavi per circa 130 milioni di euro con una crescita superiore al 10% anno su anno.

Alla base di questo risultato, ha spiegato l'azienda, c'è stata la forte crescita e differenziazione del business nei comparti Utilities, Large Enterprise e PA.

Nel corso del 2018 ha però, come evidenziato, intensificato lo sviluppo di competenze e l'assunzione di nuove energie negli ambiti tecno-



logici più rilevanti della digital transformation quali hybrid cloud, edge computing, network function virtualization, software defined networking e la citata cyber security.
Nella security, ha portato a termine l'acquisizione di Wellcomm Engineering, azienda con sede a Milano e specializzata in soluzioni e servizi di Cyber Security, con importanti Clienti in ambito Finance, Insurance e Industry. L'acquisizione, conclusa ad aprile 2019, rappresenta per Sirti una vera e propria pietra miliare per lo sviluppo del portafoglio di soluzioni digitali.
«La progressiva digitalizzazione dell'offerta per Sirti consentirà di consolidare ulteriormente la propria leadership di mercato. Grazie alla digitalizzazione coniugata alla propria capacità operativa, il Gruppo Sirti potrà cogliere meglio di altri le opportunità su mercati contraddistinti da tecnologie sempre più capillari sul territorio e in grande trasformazione», ha evidenziato R**oberto Loiola**, Amministratore Delegato di Sirti.
La strategia dell'azienda, in contemporanea all'impegno nei suoi diversi settori, ha puntato sullo sviluppo di un portfolio di soluzioni End-to-End rinnovato in modo che ognuna delle quattro Business Unit sia allo stesso tempo auto-sostenibile nella gestione del business, ma anche in grado di alimentare sinergie e maggiore valore aggiunto per i clienti in caso di progetti complessi e multi-disciplinari.
Un elemento chiave della strategia è il presidio dell'intero ciclo di vita delle infrastrutture tecnologiche e digitali, e la capacità di erogare Managed Services a partire dai due Operations Control Center attivi h24/7 su Milano e Roma.

Il rafforzamento nella Cyber Security

Come evidenziato, prima dell'estate Sirti ha annunciato l'acquisizione di Wellcomm Engineering, società molto attiva nel mercato italiano in ambito Cyber Security.
L'operazione si è inserita nella strategia di rafforzamento e sviluppo del posizionamento del Gruppo Sirti, è ha portato ad un potenziamento del portafoglio di offerta nei segmenti di mercato in cui opera la Business Unit Digital Solutions e aperto all'azienda nuove prospettive di mercato nei settori Finance e Industry.
«Il portafoglio della Business Unit Digital Solution di Sirti si arricchisce di solide competenze e tecnologie in ambito Cyber Security, grazie a questa operazione. La forte complementarietà tra le aziende consente di amplificare la nostra capacità di generare valore per i nostri clienti attraverso soluzioni e servizi ad alto contenuto tecnologico», ha commentato **Benedetto Di Salvo**, Vice President della Business Unit Digital Solutions di Sirti.

Imprenditivity per la Open Innovation

Subito dopo l'estate Sirti ha dato il via a IMPRENDITIVITY, un progetto suddiviso in due fasi. La prima fase ha visto il coinvolgimento di tutti i dipendenti dell'azienda in un contest creativo durante il quale sono state selezionate le idee più innovative proposte dai dipendenti in grado di creare valore per l'azienda risolvendo problemi reali o abilitando a nuove opportunità di business.
Con la seconda fase ora in corso, attraverso un approccio di Open Innovation, è stato aperto un bando di gara per la realizzazione delle challenge selezionate.
In pratica, dalle 5 idee più interessanti emerse, sono nate altrettante challenge che alimenteranno la seconda fase del programma.
A questo punto saranno startup e PMI a ricoprire un ruolo da protagonista, ma senza dimenticare gli "inventori", ovvero, i dipendenti Sirti che, con le loro idee, hanno contribuito alla generazione delle 5 challenge e di cui il programma prevede un ruolo attivo fino al termine del ciclo di innovazione.
«Per Sirti l'innovazione è sempre stata una sfida continua, motore per il rinnovamento di competenze e capacità operative, ed elemento cardine della propria competitività. Oggi l'innovazione è un processo pervasivo e si fa in rete, condividendo in logica aperta problemi e soluzioni con clienti, partners tecnologici e startups, anche mettendo in comunicazione filiere industriali appartenenti a settori diversi. Per questo motivo abbiamo lanciato IMPRENDITIVITY, un contest creativo volto a coinvolgere nel processo di innovazione tutta l'azienda e ad aprire le porte alle virtuose collaborazioni con le startup e PMI», ha commentato **Pietro Urbano Mimmo**, Vice President Innovation & Communication di Sirti.