Cloud & Business

n.85
Ottobre 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

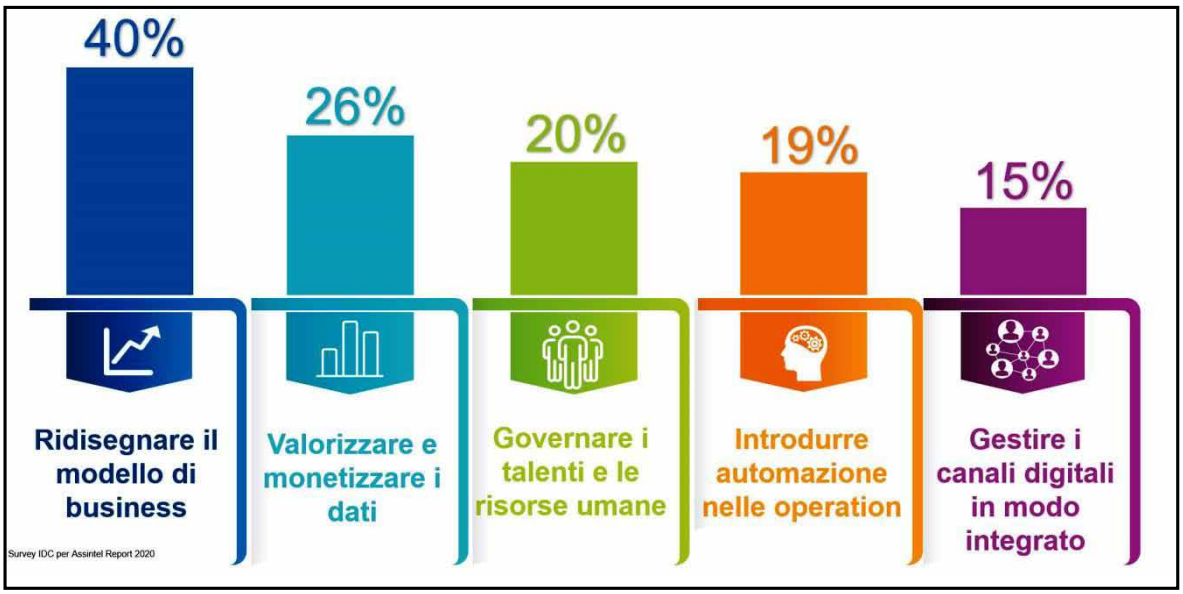
L'IT italiana raddoppia nonostante un PIL che non brilla

di Giuseppe Saccardi

Assintel Report 2020: l'Information Technology raddoppia la crescita nonostante la stagnazione del PIL. Trainano le tecnologie per la Trasformazione Digitale

Nonostante uno scenario generale in stagnazione a cui sembra difficile, con il solito gioco dei rimpalli di responsabilità, porre un tempestivo rimedio, nel 2019 il mercato dell'Information Technology italiano ha raddoppiato la crescita rispetto al 2018 ed ora vale oltre 24,2 miliardi di euro. Un rispettabilissimo, visti i tempi,+3,8% rispetto allo scorso anno. Questo trend, osserva Assintel, è

Reportec Cloud&Business - Numero 85 - Ottobre 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



Gli ambiti principali della trasformazione digitale (fonte IDC - Assintel)

previsto consolidarsi anche negli anni a venire con una crescita complessiva degli investimenti IT per il periodo 2018-2022 stimato essere pari al +2,6% (CAGR).

La crescita però non è omogenea. A questi numeri positivi fa da contrappeso (negativo) la costante flessione del comparto TLC (-2,7%), che porta come risultato il settore ICT complessivamente a crescere solo, si fa per dire, del +2,3% nel 2019, superando i 31 miliardi di euro.

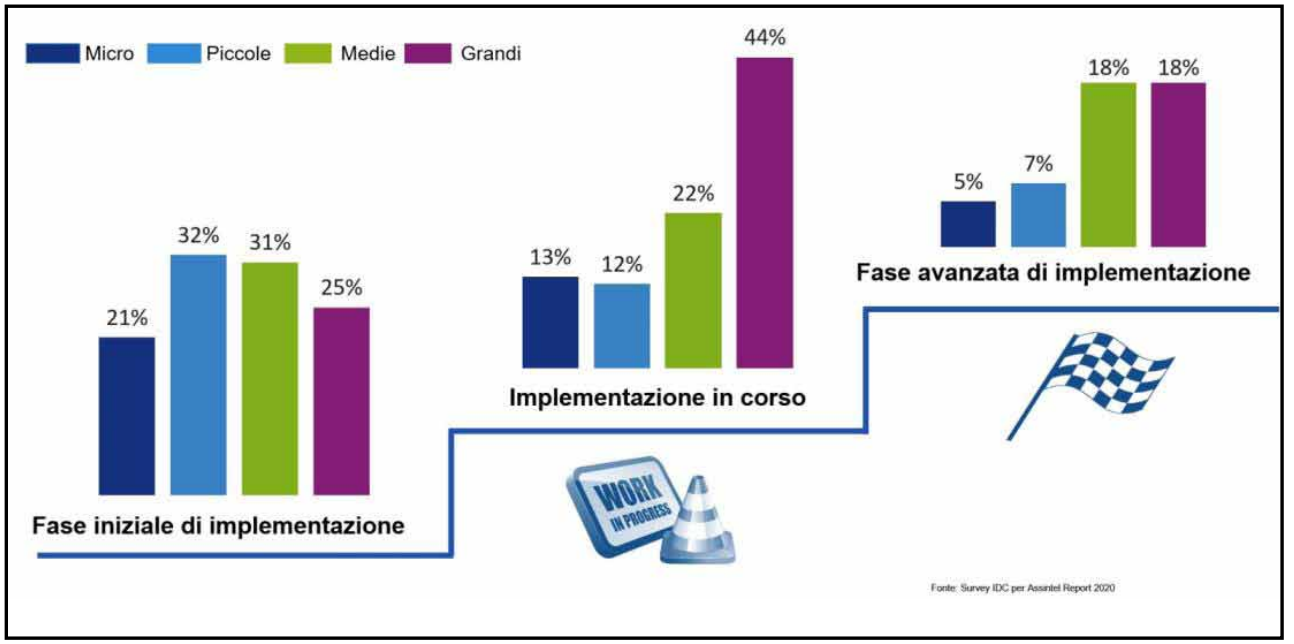
Il comparto software cresce del +5,7%, torna in positivo l'hardware a +6,2%, cresce in misura minore il settore Servizi IT +1,4%.

Quella che traina la spesa è la componente riferibile ai progetti di Trasformazione Digitale.

Tra le tecnologie emergenti, invece, a crescere esponenzialmente negli investimenti delle imprese italiane sono l'Internet of Things (+24%), l'Intelligenza Artificiale (+39,1%), le soluzioni di Realtà Aumentate e Virtuale (+160,5%) e i dispositivi Wearable (+116,2%).

Continua anche la crescita dei "pillar" della Terza Piattaforma, con la spesa aziendale italiana in servizi Public Cloud che cresce del +26,1% e le soluzioni Big Data & Analytics del +7,6%.

Sono questi i principali dati che emergono dalla presentazione del nuovo Assintel Report, la ricerca sul mercato ICT e Digitale in Italia, realizzato da Assintel, Associazione Nazionale delle Imprese ICT e Digitali, con CFMT – Centro di Formazione Management del Terziario - insieme alla società di ricerca indipendente IDC Italia. «La sfida per la community ICT è quella di guidare la trasformazione digitale, mettendosi davvero in gioco. Al suo interno, riscrivendo i propri modelli di business, e verso l'esterno, facendosi driver culturale verso il sistema delle imprese e della Pubblica Amministrazione. Vedo l'associazione come un treno super tecnologico che deve via via accogliere viaggiatori sempre più consapevoli, io mi sento come il binario sul quale esso viaggia ad altissima velocità» ha osservato **Paola Generali**, neo-eletta Presidente Assintel.



Le fasi della trasformazione digitale (fonte IDC - Assintel)

I trend di investimento delle aziende

Dalla ricerca, realizzata su oltre 1.000 aziende utenti nazionali, emerge un quadro positivo di crescita degli investimenti IT nel 2020: oltre il 16% delle imprese italiane prevede di espandere il budget nel 2020, mentre soltanto il 10% sta considerando l'eventualità di procedere a una razionalizzazione e a una riduzione complessiva delle spese.

A trascinare l'espansione sono le medie e grandi Imprese: il 25% delle Medie Imprese e il 23% delle Grandi Imprese intendono incrementare la spesa nel corso dei prossimi 12 mesi, in alcuni casi anche al di sopra del 20% (circa il 2%). A comprimere la spesa nell'anno a venire sono soprattutto le Micro e le Piccole Imprese, rispettivamente il 10 e il 7%.

Tra le aree geografiche che prevedono di ampliare il budget ICT nei prossimi 12 mesi, il Nord Ovest guida come numero complessivo di imprese (circa 39%), seguito dalle regioni del Sud e delle Isole (34%).

Alcuni settori sono particolarmente positivi nelle previsioni: quasi il 30% dell'Industria prevede di espandere il budget ICT almeno a singola cifra, oltre il 4% di PA, Sanità e Istruzione intravede una crescita a doppia cifra.

Maggiore cautela invece è espressa da parte del Commercio, dove quasi il 18% delle imprese prevede una riduzione dei budget per il prossimo anno.

«In Italia, le imprese determinate a cogliere i vantaggi del digitale stanno puntando soprattutto sul ridisegno del modello di business e sulla valorizzazione dei dati. Se questo pone il nostro Paese in linea con i trend di Trasformazione Digitale europei e più in generale mondiali, occorre purtroppo evidenziare come la velocità del cambiamento non sia ancora uniforme lungo tutto il tessuto industriale nazionale: l'Italia appare ancora spaccata in due, in base alle dimensioni aziendali» ha commentato **Daniela Rao**, senior research & consulting director di IDC Italia.

La sicurezza nel cloud e nel multicloud inizia dalla rete

La proposta di Sirti si arricchisce grazie alla recente acquisizione di Wellcomm Engineering, per favorire la trasformazione digitale e la migrazione verso il cloud

Benedetto Di Salvo, Vice President Digital Solutions di Sirti e Chairman di Wellcomm Engineering

In Sirti affrontiamo il tema del cloud, e ancor più del cloud ibrido o del multi cloud, in modo pragmatico e lo facciamo con chi realizza infrastrutture tecnologiche complesse ed utilizza il cloud per portare valore ai propri clienti in termini di qualità dei servizi, sicurezza e ottimizzazione dei costi. Sulla base delle esperienze di successo fin qui maturate, possiamo affermare che l'evoluzione delle reti di comunicazione verso architetture in grado di garantire agilità, flessibilità e sicurezza, costituisce la condizione necessaria per poter rispondere ai bisogni dei clienti, siano essi pubblici o privati.

Le soluzioni SD-WAN costituiscono l'elemento chiave per la realizzazione di questa tipologia di architetture, in quanto sono in grado di distribuire il traffico in modo dinamico su più reti con caratteristiche tecnologiche diverse.

In questo quadro evolutivo il valore aggiunto di Sirti Digital Solutions consiste nel realizzare reti intelligenti che sappiano auto-adattarsi alle esigenze di chi le gestisce e di chi le utilizza, e che sappiano individuare percorsi ottimali, con l'obiettivo di offrire la migliore quality of experience agli utenti.

Stiamo poi vivendo una trasformazione caratterizzata da una domanda di nuovi modelli di servizio con una crescita esponenziale e trasversale ai vari mercati, quali ad esempio Telco, Industries, Utilities, PA e Finance. A questi aspetti si aggiunge anche un vero e proprio cambiamento nella modalità con cui i dati sono correlati alle infrastrutture, oltre al fatto che i dati stessi non risiedono più in un unico centro, ma in più centri distribuiti anche su scala mondiale. Per questo motivo una rete efficiente, flessibile e virtualizzata deve anche garantire la sicurezza e l'integrità del dato su base end to end.

Per rispondere a questo tipo di domanda, la proposta di Sirti si è arricchita di nuove soluzioni digitali grazie alla recente acquisizione di Wellcomm Engineering, che ci permette di realizzare infrastrutture tecnologiche evolute e sicure atte a favorire la trasformazione digitale e la migrazione verso il cloud.

Governare, e gestire in maniera integrata questa trasformazione così complessa e dove le reti IoT sono parte delle evoluzioni fin qui descritte, con gli stessi principi di flessibilità, agilità, automazione e sicurezza rappresenta la grande sfida per Sirti e Wellcomm Engineering.

Il valore aggiunto di Sirti e Wellcomm in questo contesto è proprio quello di supportare il cliente nell'analisi, nella progettazione, nella realizzazione e nella manutenzione evolutiva e predittiva di tutti gli elementi che compongono la filiera tecnologica di un progetto complesso IoT con una presenza massiva di sensori, connettività, piattaforme, applicazioni ed il problema sicurezza.
La capacità di garantire una copertura completa, distribuita, sostenibile e di assicurare un livello di sicurezza adeguato, specie nell'ultimo miglio, nella tratta che va dal dispositivo al primo livello di aggregazione, è un elemento distintivo per noi, poiché siamo presenti, in modo capillare, su tutto il territorio nazionale.

Vincenzo De Lisi, CIO di Sirti

Efficienza e sicurezza: la chiave verso il cloud

Nell'analizzare il fenomeno correlato alla crescente adozione del cloud, la domanda che viene spontanea porsi è "cui prodest?".
La risposta, pur con i necessari distinguo, è che innanzitutto il cloud aiuta molto le aziende di dimensione medie o medio piccole, e cioè tutte quelle aziende che non dispongono di un IT interno importante. Di certo poi, la diffusione del fenomeno cloud è dettato anche dall'ottimizzazione dei costi che è in grado di apportare. Se poi si passa ad esaminare più in dettaglio quelli che possono essere considerati i driver del cloud, tra questi si può sicuramente annoverare il consolidamento delle reti, il fatto di poter risparmiare nelle connessioni e disporre di uno SLA migliore di quello che possono offrire le linee dedicate, ma soprattutto di non avere il vincolo della scalabilità di un progetto o delle piattaforme e di una maggiore adattabilità in funzione delle esigenze del momento e del budget. Ma il cloud è anche standardizzazione dei processi e dei modelli operativi con applicazioni semplici ed evolute.
Infatti, se ci focalizziamo sui primi driver, il cloud lo possiamo declinare nei modelli IaaS (Infrastructure as a service) e PaaS (Platform as a Service).
Questi modelli, ognuno ad un livello diverso, abilitano sia i processi di innovazione con architetture a microservizi o serverless, che processi di application modernization permettendo di trasformare un'architettura legacy in una nuova "Cloud Native" in diversi passi.
Sul tema applicativo, il SaaS è una rivoluzione per un'azienda o anche il solo dipartimento IT. L'utilizzo di piattaforme SaaS permette infatti, di poter applicare in azienda processi standard di mercato che abilitano una trasformazione dei processi core.
Non solo, la nostra esperienza di strategia "Cloud First", ci ha consentito di standardizzare modelli operativi e garantire applicazioni sempre disponibili, scalabili in base alle richieste, con un paradigma Mobile First e sempre aggiornate.
Quest'ultima caratteristica supera il vincolo tipico dei progetti di "Upgrade di Release", che ha caratterizzato gli anni 2000, con enormi soluzioni custom sviluppate su prodotti di mercato sovente in end-of-support.

Il fattore sicurezza

Le aziende italiane, dal Finance alla GDO, hanno iniziato ad approcciare il cloud partendo dalle applicazioni di disaster recovery e spostando, in parte o in toto, gli applicativi dal data center al cloud con un utilizzo in modalità "As-a-Service".
Questa trasformazione digitale ha impattato sen-

sibilmente sui processi dell'IT, sulle applicazioni native, spesso mission critical per l'azienda, sia in termini di performance che di continuità del servizio.
Ci sono inoltre altri due aspetti rilevanti da considerare: quello tecnologico, che impatta sulla sicurezza, e quello normativo, più complesso, perché dipende dal settore al quale l'azienda appartiene.
Un ulteriore ed importante elemento è la cultura, in ambito security, del Management nell'applicare quelle "regole di Security" che offrano il massimo grado di sicurezza pur mantenendo performance applicative ad ottimi livelli e garantendo un aumento della competitività dell'azienda.

Nino Marsanasco, CEO di Wellcomm Engineering

L'aspetto tecnologico

Quando parliamo di cloud lo scenario si complica perché ci si riferisce ad un perimetro non definito e spesso ci si ritrova ad affrontare quotidianamente il problema di mettere in sicurezza i flussi di informazioni, spesso sensibili, che transitano da un client remoto (pc, smartphone, tablet o altro) che accede ad un'applicazione installata in un'area estranea al perimetro dell'azienda.
Il transito dei dati, da e verso il cloud, spesso non è soggetto alle policy di sicurezza applicate all'interno della rete aziendale, entrando così in un'area di alto rischio.
I Manager IT sono coloro che vivono più da vicino questo problema, in quanto l'esigenza , sempre più diffusa di esternalizzare il più possibile le applicazioni (per garantirne un efficientamento, affidabilità e scalabilità) spesso si contrappone alla necessità di garantire un livello di sicurezza che sia in linea con le policy aziendali.
Un altro tema importante per l'IT Manager è la scalabilità, in quanto offre la flessibilità desiderata sia in termini di modifiche che di espansione della propria rete. Le risorse fisiche, logiche ed applicative diventano "liquide", ovvero è possibile usufruirne da qualsiasi punto della rete, indipendentemente da dove queste risiedano.
Per rispondere a queste nuove esigenze ormai alla portata di tutti i settori industriali, sono indispensabili soluzioni di cyber security operanti a 360° che permettano di rendere sicuro l'ambiente IT e cloud a livello end-to-end, dall'utente all'applicativo.
La possibilità di poter offrire soluzioni che mettono a fattor comune il portfolio di offerta di Sirti con quello di Wellcomm Engineering ci permette di identificare le migliori soluzioni tecnologiche disponibili sul mercato e di gestire progetti complessi e distribuiti. E' una collaborazione virtuosa tra chi progetta, realizza, trasforma e manutiene reti e tra chi dispone di soluzioni di cybersecurity in grado di mettere in sicurezza le reti.

L'aspetto normativo

Il fattore normativo, non è meno complesso di quello tecnologico quando si parla di cybersecurity. Chiaramente l'incidenza di quest'ultimo aspetto cambia a seconda del settore in cui si opera, pensiamo all'ambito finanziario o militare. Per ogni settore esistono esigenze specifiche e, considerando anche il GDPR, occorre ricordare che i "dati cloud" devono essere memorizzati in infrastrutture allocate in ambito europeo, amplificando così la complessità di gestione.
In questo scenario Wellcomm Engineering, in sinergia con Sirti, affronta la sfida di rafforzare il proprio posizionamento sul mercato come partner tecnologico di riferimento per rispondere alle esigenze aziendali considerate "mission critical".

La sicurezza IT incomincia dal controllo del multicloud

Più dati transitano da e verso il cloud pubblico, più cresce l'esigenza di proteggere gli scambi tra end point e piattaforme e di modelli di responsabilità condivisa

Giancarlo Vercellino, associate research director di IDC Italia

È un dato di fatto che la sempre più pervasiva adozione di servizi cloud da parte delle aziende sta determinando una continua e crescente migrazione di dati verso ambienti remoti e distribuiti e di conseguenza la necessità per i team di sicurezza di alzare il livello di protezione delle informazioni sensibili in contesti multi o hybrid cloud.

Le più recenti indagini condotte da IDC evidenziano in proposito come molte imprese stiano estendendo il portafoglio di soluzioni di sicurezza IT come parte del meccanismo di attuazione delle policy per l'utilizzo di risorse cloud, andando a integrare in questo portafoglio nuovi software o servizi come i Cloud Access Security Broker.

I dati parlano da soli ed evidenziano l'ampiezza del problema. La spesa mondiale in soluzioni per la sicurezza web crescerà secondo IDC con un tasso composito medio annuo (CAGR) del +9,8% al 2022.

La componente di cloud pubblico (SaaS) di questa spesa farà segnare un CAGR del +14% nello stesso periodo, quella on-premise del +5,1%.

A guidare questa crescita saranno soprattutto i Cloud Access Security Broker (CASB, conosciuti anche come Cloud Security Gateway), e i Web Application Firewall.

In particolare, i Cloud Access Security Broker stanno diventando un tassello fondamentale del puzzle della sicurezza cloud.

Considerate le enormi opportunità che possono nascere per le aziende dall'aggregazione di dati di molteplici applicazioni SaaS, queste soluzioni rappresentano il punto di controllo essenziale negli scambi di informazione tra gli end point e le piattaforme cloud, tra le Operation Technologies e i data center di nuova generazione.

Per i Cloud Access Security Broker si sta in sostanza aprendo in questo momento una seconda fase importante.

Nella prima, la loro adozione è stata dettata soprattutto dall'esigenza da parte delle aziende di governare e avere visibilità degli accessi al web.

In questa seconda fase, l'accento si è spostato, ma è meglio dire esteso, alla protezione dei dati, ovunque essi si trovino allocati.

La necessità per le imprese di "vedere" e "proteggere" interponendo un punto di controllo tra utenti e risorse cloud, osserva IDC, spiega l'incessante richiesta per questa tipologia di so-

luzioni, nonché per modelli contrattuali di condivisione delle responsabilità in cui gli obblighi di sicurezza e conformità siano ripartiti nella maniera più efficace possibile tra il fornitore e il cliente.
«La necessità di confrontarsi con strategie di attacco complesse e la proliferazione degli ambienti multicloud richiedono una profonda revisione delle strategie di gestione della sicurezza IT, soprattutto quando ci confrontiamo con architetture ibride e nuovi casi d'uso», ha evidenziato **Giancarlo Vercellino**, associate research director di IDC Italia. «La trasformazione digitale cambia radicalmente il perimetro di difesa, che si sposta dalla rete al dato e alle persone. Per rispondere a queste nuove esigenze, stanno sorgendo nuovi modelli tecnologico-organizzativi, come quello dei CASB/Cloud Security Gateways, per tutelare in modo ancora più efficace le imprese dal rischio IT».

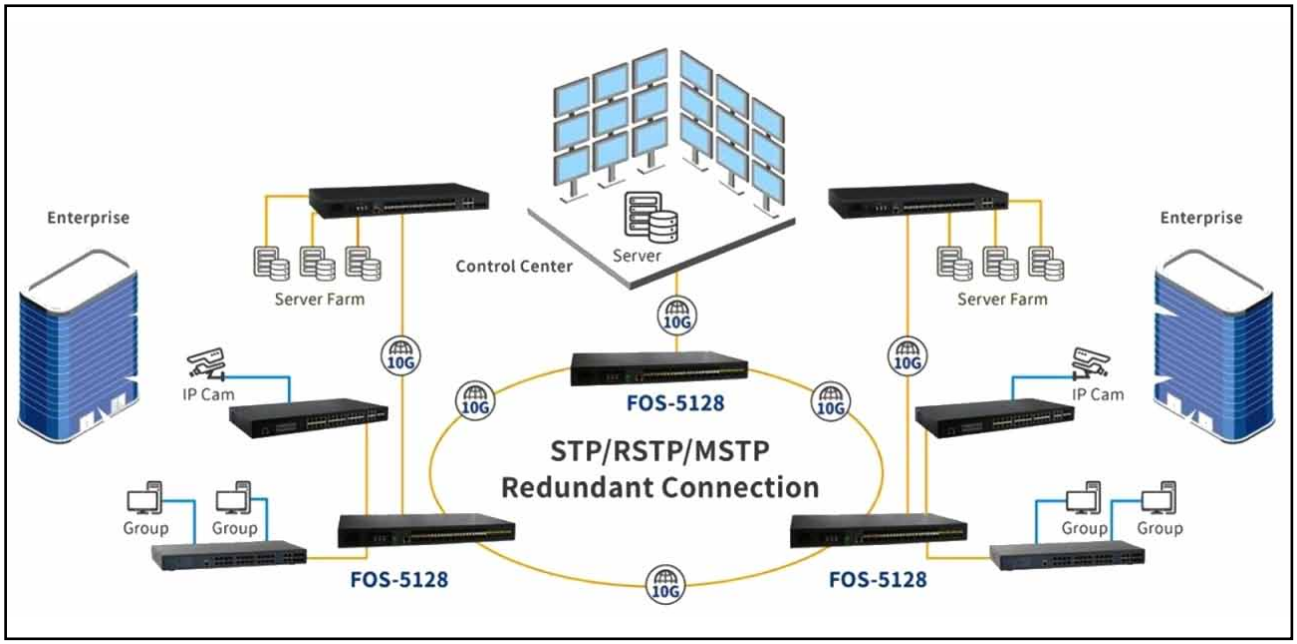
Servizi di rete e in cloud ottimizzati con lo gli switch di CTS

CIE Telematica ha reso disponibile lo switch gestito FOS-5128 per la realizzazione flessibile di reti FTTx e di multi servizi a valore e nel cloud

Connection Technology Systems (CTS) ha reso disponibile il dispositivo di rete FOS-5128, uno switch gestito per applicazioni di rete di livello 2. Equipaggia 24 porte 100/1000Base-X SFP lato utente e 4 porte
1/10GBase-R SFP di up-link in grado di far fronte alla domanda di una elevata larghezza di banda sia per servizi Internet tradizionali che per l'erogazione di servizi over-the-top, ad esempio applicazioni di tipo "rich media".
Il dispositivo è stato ideato per assicurare una elevata flessibilità installativa e di tipologia di fibre e modalità trasmissive. In pratica, tutti gli slot SFP possono essere equipaggiati con transceiver single mode, WDM o CWDM, cosa che li rende particolarmente adatti per rispondere alle esigenze di provider o di aziende che pianificano l'implementazione di reti FTTx o Metro Ethernet. La soluzione è stata progettata anche per far fronte alle esigenze dei manager di rete sia di operatori che di aziende di fascia Enterprise che hanno l'esigenza di disporre di soluzioni in grado di supportare alta velocità ed operare con un elevato grado di sicurezza nella realizzazione di

reti FTTx.
Quelle reti quindi che prevedono l'utilizzo della fibra ottica nell'ultimo tratto al posto del comune rame, o reti Metro Ethernet.
Un aspetto saliente della soluzione, ha evidenziato **Luigi Meregalli**, General manager di CIE Telematica, società partner di CTS in Italia, è che il dispositivo di rete oltre a supportare servizi e traffico voce, dati e IPTV sino a una velocità di up-link di 10 Gbps, dispone anche di una alimentazione ridondata che entra in funzione automaticamente.
Come evidenziato, il dispositivo è poliedrico e in grado di soddisfare le diverse esigenze installative e di erogazione di servizi agli utenti.
Vediamo più in dettaglio le funzionalità cominciando dalla ridondanza dell'alimentazione, un aspetto molto sentito in realtà di rete distribuite e che devono garantire l'operatività continua e il mantenimento di severi livelli di QoS.

Luigi Meregalli - CIE Telematica



Esempi di utilizzo del fos-5128

Alimentazione ridondata e gestibilità con console Web e SNMP

La ridondanza viene assicurata tramite la combinazione di due tipi di alimentazione che possono essere scelte tra 2 in corrente alternata, 2 in corrente continua o una in alternata ed una in continua. Nel caso di mancanza di alimentazione di quella primaria il dispositivo commuta automaticamente su quella secondaria.
La affidabilità , o il controllo dell'insorgere di eventuali criticità è aumentata anche dalla possibilità che ha l'utilizzatore di monitorare il comportamento di componenti hardware, come ad esempio la velocità delle unità di ventilazione o il voltaggio delle unità di alimentazione, tutti parametri che permettono di determinare lo stato di salute complessivo del dispositivo.
Ampie anche le possibilità di gestione del dispositivo, che può essere controllato tramite interfaccia Web, via console, mediante Common Line Interface Telnet o protocollo SNMP, a cui si aggiunge l'auto-provisioning DHCP, fruibile per l'aggiornamento da remoto del firmware.

Sicurezza e separazione flussi nel Cloud con la funzione Q-in-Q

Il dispositivo FOS-5128 comprende anche funzioni atte a garantire la sicurezza e la separazione dei dati e servizi di utente basati sul tunneling Q-in-Q.
Il tunneling Q-in-Q e la traslazione delle VLAN è un metodo che permette ai fornitori di servizi di creare una connessione Ethernet di livello 2 tra due diversi siti di clienti.
In sostanza, si ha la possibilità su un collegamento di rete di separare il traffico VLAN di diversi clienti o di raggruppare VLAN di più clienti in un'unica VLAN.
Ad esempio, i data center possono fruire del tunneling Q-in-Q e della traslazione delle VLAN per isolare il traffico degli utenti all'interno di un singolo sito o per abilitare i flussi di traffico dei clienti tra i data center in cloud allocati in diverse aree geografiche.
Il funzionamento è abbastanza semplice nella sua essenza. Quando un pacchetto dati viaggia da una VLAN (o Customer VLAN: C-VLAN) del cliente alla VLAN di un fornitore di servizi, al pacchetto viene aggiunto un tag che identifica in modo univoco il cliente e che permette di tenerne separato il traffico. Il tag viene trasmesso in modo trasparente attraverso la rete del fornitore di servizi e viene rimosso quando lascia la VLAN del provider del servizio.

Streaming e Dual Stack

Due altre funzioni di interesse per operatori e Enterprise caratterizzano il dispositivo, ha evidenziato Meregalli.
La prima è lo streaming multimediale. Il dispositivo supporta lo snooping IGMP, IGMP fast leaving e IGMP filtering in modo da trasmettere in modo intelligente il traffico di tipo multi-cast e distribuire servizi di IPTV.
Va ricordato che IGMP (acronimo di Internet Group Management Protocol) è un protocollo di comunicazione di rete utilizzato dagli host e dai router adiacenti in una rete IPv4 per definire i membri di un gruppo multi-cast e che lo snooping ha la funzione di osservarne il relativo traffico.
Il dual stack permette invece di supportare oltre al traffico IPv4 anche traffico IPv6, il packet forwarding e lo snooping MLD v1/v2 (Multicast Listener Discovery).

CyberArk abilita la gestione SaaS degli accessi privilegiati

La soluzione SaaS CyberArk Privilege Cloud è disponibile sul marketplace di Amazon Web Services

CyberArk, azienda specializzata nello sviluppo di soluzioni di cyber security per la protezione degli accessi privilegiati, ha reso disponibile la sua offerta as-a-service CyberArk Privilege Cloud sul marketplace di Amazon Web Services (AWS).

Va osservato che CyberArk Privilege Cloud è un'offerta SaaS che l'azienda ha sviluppato per permettere di proteggere, controllare e monitorare gli accessi privilegiati per infrastrutture on-premise, cloud e ibride.

La soluzione, ha evidenziato l'azienda, è progettata per garantire una elevata sicurezza e per essere di ausilio alle organizzazioni nel gestire in modo efficiente le credenziali degli account privilegiati e i diritti di accesso, monitorare e controllare in modo proattivo le attività degli account privilegiati e rispondere rapidamente alle minacce.

Si tratta in pratica di una soluzione che permette di disporre di un livello ulteriore di sicurezza che non richiede la necessità di gestire infrastrutture extra on-premise, in modo che le organizzazioni possano concentrarsi sulle loro competenze principali.

Come sviluppo, è la quarta soluzione di CyberArk ad essere resa disponibile su AWS Marketplace, dopo Conjur Open Source, CyberArk Privileged Access Security Solution e CyberArk Privileged Access Security Solution for GovCloud, e conferma lo stretto rapporto di collaborazione esistente tra CyberArk e AWS.

Numerosi gli elementi di integrazione della soluzione con AWS e atti a rafforzare la sicurezza delle risorse cloud delle aziende, compresa l'integrazione con AWS Security Token Service (STS) e Amazon Inspector.

I clienti di CyberArk Privilege Cloud, ha evidenziato la società, hanno anche la possibilità di scaricare la soluzione di onboarding AWS Automatic dal GitHub pubblico di CyberArk, che utilizza gli eventi AWS CloudWatch per rilevare le istanze EC2 appena create, registrarle automaticamente e gestirne gli account privilegiati.

Veeam conferma la leadership nel Cloud Data Management

Veeam si caratterizza per una significativa crescita dei ricavi ricorrenti e la crescente adozione da parte dei clienti del nuovo modello di licensing in abbonamento

Ratmir Timashev, co-founder and Executive Vice President (EVP) of Sales & Marketing di Veeam

Veeam Software, attiva nella fornitura di soluzioni di backup volte ad abilitare il Cloud Data Management, ha annunciato i risultati finanziari del terzo trimestre 2019.

In un mercato altamente competitivo, Veeam ha registrato un altro trimestre a doppia cifra con un incremento del 24% anno su anno del fatturato annuo ricorrente (ARR), cosa che conferma il successo del suo nuovo modello di licensing in abbonamento Veeam Universal License (VUL), che si è caratterizzato per un aumento del 108% del fatturato per lo stesso periodo.

Non solo. Veeam ha anche ottenuto, nella sua indagine annuale sulla soddisfazione dei clienti, un Net Promoter Score (NPS) di 75, un punteggio che è superiore alla media di mercato e ottenuto per il sesto anno consecutivo.

«Il 2019 è stato un anno ricco di successi: non solo abbiamo superato il miliardo di dollari di fatturato annuale, ma stiamo anche innovando l'esperienza dei clienti grazie al nuovo modello di licensing in abbonamento Veeam Universal License (VUL) e ai continui rilasci di nuovi prodotti - ha commentato **Ratmir Timashev,** Co-Founder and Executive Vice President (EVP) of Sales & Marketing di Veeam -. Nel nostro ultimo trimestre, abbiamo assistito a una crescita straordinaria in tutti i mercati e, in particolare, nel modello di licensing in abbonamento, che ha portato il numero di clienti a più di 365.000. All'inizio del quarto trimestre del 2019, annunceremo una serie di nuove soluzioni che confermeranno la nostra leadership di mercato e la soddisfazione dei nostri clienti, come dimostra il nostro punteggio NPS.»

Ottimi anche i risultati delle partnership. Gli accordi di rivendita con Hewlett Packard Enterprise (HPE), Cisco, NetApp e Lenovo hanno registrato una crescita delle transazioni del 92% anno su anno e del 28% trimestre su trimestre (QoQ).

«Negli ultimi anni, Veeam ha consolidato la sua leadership come fornitore di soluzioni di backup e ripristino per ambienti virtuali, fisici e cloud. La strategia incentrata sui partner e la capacità di Veeam di adattarsi al mercato con un approccio mirato sono state le chiavi del suo continuo successo e hanno consentito a Veeam di crescere in modo costante e a due cifre in un segmento di mercato ormai maturo che tipicamente registra una bassa crescita a una sola cifra» ha commentato i positivi risultati **Andrew Smith**, Research Manager in IDC's Infrastructure Platforms and Technologies group.

La cyber security amplia il ruolo dell'IT in azienda

Oltre alle nuove pratiche di lavoro il reparto IT deve pensare e centrare l'attenzione sul come prevenire le nuove minacce e rafforzare la sicurezza informatica

Nel corso degli ultimi anni non è cambiata solo la tecnologia e il modo in cui approcciare la trasformazione digitale, ma lo è anche il ruolo dell'IT e del suo personale.
Posizionato al crocevia tra tecnologia, project management, gestione generale dell'azienda, sicurezza e strategia, il dipartimento IT è notevolmente cambiato ed ha finito con l'assumere nuovi ruoli.
In concreto, si è riposizionato in modo da fornire supporto strategico ottimale per la realizzazione dei grandi progetti aziendali. Questo riposizionamento fa sì che oggi venga ritenuto un elemento chiave nel top management e che come dipartimento responsabile della gestione dei sistemi informativi ricopra una funzione essenziale nella sicurezza informatica.
Oggi, osserva **Franck Nielacny**, direttore dei sistemi informativi di Stormshield, società che sviluppa soluzioni per la cybersicurity, i responsabili IT costruiscono le imprese di domani e si stanno gradualmente facendo carico di questioni che travalicano i confini dell'informatica tradizionale aggiungendo alle proprie competenze anche capacità di comunicazione e di ascolto.
In questo nuovo approccio le diverse business unit aziendali sono sempre più coinvolte nelle decisioni IT e il risultato è che è necessario dialogare con la contabilità, gli esperti di logistica o i responsabili delle risorse umane, comprendendone ancor prima che i bisogni il rispettivo linguaggio specialistico.

Cybersecurity e le nuove sfide per l'IT

Se ci si focalizza sulla sicurezza informatica, osserva Nielacny, le crescenti minacce che le aziende devono affrontare richiedono non solo l'implementazione di soluzioni di sicurezza, ma anche e viene da aggiungere soprattutto una buona dose di formazione e un forte supporto al personale, volto quest'ultimo a favorire lo sviluppo di una consapevolezza collettiva dei rischi affrontati e di quanto sia importante rispettare buone pratiche di igiene digitale a tutti i livelli dell'azienda.
Oltre a respingere i tradizionali attacchi su larga scala, il ruolo dell'IT è anche quello di proteggere l'azienda da attacchi più sottili ma parimenti devastanti perché gli attacchi di massa rappresentano nei fatti solo la punta dell'iceberg mentre la sicurezza informatica riguarda più ciò che non si vede e riguarda indistintamente tutti i di-

pendenti e i reparti dell'azienda.
Si tratta quindi di un tema, nota il manager e si può di certo essere d'accordo con lui, estremamente ricorrente da gestire in collaborazione con il CISO qualora la cybersecurity sia affidata a personale specializzato poiché la protezione proattiva degli asset aziendali richiede un notevole investimento di risorse in monitoraggio, controllo e aggiornamento dei sistemi se si vuole rilevare anche i più deboli segnali di una potenziale minaccia.
Criticità vengono poi anche dal cambiamento di paradigma della cybersecurity a seguito dlela costante diffusione delle virtualizzazione, della mobilità, del Cloud e delle piattaforme SaaS, che trasformano le modalità operative e rendono l'IT sempre più aperto. «E' uno scenario complesso da gestire in cui al reparto IT viene chiesto di garantire la tutela di tutte le informazioni aziendali elaborate esternamente. Delegare il controllo tecnico di una piattaforma SaaS? Sì. Delegare a terzi la responsabilità di proteggere le informazioni aziendali archiviate in quel sistema? Fuori discussione» suggerisce Nielacny.
Ma non è solo questione di minacce crescenti più o meno note. Il fatto è che tecnologie come la Blockchain, l'IoT, l'IIoT e l'AI stanno apportando ulteriori complessità ai sistemi informativi e influenzeranno sempre più il ruolo dell'IT.
Il responsabile IT dovrà in sostanza assicurarsi non solo che le soluzioni che verranno implementate risultino sicure ma anche che esse si integrino con il sistema informativo esistente.
In definitiva, evidenzia Nielacny ,il dipartimento Sistemi Informativi subirà una trasformazione radicale, e rivestirà un ruolo sempre più importante all'interno dell'azienda perché oltre alle nuove pratiche di lavoro che sarà chiamato a supportare sarà sempre più coinvolto nelle misure di prevenzione contro nuove minacce e la sicurezza informatica sarà posta sempre più al centro delle sue attività.

Forcepoint espande i servizi per un cloud sicuro

Il portfolio di servizi Forcepoint Web Security è disponibile su 160 PoP in 128 paesi e garantisce bassa latenza, sovranità dei dati, localizzazione dei contenuti

Forcepoint, società di livello mondiale nella cybersecurity, ha ampliato il portfolio di soluzioni di sicurezza per il cloud. Obiettivo dichiarato è quello di consentire alle aziende e alle agenzie governative di accedere in modo sicuro ai contenuti basati sul Web, dall'ufficio, in remoto o in movimento.
L'allargamento del portfolio con la disponibilità di Forcepoint Web Security su 160 punti di presenza pubblici (public points of presence, PoP) in 128 paesi ha portato in pratica, ha osservato

la società, i servizi Forcepoint in qualsiasi parte del mondo, e mette a disposizione funzionalità ideate per garantire la sicurezza e la produttività, tra cui bassa latenza, sovranità dei dati e localizzazione dei contenuti.
In particolare, Forcepoint Web Security fornisce certificazioni compatibili con il GDPR che hanno l'obiettivo di garantire la riservatezza dei dati durante l'intero ciclo di vita delle operazioni.
L'erogazione, peraltro, avviene con un alto livello di standard di sicurezza cloud tramite data center fisici dell'azienda, inclusi SOC2, ISO 27001 e Privacy Shield,
Forcepoint Web Security ha ottenuto anche significative certificazioni, tra cui ISO 27018, che regola le informazioni di identificazione personale, e Cloud Security Alliance (CSA) Star Gold, basato sul codice di condotta GDPR, che regola la sicurezza del software e le operazioni interfunzionali in un ambiente cloud.

Le esigenze di cloud sicuro dei responsabili IT

La capillare presenza di Forcepoint su base territoriale va incontro ad esigenze ben precise. Una recente ricerca del Ponemon Institute che ha sponsorizzato ha raccolto l'opinione di oltre 600 decisori IT di agenzie federali negli USA su come affrontare la sicurezza nel cloud. Significati i dati emersi.

- Il 55% del campione afferma che la propria agenzia ha scelto con decisione il cloud, ma molti sono ancora alle prese con le questioni legate alla sicurezza.
- Il 71% ha affermato che la visibilità e la governance sono sfide per garantire l'uso del cloud.
- In molti casi, il responsabile della sicurezza IT delle agenzie federali che hanno partecipato alla ricerca è l'ultimo a sapere quando si accede a una nuova applicazione dal cloud.

Nico Fischbach, Global CTO di Forcepoint.

In tutto questo si cala poi il mondo dei CASB.I CASB (cloud access security broker, i broker di sicurezza di accesso al cloud) rappresentano una terza opzione.
La visibilità e la capacità di gestire in modo olistico un intero ambiente applicativo sono componenti chiave di un CASB.
I responsabili IT possono identificare e monitorare tutte le applicazioni utilizzate dai colleghi e applicare contemporaneamente le politiche di sicurezza a tutte le applicazioni. Inoltre, i CASB possono essere utilizzati per ottenere un'enorme quantità di informazioni sull'intelligenza delle diverse applicazioni. Possono quindi confrontare automaticamente i livelli di rischio di diverse applicazioni in modo che gli amministratori possano filtrare le applicazioni cloud che possono essere percepite come ad alto rischio.
«In Forcepoint, ci impegniamo a fornire ai clienti esperienze cloud ottimali per la prima volta in tutto il mondo. Attraverso un'esperienza per l'utente finale iper-localizzata, possiamo aumentare la produttività consegnando il contenuto direttamente al luogo in cui si trova l'utente anziché a quello in cui si trova il data center. Questa espansione consente a Forcepoint Web Security di continuare a fornire ampio supporto alle esigenze di localizzazione storicamente sottoservite in America Latina, Europa orientale e Medio Oriente» ha commentato **Nico Fischbach**, Global CTO di Forcepoint.

La tecnologia e le criticità che ci aspettano nel 2020

A un passo dal 2020 è il momento di analizzare quelli che saranno gli aspetti salienti della tecnologie a cui porre attenzione per il prossimo anno

Con il 2020 oramai all'orizzonte è il momento di considerare cosa sarà la tecnologia IT, le sue evoluzioni e i suoi aspetti strategici che le aziende si troveranno a dover considerare.
Un flash su alcuni dei punti principali è stato scattato da F5, che ha messo a fuoco quanto inerente la sicurezza, il cloud e il mobile. Vediamo cosa ne è emerso, a partire dalla sicurezza, un elemento chiave e punto dolens per qualsiasi azienda avviata o che sta intraprendendo la strada della trasformazione digitale e della esternalizzazione dell'IT.

Trafugamento dei dati, BOT e DNS critici

Per quanto concerne le criticità in cui incorrono i dati aziendali, ha osservato la società, va considerato che le violazioni dei dati e i ransomware dall'inizio al mese di aprile del corrente anno hanno comportato l'esposizione di circa 5,9 miliardi di record. Praticamente circa 1,46 miliardi di record al mese.
Un fenomeno che ha interessato l'assistenza sanitaria, i social media, l'automotive, le amministrazioni comunali, i negozi al dettaglio, le aziende tech, i ristoranti, i governi e praticamente qualsiasi settore che abbia una connessione Internet.
Critico si rivela il fatto che il tempo medio per scoprire una violazione è alla data di oltre 100 giorni, con tutto quello che ne consegue.
Un altro elemento che ha a che fare con la sicurezza (o la sua mancanza) è relativo al DNS. Il DNS, osserva F5, rappresenta uno dei componenti più importanti e fragili di un Internet funzionante. In proposito, nell'ultimo anno gli attacchi DNS siano aumentati del 34% e l'82% delle organizzazioni intervistate in un apposito sondaggio è stata colpita da un attacco DNS, con una media di nove attacchi DNS per organizzazione.
Ma anche i costi implicati stanno aumentando in modo significativo, con un 49% in più. Tra i metodi principali adottati il phishing (47%), il malware (39%) e il vecchio standby DDoS (30%). Per il prossimo anno si prevede che la necessità e la fragilità del DNS continueranno a renderlo un obiettivo atraente, visto il numero crescente di oggetti collegati.
Un terzo aspetto va considerato, quello relativo ai Bot, che sono sempre più intelligenti e con circa la metà di tutto il traffico Internet legata ai bot. Naturalmente, fa notare F5, ci sono bot buoni, come i motori di ricerca, i crawler, le chat e altri che rispettano le regole. Poi ci sono i bot

cattivi che lanciano i DDoS, sottraggono l'account, effettuano scraping, sorveglianza, frodi, attacchi brute force e altre tipologie di attacco senza scrupoli.
Questi possono avere una ripercussione sulla business intelligence, comportare perdite nei guadagni, portare al caos in azienda, generare traffico indesiderato e interrompere in molti modi diversi l'attività di business.
L'aspetto critico è che botnet e malware si evolvono in modo continuo. Ad esempio, i dati del Clusit mostrano come in Italia nel corso dell'ultimo anno siano state rilevate 212 famiglie di software malevoli, con un +10% sull'anno precedente e, soprattutto, vi sia una diffusione massiva di nuovi malware, non ancora classificati e riconducibili a una famiglia nota.

Il multi-cloud è un dato di fatto

In relazione al cloud, F5 evidenzia come RightScale, nella ricerca "2019 State of the Cloud", confermi che il multi-cloud è oggi la scelta preferita dalle aziende. L'84% di esse ha già adottato una strategia multi-cloud, nel 58% dei casi hanno scelto un cloud ibrido (pubblico e privato).
Se negli anni passati si è visto le aziende utilizzare in media circa tre cloud, oggi i dati indicano l'adozione di almeno cinque cloud diversi. Il che dimostra che la sfida non è più "andare sul cloud" ma saper gestire e ottimizzare i costi di questa scelta.
Anche l'Italia è in linea con questo trend e recenti ricerche evidenziano la crescente domanda di ambienti ibridi e Multi Cloud come la scelta principale fatta nel 2019, all'interno di un mercato che a fine anno si stima risulti pari a 2,3 miliardi di euro, con una crescita del +19% rispetto all'anno precedente.

Il mobile protagonista e 5G in arrivo

Siamo nell'era del mobile, osserva F5, ed è sin troppo facile essere d'accordo con l'assunto. I nostri dispositivi sono mobili e le applicazioni a cui accediamo sono mobili.
Tuttavia la mobilità, se rappresenta un fattore abilitante, è contemporaneamente una preoccupazione enorme per le aziende.
Il BYOD è ormai un termine vecchio, secondo gli standard odierni, ma è ancora in gioco e rappresenta un mercato che si prevede raggiunga i 367 miliardi di dollari entro il 2022. Una cifra da PIL di nazione di medie dimensioni.
E' poi un settore in cui gli strumenti tecnologici e le applicazioni continuano ad espandersi. 5G, pagamenti mobile, API, l'ascesa delle app istantanee on-demand, e, perlomeno si dovrebbe, una maggiore attenzione alla sicurezza sono tutti aspetti oggi in gioco. Il mobile è in sostanza uno degli attori principali del mondo tech, e lo sarà anche nei prossimi mesi.
In particolare, il 2019 ha visto un'attenzione crescente verso il 5G, con conflitti economici e giudiziari a livello mondiale che stanno avendo una ripercussione importante anche a livello nazionale.
Un esempio concreto è costituito da uno dei provvedimenti presi durante la riunione del primo Consiglio dei Ministri del nuovo governo, che è stato relativo al "golden power" per indirizzare gli operatori telefonici che lavorano in Italia verso una normativa più stretta in termini di sicurezza del 5G. La battaglia per la supremazia nel 5G appare però solo agli inizi e non è facile prevedere come potrà evolvere nel corso del prossimo anno.

FortiCWP migliora la security nel cloud e nel multicloud

La soluzione Fortinet è stata progettata per fornire un'ampia protezione del workload nel cloud e nel multicloud

La mancanza di collaborazione nei diversi ambiti applicativi della sicurezza spesso comporta una scarsa visibilità centralizzata per quanto riguarda le attività di importanza critica.
Tra queste, le configurazioni di servizio, il traffico di rete, o gli eventi che riguardano la sicurezza e la data hygiene.
E' una sfida complicata dal fatto che oggi si ha a che fare con le diverse piattaforme dei provider di cloud pubblici.
Specificatamente per andare incontro alle problematiche delle aziende e supportarle nel rispondere a questa criticità, Fortinet ha annunciato FortiCWP, una soluzione dedicata alla protezione del workload del cloud che ha progettato per assicurare agli utenti il rispetto delle compliance e per diminuire i rischi associati alle applicazioni basate su IaaS.
In sostanza, FortiCWP permette alle aziende, osserva Fortinet, di ottenere visibilità e controllo nella loro infrastruttura dinamica multi-cloud, essendo una soluzione di security posture management multi-cloud integrata e dinamica.
Un aspetto chiave è che risulta nativamente integrata con diverse infrastrutture cloud pubbliche, compreso l'utilizzo di API cloud-native di AWS, Google Cloud Platform e Microsoft Azure.
In questi contesti permette di rilevare le configurazioni, monitorare l'attività negli account cloud, analizzare e scansionare i dati, monitorare il traffico del cloud network e fornire report completi sulla compliance.
FortiCWP è poi integrata con i FortiGuard Labs, da cui riceve aggiornamenti sulla threat intelligence, e con FortiSandbox per analizzare i dati archiviati nel cloud ed identificare i contenuti malevoli.
I due servizi combinati permettono ai team che si occupano della sicurezza di disporre di visibilità e controllo degli eventi anche attraverso infrastrutture multi-cloud.
Una maggiore integrazione, visibilità e protezione la si ha se FortiCWP viene usato in combinazione con FortiGate-VM per la sicurezza del cloud (sia in ingresso che in uscita) e con FortiWeb per le applicazioni web e la protezione delle API. E' infatti una combinazione, ha evidenziato Fortinet, che risponde alla necessità di mettere in sicurezza la rete, le applicazioni web e le piattaforme cloud.
Un altro campo di suo utilizzo è laddove serve un supporto per le applicazioni basate su IaaS , e in generale dove le aziende hanno la necessità di estendere nel cloud le competenze dei loro security team, e mitigare i rischi nel loro percorso di trasformazione e innovazione digitale.

Retelit si rafforza nei servizi IT

Con l'acquisizione del Gruppo Partners Associates l'operatore amplia il portfolio di soluzioni infrastrutturali e di servizi

Dario Pardi, Presidente di Retelit

Retelit S.p.A., operatore italiano attivo nel campo dei servizi dati e infrastrutture, ha comunicato che la società interamente controllata Retelit Digital Services S.p.A. ha siglato un accordo vincolante per l'acquisizione del 100% del capitale sociale di Partners Associates S.p.A. (PA Group), un gruppo italiano con sede a Udine specializzato nel settore ICT che con oltre 600 professionisti eroga servizi a circa 8.000 clienti.

In particolare, l'azienda opera su tutto il territorio nazionale e si configura come un system integrator che fornisce sia a grandi imprese che a PMI soluzioni integrate di software gestionali (SAP, Microsoft Dynamics, software e prodotti proprietari), CRM, Business Analytics, Networking, Cybersecurity, servizi in Cloud e Datacenter.

I settori a cui si rivolge comprendono la Finanza, Industria, TLC e Pubblica Amministrazione. E' inoltre attiva nel mondo delle telecomunicazioni tramite la controllata InAsset , specializzata nella gestione di servizi ed infrastrutture di Datacenter e con un Datacenter proprietario ubicato a Udine, ulteriori tre Datacenter per garantire la continuità operativa e 1.700 km di fibra ottica proprietaria.

Costante la crescita di PA Group, che dai 36 milioni di fatturato del 2013 è passata agli oltre 60 milioni attuali1 con un Ebitda di circa 10 milioni di Euro.

«Questa operazione, rappresenta una tappa importante per il Gruppo Retelit che, con le nuove competenze e soluzioni acquisite, potrà giocare un ruolo primario nell'ambito dell'ICT, con proposte complete, sia in ambito infrastrutturale sia di servizi. Nasce un soggetto unico nel panorama ICT, in grado di offrire al mercato delle aziende impegnate nella Digital Transformation, soluzioni integrate, completamente realizzate su piattaforme gestite dal Gruppo. L'ingresso degli attuali azionisti di PA nel capitale di Retelit è ulteriore conferma della validità del progetto industriale e garanzia di un loro contributo fattivo al buon risultato della Business Combination» ha commentato l'operazione **Dario Pardi**, Presidente di Retelit.

L'operazione annunciata contribuirà ad espandere ulteriormente il portfolio di servizi e la forte radicazione in Italia di Retelit, un operatore italano attivo nella fornitura di servizi digitali e infra-

Federico Protto - Amministratore Delegato di Retelit

strutture di TLC che dal 2000 è quotato alla Borsa di Milano e nel segmento STAR dal 26 settembre 2016.

«L'acquisizione di Gruppo PA ci consente di accelerare ancora di più il percorso di evoluzione e poterci così presentare al mercato con un'offerta rinnovata e più ricca grazie all'inserimento di nuove expertise, mantenendo allo stesso tempo un'elevata marginalità dei profitti. Non va dimenticato infine che continueremo ad investire nella nostra infrastruttura di proprietà, una delle più complete d'Italia, che viene già arricchita da quella gestita da Gruppo PA nelle Regioni del Nord Est», ha dichiarato **Federico Protto**, Amministratore Delegato di Retelit.

A livello di rete dispone di un'infrastruttura in fibra ottica di proprietà che si sviluppa per oltre 12.529 chilometri e collega 10 reti metropolitane e 15 Data Center in tutta Italia.

La rete si estende anche oltre i confini nazionali con un ring paneuropeo con PoP nelle principali città europee, incluse Francoforte, Londra, Amsterdam e Parigi. Retelit è inoltre membro dell'AAE-1 (Africa-Asia-Europe-1), il sistema di cavo sottomarino che collega l'Europa all'Asia attraverso il Medio Oriente, con una landing station di proprietà a Bari.

Dal novembre 2018 l'azienda è anche parte di NGENA (Next Generation Enterprise Network Alliance), una alleanza globale di operatori di telecomunicazioni nata per condividere i network proprietari dei membri e fornire una rete di connettività dati globale stabile e scalabile.

Sulla rete di proprietà Retelit eroga servizi che spaziano dalla connessione Internet in fibra ottica al Multicloud, dai servizi di Cyber Security e Application Performance Monitoring ai servizi di rete basati su tecnologia SD-WAN.

Fornisce anche soluzioni di Colocation in oltre 10.500 metri quadrati di spazi attrezzati e sicuri connessi in fibra ottica, per chi opta per esternalizzare servizi di Data Center e realizzare soluzioni di Disaster Recovery e Business Continuity. I servizi Carrier Ethernet che fornisce sono certificati Metro Ethernet Forum (MEF). Alla certificazione MEF CE 2.0 ha aggiunto anche le certificazioni tecnologiche ISO 27000 per la progettazione e fornitura di servizi di rete, Colocation e Cloud e ALLA/NALLA per l'erogazione di servizi in ambito militare.