

PAG. 01-05 › IPERCONVERGENZA E DATA CENTER PER TUTTI CON NUTANIX

PAG. 06 › IL FUTURO DELLA COMUNICAZIONE NELL'ERA DEL CLOUD SECONDO SNOM

PAG. 07-08 › 7 AZIENDE SU 10 SI ORIENTANO AL CLOUD, NONOSTANTE I TIMORI DELL'IT PER LA SICUREZZA

PAG. 09-10 › PIÙ SMART E CLOUD READY GLI AMBIENTI LAVORATIVI DEL FUTURO

PAG. 11-12 › CHECKME DI CHECK POINT E CIE TELEMATICA CONTROLLA LA SICUREZZA NEL CLOUD

PAG. 13 › CHECK POINT METTE AL SICURO I DATI CON CLOUDGUARD SAAS

PAG. 14 › CLOUD MANAGEMENT E "WIRELESS AWARENESS" LE NUOVE FUNZIONALITÀ DEGLI SWITCH ENTERPRISE

PAG. 15 › DATA MANAGEMENT EFFICIENTE CON VERITAS E PURE STORAGE

PAG. 16-17 › VEEAM SUPPORTA LA DIGITAL TRANSFORMATION DI TELETHON

PAG. 18-19 › CYBERARK LEADER NEL MAGIC QUADRANT 2018 DI GARTNER PER IL PRIVILEGED ACCESS MANAGEMENT

COVER STORY

IPERCONVERGENZA E DATA CENTER PER TUTTI CON NUTANIX

Il Data Center integra il Cloud, l'iperconvergenza si afferma e Nutanix la rende disponibile a tutti. Il riconoscimento di Gartner che posiziona l'azienda tra i leader nel Magic Quadrant

di Giuseppe Saccardi

Con un processo che tende a velocizzarsi, è in atto, complice l'iperconvergenza, la trasformazione dei data center. A dare il via sono state le esigenze degli utilizzatori e del contesto di business in cui si muovono e, subito a seguire, di chi li gestisce, e cioè il personale IT alle prese con

una trasformazione digitale che in pochi anni ha proiettato il data center in uno scenario di utilizzo e un contesto architeturale del tutto nuovo.

Svariati sono i fattori che hanno portato a questo cambiamento, alcuni di natura economica e sociale, altri di natura prettamente



Alberto Filisetti, Country Manager di Nutanix Italia

tecnologica ed organizzativa.

Tra i primi va annoverata l'esigenza da parte delle aziende di concentrarsi sul core business e di ottimizzare Capex e Opex. Tra i secondi la proiezione verso l'esterno dell'azienda, la crescita tumultuosa della Mobility, l'esigenza di rispondere rapidamente alle richieste del mercato.

Il successo del cloud e dell'IT visto come servizio e come modo per esternalizzare la sua complessità deriva in definitiva dal fondersi di quanto sopra detto.

Come sottolineato da **Alberto Filisetti**, Country Manager di Nutanix Italia, l'iperconvergenza, è un ulteriore passo in questa direzione, volta a semplificare la complessità dell'IT e in questo modo permettere anche alle PMI, alle Enterprise e agli enti pubblici in generale di poter trarre beneficio dai processi che sino ad ora hanno interessato e favorito i service provider o i fornitori mondiali di servizi cloud, senza che si debbano però far carico degli oneri di una complessa gestione così come di elevati investimenti.

Magic Quadrant per l'iperconvergenza: Gartner posiziona Nutanix ancora una volta tra i leader

La posizione di rilievo nella digital transformation di Nutanix trova conferma dal suo inserimento tra i leader nel Magic Quadrant di Gartner per le infrastrutture iperconvergenti, importante riconoscimento ottenuto nel mese di novembre per la seconda volta consecutiva.

Ciò costituisce una chiara conferma della posizione dominante di Nutanix nel mercato che ha creato e della vision che la caratterizza nel fornire una reale esperienza di cloud ibrido, per consentire ai

team IT di fornire applicazioni su più piattaforme.

«Durante lo scorso anno, Gartner è stata testimone di una crescente affermazione delle soluzioni HCI nelle applicazioni aziendali business-critical.

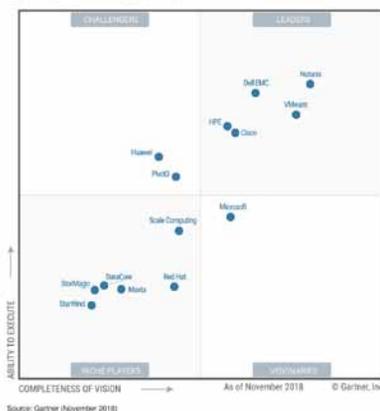
Di conseguenza, gli utenti hanno incrementato il controllo sull'assistenza e sulla certificazione delle applicazioni» hanno affermato John McArthur, Kiyomi Yamada, Philip Dawson, Julia Palmer, di Gartner. «Allo stesso tempo, i fornitori di soluzioni HCI hanno incluso nella loro strategia le distribuzioni ibride/multicloud, come obiettivi di backup o opzioni di disaster recovery o come alternativa per le infrastrutture on-premise per esigenze di risorse non prevedibili o cicliche».

Nutanix ritiene che il riconoscimento sia anche frutto del momento estremamente positivo che l'azienda ha vissuto nell'ultimo anno, anno caratterizzato dal:

- Raggiungimento del traguardo degli 11.000 clienti, di cui 720 inclusi nella classifica Forbes Global 2000.
- Trasformazione in una software company, che ha visto la sua transizione verso un'offerta focalizzata sul software, il passaggio a un modello di business basato su

subscription e un ampliamento della copertura del mercato di edge IoT.

- Ampliamento dell'offerta di prodotto, che l'ha vista recentemente annunciare la disponibilità di Xi Cloud Services, una nuova suite di servizi progettati per creare un'infrastruttura più unificata tra diversi ambienti cloud. Xi Cloud Services include cinque distinte offerte, tra cui Xi IoT, una nuova piattaforma intelligente per



Magic Quadrant Gartner novembre 2018

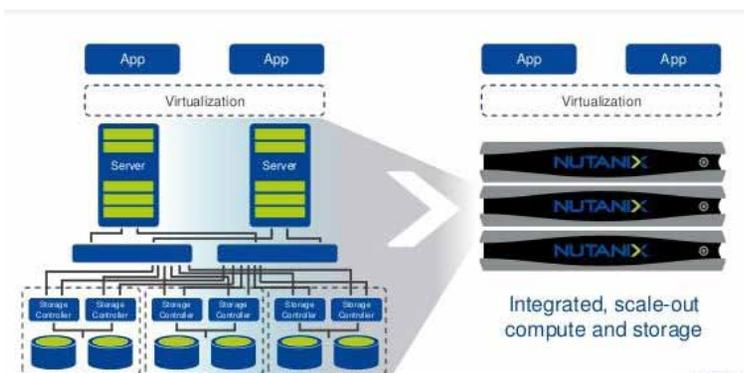
l'edge computing e Xi Leap, un'estensione nativa di Nutanix Enterprise Cloud Platform che fornisce funzionalità di disaster recovery as a service.



Dheeraj Pandey, Presidente e CEO di Nutanix

I benefici dell'iperconvergenza

Ma cosa si intende per iperconvergenza? In sostanza, consiste in soluzioni chiavi in mano che racchiudono capacità di calcolo, di storage e di rete, il tutto in un fattore di forma compatto e predisposto per l'espansione sia locale che geografica.



Oggi le aziende hanno bisogno di un ambiente cloud realmente ibrido e iperconvergente che sia invisibile all'organizzazione ma che offra un'esperienza fluida tra cloud pubblici e privati. Con il software Nutanix Enterprise Cloud OS, evidenzia l'azienda, i clienti possono concretizzare i benefici di semplicità, agilità e consumo frazionato dell'IT offerti dal cloud pubblico, con il controllo e la sicurezza necessari nel data center aziendale.

«La mission di Nutanix è di consentire ai clienti di sentirsi liberi nella scelta della propria infrastruttura, eseguire le loro applicazioni, modernizzare i loro data center e scegliere la loro piattaforma cloud - il tutto alle loro condizioni, non secondo quanto dettato da un singolo fornitore» ha sottolineato **Dheeraj Pandey**, Presidente, Fondatore e CEO di Nutanix. «Consideriamo il nostro posizionamento tra i Leader di Gartner, per la seconda volta consecutiva, come una conferma della nostra continua influenza sul mercato, di una solida offerta di prodotti e, soprattutto, del costante impegno verso i nostri clienti».

Un ruolo importante in questa evoluzione lo ricopre il software e in particolare quello di orchestrazione e di gestione.

Poiché l'obiettivo primario di un tale approccio è quello della semplificazione, e cioè del poter disporre di quello che, a parte le dimensioni di scala si configura come un vero e proprio data center senza però doverne supportare i costi di gestione, è evidente, osserva Filisetti, che il software di gestione e orchestrazione delle risorse di una soluzione per la iperconvergenza deve risultare molto user friendly e farsi carico di tutte quelle operazioni (o quasi) che in un data center convenzionale è competenza di personale specializzato che va ad influire in modo massiccio sui costi di esercizio.

I benefici del diffondersi di soluzioni iperconvergenti sono molteplici. Innanzitutto si apre la possibilità anche per medie o piccole aziende di disporre di soluzioni resilienti e con prestazioni facilmente espandibili, sia per uso locale che per realizzare infrastrutture di backup o di disaster recovery a costi di realizzazione e di esercizio molto contenuti.

Un secondo beneficio dell'iperconvergenza è che diventa più facile evolvere a livello di applicazioni e di elaborazione e gestione verso il cloud.

Si può in tale scelta strategica spostare sul cloud attività non critiche per quanto concerne la riservatezza, così come adottare il cloud per la fase di test e sviluppo di nuove applicazioni mantenendo però una gestione e un controllo locale delle applicazioni e relativi dati aventi carattere sensibili che non potrebbero essere trasferiti sul cloud, sia in base a scelte strategiche che a regolamenti nazionali e sovranazionali.

L'approccio Nutanix all'iperconvergenza

L'approccio Nutanix all'iperconvergenza si basa su uno stack che integra i layer di una soluzione IT complessa e su moduli di base su cui lo stack di applicazioni e servizi, cloud privato o ibrido compreso, opera.

Lo stack comprende a livello fisico o logico lo strato di rete che connette i moduli di calcolo e di storage, sia locali che distribuiti, e su cui agisce un software di virtualizzazione nativa che viene fornito gratuitamente assieme all'infrastruttura. Aperta è comunque la possibilità di adottare il software di virtualizzazione disponibile sul mercato preferito.

Sullo strato di virtualizzazione si calano poi le applicazioni per la gestione, l'automazione delle operation e quanto serve per una gestione nel cloud, proprietario o ibrido. Per quanto concerne il cloud è possibile ad esempio procedere alla attivazione e alla gestione delle applicazioni e disporre della visibilità e del controllo esecutivo dell'uso che si fa delle risorse pubbliche.

Ampia la scelta di soluzioni cloud pubbliche disponibili, che comprende Google Cloud Platform, AWS e Microsoft Azure.

Estesa anche la gamma di moduli di base, di-

Piattaforma iperconvergente di Nutanix



sponibili sia come elementi dotati di capacità di calcolo e di storage e anche come moduli dedicati con solo capacità di calcolo o solo capacità

di storage, quest'ultima anche con caratteristiche e dimensioni atte a soddisfare sia workload normali che workload che richiedono elevate prestazioni in termini di velocità di I/O o di resilienza del media.

Non ultimo, e atte a soddisfare le svariate esigenze, le architetture realizzabili comprendono sia una connettività locale a livello di rack o di rete per espandere il sistema in modalità scale out, che la possibilità di remotizzazione geografica dei diversi elementi fisici per far fronte a esigenze distribuite o per realizzare architetture ad elevata resilienza dotate di capacità di disaster recovery, con sistemi che possono essere connessi sia con modalità sincrona che asincrona in funzione delle distanze e delle esigenze di recovery.

Iperconvergenza certificata SAP HANA

Oltre a riconoscimenti come quello di Gartner, la soluzione per le infrastrutture iperconvergenti (HCI) Enterprise Cloud OS con l'hypervisor AHV ha soddisfatto i criteri di SAP per l'esecuzione delle distribuzioni di produzione SAP HANA. In pratica, ciò consente alle aziende che utilizzano le soluzioni SAP di beneficiare della agilità della tecnologia HCI per fornire una moderna architettura IT per la piattaforma di database relazionale in-memory di SAP.

SAP ha certificato la piattaforma Nutanix Enterprise Cloud OS con la virtualizzazione AHV per SAP HANA nell'ambito del suo programma di certificazione HCI di SAP.

Nutanix, ha osservato la società, ha dimostrato di possedere le prestazioni e la scalabilità necessarie per implementazioni di successo di SAP

HANA, oltre a semplici operazioni Day-2 degli ambienti SAP. Ciò include la capacità di fornire velocità di produzione superiori con una latenza minima, oltre a garantire un'elevata disponibilità durante periodi di utilizzo intenso del database.

Le aziende che utilizzano le soluzioni SAP possono ai fini pratici far leva sulla piattaforma Nutanix Enterprise Cloud OS in ambienti di produzione e non per un rapido provisioning, gestione e scalabilità semplificata dell'infrastruttura IT, sia per SAP HANA che altre applicazioni SAP.

Nutanix Enterprise Cloud OS è certificato per implementazioni basate su SAP NetWeaver inclusi i server applicativi SAP S/4HANA e può essere utilizzato in produzione per scalare i database SAP HANA.

Dal Cloud al Multicloud con Xi Cloud Services

Xi Cloud Services è una nuova suite di servizi progettati per creare un'infrastruttura più unificata tra diversi ambienti cloud, e che permetta

ai team IT di scegliere la piattaforma più adatta per eseguire le applicazioni, senza vincoli tecnologici.

Xi Cloud Services include al momento cinque diverse offerte, tra cui Xi Leap, un'estensione nativa di Nutanix Enterprise Cloud Platform che fornisce funzionalità di disaster recovery as a service.

L'obiettivo di molte aziende è poter usufruire di un cloud ibrido affidabile che consenta all'IT di collocare in modo strategico i carichi di lavoro. Tuttavia, osserva Nutanix, è difficile identificare

le migliori soluzioni cloud pubbliche e private e coniarle per avere un'un'esperienza omogenea, e spesso il risultato porta a silos di infrastrutture distribuite in varie implementazioni cloud on-premise e pubbliche.

Tale complessità spinge le aziende a sperimentare i nuovi carichi di lavoro sui cloud pubblici, mantenendo le applicazioni aziendali tradizionali nel private cloud del datacenter, nonostante la consapevolezza che tali carichi di lavoro sarebbero più efficienti nel cloud pubblico.

Con Xi Cloud Services, Nutanix si è proposta di semplificare l'integrazione di servizi cloud nelle loro distribuzioni multicloud. Vediamo di cosa si tratta e come.

Xi Leap

Nutanix Leap è un servizio chiavi in mano e integrato che permette di proteggere applicazioni e dati in modo intelligente all'interno di un ambiente Nutanix senza dover acquistare e gestire uno stack infrastrutturale separato. I clienti possono selezionare le macchine virtuali (VM) per la protezione e impostare la sicurezza in modo efficiente. Le VM selezionate saranno successivamente replicate in background, pronte per essere recuperate nel caso di malfunzionamento di un sito – il tutto all'interno dello stesso strumento come in una implementazione infrastrutturale estesa e più ampia dell'azienda.

Xi Cloud Services

Nutanix Xi Cloud Services include ad oggi cinque servizi distinti - incluso Leap - che rispondono alle crescenti sfide dell'era del multicloud. Forniscono la capacità di standardizzare i carichi di lavoro e armonizzare le attività negli ambienti, e anche di "sfumare" i confini tra i cloud, utilizzando applicazioni e dati su diversi cloud per numerosi requisiti di protezione dei dati, distribuzione delle applicazioni e postazioni periferiche.



IL FUTURO DELLA COMUNICAZIONE NELL'ERA DEL CLOUD SECONDO SNOM

SNOM anticipa come comunicheranno tra 5 anni le aziende nell'era del cloud, grazie a un sondaggio realizzato con la collaborazione di BitMat



Cosa ci prospetta il futuro, se non prossimo almeno nel medio termine? Condotto su un campione rappresentativo di 266 aziende dal pioniere del VoIP Snom tra settembre e novembre con l'ausilio di BitMAT, il sondaggio realizzato mostra un quadro molto dinamico, per certi versi anche contrastante, in merito al futuro della telefonia aziendale e alle tecnologie attualmente impiegate nelle aziende.

Se da un lato il 62% del campione (composto per il 68% da aziende utenti finali e per il 32% da operatori di canale) indica di usufruire già della tecnologia VoIP nell'ambiente lavorativo, è interessante notare che tale quota è divisa quasi esattamente a metà tra PMI che utilizzano soluzioni VoIP proprietarie di prima generazione (51%) e aziende che si avvalgono di piattaforme VoIP SIP e di servizi di Unified Communications (49%).

La corsa esponenziale del VoIP basato su standard aperti

Se alla quota di aziende dotatesi delle prime soluzioni VoIP anni orsono si aggiunge la percentuale di aziende (23%) che risulta avvalersi ancora di tecnologie tradizionali (analogiche / ISDN)

e una parte di chi si è dichiarato ignaro di quale tecnologia per le telecomunicazioni sia in uso presso l'azienda (15%), emerge un mercato italiano del VoIP che tra cinque anni vedrà almeno il 92% delle aziende (contro l'attuale >30% del campione) impiegare soluzioni VoIP/UC di nuova generazione basate su SIP.

Una crescita esponenziale (+60% in cinque anni, +38% ipotizzabile ancor più a breve termine) per un mercato che risulta necessitare ancora oggi di un'importante attività di evangelizzazione a fronte di un elevatissimo potenziale per produttori di piattaforme e terminali IP, rivenditori e operatori VoIP.

Dal sondaggio, nota SNOM, emerge anche un ulteriore fattore: sono soprattutto le PMI con un numero di addetti superiore a 25 ad aver adottato il VoIP proprietario ai suoi albori, con una differenza determinante tuttavia tra il canale e aziende utenti finali.

Mentre le installazioni VoIP condotte anni fa presso gli operatori di canale superano di gran lunga i rivenditori che hanno adottato il VoIP SIP di nuova generazione, nelle aziende utenti finali la situazione è diametralmente opposta. Lo stesso divario si riscontra tra chi ha dichiarato di

non sapere quale tecnologia per la telefonia si usi in azienda: una carenza di informazioni che si riscontra solo nelle micro-aziende (fino a 10 addetti) utenti finali, mentre invece in massima parte in operatori di canale con un numero di impiegati superiore a 25.

Terminali IP cordless e cablati

Interessante anche il fatto che solo poco più di un terzo del campione italiano abbia previsto un uso quasi esclusivo di smartphone con app per la telefonia aziendale collegate al centralino IP.

E' un dato che confuta il paventato predominio dello smartphone nella comunicazione aziendale e conferma quanto l'utente italiano ancora preferisca avvalersi del 'tradizionale' telefono da scrivania in azienda, insieme a soluzioni per PC (Callcenter, videoconferenze).

Quasi sorprendente invece il favore accordato dal campione ai telefoni IP cordless, sebbene l'attuale quota di mercato dei terminali IP DECT in Italia sia irrisoria rispetto a quella dei telefoni IP cablati. «Dal sondaggio emerge un forte interesse delle PMI per i cordless IP, previsti come strumento essenziale per le telecomunicazioni dal 13% del campione. Si preannunciano quindi interessantissimi margini di crescita non solo per i telefoni IP cablati, a fronte di un mercato in forte espansione, ma anche per questo tipo di terminali - ha commentato **Fabio Albanini**, Head of Sales South Europe & UK e General Manager di Snom Technology Italia -, considerata la rappresentatività del campione, si delinea un mercato mai tanto promettente come in questo momento e foriero di ottime prospettive di crescita ancora per molti anni a venire».

7 AZIENDE SU 10 SI ORIENTANO AL CLOUD, NONOSTANTE I TIMORI DELL'IT PER LA SICUREZZA

Uno studio indipendente condotto da Equinix che ha coinvolto oltre 1.200 professionisti IT senior in tutta l'area EMEA evidenzia il contrasto sull'adozione del cloud



Equinix, azienda del settore delle interconnessioni globali e dei data center, ha comunicato i risultati di uno studio indipendente che ha coinvolto oltre 1.200 professionisti IT senior provenienti da Europa, Medio Oriente e Africa. I risultati mostrano che più di sette aziende su 10 (71%) trasferiranno probabilmente più funzioni aziendali nel cloud nei prossimi anni. Il 60% dei responsabili IT dell'area EMEA menziona la prossimità ai fornitori di servizi cloud (CSP) quale fattore chiave nella scelta di un data center. Nonostante il crescente numero di aziende sposta le proprie funzioni verso il cloud, il 70% degli intervistati percepisce però ancora la presenza di rischi per la sicurezza informatica rela-

tiva all'adozione del cloud. Le grandi violazioni dei dati pubblici hanno evidentemente causato incertezza tra le aziende, portando il 45% degli intervistati a concentrarsi sul miglioramento della sicurezza informatica della propria azienda come priorità IT. Le considerazioni relative alla sicurezza informatica e al cloud sono una priorità per i responsabili IT di tutta la regione.

Per quasi la metà degli intervistati, infatti, (48%), l'adozione di servizi basati sul cloud ha rappresentato uno dei due principali fattori che avranno maggiore impatto sulla propria azienda in futuro - secondo solo ai rischi e alle violazioni della sicurezza informatica (53%). I risultati hanno inoltre dimostrato che le aziende di tutta l'area EMEA hanno il doppio delle probabilità di connettersi con i CSP rispetto a qualsiasi altro fornitore di servizi o prodotti.

I dati per l'Italia

In Italia il 49% degli intervistati ritiene che la propria azienda si sposterà maggiormente verso il cloud, una percentuale più elevata rispetto alle aziende di tutta l'area EMEA (39%).

Il 41% ritiene inoltre che prossimità ai fornitori di servizi cloud sia un fattore importante nella scelta di un data center in Italia. Inoltre, il 41% dei professionisti IT intervistati ritiene che i fornitori di servizi cloud siano il business con cui la loro azienda ha maggiori probabilità di connettersi in futuro.

Lo studio rileva inoltre che solo il 17% delle aziende in EMEA utilizza attualmente un'architettura multi-cloud.

Al fine di restare competitive e sicure, suggerisce però l'azienda, le aziende dovrebbero rivolgersi a più fornitori di servizi cloud quando sviluppano la strategia digitale della loro infrastruttura. Per supportare una tale strategia l'anno scorso Equinix ha in proposito lanciato Equinix Cloud

Exchange Fabric (ECX Fabric). Il suo obiettivo è di supportare le aziende che hanno bisogno di accedere a più CSP.

Il servizio offre connessioni private a fornitori di servizi cloud globali, indipendentemente dalla loro ubicazione. All'inizio di quest'anno l'azienda ha inoltre lanciato il servizio Equinix SmartKey, una soluzione Software as a Service (SaaS) di gestione delle chiavi e di crittografia che semplifica la protezione dei dati sui diversi tipi di cloud o destinazione.

Le cifre in gioco sono consistenti. Gartner prevede che nel 2019 la spesa IT nell'area EMEA dovrebbe ammontare a 973 miliardi di dollari, con un aumento del 2% rispetto alla spesa stimata

di 954 miliardi di dollari nel 2018.

Sempre per il 2019, Gartner prevede che il cloud, la sicurezza e il passaggio al business digitale favoriranno la crescita nell'area EMEA. La spesa degli utenti finali per i servizi cloud pubblici nell'area EMEA crescerà del 15% nel 2019, per un totale di 38,5 miliardi di dollari.

«I risultati di questo studio rivelano l'enorme spostamento verso il cloud mentre le imprese di tutta l'EMEA si

preparano a competere nell'economia digitale. I rischi e le violazioni della sicurezza informatica sono ovviamente oggetto di particolare attenzione, ma non devono impedire alle imprese di avviare la trasformazione digitale. I modelli ibridi e multi-cloud sono essenziali per l'era della competizione globalizzata di oggi. Lo scambio privato di dati, o interconnessione riduce il rischio per la sicurezza. Questo è forse il motivo per cui oltre tre quarti (77%) dei professionisti IT in tutta l'EMEA ritiene che l'interconnessione aiuterà la propria azienda a ottenere un vantaggio competitivo sul mercato nel futuro», ha commentato **Emmanuel Becker**, Managing Director Italy di Equinix.



Emmanuel Becker di
Equinix

PIÙ SMART E CLOUD READY GLI AMBIENTI LAVORATIVI DEL FUTURO

Dalla digital alla intelligent transformation è la vision di Lenovo. Smart working e investimenti di oltre 11 miliardi di dollari in soluzioni intelligenti di videocomunicazione entro il 2020



In occasione della tappa italiana del proprio roadshow europeo Intelligent Futures, Lenovo ha fatto il punto su come le più recenti tecnologie e gli attuali contesti sociali e lavorativi si incontrino per forgiare una visione futuribile dell'ambiente di lavoro.

I cambiamenti avvengono rapidamente. Gli oggetti che usiamo quotidianamente diventano sempre più intelligenti, dai PC ai sistemi di teleconferenza, addirittura alle lampadine, e cambia di conseguenza anche il nostro modo di interagire con le tecnologie che, al lavoro come a casa, evolve verso un consumo consapevole, una maggiore produttività e connessioni sempre più agevoli.

Analizzando i dati demografici, si rileva il massiccio ingresso della generazione del Millennial - i nati dopo il 1980 - nella forza lavoro e si stima che raggiungeranno il 75% dei lavoratori già per il 2025.

Il dato è significativo, osserva Lenovo, perché si tratta della prima classe demografica di lavoratori a essere stata in contatto con le tecnologie digitali per tutta la propria vita, con i più giovani tra loro abituati fin dall'infanzia a utilizzare e interagire con tecnologie online.

A questo contesto si unisce la tendenza sempre più consolidata di ridurre le dimensioni fisiche degli spazi di lavoro in favore dello smart working e delle "huddle room", sale di piccole o medie dimensioni in cui i gruppi di lavoro si riuniscono per allinearsi sui progetti a cui stanno lavorando; negli Stati Uniti si registra ad esempio una decrescita del 30% delle superfici dal 2010 a oggi.

È ormai qualche anno che questi cambiamenti si concretizzano nella Digital Transformation che, nella visione di Lenovo, è soprattutto una Intelligent Transformation.

«Per molti anni le aziende hanno messo il cliente al centro della loro mission; in Lenovo la chiamiamo customer centricity - ha commentato **Emanuele Baldi**, Amministratore Delegato e General Manager di Lenovo per l'Italia -. L'Intelligent Transformation è un passo oltre: consiste nell'unire l'attenzione al cliente con l'esperienza

d'uso dei dispositivi che proponiamo al mercato e, d'altro canto, l'abilità di attrarre i migliori talenti nelle aziende. La tecnologia, grazie alla sua capacità di ingaggiare e motivare talenti, è un importante fattore abilitante nell'impresa moderna, in grado di liberare il potenziale del più importante valore di ogni azienda: le persone che ne fanno parte».

Le esigenze che emergono sono quindi di poter disporre di tecnologie che assicurino, dal punto di vista del lavoratore, mobilità, connettività rapida e stabile per favorire la collaborazione, e strumenti di produttività sempre accessibili, senza trascurare soluzioni di sicurezza in grado di salvaguardare i dati e la privacy dell'utente, elemento fondamentale in un mondo nel quale, solo lo scorso anno, sono stati violati 1,4 miliardi di password e dove si stima che nel 2019 ci sarà un attacco ransomware ogni 14 secondi.

Per quanto riguarda l'ambiente lavorativo, il moltiplicarsi delle huddle room comporta la necessità di equipaggiare le sale riunioni con soluzioni tecnologiche di collaborazione, con investimenti stimati a livello globale di oltre 11 miliardi di dollari in soluzioni intelligenti di videocomunicazione entro il 2020.

Si tratta quindi, suggerisce Lenovo, di combinare tecnologia, spazi di lavoro e cultura aziendale per creare un'esperienza lavorativa che attiri nelle aziende i migliori talenti, oltre a guidare la produttività. Le aziende più moderne stanno già lavorando per concepire spazi di lavoro che favoriscano la collaborazione e il contatto umano, grazie anche a soluzioni di smart meeting, display interattivi e altro.

Un risposta concreta è ad esempio quali Lenovo ThinkSmart Hub 500, con cui Lenovo si è proposta di dare la possibilità di trasformare profondamente una sala riunioni e di convertire qualsiasi spazio in una sala riunioni Skype for Business. Tramite qualità del suono Dolby Audio

Premium, microfoni direzionali a 360°, display touch per gestire le riunioni e display esterni di grandi dimensioni, il dispositivo Skype Room Systems è suggerito come ideale per le sale riunioni di piccole e medie dimensioni.

Aspettative in crescita per il cloud ready

Un altro aspetto va poi considerato. Con l'ingresso nella forza lavoro di giovani sempre più abituati all'uso quotidiano della tecnologia, cresce anche l'aspettativa da parte dei dipendenti di avere dispositivi simili a quelli che utilizzano anche fuori dal contesto lavorativo, quindi interattivi, sempre connessi, sempre disponibili.

Le aziende che avranno successo in futuro saranno molto probabilmente quelle che sapranno trovare il migliore equilibrio fra produttività, inclusione e un approccio personale che tenga conto di un nuovo modo di lavorare. L'efficienza degli ambienti lavorativi passa anche dall'aver a disposizione strumenti potenti, leggeri ed eleganti che assicurano prestazioni di calcolo elevate e al contempo riflettono la personalità dell'utente, accompagnandolo tanto nel lavoro quanto nel tempo libero.

Un altro aspetto della trasformazione dei luoghi di lavoro è rappresentato dalla capacità che mostreranno le organizzazioni più lungimiranti di fornire ai dipendenti dispositivi pre-configurati e cloud-ready, che consentano di progettare spazi di lavoro agili, creativi e sempre più produttivi.

Attraverso i propri dispositivi e soluzioni, ha commentato Lenovo, la società si è proposta di contribuire a trasformare la produttività e la collaborazione in azienda, aiutando le persone a lavorare in modo più efficiente grazie a un uso efficace delle tecnologie emergenti e, con strumenti IT intelligenti aiutare la trasformazione delle pratiche aziendali attraverso la tecnologia, promuovendo l'innovazione attraverso l'Intelligent Transformation.

CHECKME DI CHECK POINT E CIE TELEMATICA CONTROLLA LA SICUREZZA NEL CLOUD

CIE Telematica, in partnership con Check Point, ha reso disponibile "CheckMe", un servizio che valuta e identifica i rischi relativi alla sicurezza di rete, endpoint, cloud e dispositivi mobili



Assicurare la sicurezza ai propri ambienti on premise o nel cloud richiede investimenti e preparazione, personale qualificato e processi organizzativi.

Si tratta di un insieme di aspetti all'altezza di grandi aziende, ma difficilmente affrontabili nel loro complesso da parte delle PMI, che soprattutto in una fase economica come l'attuale sono già impegnate nella digitalizzazione e nella migrazione dell'IT al cloud, e possono non disporre delle risorse economiche e soprattutto tecniche per farvi fronte.

La realtà IT di una PMI, a parte le dimensioni di scala, non è però diversa in quanto a esigenze di sicurezza, da quelle di una grande corporate o grande azienda e coinvolge gli stessi 4 punti chiave del processo verso la digitalizzazione, sia che si tratti della parte office che produttiva.

Ma cosa può fare una PMI senza spendere un capitale in soluzioni per poi scoprire che non coprono le sue reali esigenze o l'investimento realizzato distogliendo Capex dal core business per verificare lo stato del proprio IT e valutare la sua esposizione al rischio? Innanzitutto capire le proprie vulnerabilità.

Identifica le vulnerabilità con CheckMe

Una soluzione ritagliata sulle esigenze delle PMI l'ha identificata CIE Telematica, società di ingegneria con una forte esperienza nella realizzazione di reti di accesso fisse e mobili ad elevata sicurezza.

Tramite una partnership con Check Point propone una soluzione, "CheckMe", che permette di ottenere una valutazione proattiva e che identifica i rischi relativi alla sicurezza dei quattro punti chiave di una infrastruttura aziendale: rete, endpoint, cloud e dispositivi mobili.

Il suo obiettivo, ha osservato **Luigi Meregalli**, general manager di CIE Telematica, è di fornire rapidamente un rapporto dettagliato che evidenzia quali sono le vulnerabilità ransomware, zero day threats, malware infections, browser exploit, perdita di dati e altro ancora, che possono coinvolgere e costituire una minaccia per l'IT, dati e processi di business. Il tutto, ha aggiunto il manager, in un paio di minuti.

Per semplificarne l'uso da parte di PMI e di personale non particolarmente esperto la soluzione si presenta in modo schematico e user

friendly con una console che permette, dopo aver cliccato su CheckMe, di selezionare una delle quattro opzioni disponibili selezionando, in base a cosa si vuole valutare come sicurezza, tra:

- Network,
- Endpoint,
- Cloud
- Mobile

Dopo la selezione, CheckMe entra in funzione e procede nell'analisi della componente dell'infrastruttura IT selezionata.

Al termine, basta cliccare su "Get full Report" per ottenere un report con e le linee guida suggerite da Check Point per migliorare la postura nei confronti della propria sicurezza.

Le minacce e gli scenari di attacco esaminati da CheckMe

Il campo d'azione di CheckMe si presenta molto ampio e tale, osserva Meregalli, da rispondere in modo ampio ed esaustivo alle esigenze di PMI o anche di aziende di fascia superiore. Funzionalmente CheckMe simula i vari scenari che potrebbero costituire un punto di partenza per i principali vettori di attacco. Vediamoli nei seguenti punti:

- Ransomware: un malware che cripta i file degli utenti e richiede il riscatto per la loro

decriptazione.

- Command & Control Communication: danno la possibilità ai cyber criminali di prendere il pieno controllo del computer infettato.
 - Malware Infection: lasciano che gli aggressori assumano il controllo completo su un computer infetto
 - Browser Exploit: è un attacco che sfrutta una particolare vulnerabilità in un sistema informatico
 - Anonymous surfing: può aprire backdoor nella rete di un'organizzazione
 - Data leakage: rilascio involontario o furto di informazioni riservate al di fuori della rete dell'organizzazione
 - Cloud Segmentation: scansioni per identificare possibili accessi su dispositivi raggiungibili all'interno dello stesso ambiente, per evidenziare un'assenza di controlli d'accesso.
 - Identity Theft: raccoglie dati sensibili tramite siti fasulli.
 - Zero Day attack: sfruttano lacune software.
- «Con la partnership di lunga data e strategica con Check Point e prodotti come CheckMe, abbiamo voluto rispondere alle esigenze sempre più espresse dalle PMI, ma non solo, per quanto concerne la loro sicurezza, la mobility e il passaggio al cloud», ha osservato Meregalli.



CHECK POINT METTE AL SICURO I DATI CON CLOUDGUARD SAAS

La nuova soluzione ha l'obiettivo di proteggere dalle minacce alla sicurezza in rapida evoluzione ai dati aziendali sulle applicazioni SaaS

Check Point Software Technologies, fornitore di soluzioni di cybersecurity, ha annunciato la disponibilità di CloudGuard SaaS, una suite cloud che ha sviluppato per prevenire le minacce sofisticate che hanno come target le applicazioni SaaS. Protegge le aziende che utilizzano applicazioni SaaS e la posta elettronica cloud-based (tra cui Office 365, GSuite e OneDrive), prevenendo gli attacchi mirati e destinati al furto di dati sensibili.

«Nel panorama attuale degli attacchi informatici di quinta generazione, è fondamentale implementare una tecnologia in grado di affrontare il maggior numero di minacce dirette alle applicazioni cloud aziendali - ha dichiarato **Itai Greenberg**, VP Product Management di Check Point Software Technologies -. Le aziende si rivolgono generalmente a soluzioni di Cloud Access Security Broker (CASB), che offrono visibilità e protezione dalle perdite di dati. CloudGuard SaaS, invece, va oltre le capacità di CASB. È progettato per prevenire gli attacchi più comuni alle applicazioni SaaS, garantendo sicurezza delle imprese». In pratica, osserva l'azienda, CloudGuard SaaS può essere una soluzione fondamentale in grado di fornire alle aziende la sicurezza preventiva

capace di affrontare in pochi minuti una moltitudine di applicazioni SaaS aziendali.

Le funzioni salienti della soluzione

Vediamo i punti qualificanti evidenziati da Check Point:

Prevenzione contro i malware e gli attacchi zero-day:

CloudGuard SaaS è una soluzione di prevenzione delle minacce per malware e attacchi zero-day sulle applicazioni SaaS. Sfrutta la tecnologia SandBlast di Check Point. Sfruttando queste funzionalità, CloudGuard SaaS protegge gli allegati e-mail e i download su servizi di file hosting e tool di collaborazione. In pratica, utilizzando tecnologie avanzate di emulazione ed estrazione delle minacce blocca le minacce zero-day prima che raggiungano gli utenti e fornisce contenuti sicuri.

Stop al furto degli account: CloudGuard SaaS blocca il controllo di account SaaS da parte di utenti non autorizzati, anche se il dispositivo è già compromesso. Utilizzando la tecnologia IDGuard™, CloudGuard SaaS identifica gli accessi falsi, trova login errati e centralizza l'autenticazione multi-factor. Può anche verificare gli utenti in applicazione SaaS su qualsiasi dispositivo mobile o PC.

Protezione contro il phishing: Un ultimo punto riguarda il "pescaggio". Sotto questo aspetto, evidenzia l'azienda, CloudGuard SaaS sfruttando motori di intelligenza artificiale previene più attacchi di phishing rispetto ai servizi e-mail standard. Può bloccare ad esempio phishing sofisticati, spear-phishing e spoofing delle e-mail che possono aggirare altre soluzioni di sicurezza.

CLOUD MANAGEMENT E “WIRELESS AWARENESS” LE NUOVE FUNZIONALITÀ DEGLI SWITCH ENTERPRISE

La gestione automatizzata on premise o nel cloud dà la possibilità di configurare automaticamente gli switch e operare in modo sicuro.



Nelle reti aziendali di oggi, oltre alle consuete capacità degli switch L2/L3, appare evidente come occorrano nuove funzionalità per rendere più sicura ed efficiente la connettività interna ed esterna, cablata e wireless, con una particolare attenzione alla facilità di installazione e gestione

In proposito, Rohit Mehra, Vice President Network Infrastructure di IDC ha recentemente osservato come le aziende stiano cercando di gestire la complessità odierna con una visione unificata dell'intera rete e con policy comuni su reti cablate e wireless. La commutazione a livello aziendale gestita dal cloud, in combinazione con un'architettura wireless, può fornire una rete di accesso unificata, riducendo al contempo la minaccia di violazioni della sicurezza e migliorando l'automazione con una configurazione basata su policy, che elimina configurazioni manuali, spesso soggette a errori.

Ma quali sono, nello specifico, secondo Cambium Networks, le nuove funzionalità che permettono di rispondere queste esigenze?

Innanzitutto la gestione automatizzata basata su policy dà la possibilità di configurare automaticamente i dispositivi e le porte dello

switch in base alla policy definita per ogni tipo di dispositivo previsto all'interno dalla rete. A questo si aggiunge la cancellazione automatica delle policy.

Wireless aware

Un altro elemento importante è la segmentazione della rete: fornisce un ambiente sicuro per le risorse di rete critiche, posizionando automaticamente i dispositivi nel segmento di rete più appropriato in base al loro specifico profilo. Lo switch dovrebbe inoltre essere “Wireless Aware”, cioè in grado di riconoscere e gestire appropriatamente gli oggetti wireless in rete: questo consente l'automazione delle policy, assicura facilità di monitoraggio e la risoluzione dei problemi nella rete cablata e wireless gestita in modo realmente unitario.

La gestione nel cloud

E veniamo alla gestione cloud: la piattaforma di gestione dovrebbe poter garantire una gestione esaustiva del ciclo di vita dei dispositivi, la configurazione, il controllo e tutti i servizi di sicurezza.

Per aiutare a risolvere queste criticità Cambium

Networks ha ad esempio sviluppato una linea di switch con cui si è proposta di rispondere in modo ampio e funzionale alle esigenze evidenziate, e capace di garantire di trarre il massimo in termini di prestazioni, sicurezza e facilità di gestione da tutti gli elementi che compongono una rete aziendale moderna.

«Quando abbiamo deciso di sviluppare cnMatrix, la nostra linea di switch enterprise, eravamo consapevoli di accettare una sfida importante in un mercato già ben presidiato. La gestione facilitata, completa e centralizzata tramite le nostre piattaforme di management nel Cloud

e On-Premises, garantiscono all'utente finale un'esperienza facile ed automatizzata sia nelle attività quotidiane di monitoraggio di rete che nei casi di manutenzione ordinaria e straordinaria. Il posizionamento delle nostre piattaforme di switching sul mercato, infine, garantisce, come nel caso delle soluzioni cnPilot Wi-Fi, un ottimo livello di funzionalità nei nostri mercati di riferimento: dall'enterprise al manifatturiero, dall'hospitality al retail fino alla sanità pubblica e privata», ha commentato **Marco Olivieri**, Regional Sales Manager di Cambium Networks per l'Italia.

DATA MANAGEMENT EFFICIENTE CON VERITAS E PURE STORAGE

Le società collaborano per migliorare la gestione dei dati, dalla loro protezione alla generazione di valore per la competitività delle aziende



Il data management è un aspetto complesso per le aziende. A causa della rapida crescita e frammentazione dei dati, le imprese faticano a gestire, proteggere e ottenere informazioni dai dati. L'intelligenza moderna richiede una tecnologia che non solo memorizzi i dati, ma che sia anche in grado di generare insights da questi.

Veritas Technologies, che si occupa di protezione dei dati aziendali e di software-defined storage, in collaborazione con Pure Storage, piattaforma storage all-flash, ha annunciato una nuova collaborazione a livello globale. L'obiettivo è aiutare i clienti comuni a modernizzare la

protezione dati e a massimizzarne il loro valore per ottenere un vantaggio competitivo.

L'annuncio si inserisce nell'ambito della collaborazione tra Veritas e Pure Storage che offre l'adozione congiunta di tecnologia, miglioramenti dei prodotti, vendite e supporto. Veritas e Pure Storage forniscono ai propri clienti un approccio semplice ed economico per fronteggiare le sfide nel data management.

La collaborazione si è proposta di consolidare i moderni carichi di lavoro sull'architettura data hub di Pure Storage, powered by Pure Storage FlashBlade. Grazie all'integrazione di NetBackup, la tecnologia di punta di Veritas, i dati

aziendali possono essere condivisi, protetti e utilizzati per ottenerne più valore.

Basato su FlashBlade, il data hub di Pure Storage centralizza i dati per facilitare un approccio unificato degli analytics, del backup, dei data lake e dei cluster di intelligenza artificiale (AI). Veritas NetBackup è in grado di proteggere un'intera architettura data hub basata su FlashBlade e può anche sfruttarla come target di backup, con rapidi ripristini quando necessario. Inoltre, Veritas NetBackup, insieme a Veritas CloudPoint, è stato integrato con Pure Storage FlashArray, consentendo la gestione completa degli snapshot tramite la console di NetBackup. Il consolidamento delle tecnologie tra le due aziende consente di sfruttare l'AI e il machine learning su set di dati più grandi e diversifica-

ti. Questo consente di avere una migliore una business intelligence utile per fare innovazione.

Migliorare il recupero dei dati e la velocità

Veritas e Pure Storage aiutano le aziende multi-cloud a ottenere più agilità e velocità, grazie alla protezione integrata basata su snapshot per le soluzioni di storage scale-out flash. Con l'integrazione di Veritas NetBackup e CloudPoint, le organizzazioni possono raggiungere RTO (Recovery Time Objective) più efficaci e avere una protezione performante dei dati su storage flash. Ciò consente ai clienti di soddisfare i rigorosi obblighi in termini di RTO e RPO (Recovery Point Objective) nel settore finanziario, nella Sanità e in altri settori verticali in cui la normativa impone il recupero e la resilienza dei dati.

CASE STUDY

VEEAM SUPPORTA LA DIGITAL TRANSFORMATION DI TELETHON

Veeam Availability Suite ha fornito una piattaforma di backup sicura, scalabile ed affidabile per garantire la continuità operativa di importanti iniziative di raccolta fondi



Veeam Software, fornitrice di soluzioni di Intelligent Data Management per la Hyper-Available Enterprise e guidata nel Southern EMEAR Region di Veeam da **Albert Zammar**, ha annunciato che Fondazione Telethon, una delle principali charity biomediche italiane, ha scelto la Veeam Availability Suite come piattaforma preposta a garantire la business continuity, abilitare la disponibilità dei dati e rafforzare

la sicurezza a supporto di importanti iniziative di fundraising.

La missione di Fondazione Telethon è, come noto e viene da aggiungere meritoriamente, quella di far avanzare la ricerca biomedica sulle malattie genetiche rare e le sue campagne di fundraising rappresentano uno dei principali canali di approvvigionamento finanziario per l'attività di ricerca che assiduamente svolge.

Grazie alle diverse iniziative di raccolta fondi, tra le quali la maratona televisiva in partnership con Rai, la raccolta ha superato, solo nel 2017, i 31 milioni di euro.

Fondazione Telethon opera in sedi multiple: alle due sedi operative di Milano e Roma, si affiancano l'Istituto Telethon di Pozzuoli e l'Istituto Telethon di Milano. Per operare a livello IT l'azienda ha due data center che gestiscono 18TB di dati in ambiente VMWare e ha scelto Veeam Availability Suite per le sue caratteristiche di semplicità operativa, praticità e facilità di configurazione, garanzia di continuità operativa e solide prestazioni.

Con Veeam backup e replication scalabili

Le funzionalità di backup e replication scalabili accelerano le prestazioni di business, oltre a permettere al team di 6 addetti IT di gestire workload scalabili in modo efficiente e più semplice rispetto al passato.

In pratica, ha evidenziato Veeam, tramite una sola console di management, Fondazione Telethon ha anche un migliore controllo sui dati sensibili e le funzionalità di reporting e di monitoraggio costante dei potenziali problemi garantiscono le prestazioni necessarie durante i picchi di traffico elevatissimi raggiunti in occasione delle campagne di fundraising. La tecnologia di data loss avoidance di Veeam e la velocità di recovery assicurano inoltre la disponibilità di copie regolari dei dati ed il loro rapido ripristino in caso di malfunzionamenti.

«La business continuity è condizione essenziale per Fondazione Telethon ed è determinante per il successo di una campagna di raccolta fondi. La maratona TV che annualmente organizziamo genera un altissimo numero di visitatori al nostro sito e le donazioni online sono una componente importantissima per sostenere la ricerca. Non possiamo permetterci interruzioni dei servizi», ha commentato **Marco Montesanto**, IT Manager di Fondazione Telethon. «Con Vee-

am possiamo contare sul fatto che i dati siano sempre disponibili, protetti e al sicuro e tutto ciò ci permette di ottimizzare le prestazioni di business, evitare interruzioni e, dal ultimo, essere conformi alle normative GDPR».



Albert Zammar - Veeam

Albert Zammar, ha aggiunto: «Affidabilità, sicurezza e disponibilità sono essenziali per l'operatività di Fondazione Telethon, che deve gestire dati sensibili, da quelli relativi ai versamenti durante le campagne di fundraising a quelli relativi alla ricerca. La priorità di Fondazione Telethon deve essere di trovare cure adeguate per salvare delle vite, non quella di preoccuparsi dei backup dei dati. Le nostre soluzioni riducono i tempi e gli sforzi che i team IT dedicano alla protezione e alla gestione manuale dei dati, permettendo loro di focalizzarsi sul portare valore aggiunto al business».

Dati di mercato

A livello di portfolio Veeam, la sua Hyper-Availability Platform è una soluzione sviluppata per aiutare le aziende ad automatizzare la gestione dei dati e ad assicurare la Hyper-Availability dei dati.

Significativi i dati economici, di mercato e di soddisfazione della clientela. Alla data annovera oltre 307.000 clienti nel mondo, tra cui il 75 per cento delle aziende Fortune 500 e il 58 per cento delle aziende Global 2000. L'indice di soddisfazione dei clienti, al 3.5X della media, è tra i più alti di mercato. Dispone poi di un ecosistema globale che include 57.600 partner di canale, con società di primissimo piano come Cisco, HPE e NetApp quali rivenditori esclusivi; circa 19.800 cloud e service provider.

CYBERARK LEADER NEL MAGIC QUADRANT 2018 DI GARTNER PER IL PRIVILEGED ACCESS MANAGEMENT

Gartner ha posizionata CyberArk al vertice del suo Magic Quadrant nell'esecuzione e al massimo livello nella vision strategica e l'efficacia delle soluzioni on-premise e nel cloud

CyberArk ha annunciato di essere stata nominata leader nel Magic Quadrant 2018 di Gartner per il Privileged Access Management, identificato come la massima priorità di sicurezza per i CISO per difendersi dai moderni attacchi informatici.

Il riconoscimento di Gartner l'ha peraltro posizionata al vertice nell'esecuzione e al massimo livello nella vision strategica e per soluzioni disponibili

Al riconoscimento ha contribuito anche il fatto che la sua soluzione CyberArk Privileged Access Security è utilizzata dalla maggior parte delle società Fortune 500 e da organizzazioni governative in tutto il mondo.

«Da quando è emerso il mercato della gestione degli accessi privilegiati, CyberArk è stata assiduamente impegnata nella sua missione di continua innovazione e nel guidare il mercato con soluzioni che incrementano

enormemente la sicurezza, riducono il rischio e migliorano la soddisfazione del cliente», ha commentato il riconoscimento ottenuto **Marianne Budnik**, CMO di CyberArk.

Un Magic Quadrant in forte crescita come interesse

La crescita dell'interesse per Magic Quadrant per il Privileged Access Management è una sorta di pietra miliare significativa per il mercato della sicurezza ed evidenzia il crescente interesse dei CISO.

Quella che sino a poco tempo costituiva poco più che un sorta di nicchia nel settore e nel mercato della sicurezza ora, secondo quello che è riconosciuto come uno dei maggiori analisti del settore al mondo, si avvia a diventare una vera e propria priorità strategica.

La maggior parte delle violazioni dei dati, osserva infatti CyberArk, inizia con l'uso im-



Marianne Budnik - CyberArk

proprio di credenziali e segreti aziendali, come dimostra la proliferazione di violazioni dei dati di alto profilo verificatisi al mondo e in diversi settori critici quest'anno.



È uno scenario in cui la gestione degli accessi privilegiati si evidenzia essere sempre più cruciale per garantire e proteggere le organizzazioni, nonché i loro account business-critical, dagli attacchi maligni di vario tipo che oramai si trovano a fronteggiare su base pressoché regolare.

A livello di analisi e di contenuti il rapporto che accompagna il Magic Quadrant mette in primo piano l'importanza dei privilegi come strumento critico per il controllo della sicurezza.

Annunciato al Gartner Identity & Access Management Summit di Las Vegas può essere scaricato gratuitamente, tramite CyberArk, all'indirizzo: <https://www.cyberark.com/pr/gartner-mq-pam-leader-it/>.

Perché cresce l'importanza del Magic Quadrant

La crescita dell'importanza della protezione degli account privilegiati è confermata dai dati di mercato e dalle statistiche, che evidenziano come il 100% degli attacchi avanzati interessi oramai le credenziali privilegiate, indubbiamente quelle a maggior valore per un attaccante

(CyberSheath, The Role of Privileged Accounts in High Profile Breaches, 2014). È un obiettivo di attacchi che, come già evidenziato, è al centro degli interessi e in

modo prioritario dei progetti di sicurezza dei CISO. Altri dati significativi evidenziati da analisti e società di ricerca sono parimenti:

- Costo medio di un data breach pari a 3.86 milioni di dollari (Ponemon Institute, 2018 Cost of a Data Breach Study)
- 101 i giorni che trascorrono prima che un attacco venga individuato (Mandiant M-Trends 2018 Report)
- 90% il numero di organizzazioni che si sentono vulnerabili a un attacco portato dall'interno (Crowd Research Partners, 2018 Insider Threat Report)

Non ultimo, si prevede che entro il 2019 un business cadrà vittima di un attacco di tipo ransomware ogni quattordici secondi (Cybersecurity Ventures, 2017 Annual Cybercrime Report) mentre il 72% delle stesse aziende ritiene di non essere in grado di gestire e controllare adeguatamente l'accesso dei propri dipendenti ad informazioni di alto valore (Risky Business: How Company Insiders Put High Value Information at Risk," Ponemon Institute).