Cloud & Business

n.94
Settembre 2020

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

GESTIONE E SICUREZZA LA CHIAVE PER UN CLOUD EFFICIENTE

di Giuseppe Saccardi

Il cloud ibrido e il multicloud richiedono una efficace gestione dei dati e adeguati servizi di sicurezza

Se l'esternalizzazione della complessità dell'IT permette di ottimizzare Capex e Opex, ciononostante presenta aspetti che coinvolgono il come gestire l'insieme delle risorse locali e nel cloud, come gestire i servizi di business continuity e di recovery, come orchestrare le risorse, gestire la sicurezza complessiva.

Sono aspetti critici e che richiedono estrema attenzione sia nell'orchestrazione delle risorse che nella scelta delle tecnologie atte ad implementare una strategia di gestione e di protezione efficace e sicura nel tempo

E' una sorta di condizione sine qua non al fine di garantire che l'infrastruttura IT fisica e virtuale e i servizi erogabili tramite essa sia in forma di cloud, che cloud ibrido o multicloud sia sempre "always-on" e disponibile.

Numerosi i problemi che si presentano, dalla gestione dei dati non strutturati, ad esempio, sino al come garantire la sicurezza dei dati, soprattutto nel caso di utenza privilegiata. I

Reportec Cloud&Business - N.94 Settembre 2020 - società- Editore: Reportec Srl (**www.reportec.it**) - Direttore responsabile: Giuseppe Saccardi
In redazione: Gaetano Di Blasio - Paola Saccardi - Immagini: Dreamstime.com

paragrafi seguenti espongono il punto di vista e cosa fatto in proposito da aziende specializzate del settore.

LA GESTIONE DEI PETABYTE NON STRUTTURATI E L'APPROCCIO FINIX

La gestione dei dati verte necessariamente su piattaforme storage e su nuovi approcci architetturali che rispondono alla distribuzione dei dati in data center a livello di edge. In proposito, Fujitsu, distribuita in Italia da FINIX Technology Solutions, ha sviluppato e introdotto sul mercato una nuova soluzione storage che fa leva sulla tecnologia software-defined per permettere alle aziende di gestire petabyte di dati sparsi all'interno del cloud e di differenti data center.

La nuova piattaforma per dati organizzati in file (realizzata da Qumulo) è una soluzione ideata per poter gestire e accedere ai dati organizzati in file ed abilitare la creazione di nuovi servizi e nuove applicazioni all'interno dello storage enterprise su larga scala.

Le aziende, osserva Fujitsu, si stanno rendendo conto delle opportunità che possono scaturire dall'analisi di molteplici fonti di dati per dare un impulso significativo alle rispettive operazioni di business.

Processi differenti tra loro come l'imaging diagnostico, la modellazione, le simulazioni, le applicazioni LIDAR, i sistemi GIS, il sequenziamento genetico e la produzione video ruotano tutti intorno alla creazione e all'utilizzo di dati non strutturati.

Tuttavia, la gestione di volumi sostanziali di dati organizzati in file si rivela spesso difficile, specialmente dal momento che essi possono essere distribuiti tra l'edge di rete – provenienti da dispositivi IoT – oltre che on-premises e nel cloud.

Cristian Antonucci - Finix

Nello specifico, il file system di Qumulo, in un tale scenario, si propone proprio di mettere a disposizione scala, controllo dei dati e visibilità in tempo reale sia on-premises che nel cloud, anche a livello granulare.

LA GESTIONE DEI DATI NON STRUTTURATI

Appositamente progettato per ambienti ibridi che abbracciano il data center, i cloud privati e i cloud pubblici, Qumulo, ha spiegato FINIX, permette agli utenti di condividere informazioni supportando nel contempo molteplici protocolli storage che rendono possibile il consolidamento dei dati.

L'accorgimento semplifica la gestione dei dati all'interno degli ambienti distribuiti e fornisce la capacità di assorbire la crescita imprevedibile dei dati non strutturati e rispondere alle richieste di dati proviene da crescenti quantità di applicazioni residenti sia nel cloud che al di fuori di esso.

In particolare, il nuovo approccio seguito da Fujitsu con la soluzione Qumulo si basa su una information repository ad alte prestazioni realizzata su misura, "in grado di scalare illimitatamente per permettere ai clienti di setacciare enormi quantità di dati per trovare quelle pepite che possiedono un valore effettivo".

TRASFORMAZIONE DATA-DRIVEN

Va osservato che la soluzione Qumulo si inserisce nel secondo dei quattro livelli in cui è suddivisa la strategia di trasformazione data-driven di Fujitsu – quella che comporta la creazione dell'architettura dati di destinazione una volta che sia stata definita la baseline della trasformazione dei dati.

«La soluzione Qumulo, basata su un file system di tipo 'cloud-native', grazie al quale è possibile scalare non solo in termini di capacità, ma anche di numerosità degli oggetti, arriva a supportare diverse decine di miliardi di file - ha spiegato **Cristian Antonucci**, Sales Specialist di FINIX Technology Solutions -. La capacità locale e quella in cloud possono essere gestite come un 'unico file system'; in questo modo Qumulo permette il trasferimento di workload da e verso il cloud pubblico. Per un cliente, questo significa poter estendere – temporaneamente - la potenza di calcolo che ha localmente con quella disponibile sul cloud pubblico e rispondere quindi a eventuali picchi di domanda. Inoltre, il dato è sempre fruibile dalle applicazioni, a prescindere dalla propria posizione; mediante API, infatti, è possibile definire dei microservizi che consentono alle applicazioni l'access ai dati indipendentemente che siano in locale o nel cloud».

DATI SICURI CON CYBERARK SU MICROSOFT AZURE

Un problema correlato ai dati nel cloud è come proteggerli , e farlo in modo efficace si aa livello di dato in sé che di utente. CyberArk, attore globale nella gestione degli accessi privilegiati, ha annuncia in proposito la disponibilità della propria soluzione di protezione degli accessi privilegiati sul Marketplace Microsoft Azure.

La soluzione CyberArk Privileged Access Security, ha spiegato la società, offre un approccio esaustivo alla sicurezza e all'efficienza operativa nel cloud attraverso il rilevamento continuo e la protezione degli account privilegiati; funzionalità just-in-time per un accesso flessibile ai sistemi Windows sia in cloud che on-premise, un rilevamento e risposta alle minacce in grado di prioritizzare gli avvisi in base a comportamenti potenzialmente rischiosi, nonché la possibilità di prendere il controllo rapidamente degli account pericolosi.

PROTEZIONE ELEVATA DELLE CREDENZIALI PRIVILEGIATE

Per i clienti Azure, l'accesso a CyberArk ha il compito di garantire una maggiore flessibilità ed efficienza nella protezione delle credenziali privilegiate nel cloud e una riduzione dei rischi legati ai privilegi, ottimizzando inoltre i vantaggi aziendali delle strategie cloud-first.

Con le soluzioni CyberArk le organizzazioni possono, in sostanza, dare priorità alla gestione degli accessi privilegiati e proteggere applicazioni, servizi e altre risorse nel cloud.

«Con la disponibilità su Microsoft Azure Marketplace, CyberArk continua a supportare le organizzazioni nel semplificare e automatizzare la protezione degli account privilegiati ovunque siano, aiutando al

Adam Bosnian - Cyberark

contempo i clienti che scelgono di investire in numerosi ambienti cloud» sottolinea **Adam Bosnian**, Executive Vice President Global Business Development di CyberArk.
Sul piano del suo utilizzo Azure Marketplace è una piattaforma online dedicata all'acquisto e alla vendita di soluzioni cloud certificate per operare su Azure e aiuta a mettere in contatto le aziende che cercano soluzioni innovative basate su cloud con i partner che hanno sviluppato soluzioni pronte all'uso.

SERVIZI DI FIREWALL DI ACANTHO E RADWARE A PROTEZIONE DALLE MINACCE


Gianluca Ulisse - Acantho

Proteggere dati e applicazioni è sempre più complesso a seguito della diffusione del cloud, dell'IoT e di strumenti di attacco sofisticati reperibili sul Web.
Un punto sulla situazione e sul cosa fare è stato fatto da **Gianluca Ulisse**, Product marketing manager dei servizi data center di Acantho (www.acantho.com), che ha esaminato per noi lo stato dell'arte e di come sia possibile difendersi efficacemente e con quali strumenti.
Acantho è la digital company del Gruppo Hera che fornisce ad aziende e privati una connettività in fibra ottica ad alte prestazioni, elevata affidabilità, con alta sicurezza di sistemi, dati e continuità del servizio tramite Data Center di proprietà situati a Imola e a Milano.
«Gran parte delle attività che svolgiamo su Internet inizia dal web e dai suoi server, un ambiente che comprende a sua volta altre tipologie di server (di autenticazione, database e così via) che tramite interfacce software dialogano con altri server terzi nel cloud. Con il diffondersi dell'IoT vi sono poi macchine che dialogano con altre macchine, a cui si aggiungono le app degli smartphone. Questa evoluzione è la causa di nuove tecniche e ambiti di attacco e il cybercrime è diventata una delle più profittevoli attività criminali.
Il cybercrime è molto articolato ed è naif associarlo al mero furto delle carte di credito. Ora esistono strumenti per bloccare i servizi web dell'azienda, trafugarne informazioni e dati dei clienti, distorcere la vendita o la disponibilità dei beni, agire sulla reputazione tramite i commenti dei clienti o chiedere riscatto per i dati aziendali.
Per analizzare i nuovi ambiti di attacco è stata fondata nel 2001 OWASP (Open Web Application Security Project) una fondazione no-profit americana per la sicurezza delle web application, che annovera come membri le aziende di cybersecurity e cura un report sulle 10 principali minacce in ambito delle Web Application (OWASP Top 10).

IL RISCHIO DEI BOT E ZERO DAY

Ma se conosciamo le principali minacce il percorso è da considerarsi concluso? Non proprio, in quanto si devono considerare i web robot (Bot) ovvero programmi che girano sul web per specifici compiti e il cui traffico è quasi equivalente a quello degli "umani".
E anche nei Bot vi sono i buoni e i cattivi. I buoni esaudiscono le nostre richieste tramite Siri, Alexa, Google, cercano contenuti, reperiscono news, valutano offerte, dialogano con gli utenti. I cattivi invece possono mettere in atto

varie azioni: ottenere i dati degli utenti di un sito, simulare un utente, falsare le richieste, operare recensioni, variare i prezzi, distorcere le analisi dell'utenza per il sito.
Il problema è che i Bot "cattivi" si presentano come utenti normali, ed è attraverso l'impronta digitale di tali Bot (il Device Fingerprinting) e il loro comportamento che si riesce a desumerne la natura digitale.
Anche l'intelligenza artificiale può dare una mano. Gli algoritmi basati sul machine-learning forniscono una protezione in tempo reale aggiornando automaticamente le policy di sicurezza per salvaguardare le applicazioni web, mobile e cloud, ivi incluse le API, e minimizzando i falsi positivi. Quest'ultimo aspetto è però possibile per le grandi organizzazioni di sicurezza digitale che dispongono di quantità di dati globali e in tempo reale e team di esperti che valutano le situazioni ambigue.
Ma vi è un altro aspetto da considerare, il cosiddetto "Distributed Denial of Service" (DDoS) il cui scopo è di bloccare l'accesso al sito, e di farlo in modo apparentemente corretto.
È come se ad un ufficio postale, abituato ad avere 10 clienti all'ora ne arrivassero 10.000. L'effetto è che non sarebbe in grado di servire i clienti reali, poiché, tornando nel mondo web, quei 10.000 clienti sono degli "zombie" digitali, ovvero dispositivi ignari e non protetti (ad esempio telecamere IP) utilizzati per inoltrare le richieste. Essendo distribuite si può bloccarne una ma bloccarle tutte implica bloccare anche le richieste valide degli umani.
Ma non è tutto, vi sono anche gli "zero day". Sono nuovi attacchi così giovani da avere zero day di anzianità. Essendo sconosciuti i sistemi basati su un archivio dei "cattivi", riferito come "negative security model", li lasciano passare. Il metodo complementare è il "positive security model", che fa passare solo gli accreditati ma che comporta un maggiore lavoro nell'aggiornare le liste degli utenti accreditati e che richiede sistemi di machine learning e il contributo di esperti.
Questo ecosistema di attacchi ha caratteristiche comuni: sono massivi, automatici, provengono da fonti diverse (IoT, microservizi e server in cloud) e attaccano e si adattano in real time. Ciò comporta capacità di risposte a loro volta in real time, che si adeguano alla tipologia dell'attacco e riescono a far fronte a molteplici (sia in tipologia che quantità) attacchi.

COSA FARE PER PROTEGGERSI

Cosa è possibile fare? Una risposta è il servizio di Cloud Web Application Firewall di Acantho (powered by Radware), in grado di rispondere a questo ecosistema di minacce perché copre totalmente le minacce OWASP Top 10, ha un suo Device Fingerprinting per riconoscere gli attacchi indipendentemente dall'indirizzo IP di provenienza, fornisce la protezione completa delle API, abilita policy auto evolutive tramite il machine learning e adotta il positive security model per proteggere dagli zero day. A questo aggiunge la protezione proattiva dai Bot verso gli attacchi massivi e la protezione dagli attacchi DDoS, il tutto con un servizio gestito H24 dal team di esperti Radware.
Non ultimo, è un servizio di tipo aperto che non richiede come precondizione di essere clienti Acantho per quanto concerne la connettività utilizzata o il luogo in cui risiedono le proprie applicazioni.
E' in sostanza un servizio tramite il quale Acantho ha voluto dare, assieme a Radware, una concreta ed efficace risposta alle esigenze di cybersecurity dei clienti».

DAL BACKUP AL RIPRISTINO LE OPPORTUNITÀ DI SOLARWINDS PER GLI MSP

Salvare i dati non basta, poi viene il ripristino. SolarWinds, fornitore di software di gestione, ha annunciato la percentuale di adozione dei test del ripristino di SolarWinds Backup da parte degli MSP.

Alex Quilter - Acantho

Le cifre confermano l'elevata esigenza di automazione nel mercato per migliorare la velocità di risposta a eventuali disastri e aumentare l'efficienza.

In pratica, oltre 400 partner di SolarWinds MSP hanno iniziato a utilizzare la funzionalità a partire dal suo lancio sul mercato nel mese di giugno 2020 e l'hanno implementata su oltre 3.110 dispositivi.

Utilizzando il test del ripristino, gli MSP hanno avuto la possibilità di trasformare i servizi di sicurezza in un fattore di differenziazione.

Con SolarWinds Backup, spiega l'azienda, è possibile verificare a prima vista se le attività di backup sono state completate correttamente, con errori o se non sono andate a buon fine.

Il test del ripristino offre funzionalità specifiche per il ripristino automatizzato dei server più importanti, oltre a report programmati che includono la verifica tramite screenshot dello stato del sistema ripristinato.

Automatizzando la procedura di test del ripristino, gli MSP hanno in pratica la possibilità di affidarsi in sicurezza ai backup eseguiti, risparmiare tempo e risorse e accelerare la risposta a eventuali disastri per i clienti.

Non è necessario, ha evidenziato la società, alcun dispositivo hardware e la funzionalità può essere attivata direttamente da SolarWinds Backup, selezionando report automatici programmati ogni 30 o 14 giorni. «Il backup non consente solo di conservare una seconda copia dei dati - ha spiegato **Alex Quilter,** Vicepresidente dei prodotti, SolarWinds MSP -. Offre anche un'adeguata protezione dei dati e la possibilità di tornare operativi rapidamente in caso di disastri. Volevamo semplificare e rendere economica questa procedura il più possibile per i nostri MSP e offrire loro la possibilità di dimostrare ai clienti quanto sia importante. Ecco perché abbiamo lanciato sul mercato le funzionalità di test automatizzato del ripristino: la relativa implementazione è semplicissima e offre risultati di reportistica rapidi».

Arrow Electronics e AWS assieme per il cloud multi-tier

Arrow ha superato il traguardo delle 100 Certificazioni AWS e ha integrato i servizi in ArrowSphere, la propria piattaforma di gestione del cloud multi-tier

Alexis Brabant - Arrow ECS

Arrow Electronics, fornitore di soluzioni tecnologiche IT, ha esteso la collaborazione con Amazon Web Services (AWS) con l'obiettivo dichiarato di aumentare significativamente le certificazioni AWS e dare il via a un programma dedicato di training.

Sul piano pratico ha già integrato AWS nella piattaforma cloud ArrowSphere in 19 paesi europei e ora dispone delle certificazioni praticamente in tutti i principali comparti, tra cui quelli legati alle infrastrutture, alle operation, ai developer e alla specializzazione in sicurezza.

Complessivamente, ha evidenziato, ha superato il traguardo delle 100 Certificazioni AWS attraverso l'AWS Partner Network (APN). Le certificazioni AWS convalidano l'esperienza accumulata nel cloud computing per permettere ai clienti di distinguere i partner APN in possesso di una approfondita esperienza e competenza nel settore ed è basata sul livello consolidato di relazioni che ha portato Arrow a disporre su scala europea di un ampio portfolio di servizi AWS.

Operativamente, ArrowSphere, una piattaforma di gestione del cloud multi-tier, è stata progettata per semplificare la connessione tra i fornitori di servizi cloud, i rivenditori e i clienti finali.

La piattaforma abilita i rivenditori fornendo loro un'unica piattaforma per acquistare e gestire prodotti e servizi cloud (IaaS, PaaS e SaaS), monitorare l'attività e i consumi con strumenti di business intelligence integrati, vendere i propri servizi con una vetrina personalizzabile, e semplificare il processo di fatturazione.

«Aver raggiunto il traguardo delle 100 certificazioni AWS è una grande conquista e convalida il duro lavoro e l'impegno dei nostri specialisti. Come distributore a valore aggiunto leader nel canale cloud, ci impegniamo ad aiutare i clienti a sviluppare nuove potenzialità, assicurando la miglior practice in cloud e ottimizzando la loro esperienza AWS», ha commentato **Alexis Brabant**, Vice President Sales di Arrow Enterprise Computing Solutions in EMEA.

Affrontare la fase 2 con PC e Workstation Linux di nuova generazione

Lenovo ha annunciato nuovi PC ThinkPad e ThinkStation con sistema operativo Ubuntu preinstallato che semplifica il passaggio alla fase 2 in house e nel cloud

Lenovo ha annunciato un'estensione globale del proprio portfolio Linux, includendo nel programma di certificazione, annunciato lo scorso giugno, i PC con sistema operativo Ubuntu LTS di Canonical preinstallato.
Già disponibili per le aziende su richiesta specifica, è da oggi possibile, ha osservato, accedere a un portfolio di circa 30 dispositivi con sistema operativo Ubuntu preinstallato.
Il portfolio di PC comprende: 13 workstation ThinkStation e ThinkPad Serie P e 14 laptop ThinkPad T, X, X1 e serie L, tutti con la versione 20.04 LTS di Ubuntu, tranne la serie L che sarà dotata della versione 18.04.
«La vision di Lenovo 'Smarter Technology for All' significa veramente che le tecnologie intelligenti saranno a disposizione di tutti. L'annuncio di giugno sulla certificazione dei dispositivi è stato un passo nella giusta direzione di abilitare gli utenti a installare Linux direttamente e con maggiore flessibilità. Il nostro obiettivo è di rimuovere le complessità e fornire alla comunità Linux l'esperienza di alto livello per cui siamo rinomati fra i nostri clienti. Ecco perché siamo andati un passo oltre in modo da fornire dispositivi predisposti per Linux», ha dichiarato **Igor Bergman**, Vice President, PCSD Software & Cloud di Lenovo.
L'estensione è volta favorire una maggiore accessibilità alle app, librerie e tool open source per aumentare la produttività degli sviluppatori, senza dover affrontare i dispendiosi processi di installazione di Linux sul proprio dispositivo.
«L'estensione della certificazione di Lenovo ai dispositivi precaricati con Ubuntu mostra un grande impegno verso l'open source e la comunità Linux. Con il crescere dell'adozione di Linux da parte di sviluppatori e analisti di dati, che va di pari passo con il presentarsi di nuovi carichi di lavoro, questa collaborazione consente alle imprese di fornire ai propri dipendenti dispositivi stabili nel lungo periodo, oltre a una maggiore sicurezza e a una gestione semplificata dell'IT», ha commentato **Dean Henrichsmeyer,** VP Engineering di Canonical.
In pratica, tramite dispositivi precaricati con la versione OEM di Ubuntu, Lenovo ha inteso rimuovere un elemento di complessità, fornendo anche agli utenti un supporto telefonico e via web per la gestione di soluzioni legate alla piattaforma Linux.

Per la new economy serve business agility e resilienza

La release Paris della Now Platform di ServiceNow accelera la digital transformation e si propone di aiutare le aziende nel connettere i team e i sistemi

Filippo Giannelli - ServiceNow

Con l'obiettivo dichiarato di facilitare l'interazione nell'epoca del Covid e, auspicabilmente, post Covid, ServiceNow, azienda attiva nei workflow digitali, ha annunciato Paris, la nuova release delle Now Platform.

L'obiettivo è di aiutare le organizzazioni a rimanere agili e resilienti e a migliorare la produttività nell'economia della nuova normalità. In pratica, le persone potranno lavorare in maniera più intelligente e le aziende capitalizzare velocemente gli investimenti tecnologici.

La genesi e il perché della nuova proposta la si trova nelle crude cifre. Secondo IDC, il 45% delle organizzazioni in tutto il mondo è in recessione, con il 64% delle aziende che pianifica di adottare tecnologie emergenti al più presto.

Le imprese che sono in ritardo sono quelle più inclini ad adottare nuove tecnologie, per uscire dall'emergenza.

Con quasi l'80% delle aziende Fortune-500 che utilizzano la Now Platform, osserva l'azienda,, ServiceNow si è in pratica impegnata a fornire soluzioni in grado di aiutare le aziende nella loro trasformazione digitale, sia che i dipendenti siano ancora impiegati in remoto o nel caso si stia pianificando il ritorno in sede.

Con la release Paris, ServiceNow ha presentato sei nuovi prodotti e nuove funzioni volte a permettere alle aziende di usufruire di un'unica piattaforma per:

- Rispondere ai cambiamenti nel business con nuove app di workflow
- Fornire ai dipendenti la giusta esperienza in ogni luogo
- Indirizzare la fidelizzazione dei clienti attraverso workflow connessi
- Ottimizzare la produttività dell'IT, i costi e la resilienza per modernizzare e automatizzare con l'ITSM e gli AIOps, fornire operazioni resilienti e ridurre la spesa software, hardware e cloud

«I C-Level hanno capito che le architetture del ventesimo secolo sono troppo lente e a silos, in un moderno ambiente di lavoro fluido che richiede velocità e agilità - ha dichiarato **Filippo Giannelli**, Responsabile ServiceNow Italia -.Il vantaggio di ServiceNow è sempre stato quello di avere un'architettura

unica, un solo modello dati e una piattaforma cloud nativa che fornisce i workflow di cui hanno bisogno le aziende, abilitando grandi esperienze per i dipendenti e i clienti. La release Paris della Now Platform permette esperienze più smart grazie all'intelligenza artificiale, e a una maggiore resilienza e ottimizzazione dei costi». Per i Partner, che hanno un ruolo critico nell'accelerare la trasformazione digitale delle aziende, ServiceNow ha poi annunciato integrazioni con Microsoft e Twilio, così come il nuovo ServiceNow Service Graph Connector Program, che aiuta i clienti a razionalizzare i processi interni collegando nuovi e vecchi strumenti e far fronte al nuovo modo di lavorare.

Il cloud si distribuisce: come monitorare e potenziare i data center periferici

Vertiv Environet Alert è una soluzione di monitoraggio che permette di potenziare i data center periferici di piccole e medie dimensioni

Environet Alert tablet

Vertiv, fornitore di soluzioni per le infrastrutture digitali critiche, ha annunciato Vertiv Environet Alert, un software che eleva a livello Enterprise le capacità di monitoraggio e gestione delle infrastrutture di data center più piccoli e risorse Edge.

In pratica, osserva Vertiv, la soluzione ha l'obiettivo di eliminare di fatto le due barriere più comuni all'implementazione degli strumenti di monitoraggio e gestione in questi ambienti.

Punto chiave è che è uno strumento indipendente dal produttore dell'infrastruttura adottata e fornisce un monitoraggio in tempo reale, avvertendo il personale quando il sistema critico si trova in una situazione di rischio.

Il software è gestito attraverso un unico pannello di controllo, con un'interfaccia utente che fornisce visibilità e dati agli utenti, che possono così concentrarsi su ciò che devono proteggere personalizzando i dati che vengono monitorati e segnalati.

«Il monitoraggio dei data center costruiti ad hoc è fondamentale per assicurare visibilità alle operazioni e ridurre rischi e costi, ma sono poche le soluzioni dotate delle funzionalità necessarie a scalare economicamente per le operazioni più piccol», ha commentato **Mike O'Keeffe**, vice president for service and software solutions di Vertiv in Europa, Medio Oriente e Africa. «Vertiv Environet Alert fornisce le funzionalità di monitoraggio essenziali per garantire alle piccole e medie imprese la connessione con le infrastrutture critiche e la necessaria continuità operativa».

A livello operativo, ha spiegato l'azienda,

Vertiv Environet Alert fornisce funzionalità di monitoraggio, generazione di alert, analisi dei trend e gestione dei dati per aziende che operano in settori verticali come la sanità, i servizi finanziari, gli enti governativi, l'istruzione e altri comparti che si affidano a data center più piccoli e strutture edge.

A livello di software per il management in ambienti complessi è compatibile con i dispositivi SNMP e si integra tramite un'API dedicata con altri strumenti di gestione della rete, con il software di gestione delle infrastrutture dei data center (DCIM) e con i sistemi di gestione degli impianti.

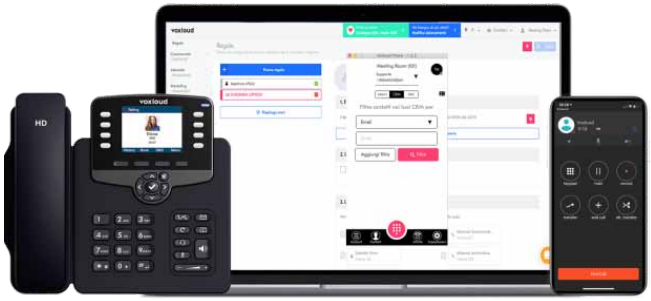
Anche il centralino va nel cloud ed è accessibile da ovunque

Il Pabx nel cloud va incontro alle esigenze delle PMI e dello smart working, ma bisogna fare attenzione a cosa si prende

L'attuale situazione di incertezza che si sta vivendo sta spingendo sempre più aziende verso lo smart working come modalità primaria da adottare per svolgere al meglio il proprio lavoro. Il problema è come farlo e comunicare in modo flessibile e in sicurezza.

Questo problema di aggiunge al fatto che a seguito del processo di digitalizzazione appare necessario ripensare i luoghi di lavoro, cercando di andare maggiormente incontro alle esigenze de team, senza però minare la autorevolezza aziendale o abbassando gli standard di professionalità e di efficienza che i clienti si aspettano.

Tra le innovazioni che hanno avuto maggiore risonanza nel periodo di lockdown c'è il centralino telefonico in cloud, un servizio che sta permettendo a tante PMI e attività commerciali di affrontare lo smart working in



modo efficiente, rapido e semplice.

Si tratta nella sua essenza di uno strumento che permette di poter gestire il proprio centralino da remoto, con la possibilità quindi di poter rispondere al proprio numero aziendale pur lavorando da qualunque altra parte del mondo.

«Ci sono dei capisaldi fissati nella testa delle persone che non si possono scardinare - osserva **Leonardo Coppola,** co-founder di Voxloud, una startup italiana che ha ideato e commercializzato un sistema di centralino in cloud -. Tutti percepiamo il numero di telefono

fisso come più professionale e istituzionale. Il fatto che dall'altra parte ci sia una cornetta da sollevare, dà nella nostra mente un valore completamente diverso al numero che stiamo per chiamare».

Mantenere professionalità e flessibilità

Sono diversi i benefici, osserva Coppola, che un centralino in cloud genera all'interno di un'azienda. Prima di tutto trasmette la massima professionalità fin dal primissimo contatto con il cliente, questo anche se l'attività è agli inizi e con pochissimi dipendenti.

Un numero fisso rispetto a un semplice numero di cellulare infatti dà subito l'impressione di avere davanti una vera e propria azienda ben organizzata, con una struttura pronta ad aiutarlo nelle sue necessità.

A prescindere dalla grandezza della stessa. In secondo luogo un sistema in cloud permette di gestire ogni telefonata con la massima efficienza.

È possibile infatti interfacciarsi subito con il referente che stiamo cercando, il cui numero aziendale sarà presente all'interno del centralino, permettendo quindi sia al dipendente che al cliente di risparmiare tempo prezioso. Il maggior beneficio infatti che si può trarre da un simile sistema è proprio quello di indirizzare velocemente e in maniera automatizzata le diverse chiamate verso la persona giusta, permettendo di ottimizzare i tempi di recepimento della chiamata e garantendo un servizio rapido ed efficiente al cliente.

Ampia disponibilità di funzioni

Ogni attività, continua Coppola, ha esigenze differenti, ma ci sono un paio di aspetti generali che andrebbero sempre verificati per essere certi di che il centralino in cloud sia utile per il proprio smart working. Quattro i punti imprescindibili: contemporaneità, multisede, possibilità di creare reparti interni separati, controllo.

È importante, e di certo si è d'accordo con Coppola, che il centralino in cloud permetta di poter effettuare o ricevere più chiamate contemporaneamente nello stesso istante. Importante anche che ci sia la possibilità di avere un unico centralino e un unico numero telefonico per tutti i propri punti vendita o le sedi in modo da facilitare la comunicazione e abbattere i costi.

Non ultimo, è importante che il centralino in cloud sia dotato di alcune funzioni utili quali ad esempio registrare le telefonate o sapere quante e quali telefonate si ricevono nell'arco della giornata. In questo modo le registrazioni diventano un asset fondamentale per la formazione interna dei dipendenti, permettendo così di migliorare costantemente e in maniera incrementale l'esperienza dei clienti.

«Prima di qualunque acquisto è importante analizzare lo stato della propria azienda e i suoi bisogni attuali per quanto riguarda la comunicazione con clienti, fornitori ed eventuali partner» sottolinea Coppola.

Non meno importante, va aggiunto, fare sempre attenzione ad eventuali costi nascosti e clausole inserite nei contratti delle diverse compagnie telefoniche. Un altro vantaggio di un centralino in cloud rispetto ad una piattaforma tradizionale è quello di non avere necessità di alcun tipo di installazione e manutenzione da parte di tecnici specializzati, e non è poco.

Qualys supporta la Cyber Next Platform di Infosys

Qualys VMDR, insieme a EDR Multi-Vector, rileva e risponde in tempo reale agli utenti dei Managed Security Service di Infosys per la sicurezza gestita

Qualys, fornitore di soluzioni IT di sicurezza e compliance basate sul cloud, ha annunciato che la società Infosys, che offre servizi digitali e consulenza, integrerà Qualys VMDR e EDR Multi-Vector all'interno della propria Cyber Next Platform, un'offerta di servizi di sicurezza gestita.

Alimentate dalla Qualys Cloud Platform, le soluzioni Qualys VMDR (acronimo di Vulnerability Management, Detection and Response) e Qualys EDR Multi-Vector (Endpoint Detection and Response) raccolgono grandi quantità di dati telemetrici attraverso i Cloud Agent di Qualys e i sensori multipli che vengono associati alle informazioni di rete.

Philippe Courtout - Qualys

L'obiettivo del combinato è di assicurare una visione più ampia dell'ambiente e dell'endpoint. In questo modo è possibile, osserva Qualys, eliminare i falsi positivi e prevenire in modo efficace anche le tecniche di attacco basate su attività collaterali.

Il risultato è una offerta di rilevamento e risposta gestita (MDR) h24 che consentirà a Infosys di individuare e rispondere velocemente agli incidenti in ambienti eterogenei.

I clienti di Infosys possono inoltre ampliare l'utilizzo del Cloud Agent di Qualys, includendo anche la gestione delle patch, il monitoraggio dell'integrità dei file e altre funzionalità.

«Infosys è una delle aziende leader a livello globale nella fornitura di servizi digitali di nuova generazione e siamo lieti di averli come partner - ha commentato **Philippe Courtot**, Chairman e CEO di Qualys -. L'integrazione delle soluzioni Qualys VMDR ed EDR Multi-Vector all'interno dei servizi per la sicurezza gestita offerti da Infosys permette ai clienti di Infosys di beneficiare di una totale visibilità, riducendo notevolmente i falsi positivi e neutralizzando velocemente le vulnerabilità. Il tutto con una soluzione end-to-end negli ambienti IT ibridi».

Un'App in cloud

A livello applicativo Qualys VMDR è un'App

all-in-one in cloud che automatizza il ciclo di gestione delle vulnerabilità in ambienti on-premise, endpoint, cloud, mobile, container, OT e IoT, e che permette alle aziende di rispondere velocemente alle minacce e prevenire le vulnerabilità.
Per le aziende che desiderano individuare schemi sospetti e portare alla luce incidenti nascosti, Qualys offre anche una soluzione per il monitoraggio e la neutralizzazione delle minacce informatiche sugli endpoint.
Qualys EDR Multi-Vector fornisce informazioni relative al contesto e alla visibilità completa sull'intera catena d'attacco, dalla prevenzione, al rilevamento, alla risposta, tutto all'interno di un'unica soluzione.

Il workflow finanziario di Bolzoni viaggia con Talentia

Bolzoni SpA ha adottato la soluzione Corporate Performance Management di Talentia anche per la gestione del workflow finanziario, in house e nel cloud

Talentia Software, azienda attiva nello sviluppo di soluzioni per la gestione delle risorse umane e finanziarie per le imprese di medie e grandi dimensioni, ha consolidato la collaborazione con Bolzoni SpA, azienda che da oltre 70 anni è attiva nella progettazione, produzione e commercializzazione di attrezzature per carrelli elevatori e soluzioni per la movimentazione industriale.
Dopo aver supportato l'azienda nell'implementazione di processi economico-gestionali, Talentia ha ora affiancato Bolzoni anche in un progetto di workflow finanziario realizzato attraverso il sistema gestionale Talentia CPM (Corporate Performance Management) che ottimizza e integra i processi di pianificazione finanziaria, budget e reporting, per realizzare il Bilancio Consolidato dell'azienda secondo i principi contabili internazionali IAS/IFRS.
Bolzoni è quotata in Borsa dal 2006 e qualche mese prima della quotazione era stato chiesto all'azienda di dotarsi un sistema di consolidamento adeguato alle nuove esigenze. Analizzando le offerte sul mercato Bolzoni ha selezionato la soluzione CPM di Talentia Software perché in grado di garantire la migliore flessibilità nella gestione degli aspetti economico-finanziari.
Nel 2016 l'azienda, a seguito dell'acquisizione da parte di una società americana, ha dovuto ulteriormente stravolgere le procedure adottate

Marco Bossi - Talentia Software

nel controllo di gestione con il passaggio da chiusure a 45 giorni e trimestrali a chiusure di 4 giorni lavorativi.

Il sistema da adottare dunque doveva essere ancora più user friendly, in grado di gestire nuove procedure.

«La nostra azienda è costituita da 17 società (è in previsione l'apertura di una diciottesima) e 7 di queste sono realtà produttive con oltre 100 dipendenti, mentre le altre società sono solo commerciali, più piccole ma dotate di un controller interno - ha evidenziato **Eleonora Palumbo**, CFO di Bolzoni -. Da sempre, gestiamo il conto economico con la suddivisione del fatturato, una situazione finanziaria che prevede la pianificazione della parte debitoria e dei crediti, dove ogni filiale ha la propria autonomia finanziaria e con la necessità di aggregare i dati. Grazie a Talentia CPM i risultati richiesti sono stati raggiunti in breve tempo e con un'ottima soddisfazione anche da parte degli utilizzatori del software».

Bolzoni con Talentia ha implementato anche il workflow finanziario. Centralmente l'azienda apre il ciclo due o tre giorni prima della chiusura del mese, dal primo giorno del mese le filiali possono caricare i dati effettivi di posizione finanziaria con analisi di pagamenti e incassi.

«Attraverso il workflow si definisce l'andamento e la previsione. Una volta definite e concluse, le previsioni vengono inviate a sistema per una conferma di primo livello. Centralmente un ufficio preposto alla verifica delle varie entrate valuta se sono distribuite in maniera corretta nelle varie filiali. Si possono quindi rifiutare i dati a livello centrale, dare suggerimenti di modifica per compensare i pagamenti a seconda delle filiali e dei territori. Questo permette, rispetto a prima, di avere una visione diretta con un processo semplice e rapido che il software di Talentia è perfettamente in grado di offrire», ha spiegato **Marco Bossi**, Managing Director di Talentia Software.

A livello funzionale Talentia CPM è una suite software modulare. E' composta da Budgeting & Planning e Talentia Consolidation & Reporting, che possono essere acquistati anche separatamente.

In modalità on-premise e cloud, offre tutti i servizi utili per elaborare dati, condurre analisi e presentare reportistica per fornire una visione completa della situazione aziendale in tempo reale, garantendo l'allineamento tra operatività e strategia d'impresa.