Cloud & Business

n.78
Febbraio 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

COVER STORY

IL MODO DI LAVORARE CAMBIA. È IL MOMENTO DELL'INTELLIGENT TRANSFORMATION

di Giuseppe Saccardi

Mobility, IoT, smart working, smart city, Artificial Intelligence…. Nuovi paradigmi cambiano il modo di lavorare. E' il momento, osserva Lenovo, dell'Intelligent Transformation

Emanuele Baldi, AD di Lenovo

Reportec Cloud&Business - Numero 78 - Febbraio 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

Se pensiamo al futuro prossimo, nella visione di Lenovo l'intelligenza artificiale gioca un ruolo primario, quello di fattore abilitante per un costante miglioramento della qualità della vita. Solo per fare qualche esempio, con l'AI vediamo un utilizzo più efficiente dell'energia in casa e sul posto di lavoro, maggiore capacità nella produzione alimentare, diagnosi mediche più rapide e accurate, e in generale la possibilità di migliorare la qualità del lavoro.

Se prendiamo l'esempio del settore sanitario, l'applicazione dell'AI consente di ridurre i tempi d'attesa ai pronto soccorso, ma anche di rilevare e diagnosticare precocemente i tumori, migliorando notevolmente il decorso per i pazienti. L'AI sarà inoltre utilizzata per rendere i PC e i dispositivi per la smart home più intelligenti che mai. In campo education, in futuro si possono immaginare sensori nelle aule che aiutano gli insegnanti a rilevare il tasso di attenzione degli studenti per indirizzare meglio la loro didattica. In linea con la strategia di Intelligent Transformation di Lenovo, stiamo inserendo sempre più intelligenza artificiale nei nostri dispositivi e nelle nostre soluzioni con l'obiettivo di migliorare il modo in cui viviamo, lavoriamo e ci svaghiamo.

Lenovo utilizza l'AI anche nella propria supply chain e nella pianificazione della fornitura dei componenti per migliorare costantemente l'esperienza che il cliente ha con i nostri prodotti. Ad esempio, utilizziamo il machine learning per sviluppare modelli predittivi di gestione della domanda.

La smart home è un altro ambito in cui vediamo miglioramenti nel modo in cui gli utenti finali interagiscono con la tecnologia nelle proprie case per risparmiare tempo e vivere in maniera più confortevole e connessa ad esempio con prodotti quali Lenovo Smart Clock e Lenovo Smart Display con Google Assistant, oltre ai Lenovo Smart Tab con Amazon Alexa.

Una simbiosi smart tra dispositivi e persone

Pensando agli spazi fisici o virtuali dove le persone, i dispositivi e i sistemi interagiscono, gli smart space diventano sempre più numerosi. Risparmiare tempo, vivere in ambienti confortevoli e avere contatti umani autentici, sono le caratteristiche che le persone apprezzano di più tra ciò che offre tecnologia. Se un dispositivo non risponde a queste esigenze fondamentali, gli utenti l'abbandoneranno tanto rapidamente quanto l'hanno adottato.

Grazie alla potenza dell'AI e dell'IoT, già oggi i dispositivi reagiscono agli input dei singoli utenti. Con l'avvento del 5G, tuttavia, le opportunità si estenderanno anche all'ambiente, grazie a una banda sempre più ampia che consentirà una connettività esperienziale. Le aziende e le amministrazioni pubbliche, ad esempio, potranno analizzare l'utilizzo di spazio e risorse,

rivoluzionare il modo in cui i trasporti, i centri commerciali o le comunità sono progettati e – in ultima analisi – come interagiremo con essi in futuro.
La categoria di prodotti per la smart home continuerà quindi ad espandersi con prodotti e soluzioni configurabili rapidamente, che offrono un'esperienza d'uso senza problemi e interoperabilità fra dispositivi ed ecosistemi. L'adozione di PC con funzionalità intelligenti e connesse quali il riconoscimento vocale, l'autenticazione biometrica e la connettività always-on, assieme a una categoria emergente di smart display che riuniscono visione (display touch) e suono (assistenti vocali) cambieranno il modo in cui interagiamo con
la tecnologia per un accesso più rapido alle informazioni e collegamenti più comodi.

L'importanza di workplace configurabili e flessibili

Passando all'ambiente lavorativo, si parla di una migliore esperienza non solo in termini di tecnologia e spazi, ma anche in termini di cultura e di come questi tre elementi si fondono.
Per attrarre e mantenere i migliori talenti in azienda, oltre che per dirigere aziende innovative e redditizie, i datori di lavoro devono riconoscere e tenere conto di come cambia il modo in cui le generazioni dei Millennials e dei Post-millennials lavorano ed esprimono le loro aspettative circa il posto di lavoro.
Spazi lavorativi altamente tecnologici, configurabili e flessibili, saranno sempre più diffusi. Le organizzazioni più lungimiranti, inoltre, inizieranno a rivolgere le loro attenzioni verso spazi che si mostrino in grado di favorire maggiore collaborazione e contatto umano. Questi spazi richiedono strumenti veloci e agili che favoriscano la collaborazione istantanea, comprese le soluzioni di smart meeting quali Lenovo ThinkSmart Hub.
Soprattutto i lavoratori più giovani, abituati fin dall'infanzia all'uso della tecnologia, si aspettano inoltre di poter scegliere e controllare dispositivi che l'azienda mette a loro disposizione, confrontandosi con l'IT invece che adeguarsi alle scelte del manager.
Un altro aspetto della workplace transformation sarà la possibilità di fornire ai dipendenti dispositivi già configurati per il cloud. Facendo buon uso delle nuove tecnologie di smart office, le imprese possono costruire un nuovo ambiente di lavoro agile, creativo e maggiormente produttivo.

I benefici della realtà virtuale e aumentata

Anche la realtà virtuale e aumentata è interessante per le sue implicazioni future. Ad esempio l'AR/VR può essere utilizzata per consentire ai pazienti di visitare virtualmente un ospedale prima di essere ricoverati, oppure aiutare i pazienti a visualizzare le procedure mediche, in modo da ridurne l'ansia.
La realtà virtuale può anche dare ai bambini ricoverati in ospedale un elemento di distrazione grazie a esercizi di meditazione divertenti e dinamici o giochi terapeutici che li aiutino ad affrontare la loro degenza.
In Lenovo lo stiamo già facendo con il visore Lenovo Mirage Solo VR con Daydream, mentre in

Italia abbiamo avviato un progetto con la Città Metropolitana di Milano e la Clinica De Marchi del Policlinico di Milano per aiutare i bambini ricoverati al reparto Fibrosi Cistica a rimanere in contatto con i loro compagni di classe durante i periodi di degenza.

Manufacturing e Retail, realtà in profonda trasformazione

Nel campo dell'industria manifatturiera e di processo, l'utilizzo di occhiali AR come componente di un sistema tecnologico più ampio può fornire agli operatori i dati necessari a ridurre gli errori e a migliorare la precisione, la sicurezza e la qualità.

Per esempio, con l'assistenza remota in AR un operatore su una piattaforma petrolifera offshore può lavorare in tempo reale con l'assistenza di un tecnico da remoto che vedrà ciò che accade attraverso il visore dell'operatore stesso.

Con il riconoscimento degli oggetti, un visore AR indossato da un meccanico aeronautico sulla pista di un aeroporto si può collegare a un server remoto per identificare automaticamente il componente su cui sta lavorando e recuperare gli schemi di installazione e altre informazioni importanti.

Il retail è un altro mercato in trasformazione, con nuove modalità con cui identificare e ingaggiare i clienti nella loro esperienza d'acquisto, offrendo loro la possibilità di fare acquisti in modo flessibile, online, sui propri dispositivi mobili o sul punto vendita, attraverso casse automatiche o tradizionali. La spinta verso applicazioni di acquisto unificate nel retail sta inoltre portando a una rivoluzione nei dispositivi di gestione delle transazioni sul punto vendita. Questi dispositivi interagiscono con i clienti attraverso tecnologie IoT creando offerte in tempo reale sulla base delle loro abitudini di acquisto.

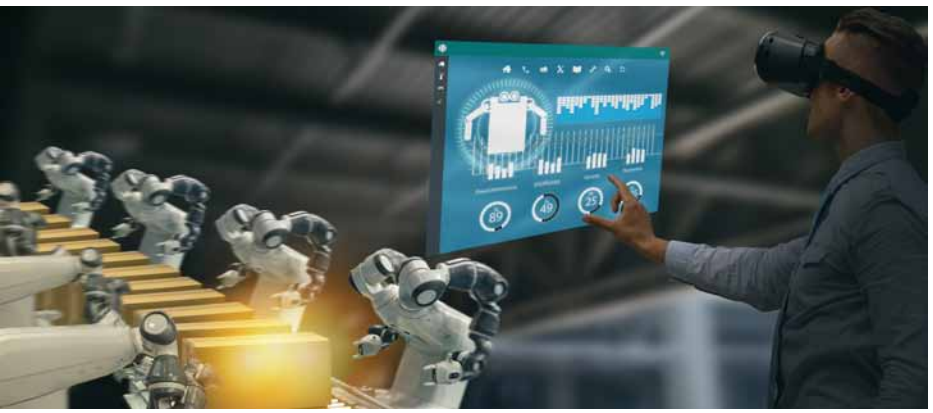
Più sicurezza con il machine learning

Nel campo della sicurezza, ci potremo aspettare una maggiore attenzione verso il machine learning per affrontare i punti di vulnerabilità dei sistemi IT, oltre a una maggiore attenzione verso le soluzioni di sicurezza end-to-end integrate, come ad esempio Lenovo ThinkShield.

Ci sono quattro spazi su cui le aziende e gli utenti finali si potranno concentrare per proteggersi – dati, identità, online e dispositivi – ed è di vitale importanza sviluppare piani di azione che tengano conto delle minacce in ciascuno di questi spazi.

La tendenza a passare a sistemi di autenticazione a molteplici fattori continuerà ad affermarsi con il crescere dell'importanza di associazioni di settore quali FIDO Alliance.

Nel loro insieme, il sempre maggior numero di smart device interconnessi in casa e in ufficio porterà con sé vantaggi e sfide.



Oltre a promuovere l'applicazione delle nuove tecnologie in settori produttivi molto diversi quali, il manifatturiero e il retail, la sanità e la scuola, e tanti altri, le aziende dovranno capire le esigenze e abitudini delle loro forze lavoro multi-generazionali, in modo da sviluppare appieno il potenziale della Intelligent Transformation.

AZIENDA PIÙ FLESSIBILE AUTOMATIZZANDO LA GESTIONE DELLE APP MULTI-CLOUD

Automatizzare il servizio di consegna e gestione delle applicazioni multi-cloud rende flessibile e sicura l'azienda

Alberto Crivelli, A10 Networks

Le aziende mirano ad essere sempre più rapide e flessibili nel rispondere agli inevitabili cambiamenti dettati dall'IT e dall'uso dei software. Per questa ragione roll-out veloci, controllo ed ottimizzazione delle applicazioni generano ricavi, vantaggio competitivo e soddisfazione del cliente. Inoltre, le applicazioni devono essere sicure e facilmente accessibili indipendentemente da dove si trovi l'utilizzatore.

È questo il compito svolto dagli Application Delivery Controller o ADC. Il problema è legato alla tipologia di dispositivi di prima generazione: mancavano di visibilità e supporto per la gestione centralizzata necessari per collegare e mettere in relazione infrastrutture on-premise e cloud con le diverse API ed i relativi insiemi di strumenti.

Quello che ne deriva è che i processi attuali sono manuali, inefficienti, facilmente soggetti a errori e comportano l'impossibilità di modificare in modo proattivo e automatico l'infrastruttura in base a profili di traffico soggetti a forti oscillazioni.

A10 Networks (www.a10networks.com), società fondata nel 2004 e specializzata in Application Visibility Performance and Security, con a portfolio una gamma di soluzioni ad alte prestazioni volte ad assicurare che applicazioni e reti di data center siano sempre altamente disponibili e sicure, ha come obiettivo proprio il superamento di questi ostacoli.

Un esempio dell'impegno profuso è il recente potenziamento apportato agli ADC della famiglia Thunder Application Delivery Controller, tramite il supporto di Harmony Controller per la gestione centralizzata e multicloud, l'analisi esaustiva per app e l'integrazione di strumenti DevOps.

I miglioramenti apportati consentono inoltre l'integrazione con Kubernetes e la configurazione semplificata della policy di controllo e delivery delle applicazioni.

In sostanza, con questo sviluppo gli ADC di A10 permettono agli amministratori di gestire, controllare ed automatizzare in modo intelligente l'implementazione dei servizi di distribuzione delle applicazioni.

Le aziende, in questo modo, hanno la possibilità di massimizzare la loro agilità, ricevere informazioni utili e garantire la disponibilità e la sicurezza delle applicazioni e, non meno importante, semplificare le operazioni e ridurre i costi di proprietà.

Tra le nuove features figurano aspetti connessi ai paradigmi in forte crescita come interesse del

multicloud e dei container quali:

- Gestione multicloud centralizzata, incluse piattaforme on-premise, Amazon Web Services e Microsoft Azure per distribuire le policy a tutti i servizi applicativi.
- Espansione del sistema di analisi ai livelli 4-7 per l'applicazione sul cloud per centinaia di metriche su base aggregata o su richiesta in tempo reale.
- Integrazione con strumenti DevOps, tra cui Ansible Playbooks ed A10 Ingress Controller per ambienti Kubernetes.

A questo si aggiunge l'integrazione con strumenti di orchestrazione del cloud privato tra cui quelli di VMware e di Cisco, e la certificazione di Nutanix per le soluzioni A10 vThunder e Harmony Controller sulla piattaforma Nutanix Hyperconverged Infrastructure.

Si tratta nel complesso di funzioni che forniscono una visibilità completa sull'esperienza di utente, sulla latenza end-to-end, abilitano profili di traffico contestualizzati, rilevano anomalie e intrusioni dannose nonché i livelli di utilizzo e integrità del server che consentono di modificare una infrastruttura IT in modo proattivo.

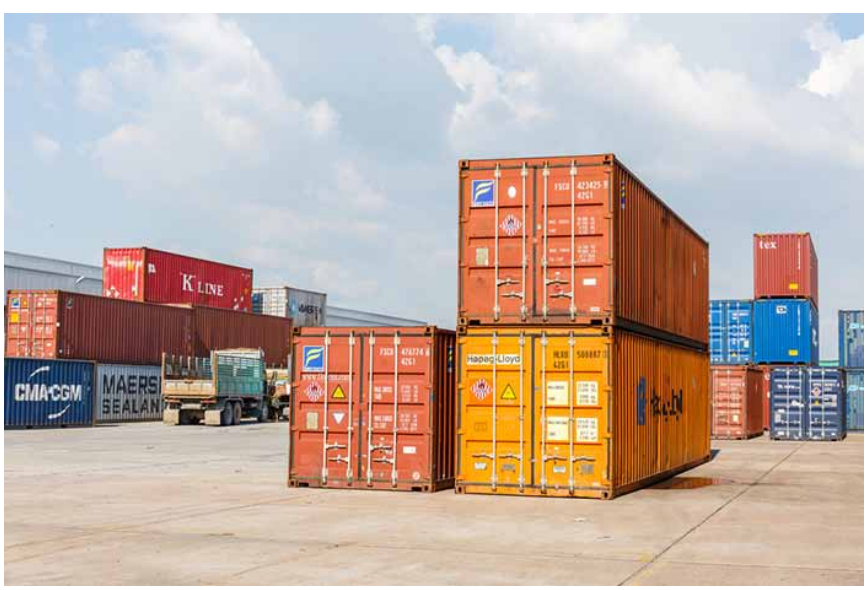
Particolare attenzione abbiamo poi posto agli ambienti cloud e multicloud, con il supporto della transizione delle applicazioni agli ambienti cloud ibridi con gli stessi servizi, gestione e visibilità di tipo on-premise.

Per quanto concerne gli ambienti DevOps, su cui molte aziende sono fortemente impegnate, abbiamo investito per migliorarne l'agilità tramite lo sviluppo di funzioni software centralizzate che consentono la collaborazione tra team di sviluppo e di rete.

Container di applicazioni e sicurezza nel multicloud

Un secondo paradigma che ci vede fortemente impegnati è quello della containerizzazione delle applicazioni e di come garantirne la sicurezza nel cloud. Un esempio di questo impegno è costituito dalla soluzione A10 Secure Service Mesh per applicazioni disponibili nel sistema open-source di orchestrazione e gestione di container Kubernetes.

In pratica, la soluzione fornisce ai team di esperti, che utilizzano applicazioni basate su microservizi, la possibilità di aumentare il livello di sicurezza aggiungendo funzionalità specifiche, oltre che a dare visibilità e fornire analisi molto dettagliate sul comportamento delle applicazioni.



Nella sua essenza A10 Secure Service Mesh è una soluzione in grado di proteggere le informazioni crittografando in modo trasparente il traffico tra i microservizi, senza richiedere la modifica delle applicazioni. Quello che ne consegue è un più alto livello di sicurezza ed elevate prestazioni per le applicazioni.

Per quanto concerne la sicurezza tra i microservizi, la so-

luzione include anche l'applicazione di policy di micro-segmentazione per il traffico tra i servizi. Il sistema inoltre può anche crittografare automaticamente il traffico tra i servizi, aumentando ulteriormente il livello di privacy e di sicurezza di tale tipologia di comunicazioni. Sono previste infine funzionalità aggiuntive di sicurezza, che includono applicazioni di limitazione della velocità del traffico per ogni servizio, l'applicazione DDoS e l'offload SSL/TLS.

Va poi considerato che Secure Service Mesh include A10 Harmony Controller, che abilita una gestione centralizzata della policy multi-cloud oltre ad analisi metriche e log che mettono a disposizione informazioni utili per singolo microservizio. Tra quelle disponibili, la latenza delle transazioni end-to-end, il throughput, il tasso di richiesta e altre metriche storiche ed in tempo reale.

Per quanto concerne il traffico dati, le funzionalità di gestione comprendono il rilevamento automatico dei servizi, il monitoraggio dello stato, il bilanciamento del carico, il cambio URL/content switch e il supporto per le implementazioni Blue-Green o Canary.

Un aspetto a cui abbiamo posto molta attenzione è che nessuna delle funzionalità citate richiede l'apporto di modifiche alle applicazioni e può essere del tutto automatizzata sotto il controllo dei team operativi. La soluzione, peraltro, si integra perfettamente con i sistemi di gestione dei container come Kubernetes e Red Hat OpenShift.

Volendo sintetizzare, A10 Secure Service Mesh risolve i problemi di sicurezza senza per questo imporre alcun modello specifico di implementazione delle applicazioni o richiedere loro modifiche. Il servizio di analisi del traffico al livello dell'applicazione aiuta notevolmente i team operativi, rendendo ancora più efficiente l'intera infrastruttura, oltre ad aumentarne la sicurezza.

A10 Networks nel Marketplace Azure

Un ulteriore sviluppo che abbiamo intrapreso concerne la disponibilità sul Marketplace Azure di Microsoft della soluzione di Application Delivery cloud-native: Harmony Controller, vThunder ADC e Lightning ADC.

Le aziende possono, tramite questi strumenti, ottenere benefici quali la scalabilità, l'alta disponibilità e la sicurezza di Azure, il tutto con sistemi di implementazione e gestione semplificati.

In particolare, A10 Harmony Controller fornisce il management centralizzato ed un'analisi accurata dei servizi di A10 per la sicurezza delle applicazioni in ambienti multi-cloud nella configurazione dell'applicazione garantendo il rispetto delle policy.

Tra le funzioni disponibili citiamo la gestione centralizzata delle policy, l'analisi del traffico e della sicurezza, il multi-tenancy e self-service, la scalabilità e l'indipendenza della architettura dei servizi basata su ambienti containerizzati, la gestione del ciclo di vita dei dispositivi e l'integrazione con gli ambienti Kubernetes.

A fini operativi le aziende hanno la possibilità di automatizzare in modo efficiente la distribuzione e le operazioni dei servizi applicativi, aumentare l'agilità e l'efficienza operativa per migliorare l'esperienza degli utenti finali.

Grazie all' adozione dell'intelligenza artificiale si semplifica la gestione dei servizi di distribuzione delle applicazioni, riducendo drasticamente i tempi di risoluzione dei problemi, oltre a ricevere avvisi sulle performance e sulle anomalie in termini di sicurezza, migliorando la capacità di pianificazione e ottimizzazione dell'infrastruttura IT anche in ambienti multi-cloud.

Grazie al Marketplace Azure di Microsoft, le aziende possono facilmente trovare, acquistare e implementare soluzioni affidabili, certificate e ottimizzate per l'esecuzione su Azure.

MULTICLOUD E SOFTWARE DEFINED MIGLIORANO I PROCESSI E RENDONO PIÙ SICURA L'AZIENDA

Processi di business migliori e più efficaci, azienda più sicura con il multicloud e il software defined. Ma è importante come e con chi farlo, osserva BCLOUD

Roberto Castelli, BCloud

Definire una infrastruttura software, facile o perlomeno semplice da gestire, che consenta di erogare rapidamente nuovi servizi utilizzando hardware con costi contenuti, è diventato il punto centrale delle architetture di storage, da parte di chi sviluppa e fornisce servizi, come avviene con il cloud nelle sue diverse interpretazioni.
Il Software Defined Storage richiede però partner specializzati e focalizzati e che accomunino capacità di sviluppo, risorse e un approccio in linea con quello di chi i servizi propone poi alla propria clientela in base a precisi contratti e qualità di erogazione.
E' questa la mission che si è data BCLOUD, azienda di Dalmine (BG) fondata nel 2011 da Roberto Castelli, società che opera come Software Defined System Integrator italiano specializzata in soluzioni cloud oriented per Enterprise e Service Provider.

Soluzioni e centri di competenza di valenza internazionale

Il compito che si è assunto BCLOUD è quello di selezionare soluzioni e piattaforme a livello mondiale esclusivamente in ambito Software-Defined IT. Tramite queste soluzioni ha sviluppato un portfolio di soluzioni e servizi con cui si propone al mercato come Software Defined System Integrator, soluzioni e servizi che implementa ed eroga tramite il proprio Competence Center dove risiede personale certificato che si affianca alle aziende, ai service provider e agli enti della Pubblica Amministrazione nelle diverse fasi di evoluzione e di adozione di queste tecnologie.
In fase progettuale ed operativa BCLOUD si affianca ai clienti, assistendoli sin dalle fasi iniziali di analisi delle esigenze, per proseguire poi con le attività di assessment che precedono l'entrata in esercizio, nella redazione del successivo progetto e nelle analisi del TCO e del ROI fatti tenendo conto degli investimenti aziendali già effettuati.
«Quello del software defined non è però l'unico campo di specializzazione della società - evidenzia **Marco Spoldi**, Software Defined Storage BU director di BCLOUD -. Altre aree interessano data management e data governance con soluzioni Enterprise Storage, Object Storage (di cui BCLOUD ha al suo attivo diverse implementazioni con capacità di molti Petabyte), High Performance Computing, Iperconvergenza, EFSS (enterprise

file sync & share), backup & disaster recovery. Le soluzioni che BCLOUD propone, sono il risultato di partnership consolidate con vendor focalizzati in ambiti specifici: per il Data Management Cloudian e Infinidat e in ambito Hyperconverged, Acuutech, Cohesity e Scale Computing».

La #lab2reality experience al servizio delle aziende

Per supportare le aziende nel loro percorso di trasformazione digitale e verso il multicloud, BCLOUD ha attivato un servizio specifico denominato #lab2reality experience. Costituisce nella sua essenza un percorso di affiancamento alle aziende, ai service provider, alle università e alle pubbliche amministrazioni per la definizione congiunta delle soluzioni ottimali in ambito data governance e data management, siano esse di tipo hybrid, cloud o multicloud.

«Con il servizio #lab2reality experience proponiamo uno strumento di lavoro che fonda la propria unicità sull'ascolto, l'osservazione e l'implementazione di soluzioni Software Defined in grado di rispondere alle esigenze di business dei nostri clienti con tecnologie cloud native, multicloud e scale out. Questo approccio permette di passare dall'esigenza iniziale, che di solito prevede una fase di sperimentazione specialmente per l'adozione di nuove tecnologie, sin da subito alla fase di produzione ed erogazione dei servizi da parte dei nostri clienti. Questo è il nostro approccio #lab2reality», ha commentato **Roberto Castelli**, CEO di BCLOUD.

Il servizio fa peraltro parte di un portfolio in continua crescita e aggiornamento che deriva da una attività di continuo scouting internazionale alla ricerca di fornitori di tecnologie di base focalizzati in ambito software defined.

Dal multicloud all'IoT

Un altro settore in cui è attiva BCLOUD è quello dell'Industry 4.0, in fase di profonda trasformazione e di adozione di soluzioni IoT.

Obiettivo dichiarato di BCLOUD è quello di supportare il mercato in forte espansione dell'Internet of Things che attraverso il cloud computing sta guidando lo sviluppo della quarta rivoluzione industriale. La maggior parte delle organizzazioni si sta infatti preparando a questi nuovi modelli di business e necessita di soluzioni di data analytics, piattaforme hedge computing e architetture cloud, usabili, flessibili, sicure e che siano in grado di supportare il rinnovamento digitale. Il portfolio di BCLOUD sposa perfettamente questo tipo di esigenze, grazie al modello software defined pietra miliare della sua proposizione.

Struttura in crescita e approccio #neverconventional

La crescita dell'interesse per le soluzioni BCLOUD è confermata, dopo l'apertura della sede di Dalmine, dalla presenza sul territorio del Nord-est e dell'area Emilia e Toscana con professionisti di grande esperienza.

«Sono due punti strategici per ampliare il nostro business non solo in queste regioni ma anche in tutto il centro Italia. Abbiamo già diversi clienti in zona che hanno ottenuto benefici importanti dal percorso avviato e concluso insieme. Siamo sicuri che le soluzioni software defined da noi proposte in ambito cloud, storage e data management saranno un'opportunità di business per quei clienti di fascia enterprise, service provider e PA che vorranno stare al passo con un mercato in continua evoluzione», ha osservato Roberto Castelli.

«Il nostro è un approccio #neverconventional che propone soluzioni in ambito software defined di vendor focalizzati in questo ambito ai nostri clienti. Proponiamo uno strumento di lavoro che fonda la propria unicità sull'ascolto, l'osservazione e l'implementazione di soluzioni Software Defined in grado di rispondere alle esigenze di business dei nostri clienti con tecnologie cloud native e scale out. Stiamo crescendo molto rapidamente

- continua Castelli - e proprio per questo abbiamo rafforzato e strutturato la forza vendita. E' prossima anche l'apertura di una nuova sede a Milano».

Marco Spoldi, BCloud

In Zucchetti e Brennercom dati e documenti al sicuro nel Cloud

La conferma più diretta della qualità dei servizi offerti e la loro corrispondenza alle esigenze aziendali dei diversi settori viene dai clienti che si sono rivolti a BCLOUD per affrontare la trasformazione digitale, società che annoverano, tra gli altri, nomi di prestigio come Zucchetti e Brennercom, accomunate dalla necessità di implementare soluzioni innovative, sicure, affidabili, facilmente scalabili e con un ritorno dell'investimento e costi di gestioni certi e allineati al mercato di riferimento.

L'esigenza di Zucchetti era quella di soddisfare la richiesta sempre più pressante da parte dei suoi clienti di soluzioni affidabili ed economiche al tempo stesso, nella sfera della conservazione dei documenti in ambito cloud.

Per soddisfarle, BCLOUD ha utilizzato HyperStore di Cloudian - società americana specializzata in object storage -, un'architettura di tipo scale-out basata su protocollo S3 in grado di creare infrastrutture di storage ad oggetti da tre a più nodi, on premise, nei data center e nei cloud pubblici, differenziandosi dallo storage tradizionale per la maggiore scalabilità, flessibilità e sicurezza.

BCLOUD con Cloudian, ha consentito a Zucchetti di uscire sul mercato, con la sua soluzione, partendo da una installazione con una capacità iniziale estremamente contenuta di pochi terabyte (implementata in un ambiente di test) sino ad arrivare alle attuali e numerose attivazioni di server localizzati su tre siti geografici.

«Va considerato - ha osservato Spoldi - che l'object storage aiuta le aziende a gestire in modo corretto la crescita dei dati che quotidianamente vengono creati e utilizzati al loro interno e nel mondo ed è una tecnologia particolarmente indicata per la conservazione a lungo termine di grandi volumi di informazioni digitali come documenti critici, legali, certificati (come fatturazione, documenti a uso governativo, immagini e filmati prodotti in campo ospedaliero, e altro ancora)».

L'architettura di storage ad oggetti di Cloudian è stata adottata anche da Brennercom, affermato provider del mercato ICT e TLC che opera principalmente sull'asse Milano - Monaco di Baviera.

I tre data center certificati di Bolzano, Trento e Innsbruck, la rete in fibra ottica e le centrali telefoniche di ultima generazione permettono a Brennercom di offrire servizi di telecomunicazioni, telefonia e soluzioni IT nel mercato nord-est italiano, in Austria e in Germania.

«Brennercom aveva bisogno di un'architettura di object storage per gestire milioni di file e HyperStore è una soluzione perfetta per i service provider - ha commentato Marco Spoldi -. La scalabilità verso gli Exabyte di cui è caratterizzata le consente di essere una soluzione flessibile, ed essendo basata su protocollo S3 nativo e compatibile al 100% con AWS, permette di gestire le informazioni in Cloud, utilizzando l'infrastruttura locale. Inoltre in questo specifico caso la particolarità del doppio supporto magnetico, nastro e disco, è stata poi di fondamentale importanza per rispondere alle normative internazionali».

Non ultimo, ha evidenziato BCLOUD, con un risparmio del 70% di costi rispetto ai sistemi di archiviazione basati su disco tradizionali.

LA COMUNICAZIONE SECURE-BY-DESIGN ABILITA AMBIENTI E CITY SMART

Crescono gli ambienti aziendali, quelli produttivi e le città smart, ma per renderli sicuri necessita una comunicazione secure-by-design

Luigi Meregalli, CIE Telematica

Nell'affrontare il tema di ambienti smart e del come realizzarli, dal workplace ai sistemi industriali, dal telecontrollo di impianti di public utilities sino alle Smart City, emergono subito una serie di aspetti che si evidenziano come essenziali al fine di garantire il funzionamento continuo e sicuro di tali infrastrutture.

In particolare, la dispersione degli oggetti infrastrutturali di rete da controllare e dei fruitori a cui erogare servizi privati o pubblici anche su base on-demand richiede particolare attenzione per quanto riguarda prestazioni e sicurezza.

In sostanza, una Smart City, un workplace sicuro o una ambiente industriale efficiente, lo è in quanto persone e dispositivi di ufficio o di produzione che lo costituiscono sono posti in grado di comunicare rapidamente tramite reti sicure, e di farlo sia tramite reti fisse che mobili a prestazioni garantite.

Quello di garantirlo è il compito che si è assunta RAD, rappresentata in Italia dalla società di ingegneria specializzata nelle infrastrutture di reti e di sicurezza CIE Telematica, tramite lo sviluppo di soluzioni innovative, virtualizzate, adatte per ambienti industriali e pubblici sia al chiuso che all'aperto in ambienti ostili, e in grado di trattare dati con prestazioni controllate atte all'erogazione di servizi di accesso garantiti.

La corrispondenza dell"approccio di RAD alle specifiche esigenze del mondo Smart è stato confermato dall'attribuzione del riconoscimento MEF 2018 Technology of the Year Award per la categoria NFV e nello specifico per la sua soluzione vCPE Toolbox (virtual Customer Services Equipement), uno strumento che fornisce ai provider un ampio ed esaustivo insieme di funzioni necessarie per la diffusione e il roll-out di servizi business di classe operatore e basati sulla virtualizzazione delle funzioni di rete (NFV: Network Function Virtualization). Il tutto garantendo la completa apertura e la possibilità di operare con qualsiasi ambiente e apparato VNF, controller SDN (Software Defined Network), orchestrator o white box di terze parti.

Il riconoscimento ottenuto non è giunto inaspettato. E' il risultato di continue attività di ricerca e sviluppo che hanno avuto l'obiettivo di permettere la realizzazione di reti in modo semplice e adattabili facilmente alle esigenze di fornitori di servizi a valore aggiunto e degli utilizzatori alle prese con la digital transformation e la l'evoluzione smart degli ambienti privati e pubblici.

Nel tempo, RAD e CIE hanno poi espanso il proprio portfolio di soluzioni di rete geografica con

nuove funzionalità di Software Defined WAN. Punto chiave di questi sviluppi è un sistema operativo carrier class unico per tutti gli uCPE del suo portfolio. Tramite questa e altre funzionalità e caratteristiche diventa possibile realizzare una integrazione soft con qualsiasi orchestratore di servizi di rete, disporre di una Service Assurance per quanto concerne WAN e VNF (Virtual Network Function), disporre di dispositivi "pluggable" atti a semplificare il roll-out a livello globale di rete e servizi nonché controllare i dispositivi di rete tramite RADview e un apposito portale.

Switch ideati per reti Smart industriali e pubbliche

La progressiva diffusione di ambienti Smart e il crescente interesse per Smart City, l'adozione del protocollo IP per facilitare la trasformazione digitale e l'adozione di tecnologie IoT e Industrial IoT, richiede soluzioni adatte, robuste e in grado di essere posizionate anche in ambienti dove per motivi costruttivi o di sicurezza non sono disponibile le usuali prese di alimentazione elettrica, e dove la connettività deve essere assolutamente garantita.

Una risposta a questi problemi e volta a favorire l'adozione di un trasporto dati basato su rete ottica è stata data da RAD con la sua linea di switch rugged PowerFlow a 10G e disponibili in più versioni.

La soluzione è ottimizzata, come evidenziato, per reti ottiche e geografiche che necessitano a livello impiantistico di poter fruire anche in modo intensivo di una alimentazione PoE, ovverossia tramite la medesima connessione di rete Ethernet.

Gli apparati possono essere gestiti sia con piani di indirizzamento IPv4 che Pv6 e SNMP v1/v2c/v3 e in modalità Web tramite http e https laddove serve una elevata sicurezza operativa. I criteri di sicurezza prevedono anche il controllo a livello di singola porta e basata sull'indirizzo MAC a standard IEEE802.1X, RADIUS, ACL,TACACS+ e SSL/SSH v2.

Se robuste sono le caratteristiche e ricca la dotazione di funzioni e standard per la sicurezza della comunicazione tra impianti e dispositivi, altrettanto ampie e flessibili sono le modalità disponibili a livello di configurazione e installazione della rete, che prevedono l'aderenza a standard quali MSTP, RSTP, ERPS (G.8032) e funzioni di recovery proprietarie ultraveloci PF-Ring, che permettono di recuperare i pacchetti anche operando a velocità wire speed e senza perdite in ogni condizioni di traffico.

A livello di rete e di connessioni la resilienza della WAN e degli anelli di rete è assicurata anche da link di rete ridonati operanti in dual homing. Estesa anche la gamma di temperatura operativa, che spazia da -40 a +75 gradi centigradi.

L'apparato, che ha ottenuto le certificazioni IEC 61850-3, IEEE 1613, EN50121-4, è aderente anche a NEMA TS2, lo standard per controlli di dispositivi installati in ambienti pubblici quali i semafori, le segnalazioni stradali di emergenza e le segnalazioni di "walk/don't walk".

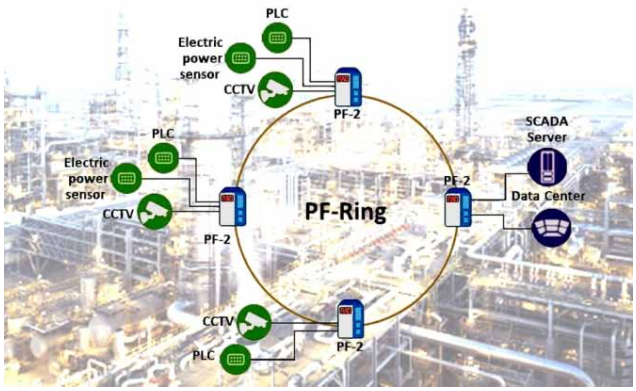
Servizi di smart business garantiti per SDN e Cloud

Un ulteriore elemento chiave del portfolio RAD e CIE Telematica e atto a favorire l'evoluzione verso reti SDN e la migrazione al Cloud è ETX-2i-100G, un dispositivo di rete che fa parte di un ampio portfolio di dispositivi di accesso Ethernet (EAD).

L'apparato abilita i service provider a rispondere alla crescente domanda di servizi business con larghezza di banda garantita necessaria in infrastrutture di mobile backhaul e nell'erogazione di servizi business MEF 3.0, incluso tra questi quelli relativi alla connessione di data center e di sedi centrali a livello Enterprise, nonché laddove necessita alta capacità per l'erogazione di servizi wholesale E-NNI.

E' anche una soluzione ideale per la connettività in Cloud e permette di aggregare e demarcare

Rete ad anello sicura con gli switch PowerFlow-2



senza necessità di servizi di demarcazioni aggiuntivi il traffico proveniente da diverse sedi remote e clienti business.
A questo aggiunge il supporto di controllo e gestione di ambienti SDN, oltre ad un insieme di funzionalità per la network transformation oggigiorno sempre più richiesta dal mercato business.
A livello di servizio dà la possibilità di aggregare flussi tributari n x 10 GbE e 100GbE in link a 100 GbE.
Non ultimo, implementa l'approccio RAD per un processo di provisioning zero-touch (ZTP). In pratica, questo abilita l'automazione dei servizi di rete e permette di minimizzare gli interventi da operatore o manutentore.
Va anche osservato che il nuovo dispositivo è già ampiamente usato da provider europei fornitori di servizi di Tier-1, a cui permette di assicurare servizi SLA estremamente affidabili supportati da una diagnostica multilivello, altamente granulari, con un accurato monitoraggio delle prestazioni.

Soluzioni per un IoT smart e sicuro

Il procedere della digitalizzazione e della "smartizzazione" del mondo industriale e pubblico tramite l'adozione di tecnologie IoT è di certo un abilitatore per trasformare profondamente il modo di produrre e di gestire fabbrica, impianti pubblici, public utilities e correlate attività di gestione e amministrative. Pur tuttavia, il contraltare è che l'automazione e la connessione in rete dei dispositivi apre la strada ai rischi che oramai da tempo coinvolgono il mondo office.
Il problema di come affrontare il tema della sicurezza nel mondo Industry e più in generale in infrastrutture distribuite è al momento molto dibattuto, perché non è pensabile dotare di applicazioni di sicurezza i dispositivi IoT finali dato che devono caratterizzarsi per costi molto contenuti e devono essere semplici per non appesantire quanto connesso alla loro gestione e manutenzione venendo spesso installati in siti privi di tecnici di manutenzione locale o di non facile accesso.
Quello che RAD ritiene essere il punto ideale dove rendere disponibili le funzioni di sicurezza sono i Gateway IoT, ovverossia quei dispositivi che da una parte sono connessi ai dispositivi IoT (sensori, attuatori, rilevatori, eccetera) e dall'altro alla rete Ethernet aziendale locale o geografica su cui colloquiano tramite il protocollo IP.
Oltre a questo una caratteristica indispensabile per dispositivi di tale natura per il mondo industry o applicazioni in ambito urbano è che devono essere molto robusti e in grado di resistere a condizioni ambientali severe in termini di umidità, temperatura, polvere o campi elettromagnetici.

RAD rende sicura la comunicazione IoT e gli ambienti Smart

Per rispondere a queste esigenze RAD ha sviluppato SecFlow, una famiglia di dispositivi gateway Ethernet dotati di funzioni di sicurezza e anche in versione rugged. Le funzioni che li caratterizzano sono molteplici e comprendono funzioni di sicurezza quali quelle di stateful firewall, di VPNs o di Automated PKI.
A queste aggiungono anche la possibilità di disporre di tecnologie di connettività in uplink su rete cellulare resiliente HSPA+/LTE in modo da assicurare la continuità del servizio di gateway nei confronti dei dispositivi IoT se dovesse venire a mancare la connessione su rete fissa primaria.
Un elemento chiave del gateway Ethernet rugged è che si tratta di un dispositivo "open" che, oltre

alle sue funzioni native, già di per sé molto ampie, può ospitare anche applicazioni di terze parti. Ampie anche le funzioni di rete, che comprendono quattro porte i GbE ed una porta GbE SFP, due porte seriali RS-232 oppure una porta RS-232 più una RS-485, alimentazione PoE, e un modem per reti cellulari dotato di due SIM card per funzioni di resilienza di rete.
Come evidenziato, un aspetto chiave è il supporto di applicazioni di terze parti. Nello specifico, le applicazioni sono ospitate ed eseguite tramite un container Linux che permette una rapida messa in produzione delle applicazioni.
Ambienti tipici di utilizzo sono quelli relativi alla distribuzione e alla automazione in sottostazioni secondarie, lo smart metering, la gestione delle risorse idriche e la gestione fuori banda di impianti tramite uplink cellulari.
Per quanto concerne la sicurezza di rete il gateway prevede funzioni di routing statico, OSPF BGP, VRF e NAT/NAT-Traversal. Per la connettività tra siti Ethernet sono poi utilizzabili link con tunnel VPN IPSec criptati che assicurano connessioni sicure e trasparenti di livello 3.
Per quanto relativo all'accesso remoto il dispositivo utilizza un tunnel SSH criptato che prevede l'autenticazione dell'utente e specifiche autorizzazioni per l'accesso.
Ampie anche le possibilità di gestione, che comprendono diverse tipologie di protocolli di accesso, compreso il common line, Telnet e TFTP/SFTP.

GARANTIRE LA SICUREZZA DI UTENTI PRIVILEGIATI IN AMBIENTI SAP E MULTICLOUD

David Higgings, Director of Customer development EMEA di CyberArk, spiega mette in luce i punti critici nella sicurezza degli account privilegiati e come mettervi rimedio

Oggigiorno le organizzazioni fanno affidamento su sistemi informativi dalla struttura complessa che ha fatto propri paradigmi come il Cloud, la mobility, l'AI, l'always-on e i servizi forniti da operatori qualificati.
Nel loro insieme quanto fornito da queste infrastrutture ha lo scopo primario di permettere ai dati e alle applicazioni di essere sempre raggiungibili e di cooperare in modo da costituire una potente leva per il loro business e garantire un flusso ininterrotto e sicuro delle informazioni.
Se fornitori di tecnologie e provider di servizi ricoprono un ruolo primario nell'assicurare l'infrastruttura di base, sono però le applicazioni che rappresentano il vero fulcro di un sistema informativo e che abilitano l'operatività funzionale e lo svolgimento dei compiti precipui delle diverse entità aziendali.

David Higgins, CyberArk

E in tutto questo, osserva CyberArk (www.cyberark.com), società con una presenza mondiale e posizionata tra le aziende leader nello sviluppo e commercializzazione di soluzioni per la sicurezza degli accessi privilegiati, SAP ricopre un ruolo essenziale. SAP fornisce il software di Enterprise Management che necessita alle aziende per condurre il proprio business, gestire i propri dati ed aiutare nel predire e interpretare le esigenze future dei propri clienti.

Ma come per ogni medaglia, anche in questo caso esiste un rovescio. Lo stesso successo e la diffusione di SAP tra aziende di caratura mondiale attrae l'interesse di hacker e di chi può essere interessato a penetrare nel mondo SAP ed impossessarsi di dati aziendali critici.

In pratica, più cresce il numero delle aziende che adottano sistemi, applicazioni e database SAP per il proprio business, parimenti cresce l'interesse di malintenzionati e maggiore è l'esigenza da parte dell'organizzazione di proteggere il proprio asset e ridurre la superficie e i vettori di attacco, e questo soprattutto per quanto riguarda la parte più critica in termini di utenti a contatto con dati di valore, quelli privilegiati.

Proteggere le applicazioni critiche per il business e chi vi accede diventa quindi sempre più mandatorio.

In proposito ai rischi per il business derivanti da un fuori servizio di applicazioni critiche conseguenza di malfunzionamenti o di attacchi informatici, CyberArk ha realizzato un sondaggio tra decision maker sia IT che di altre divisioni aziendali.

Quasi sei su dieci dei manager hanno risposto che persino un breve e non pianificato fuori servizio avrebbe avuto un effetto traumatico sul business aziendale.

Quasi i tre quarti hanno invece dichiarato che la loro vita lavorativa sarebbe divenuta più difficile se applicazioni critiche si fossero interrotte per un periodo di tempo significativo.

Per i due terzi, infine, le ordinarie operazioni sarebbero divenute impossibili nel caso di non funzionamento di applicazioni cruciali.

Tralasciando quanto derivante da eventi naturali o malfunzionamenti applicativi e concentrandosi su possibili attacchi di malintenzionati, il rischio in cui si può incorrere è enfatizzato dal fatto che in molti casi i criteri di autenticazione forte posti in essere per proteggere le informazioni sensibili da cui può dipendere il coretto funzionamento delle applicazioni di business critiche sono condivisi tra più dipendenti di una medesima divisione o ufficio e le password finiscono con l'essere ampiamente conosciute nell'ambito dell'organizzazione.

Ad esempio, gli utenti che hanno accesso a NetWeaver, la piattaforma che garantisce la sicurezza di ambienti SAP, possono avere libero accesso a database, applicazioni e analitiche. A questo si aggiunge la difficoltà di controllare dove queste password sono utilizzate e in quali circostanze.

Seppur SAP disponga di misure di sicurezza ideate per indirizzare tali vulnerabilità, evidenzia CyberArk, il dover garantire un accesso sicuro a utenti privilegiati può costituire una complessità operativa addizionale che spesso porta a mancare gli obiettivi mandatori di sicurezza e di compliance.

Funzionalmente, le soluzioni sviluppate da CyberArk complementano quanto vi è di caratteristico di SAP in termini di sicurezza, incluso in questo la rilevazione dei rischi e quanto concerne il controllo GRC (Governance, Risk, Compliance), in modo

da rafforzare la postura complessiva di una organizzazione per quanto concerne la sicurezza.
Ampio il loro campo di azione. CyberArk supporta sia i classici sistemi SAP ERP, così come un'ampia gamma di prodotti e tecnologie SAP, compreso tra queste SAP CRM, SRM, SCM, SAP NetWeaver Java, SAP HANA e Sybase ASE.
Innanzitutto rende possibile gestire e proteggere le credenziali SAP mediante l'integrazione degli account nel repository centralizzato crittografato di CyberArk.
Si ha inoltre la possibilità di automatizzare la rotazione delle password e abilitare il controllo della sicurezza dell'accesso privilegiato a più livelli attraverso lo stack SAP, dal livello dell'applicazione ai database, al sistema operativo, le macchine virtuali e ai server.
La gestione centralizzata si estende anche ai database più comunemente usati in SAP quali Oracle, SAP HANA, Sybase, SQL Server e DB2.
E' inoltre possibile isolare le sessioni di utenti privilegiati e rafforzare il controllo degli accessi al fine di proteggere i sistemi SAP da utenti e dispositivi non autorizzati.
Non meno importante di questo, è la capacità di soddisfare i requisiti di conformità, con la possibilità di dimostrare l'aderenza alle politiche aziendali interne e alle varie normative del settore - tra cui SOX, PCI DSS, GDPR - con visibilità elevata sui controlli dell'account privilegiato SAP e sui record di attività. «La soluzione CyberArk di protezione degli accessi privilegiati consente alle organizzazioni che adottano SAP di procedere con la certezza che solo una soluzione certificata SAP fornisce. CyberArk migliora le attuali iniziative di gestione e conformità dei rischi negli ambienti SAP ed estende la sicurezza degli accessi privilegiati, un livello critico di sicurezza IT, ai sistemi aziendali essenziali e alle applicazioni critiche», ha evidenziato **David Higgings**, Director of Customer development EMEA di CyberArk.

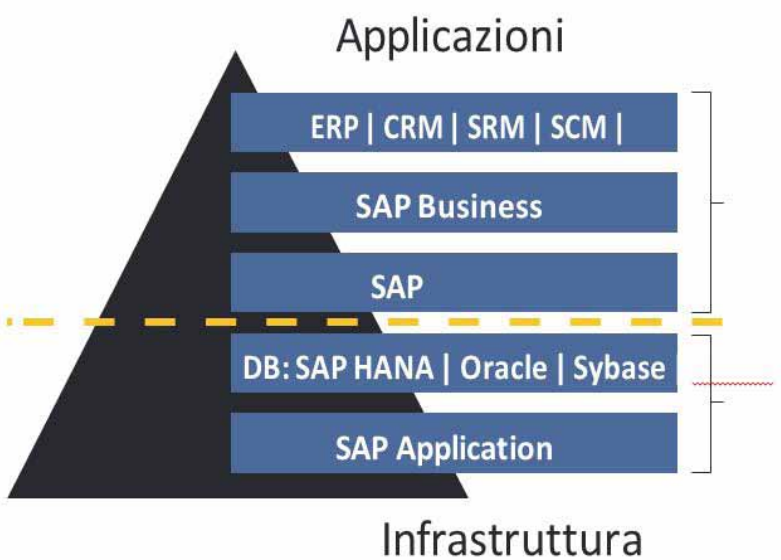
Advanced Privileged Session Manager for Cloud

Proteggere adeguatamente ambienti SAP critici è il primo passo da compiere, ma non sufficiente se in azienda si sfruttano in modo progressivo la flessibilità e le funzioni del cloud e del cloud ibrido.
Un punto critico, ad esempio, in modo del tutto simile a quanto avviene per ambienti SAP, è costituito dal fatto che i Cloud Administrator e gli utenti business privilegiati dispongono di sovente di diritti elevati nell'accesso a dati sensibili e alle applicazioni web, ma ciononostante le loro attività non sempre ricadono sotto la gestione del team IT dedito alla sicurezza.
In questo modo si apre la strada a forti rischi, in quanto gli utenti con privilegi elevati hanno la possibilità di operare all'esterno del robusto e articolato contesto di sicurezza aziendale, esponendo potenzialmente a rischi sconosciuti l'intera organizzazione.
Per estendere la protezione degli account privilegiati, le applicazioni e i dati a cui questi hanno accesso, ad ambienti esterni al perimetro aziendale fisico, CyberArk ha sviluppato una specifica applicazione, CyberArk Privileged Session Manager for Cloud.
Il punto chiave dell'approccio adottato nel suo sviluppo, ha osservato David Higgings, è che mediante una user experience trasparente l'applicazione estende la protezione per le sessioni di accesso privilegiate e il monitoraggio delle attività oltre che il loro controllo, alle più comuni applicazioni web, nel cloud e sui social media, come ad esempio AWS, Azure o SalesForce.
Parte integrante del portfolio CyberArk, Privileged Session Manager for Cloud fa inoltre leva sulle capacità delle piattaforme di sicurezza CyberArk di individuare e allertare su attività connesse agli utenti privilegiati.
Numerose le possibilità offerte dalla soluzione al fine di migliorare la sicurezza in ambienti cloud

ibridi per la protezione degli utenti privilegiati. Tra queste:

- Supporto delle piattaforme cloud e web: sono supportate le principali piattaforme cloud IaaS e PaaS, SaaS e social media, compreso Amazon Web Services (AWS), Red Hat OpenShift, Salesforce.com e applicazioni social media quali Twitter, LinkedIn, Facebook e Instagram.
- Accesso trasparente e veloce: l'accesso utente trasparente permette di stabilire una connessione sicura ed estremamente veloce verso le piattaforme cloud e le applicazioni web.
- Isolamento delle sessioni: gli utenti business privilegiati e le sessioni degli amministratori cloud sono isolate. L'approccio permette di mantenere riservati dati critici e che gli stessi siano usati solo al fine di stabilire una connessione sicura.
- Monitoraggio delle sessioni: permette di condurre attività di auditing dettagliate di tutte le attività degli utenti privilegiati all'interno della piattaforma cloud e delle applicazioni web. In pratica è possibile accelerare le attività forensi e di investigazione sulla sicurezza, così come fornire il supporto per la corrispondenza ai numerosi regolamenti e normative industriali.
- Valutazione del rischio: fornisce una comprensione del rischio inerente le sessioni privilegiate e la visibilità dei rischi connessi ad operazioni condotte da singoli utenti privilegiati. Tramite questa funzionalità un'organizzazione ha la possibilità di essere allertata su attività ad alto rischio in cui potrebbe incorrere, nonché di avviare in modo prioritario attività di auditing di tipo periodico e in base al rischio. La valutazione è abilitata da una combinazione di potenti strumenti statistici, algoritmi deterministici, machine learning e di analisi comportamentale.

«CyberArk Privileged Session Manager for Cloud risponde alle esigenze aziendali di elevata sicurezza per utenti privilegiati nei percorsi di trasformazione digitale e la migrazione al cloud ibrido, entrambi fattori che stanno impattando profondamente sia sul business che sulle applicazioni critiche», ha evidenziato Higgings. «Al fine di supportare le strategie di difesa in profondità dei nostri clienti è vitale bilanciare un facile accesso alle piattaforme cloud e alle applicazioni web con un controllo degli accessi basato su policy, workflow di sicurezza, e una strategia consistente che abbracci sia ambienti on-premise che cloud, e questo è quello che è possibile fare con CyberArk Privileged Session Manager for Cloud».



Sicurezza complementare per utenti SAP privilegiati

LA NUOVA FRONTIERA NELLA SICUREZZA DEI SERVIZI GESTITI

Uomo e macchina assieme in servizi gestiti garantiscono la sicurezza informatica. Lo spiega F-Secure

Antonio Pusceddu, F-Secure

La diffusione della digitalizzazione e delle smart technology stanno cambiando profondamente la natura stessa delle aziende, indipendentemente dal settore di appartenenza e prodotto fornito al mercato. E' una trasformazione in chiave digitale che ha in sostanza mutato ogni azienda in una software company, e questo vale ancora di più per le aziende che vendono online.
In quanto tali, tutte indistintamente dovrebbero preoccuparsi di proteggere al meglio i propri asset e le risorse digitali accedute da locale, remoto, via dispositivi mobili o nel cloud.
La realtà di cui va preso atto è che Il panorama delle minacce a cui un ambiente IT o produttivo è sottoposto è profondamente mutato. Attacchi avanzati, spear phishing e violazioni di dati sono all'ordine del giorno, e non più l'eccezione. Serve quindi affrontare queste minacce con nuove tecnologie e crescenti investimenti in risorse di talento. Ma non sempre i budget lo consentono.
E il problema non è solo di budget ma anche di competenze atte a contrastare le minacce. Le previsioni parlano di 3.5 milioni di posizioni nella sicurezza informatica che resteranno vacanti entro il 2021. Nel frattempo, oltre il 67% delle Enterprise globali ha subito una violazione di dati (Fonte: 2018 Thales Data Threat Report).
E, cosa ancor più allarmante, è che molti di questi attacchi si basano su tattiche di attacco avanzato che sono impossibili da rilevare con soluzioni standard anti-malware o di protezione degli endpoint.
Ne consegue che questo panorama minaccioso non può più essere ignorato, soprattutto se si pensa che il costo medio di un data breach si aggira sui 3.62 milioni di dollari, senza considerare i possibili aspetti ed impatti legali dovuti a cause da parte di utenti.
In sostanza, il problema più grande da risolvere riguarda le risorse: non semplicemente i soldi, bensì il tempo e l'esperienza accumulata.
Ed è qui che interviene in aiuto il paradigma dei servizi, come quello sviluppato da F-Secure, L'idea che sta alla base dei servizi di sicurezza gestiti è semplice. La parola "gestiti" significa proprio questo: il servizio è completamente gestito da un partner esterno, che richiede pochissimo input dal team IT interno di un'organizzazione.
"Rilevazione e risposta" (detection and response) si riferisce in un tale contesto innovativo come

approccio al modo in cui funziona il servizio.
Inserendo sensori sofisticati su endpoint e reti di un'azienda, una soluzione basata su un servizio abilita rapidamente una visibilità completa in un ambiente IT anche molto ampio e dai confine estesi al mobile e al multicloud.
Quello che ne risulta è una architettura, una soluzione che può rilevare le violazioni analizzando il comportamento, e non gli ovvi segnali di un'attività malevola.
E questo è quello che abbiamo fatto in F-Secure con lo sviluppo dei servizi di sicurezza gestiti MDR, che hanno l'obiettivo precipuo di consentire anche azioni di risposta rapide ed efficaci, supportate dall'automazione o dalle decisioni umane, o da un loro intimo e sinergico connubio.

Il fattore uomo - macchina

Una cosa appare evidente: nessun essere umano sarebbe in grado di rilevare da solo le minacce avanzate così come sono andate delineandosi. Queste minacce non danno chiari segnali che qualcosa non va. Gli allarmi del software di endpoint non li rilevano e, ad esempio, la protezione della posta elettronica non cattura le e-mail di phishing sul gateway che le inoltra all'ignaro utente.
L'unico modo per rilevare attacchi come questi è mediante una combinazione di uomo e macchina tramite l'unione di sensori che raccolgono dati rilevanti, l'intelligenza artificiale che processa questi dati e la competenza di risorse esperte che analizzano rilevazioni sospette di violazioni.
In presenza di hacker sempre più agguerriti e che ricorrono a tecniche sofisticate una cosa si può affermare senza timore di smentita: se non stai rilevando incidenti alla tua sicurezza, probabilmente è perché ti stai perdendo qualcosa.
Questo è il messaggio di allarme che come F-Secure lanciamo e che sta alla base della nostra vision di servizio e di connubio uomo-macchina, e come il modo più efficace e rapido per contrastare le minacce tramite un nuovo servizio di rilevazione delle intrusioni e di risposta agli incidenti che permette di scoprire e bloccare al loro insorgere e in tempi utili le minacce presenti sulla rete aziendale.

Un servizio di allarme entro 30 minuti

Il fattore "Tempo" è un punto chiave nella sicurezza. In media le violazioni di dati possono durare settimane, mesi o persino anni prima di essere rilevate. Secondo Gartner, la più grande area di bisogni insoddisfatti è rappresentata proprio da un'efficace rilevazione di attacchi mirati e di violazioni.
Le organizzazioni non riescono ad effettuare diagnosi precoci di una violazione, con oltre il 92% di violazioni che restano nascoste all'organizzazione che è stata colpita.
Inoltre, numerose sono ancora le aziende che si basano solamente sulla difesa perimetrale per proteggere sé stesse, che è sì importante ma solo come parte di una strategia di sicurezza informatica globale. Con attori di minacce avanzate che colpiscono le organizzazioni con attacchi altamente mirati, un tentativo di attacco finirà quasi certamente col superare i controlli di sicurezza e penetrare nella rete.
La capacità nel riuscire a rilevare velocemente le intrusioni e a rispondere in modo immediato è fondamentale, ma però non è semplice da mettere in atto.
E' a questo vulnus temporale che pone rimedio un servizio gestito come quello sviluppato da F-Secure, che combina il meglio dell'uomo con l'intelligenza delle macchine con la promessa di informare le aziende in soli 30 minuti della rilevazione di una minaccia.
Le aziende che si stanno rendendo conto che da sole fanno realmente fatica a rilevare intrusioni e a rispondere agli incidenti hanno con F-Secure la possibilità di affidarsi a un team di esperti di sicurezza informatica, costruire un'infrastruttura

di monitoraggio, e ottenere validi dati per un'efficace intelligence delle minacce.
Creare al proprio interno un sistema appropriato di questo tipo è estremamente difficile e costoso e richiede anni per poterlo fare. Ecco perché ha senso affidarsi a un servizio gestito, che fornisce un immediato e tangibile ritorno sull'investimento.

Il servizio gestito di Rapid Detection&Response

Per scenari del tipo analizzati, in F-Secure abbiamo sviluppato "F-Secure Rapid Detection & Response Service" (RDS), un servizio gestito di rilevamento e risposta ai cyber attacchi mirati.
RDS include sensori leggeri per il rilevamento delle intrusioni per endpoint, reti e server esca distribuiti nell'intera infrastruttura IT. I sensori monitorano le attività avviate dagli attaccanti e trasmettono tutte le informazioni al cloud di F-Secure in tempo reale.
Il servizio basato su cloud ricerca eventuali anomalie nei dati utilizzando una combinazione di tecnologie avanzate, come l'analisi del comportamento in tempo reale, l'analisi dei Big Data e l'analisi della reputazione.
La ricerca delle anomalie procede in due direzioni: comportamenti malevoli noti e sconosciuti. Questo perché l'adozione di tipologie di analisi differenti garantisce il rilevamento degli attaccanti, anche se usano tattiche di evasione progettate per eludere metodi di rilevamento specifici.
Una volta rilevate, le anomalie riscontrate vengono segnalate al team di esperti di sicurezza del Rapid Detection & Response Center di F-Secure che ricercano minacce operando h24 per verificarle e filtrare i falsi positivi.
Il processo di alert è peraltro molto rapido. Quando viene confermato che un'anomalia costituisce una minaccia effettiva, il cliente riceve un avviso entro 30 minuti. Ma non è tutto. Gli esperti di F-Secure propongono contestualmente i passaggi necessari per contrastare e correggere la minaccia. E non ultimo, vengono anche fornite informazioni dettagliate sull'attacco, che possono essere anche utilizzate come prova nell'ambito di procedimenti forensi.
Nei casi più difficili o laddove le risorse IT del cliente non siano disponibili, è poi sempre possibile contare sull'assistenza del servizio di risposta agli incidenti on-site di F-Secure.
Detto semplicemente, RDS incarna una vision di F-Secure orientata al servizio che consente ad una azienda cliente, e ai suoi manager, di dormire sonni tranquilli, potendo contare su un team di altissimo livello per l'identificazione delle minacce al proprio servizio.

LA SICUREZZA DIVENTA HUMAN-CENTRIC, DINAMICA E COMPORTAMENTALE

Cybersecurity human-centric e protezione dinamica e comportamentale abilitano la Smart Economy, l'IoT e il cloud e ne favoriscono l'adozione

Emiliano Massa, Forcepoint

La rapida evoluzione tecnologica, la diffusione dirompente della mobility, gli workplace smart e il crescente ricorso al cloud e ancor più al multicloud, impongono alle aziende nuove e non facili scelte strategiche nel realizzare infrastrutture sicure e trusted, che garantiscano gli utilizzatori per quanto riguarda la sicurezza, la protezione e l'inalterabilità dei dati trattati e scambiati tra entità umane e logiche, come avviene nel caso di infrastrutture IoT e IIot a seconda che si abbia a che fare con ambienti office, di fabbrica o di public utilities ad alto tasso di rischio la cui operatività deve essere assolutamente garantita per l'impatto che un loro malfunzionamento potrebbe avere su servizi sociali di particolare criticità.

Ma non si tratta solo di affrontare il tema dal punto di vista infrastruttura, è anche questione di fattore umano. In quanto tale, la "sicurezza" o security di un'organizzazione, indipendentemente dal settore o dalle dimensioni di un ente privato o pubblico, non può essere disgiunta dalla sua cultura lavorativa e l'unico modo efficace perché la forza lavoro contribuisca ad ostacolare il crimine informatico è quello di creare una cultura della security in azienda, a partire dai vertici aziendali sino ad includere in un tutt'uno omogeneo tutti i suoi livelli.

La sicurezza informatica per essere realmente efficace, è la vision che abbiamo sviluppato in Forcepoint e concretizzato in un ampio portfolio di soluzioni, deve proteggere le persone e i dati utilizzando metodi adattativi che rispondano automaticamente al rischio comportamentale, senza imporre policy restrittive o drastiche limitazioni che potrebbero causare un loro rifiuto da parte degli utilizzatori o apportare complessità e rallentare i processi di business.

I punti critici della sicurezza

Nel corso dell'anno da poco conclusosi e ancor più in quello appena iniziato sono andati delineandosi i paradigmi della cyber security a cui le aziende devono far fronte in modo crescente. Si tratta di temi evidenziatisi negli studi come il "Cybersecurity Predictions Report" che Forcepoint realizza su base annua con i propri specialisti della sicurezza, ricercatori di intelligence comportamentale e data scientist che hanno fornito indicazioni sulle minacce che dovranno affrontare le organizzazioni nei mesi a venire.

Tra queste, a rischio si sono evidenziate le infrastrutture IIoT e Cloud, l'identificazione biometrica e l'eccessivo affidarsi all'intelligenza artificiale

nella cybersecurity.
Il report esamina sette aree in cui si prevede che il rischio possa aumentare nel 2019, per le quali gli esperti di Forcepoint hanno approfondito le tendenze tecnologiche e le motivazioni che stanno dietro gli attacchi informatici, in modo che le aziende e i team di sicurezza possano prepararsi ad affrontare la nuova ondata di minacce.
Il problema alla base di tutto, una sorta di denominatore comune per le crescenti criticità nella sicurezza aziendale, è che le imprese e i governi, pur coinvolti in consistenti e severi processi normativi, si trovano ad affrontare una evoluzione molto rapida e un mondo iperconvergente in cui i sistemi connessi stanno crescendo in modo esponenziale e mettono a rischio non solo i dati critici e la proprietà intellettuale, ma anche la stessa sicurezza fisica degli ambienti di lavoro e quelli pubblici.
Dall'ultimo report realizzato in Forcepoint, quello che si evince è che quando le persone riescono a collaborare in maniera fidata, sfruttando i dati in modo creativo e libero attraverso la tecnologia, le aziende possono innovare in modo sicuro per creare valore.
Va tuttavia osservato che l'industria della sicurezza informatica e gli aggressori spendono grandi sforzi in un ciclo senza fine di violazione, reazione ed aggiramento, un vero gioco a precedersi e a rincorrersi.
Quello che come obiettivo ci siamo prefissati, e perseguito attivamente con le nostre soluzioni, è stato quello di interrompere questo ciclo poco virtuoso e produttivo per le aziende delineando approcci basati sulla protezione dinamica e comportamentale e sulla cybersecurity human-centric come abilitatori di Smart Economy in cui i diversi attori siano riconosciti come sicuri e trusted.
Una cosa si evidenzia in tutta la sua ampiezza: i professionisti della cybersecurity e i manager dovranno adattarsi ai cambiamenti sempre meno statici e in continuo divenire e in base al rischio che rappresentano dal punto di vita economico e sociale, così da abilitare i comportamenti leciti e bloccare anticipandoli quelli malevoli.

Digital Transformation e cloud più sicuri con la clusterizzazione comportamentale

Uno dei temi più critici da affrontare si evidenzia essere costituito dal binomio Digital Transformation e Cloud. Nella sua analisi l'ultimo rapporto analizza nello specifico l'impatto sul business a seguito della fiducia riposta nei fornitori di servizi cloud, l'impatto sugli utenti nella protezione dei dati personali con l'utilizzo della biometria e il potenziale impatto a cascata su tutta la supply chain.
In un recentissimo sondaggio condotto tra i clienti Forcepoint, il 94% di essi, in pratica la quasi totalità, ha identificato la sicurezza durante il passaggio al cloud come un problema importante. Il 58% cerca attivamente fornitori affidabili con una solida reputazione in ambito security e il 31% limita con un appena velato scetticismo la quantità di dati inseriti nel cloud a causa di problemi di sicurezza reali o immaginari.
Qualcosa di molto concreto si può però fare, ed è quello che Forcepoint rende possibile con le proprie soluzioni. Un modo per incrementare

il rapporto di fiducia e migliorare il controllo è ad esempio attraverso la clusterizzazione comportamentale degli utenti o, più specificamente, delle loro identità digitali, al fine di comprendere le ragioni della loro attività. Capire come un utente agisce sulla rete, nel cloud e all'interno delle applicazioni può consentire di identificare anomalie comportamentali che aiutano a fornire risposte adattive al rischio.

Con Forcepoint la protezione del dato è dinamica e comportamentale

Il problema della prevenzione della perdita dei dati, riferita in letteratura con l'acronimo DLP: Data Loss Prevention, è sempre più stringente ed è un'esigenza generale e trasversale a tutte le tipologie di aziende e di settori, enfatizzata anche dall'entrata in vigore del regolamento europeo sulla sicurezza e protezione dei dati.

Quello della protezione del dato è un settore dove sempre più si fa ricorso a metodologie di cybersecurity di tipo human centric, in modo da adattare la protezione di dati e utenti in base al loro comportamento e all'interazione tra le entità, sistemi e dati.

Quello del ricorso a soluzioni basate sul comportamento umano è poi andato incontro ad una ulteriore evoluzione come conseguenza dell'integrazione tra DLP e CASB, acronimo quest'ultimo di Cloud Access Security Broker. Ciò ha permesso non solo di meglio ritagliare una soluzione in base alle esigenze dell'utente e del contesto ma anche di rispondere all'evoluzione strategica sul modo di come viene fruito in azienda l'IT.

Il problema che è però andato evidenziandosi è che la maggior parte se non tutte le soluzioni DLP sul mercato bloccano o permettono un'azione basandosi su insiemi statici di policy predefinite. In sostanza il comportamento è del tipo "Permetti" o "Blocca" e vi è la mancanza di un meccanismo flessibile che permetta di gestire le eccezioni.

Il rischio concreto è che la frustrazione che sperimenta un amministratore di sistema qualora non riesca a gestire una eccezione lo porta a disabilitare le regole stabilite o a perdere fiducia nella tecnologia.

Per evitare l'incorrere in queste critiche situazioni Forcepoint ha sviluppato Forcepoint Dynamic Data Protection, una soluzione ed un approccio che ha come obiettivo primario quello di porre in grado di monitorare e rafforzare il controllo dinamico, e di proteggere i dati in base a livelli di rischio comportamentale da parte dell'utente e del valore dei dati coinvolti. Tra gli elementi chiave della soluzione va annoverato:

- Sistema per la collezione dei dati dagli endpoint.
- Utilizzo dei dati in accordo a un modello comportamentale flessibile e dinamico.
- Determinazione di un punteggio di rischio assegnabile ad un utente.
- Punteggio di rischio correlabile a un livello di rischio da 1 a 5.
- Possibilità di assegnare un piano unico di protezione dei dati ai differenti livelli di rischio e per singolo utente.
- Rivalutazione nel tempo del punteggio e del livello di rischio, che può essere alzato od abbassato in base ai cambiamenti intervenuti nel comportamento umano.

In pratica, ASI e machine learning sono state utilizzate in modo sinergico ed integrato al fine di automatizzare rafforzamenti delle policy di sicurezza e così perseguire nel concreto l'obiettivo di ridurre la quantità di alert che necessitano di ulteriori investigazioni.

La Risk Adaptive Protection ottimizza la sicurezza dei dati

Un ulteriore problema per la sicurezza che nel corso dello scorso anno Forcepoint ha rilevato è costituito dal fatto che le soluzioni legacy per la sicurezza informatica fanno molto affidamen-

to sul tradizionale blocco delle minacce e sulle valutazioni statiche. Ciò non solo introduce la sicurezza come un elemento bloccante nelle transazioni commerciali, ma inonda gli analisti di security con milioni di alert provenienti da ogni tipo di minaccia.
Per eliminare questo problema Forcepoint ha sviluppato la Risk Adaptive Protection, che si basa su una valutazione continua del rischio e adegua automaticamente il livello di protezione, che può essere alzato o abbassato in base alle effettive esigenze di business. La funzionalità viene abilitata attraverso analisi del comportamento human-centric che includono le interazioni con i dati per utenti, macchine e account.
Nell'insieme, si tratta di un contesto intelligente che accelera i processi decisionali e di sicurezza specifici al fine di modificare il livello di rischio nelle reti aziendali. Sul lato pratico, gli analisti della sicurezza hanno altresì la possibilità di concentrarsi su attività ad alto valore ed eliminare l'arretrato di alert che derivano dai tradizionali strumenti di sicurezza. Non ultimo, CISO e CIO possano ridurre i tradizionali punti dolenti dovuti all'impatto della security per consentire recuperi di produttività, riducendo inoltre il tempo necessario per rilevare e mitigare i rischi da giorni o mesi a pochi secondi.
In sostanza, la vision di Forcepoint prende atto che la protezione dei dati basata su point solutions è obsoleta e che un approccio convergente si evidenzia sempre più come la corretta via da intraprendere. Ciò corrisponde ad agire sulla specifica applicazione anziché sulla sola tecnologia, cosa questa resa possibile proprio dall'approccio adottato nello sviluppo di Forcepoint Dynamic Data Protection vista come prossima generazione di DLP.

Protezione basata sull'analisi del comportamento umano

Nella sua essenza l'idea alla base della soluzione è semplice. Basato su analisi human-centric del comportamento, Dynamic Data Protection applica un punteggio comportamentale del rischio anonimo e continuamente aggiornato per stabilire una linea di base del comportamento "normale" di ciascun utente su reti aziendali o non gestite.
I sistemi intelligenti di Forcepoint, informati dalla valutazione del rischio individuale, applicano di conseguenza una serie di contromisure di sicurezza per affrontare il rischio identificato.
Ad esempio, Forcepoint Dynamic Data Protection può consentire e monitorare l'accesso ai dati, consentire l'accesso ma crittografare i download o bloccare completamente l'accesso ai file sensibili a seconda del contesto delle singole interazioni con i dati aziendali e del conseguente punteggio di rischio.

Efficacia nella sicurezza con Forcepoint NGFW

Una conferma indipendente della qualità delle soluzioni Forcepoint è il riconoscimento ottenuto da Forcepoint NGFW, un dispositivo studiato studiato per realtà laddove serva gestire in modo centralizzato centinaia o migliaia di nodi. Il test effettuato su un singola unità è quindi stata per noi penalizzante, ma anche così l'esito dei test indipendenti è risultato estremamente soddisfacente.
Con Forcepoint NGFW, non abbiamo solamente aggiunto la sicurezza al networking ad alte prestazioni, l'abbiamo integrata direttamente nella nostra connettività multi-ISP, basata su gateway cluster ad alta disponibilità gestiti centralmente, anche a livello Enterprise.
Di conseguenza, i meccanismi di difesa integrati di Forcepoint NGFW contro le tecniche e gli exploit di evasione hanno nuovamente ottenuto il punteggio più alto e il voto "RECOMMENDED" di NSS Labs, continuando una sequenza vincente, ininterrotta dal 2012, nei test comparativi

NGFW.
Peraltro il test, realizzato alla fine dello scoro anno, è stato significativamente più difficile, con il 39% in più di test basati su Evasioni Avanzate e con la piattaforma Forcepoint NGFW che ha bloccato il 99,7% di tutti gli attacchi e il 100% delle evasioni. Non ultimo, il throughput reale misurato da NSS Labs ha sovraperformato anche i valori anticipati dalla stessa Forcepoint, raggiungendo il 102% per il traffico non crittografato e il sorprendente 148% per il traffico SSL / TLS.
Non meno importante in un momento di crescente attenzione ai costi aziendali è anche il buon punteggio ottenuto nella quantificazione del TCO, ovvero il costo totale di acquisto e gestione di una soluzione nel corso della sua vita operativa.

GESTIRE GLI ENDPOINT E LA SICUREZZA DEGLI ACCESSI DA UNA SINGOLA POSTAZIONE

Cybersecurity human-centric e protezione dinamica e comportamentale abilitano la Smart Economy, l'IoT e il cloud e ne favoriscono l'adozione

Jacopo Bruni, Praim

Uno dei problemi che si devono affrontare quando si riorganizzano le modalità di lavoro, le postazioni e i processi di business è quello della gestione degli endpoint, sia che si tratti di postazioni fisse che mobili.
A renderlo possibile ci ha pensato Praim (www.praim.com), azienda fondata nel 1987 e nata come produttore globale di soluzioni Thin & Zero Client.
L'azienda ha vissuto e sta vivendo ancor oggi da attore protagonista, ha osservato **Jacopo Bruni**, Marketing Manager di Praim, i processi di trasformazione tecnologica e digitale in corso e l'emergere dei nuovi paradigmi, assistendo alla nascita e al consolidamento di vari trend: da Internet all'avvento del mobile e del cloud computing, fino all'IoT e ai Big Data.
«Praim si è guadagnata la leadership nella fornitura di sistemi completi per la creazione e gestione di postazioni di lavoro software e hardware Thin & Zero Client. Gli investimenti in Ricerca & Sviluppo per creare soluzioni performanti che rispondano sempre meglio alle esigenze delle aziende e del mercato, per tenere il passo con i tempi e supportare al meglio i clienti, sono elementi costanti di Praim», evidenzia Bruni.
Negli ultimi 10 anni l'azienda ha peraltro registrato un aumento progressivo del numero di clienti attivi e delle attività, riscontri che hanno spinto

il management a investire e potenziare ulteriormente il supporto nella fornitura di soluzioni a prova di futuro.
«Il nostro approccio evolve dalla realizzazione di soluzioni endpoint, garantiamo oggi una suite completa che rappresenta per i nostri clienti una risposta semplice per far fronte alla complessità della gestione di postazioni di lavoro nella sua totalità - sottolinea Bruni -. Infatti, la necessità di aggiornare le infrastrutture IT e di inserire nuove applicazioni in azienda, spesso provenienti da provider differenti, rende difficoltosa la gestione delle postazioni di lavoro. In particolare, nell'utilizzo di infrastrutture ibride, riuscire a mantenere le connessioni aggiornate e poter distribuire le applicazioni velocemente e in maniera differenziata è oggi un requisito fondamentale. Questo cambiamento ci vede di fronte al mercato in una veste rinnovata, pronti ad affrontare con i nostri partner le nuove sfide che l'evoluzione del mondo IT ci pone ogni giorno, e certi di offrire soluzioni che semplificano l'uso della tecnologia».

Gestione semplificata degli endpoint

Un punto essenziale per affrontare le sfide di business è costituito dall'agilità, dalla scalabilità e dalla facilità di gestione e amministrazione che devono caratterizzare le infrastrutture IT.
Per abilitare entrambe Praim ha sviluppato un ampio portfolio di soluzioni hardware e software Thin & Zero Client con l'obiettivo primario di mettere a disposizione delle aziende un sistema molto ampio e semplice per creare ed amministrare postazioni di lavoro flessibili e intelligenti.
«L'elemento chiave di queste attività è la console ThinMan, che permette di gestire centralmente i dispositivi Thin & Zero Client e PC, e consente alle aziende di realizzare un investimento efficace, contenendo tempo e spese», evidenzia Bruni.
ThinMan è uno strumento di gestione che sta diventando sempre più importante per l'IT Manager perché è una console che consente di gestire in maniera centralizzata Thin Client e PC, in versione locale, remota e da web.
Nello specifico, le operazioni di gestione e manutenzione sono eseguite in modo programmabile, automatizzando le fasi di installazione e, tramite ad un sistema di profilazione, rendendo le operazioni di amministrazione possibili anche per gruppi eterogenei di dispositivi ed utenti.
Un aspetto saliente della soluzione è che dispone di una interfaccia grafica semplificata con menu contestuali che permettono di effettuare dalla stessa postazione anche operazioni ordinarie quali accensione, spegnimento, aggiornamento, controllo e assistenza remota di tutti gli endpoint aziendali.
Questo sostanziale contributo di semplificazione e gestione fornito dalla console di Praim ha però anche un altro obiettivo, quello di favorire il contenimento dei costi tramite la consistente riduzione dei tempi di intervento sui dispositivi di rete periferici, e per installazioni anche di ampia dimensione.
In particolare, osserva Bruni, la versione Premium della licenza ThinMan può gestire fino a 10.000 endpoint e racchiude al suo interno molteplici funzionalità.

Accesso gratuito alla piattaforma

Un aspetto di sicuro interesse per le aziende in un momento di forte competitività sui mercati e impegnate su più fronti interessanti la trasformazione digitale è che la piattaforma di gestione è fornita gratuitamente a tutti i clienti attraverso la semplice registrazione sul sito web aziendale, ed inoltre include un primo anno gratuito di Software Subscription, che dà accesso al supporto tecnico, all'assistenza da remota e ad altri servizi.
«La licenza ThinMan Premium è la diretta testimonianza del nostro impegno costante a dare sempre più valore ai nostri clienti - spiega Bruni -.
Le funzionalità di gestione e controllo remoto dei dispositivi da parte della console Praim, possono

essere estese a dispositivi di tipo PC convertiti a Thin Client grazie aThinOX4PC, a PC con sistema operativo Windows con Agile4PC e a dispositivi Raspberry adottando la soluzione Agile4Pi».
Le caratteristiche della release Agile4PC sono molteplici, tra cui il fatto che sia installabile su dispositivi Windows e disponibile come funzionalità Agile Mode in tutte le soluzioni Thin Client Praim Windows Embedded Standard 7 e Windows 10 IoT, ed installabile anche su PC che utilizzino i sistemi operativi Windows 7 e Windows 10. Un range molto ampio indubbiamente e in grado di soddisfare ampie e molteplici esigenze di gestione dei diversi tipi di endpoint.
Una variante della soluzione, la Agile4Pi entrata recentemente nel portfolio software di Praim, è invece rivolta ad endpoint Raspberry Pi 3 e Pi 3 B+.
In pratica trasforma i dispositivi in Thin Client ottimizzati per l'accesso alle infrastrutture Citrix HDX, abilita una user experience Full HD con video rendering client-side e, mediante l'integrazione di Citrix Receiver, garantisce la assoluta compatibilità con i sistemi Citrix Virtual Apps and Desktop.
Ai fini pratici entrambe le soluzioni software Agile condividono l'obiettivo di semplificare l'accesso e l'esecuzione delle risorse locali ed esterne, e facilitare l'utente attraverso un'interfaccia che garantisca una user-experience simile a quella di uno smartphone, comprensiva di possibilità di personalizzare risoluzione video e configurazioni quali lingua, mouse e tastiera.

Accesso protetto dei dispositivi

Se la gestibilità è importante non meno lo è garantire ai dispositivi un accesso sicuro. Per assicurarlo, nel corso dell'ultimo anno, Praim ha rilasciato la soluzione ThinMan Smart Identity, un add-on che ha sviluppato per ThinMan Platinum Edition con cui si è posta l'obiettivo di garantire un accesso controllato e ottimizzato degli utenti ai propri dispositivi tramite l'utilizzo di smart card. ThinMan Smart Identity permette sul piano funzionale e operativo di implementare una soluzione di autenticazione basata su più fattori, gestire gli accessi degli utenti e contribuire a rafforzare la postura di sicurezza complessiva dell'infrastruttura IT a partire dagli endpoint. Sicurezza e controllo dell'accesso rafforzati inoltre anche da parametri di autenticazione che seguono una logica "policy-based" che può essere stabilita unicamente dall'amministratore del sistema.
ThinMan Smart Identity è stato sviluppato in modo da rendere più rapido il processo di autenticazione su diverse postazioni di lavoro e dare la possibilità all'utente di accedere alle proprie risorse su più dispositivi grazie al "roaming" della sessione, in modo da evitare perdite di dati e tempo con ulteriori log-in.
«La sicurezza, la velocità e semplicità di accesso, così come il controllo degli utenti, sono esigenze sempre più diffuse tra le aziende. E sono solo alcune delle motivazioni che ci spronano nella ricerca costante e che ci hanno permesso di sviluppare questo nuovo add-on» evidenzia Bruni.
Ampie le casistiche di utilizzo. L'applicazione di identificazione intelligente delle identità funziona con numerose smart card e con i lettori più diffusi sul mercato, sia con lettura fisica della carta tramite inserimento (contact), che con card di prossimità con tecnologia NFC (contactless).
A questo si aggiunge il supporto delle carte più diffuse, come la Carta Nazionale dei Servizi o il badge aziendale. Non ultimo, la soluzione è compatibile con Agile4PC, Agile4Pi e tutti i dispositivi Thin Client Praim (Windows e ThinOX).
«Praim ha in piano un anno ricco di attività per continuare ad ampliare l'ecosistema di clienti e rafforzare le relazioni con i Partner di canale, sia in Italia che all'estero, per continuare a rispondere con puntualità, efficacia ed efficienza alle esigenze di un mercato in continua evoluzione» ha affermato Bruni.

COME COMUNICHERANNO LE AZIENDE NELL'ERA DEL CLOUD E CON QUALI TELEFONI?

Quando si valuta una nuova infrastruttura per la telefonia IP è necessario soppesare il livello di sicurezza garantito dalla centrale e dai terminali a fronte della reale esigenza e del costo

Fabio Albanini, Snom Technology Italia

Quando si decide di intraprendere la strada della trasformazione digitale uno dei punti chiave è lo svecchiamento degli strumenti utilizzati nelle postazioni di lavoro, adottando soluzioni e device attraverso cui comunicare efficacemente con le altre entità aziendali, clienti e fornitori.
Per un produttore, prevedere, ideare, realizzare e fornire soluzioni che si rivelino valide sin da subito oltre che in grado di confermarsi tali negli anni per giustificare l'investimento tecnologico nel tempo, rappresenta una delle sfide del momento. Un momento interessato da una profonda trasformazione in chiave digitale che coinvolge paradigmi che spaziano dal multi cloud allo smart place alla mobility e alla necessità di comunicare su reti IP tramite VoIP e a breve 5G.
Per capire a fondo le esigenze degli utenti e fornire loro soluzioni di classe business per la telefonia IP adeguate alle loro esigenze attuali e future, in Snom, pioniere della telefonia aziendale e VoIP (Voce su IP), abbiamo affrontato il problema in modo pragmatico realizzando uno studio su centinaia di aziende. I risultati evidenziano 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%).
Degno di attenzione 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 da qui a cinque anni. 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).
Dallo studio emerge altresì la crescente rilevanza dei telefoni IP cordless presso le PMI, che desiderano garantire ai propri dipendenti una buona mobilità anche all'interno degli stabili aziendali.

Quello di fornire soluzioni di comunicazione evoluta basata su solidi standard internazionali e in linea con le esigenze delle aziende in profonda trasformazione è il compito che ci siamo assunti in Snom, progettando terminali VoIP aperti e in grado di soddisfare qualsiasi necessità di comunicazione aziendale oltre che di inserirsi in modo trasparente in infrastrutture basate su Pbx virtuali o fornite come servizio da operatori telefonici qualificati.

Smart place intelligente e aperto al cloud

Un esempio concreto di soluzioni che in Snom abbiamo ideato in base alle esigenze espresse dalle aziende per la propria comunicazione su IP è la nuova linea premium di terminali IP, oggetti che colpiscono non solo per l'estrema versatilità e la nota robustezza ma anche per il design, fino agli accessori (dagli headset alle soluzioni portatili DECT-based per teleconferenze) che assicurano piena mobilità all'interno degli uffici.
Soluzioni come i telefoni IP da tavolo D785 e D735, nella versione bianca, trovano riscontro positivo ovunque sia necessario che il telefono si differenzi visivamente rispetto ai convenzionali terminali neri o grigi, come ad esempio nel settore sanitario, o presso uffici particolarmente attenti al fattore estetico delle componenti d'ufficio.
L'ultimo nato della serie di terminali IP Snom D7xx, lo Snom D735 nello specifico, è dotato anche di un sensore di movimento che rileva l'avvicinarsi della mano dell'utente, attiva quindi automaticamente il display e presenta le funzioni più utilizzate e i favoriti, evitando all'utente la tediosa navigazione nel menu alla ricerca della funzione di cui desidera avvalersi.

"Telefonia as a Service" e telefoni IP sicuri con Snom

Le esigenze di un mondo business o di customer relationship sempre più accelerate e multicanale hanno apportato un profondo mutamento nel

Snom D785 bianco

mondo della telefonia e dell'UCC, nonché nel modo di predisporre una postazione di lavoro in grado di far fronte alle esigenze di mobilità aziendale e di incanalare le comunicazioni verso un unico punto di contatto sempre raggiungibile da colleghi e clienti ovunque ci si trovi.
I ritmi della telefonia sono però da sempre più lenti di quelli dell'IT, e per ragioni oggettive. Cambiare un sistema telefonico non è mai stato semplice come cambiare un server o un Pc. I fattori da analizzare sono tanti, non ultimo il piano di ammortamento, la confidenza degli utenti con i dispositivi a disposizione, i servizi forniti, il supporto specializzato, eccetera.
Per queste e numerose altre ragioni quando scadono i contratti di manutenzione della piattaforma di telefonia, a volte ancora di tipo proprietario, gli IT manager si trovano di fronte a un bivio: rinnovare l'impianto esistente o sostituirlo con soluzioni aperte, più al passo con i tempi a livello funzionale e meno impattanti in termini di TCO e di Opex.

Interoperabilità e qualità del servizio: un must

A fronte della trasformazione digitale di imprese pubbliche e private di ogni ordine e grado, considerazioni sull'interoperabilità, qualità e sicurezza delle componenti per le telecomunicazioni

assumono oggi un'importanza crescente presso organizzazioni di qualsiasi dimensione.
Nel percorso verso la postazione di lavoro smart, l'interoperabilità delle componenti è un criterio di valutazione essenziale, specie alla luce della progressiva e ormai pervasiva migrazione a infrastrutture dati e voce "all-IP". Non stanno solo cambiando le applicazioni individuali, ma anche l'intera infrastruttura e le modalità operative in maniera orizzontale. Trovare la piattaforma e i terminali ideali, che non vincolino l'azienda ad un solo brand o a sistemi chiusi, è la vera sfida per le organizzazioni. Si tratta di un processo con così tante variabili da richiedere ai responsabili IT/TLC di prendersi il proprio tempo e possibilmente di rivolgersi a specialisti.
Le soluzioni UC, i telefoni IP avanzati, le applicazioni più moderne e i servizi basati sul cloud, tutti si avvalgono della stessa infrastruttura di rete e promettono alle aziende un incremento della produttività ed una semplificazione della collaborazione tra gli addetti. La convergenza delle applicazioni contribuisce a migliorare la coordinazione sui progetti e a limitare la perdita di informazioni. Un motivo sufficiente per dotarsi di soluzioni UC e terminali IP altamente interoperabili, personalizzabili e dotati di un'interfaccia utente non complessa per non sovraccaricare gli utenti.
Quando si seleziona un terminale IP è utile tenere a mente il principio della funzionalità "plug & play": i dispositivi devono potersi configurare automaticamente non appena collegati alla rete aziendale. Un altro punto da considerare è la personalizzazione dell'endpoint.
La receptionist vuole essere in grado di contattare i colleghi utilizzando la selezione automatica, mentre l'assistente del direttore esecutivo preferisce utilizzare il tasto BFL (Busy Lamp Field) per rispondere alle chiamate in entrata.
Se più persone condividono la stessa postazione di lavoro, ognuno vorrà avere il proprio accesso personalizzato allo stesso terminale (hot desking). Tutte personalizzazioni che vanno garantite.
Poter impostare configurazioni specifiche per gli utenti interni e remoti tramite una console centralizzata è essenziale per evitare che l'amministratore di sistema venga assediato con problematiche inerenti l'uso dei terminali. Tutti criteri da valutare in termini di interoperabilità tra l'infrastruttura, la centrale telefonica e il terminale sulla scrivania.
Altro criterio essenziale è la qualità del servizio: nelle infrastrutture "tutto su IP" la velocità e le prestazioni di rete sono essenziali per la fruibilità dei servizi. Per evitare lamentele da parte degli utenti la nuova infrastruttura deve basarsi su un approccio votato alla qualità. Anche la più performante delle linee internet perde valore di fronte ad una malgestione del flusso traffico (voce/dati) nella rete IP aziendale.
L'impiego di una rete virtuale prioritaria per il traffico voce (Voice VLAN), unitamente a switch che supportino il protocollo LLDP-MED consente ai terminali IP di autoconfigurarsi per l'accesso alla rete "voce" mentre ai PC di collegarsi alla rete "dati". Il telefono IP attualmente in uso in azienda è in grado di operare tale selezione?
Non da ultimo, il punto "sicurezza" e VoIP crea grattacapi a moltissimi IT-Manager. Le intercettazioni telefoniche sono da sempre una minaccia: una volta bastava un collegare un chip con doppino al microfono per ascoltare le conversazioni su linea analogica, collegarsi alla centralina di distribuzione in strada in presenza di linee ISDN, scansire le frequenze DECT per hackerare le conversazioni condotte con telefoni cordless e, per quelle condotte su rete GSM, installare semplicemente celle fasulle. Agli albori del VoIP c'era un firewall che proteggeva l'accesso a internet e tutti i dati erano archiviati localmente.

Oggi non è più così facile hackerare le conversazioni telefoniche a fronte dell'introduzione di numerose tecniche di cifratura per il DECT, la voce trasportata via IP, la connessione dati e le piattaforme UC, fino a sistemi di cifratura impenetrabili da terminale a terminale

Quando si valuta una nuova infrastruttura per la telefonia IP evoluta è necessario soppesare il livello di sicurezza garantito dalla centrale e dai terminali a fronte della reale esigenza e del costo.

Inoltre varrebbe la pena chiedere agli operatori e ai fornitori del centralino e dei terminali dove siano archiviati effettivamente i dati sensibili (log del centralino, contatti della rubrica / CRM, impostazioni utente su telefono e centrale) e come essi vengano trattati, una domanda lecita, visto che oggi numerose soluzioni e servizi sono dislocati "fisicamente" in luoghi diversi e i dati si trovano spesso nel cloud.

Di interesse ancora maggiore è sapere se i dati sono ospitati su server nel proprio Paese o distribuiti in tutto il mondo. Un problema di sicurezza che riguarda meno il rischio di hackeraggio quanto più l'uso dei dati a scopo statistico o per spionaggio industriale ad opera di terzi.

Telefoni IP e Cloud sicuro all'Università di Greifswald

Un esempio reale di come tali valutazioni si concretizzano è l'Università di Greifswald, che ha preferito fruire di una piattaforma per la telefonia cloud-based totalmente ridondata, ospitata presso l'operatore di telefonia IP selezionato dotandosi di telefoni VoIP flessibili, configurabili con un click e soprattutto sicuri.

L'Università di Greifswald voleva assicurarsi che i terminali si identificassero e autenticassero sulla rete dell'Istituto attraverso certificati specifici (IEEE 802.1x e x509), al fine di tutelare le reti virtuali dedicate alla telefonia contro accessi indesiderati.

La sfida per gli attori coinvolti (l'operatore di telefonia "as a Service", l'Università di Greifswald e Snom come fornitore dei terminali) è stata quella di automatizzare il processo di trasferimento protetto della chiave di sicurezza ai numerosi telefoni, garantendo che in caso di furto di un terminale l'intero parco installato di telefoni Snom potesse essere dotato con un click di nuove chiavi di sicurezza, rendendo quella presente sul telefono trafugato quasi immediatamente inutilizzabile, vanificando in sostanza qualsiasi tentativo di estrazione dei parametri di cifratura. Al momento sono circa 2000 i telefoni Snom D765 attualmente installati presso l'Istituto Universitario da oltre un anno e mezzo.

Optare per la telefonia "as a Service" fruita con terminali di nuova generazione come quelli forniti da Snom ha dato già i suoi frutti sia in termini di sostituzione dei vecchi apparati, realizzata in circa 2 mesi senza interruzione dei servizi di telefonia, sia in termini di flessibilità operativa, funzionale e per la sicurezza.

GARANTIRE LA SICUREZZA DEI SISTEMI INFORMATIVI INDUSTRIALI 4.0, FINANZIARI E AZIENDALI È UNA PRIORITÀ

Allargare ai sistemi periferici la stessa protezione fornita nel perimetro aziendale è un passo avanti ma può non bastare. Alberto Brera suggerisce cosa fare per garantirla

Alberto Brera, Stormshield

Nel processo di digital transformation e nell'adozione progressiva di tecnologie per un ambiente e un modo di lavorare e produrre smart che sta trasformando profondamente il mondo aziendale, industriale e finanziario, la sicurezza costituisce uno dei criteri da considerare.
In termini di cyber security, l'anno trascorso è stato di certo un anno buio, osserva l'Ing. **Alberto Brera**, Country Manager per l'Italia di Stormshield, società specializzata nello sviluppo di soluzioni per la protezione delle reti aziendali certificate EU RESTRICTED, NATO e ANSSI EAL4+, oltre che per la tutela delle workstation e dei dati.
L'ampia copertura mediatica di attacchi perpetrati ai danni dei sistemi informativi anche di colossi del mondo aziendale o finanziario ha avuto il merito di incrementare la consapevolezza anche degli operatori industriali e dei fornitori di servizi sulle proprie vulnerabilità, alla luce di criticità oggettive, dovute ad un'errata valutazione dei rischi cagionati dall'apertura di sistemi progettati per operare in modo isolato all'universo iperconnesso del 4.0.
Criticità che mettono in luce oggi più che mai quanto sia necessario adottare misure appropriate, sia in termini di infrastruttura IT sia di integrità OT.
E' un dato di fatto che la continuità del servizio, quando c'è di mezzo la produzione, è cruciale e il suo impatto è ben superiore a quello dei sistemi IT, poiché è determinante non solo per l'integrità dei beni ma soprattutto per quella del personale addetto agli impianti.

I problemi dei sistemi informativi industriali

Quando si parla di Industry l'assunto di partenza è che il sistema informativo di un'azienda manifatturiera differisce da quello di altri settori di mercato e le sue specificità richiedono dispositivi di protezione che integrino la logica legata al tipo di attività. Di conseguenza sovente le tradizionali soluzioni multifunzione trasversali proposte sul mercato non offrono un livello di sicurezza appropriato.
«A nostro avviso solo i fornitori che hanno sviluppato competenze specifiche sono in grado di offrire un supporto concreto nell'affrontare le sfide poste dal settore industriale. Occorre adot-

tare un approccio il cui risultato consta nella semplificazione della gestione dei sistemi impiegati, soprattutto lato amministrazione delle soluzioni, sviluppando sinergie tra i team informatici e i responsabili degli impianti aziendali coinvolgendoli contemporaneamente nella messa in sicurezza dei sistemi IT e OT. La necessità di sinergie e la peculiarità del mondo industriale sono anche il motivo per cui ultimamente si assiste allo sviluppo di un intero ecosistema imperniato sulla protezione dei sistemi informativi industriali» spiega Brera.

La direttiva NIS e il ruolo chiave delle partnership

L'importanza che il mondo industriale assume per le economie avanzate ha fatto sì che i legislatori abbiano affrontato la tematica giungendo alla conclusione che la messa in sicurezza dei sistemi informativi industriali sia essenziale. Affermazioni concretizzatesi in molteplici leggi nazionali o europee, come ad esempio la Direttiva UE 2016/1148, meglio nota come Direttiva NIS. L'intento della Direttiva è assicurare a tutte le infrastrutture critiche a livello nazionale un'adeguata tutela contro incidenti informatici che potrebbero cagionare la non disponibilità di servizi primari per il Paese.

A fronte dell'intervento del legislatore e consapevoli della crescente pervasività di IoT e sistemi Industry 4.0, i professionisti del settore industriale devono necessariamente riconsiderare radicalmente le proprie politiche di cyber security.

«Una cosa però appare chiara, Un progetto di questo peso e rilevanza può prendere forme concrete solo con il supporto di specialisti. E' quindi imperativo che il settore della sicurezza continui a sviluppare soluzioni per fronteggiare queste minacce – anche e forse in primo luogo – formando nuove alleanze, al fine di consentire alle organizzazioni industriali di evolvere in ambienti effettivamente sicuri. Stormshield ad esempio intrattiene partnership tecnologiche e commerciali con produttori e operatori complementari. Unendo le nostre forze abbiamo sviluppato sistemi ad alto valore aggiunto frutto della combinazione di soluzioni, integrazione, consulenza, formazione» evidenzia Brera.

In Italia il settore manifatturiero pare focalizzarsi primariamente su esigenze business quali la remotizzazione delle operazioni e del monitoraggio di sistemi esistenti, più che trasformarsi in una industria smart di nuova generazione, mettendo in secondo piano la valutazione dei rischi connessi a questa innovazione.

Il caso dei sistemi SCADA è emblematico. «I sistemi SCADA sono stati progettati oltre 20 anni fa per ambienti chiusi e non esposti su internet. Calare processi produttivi basati su macchinari e sistemi progettati qualche decennio fa in infrastrutture interconnesse è una sfida, anche e soprattutto in termini di tutela delle comunicazioni tra i diversi sistemi di produzione.

Una comunicazione che, in ottica "Industry 4.0", dovrebbe aver luogo tramite dispositivi non pensati per inviare comandi ai macchinari (smartphone, tablet, notebook) e difficilmente monitorabili tramite i tradizionali sistemi IT/OT.

«Stormshield è da tempo attenta alla protezione specifica dei sistemi di produzione e con la propria soluzione SNi40 propone una soluzione di sicurezza UTM/IPS sviluppata attorno al mondo SCADA, in grado di reagire proattivamente contro le minacce che nascono al crocevia tra l'automazione industriale e la rete informatica, con l'obiettivo primario di supportare le aziende manifatturiere nel trasformarsi in Industry 4.0 in accordo con il principio della sicurezza 'by design'», evidenzia il manager.

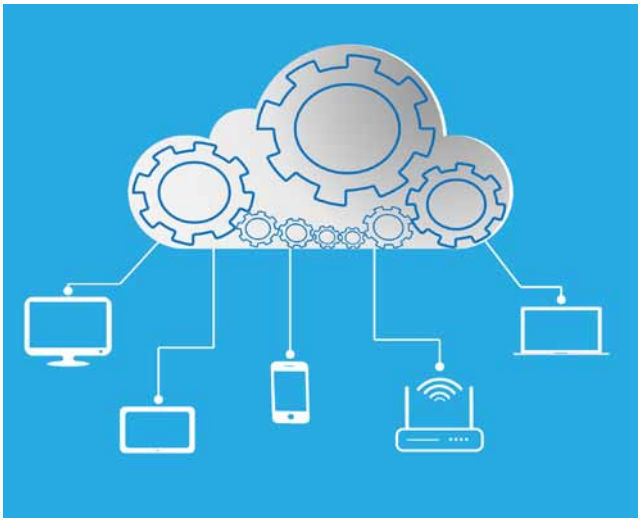
Le criticità nel mondo Finance e come affrontarle

I problemi connessi alla trasformazione digitale e a un ambiente di lavoro smart non sono esclusivi del mondo industriale. Secondo uno studio condotto da Ponemon Institute e Accenture in 7 Pa-

esi con il coinvolgimento di 254 operatori finanziari, gli istituti bancari e assicurativi subiscono in media 125 intrusioni all'anno.
Queste violazioni della sicurezza implicano una perdita di profitto, minano l'integrità dei dati e delle risorse dei clienti e hanno un impatto negativo sulla reputazione degli istituti in questione. In questo contesto, un altro studio di B2B International, ha rilevato che la perdita media degli Istituti finanziari si aggira attorno a poco meno di un milione di dollari per singolo incidente di sicurezza informatica.
Il mondo della finanza in generale è stato meno colpito dalle forme più comuni di attacco informatico, come il malware tradizionale, rispetto ad altri settori. Tuttavia, gli operatori finanziari risultano particolarmente esposti ad attacchi mirati e di Denial of Service (DDoS). È molto aumentato anche il numero di sistemi infettati da trojan bancari, il cui scopo principale è quello di sottrarre i dati dei clienti. Il phishing mirato, l'ingegneria sociale e le backdoor nei sistemi di sicurezza o nei dispositivi di rete, attraverso cui i cyber criminali si infiltrano abusivamente nei sistemi informativi degli operatori, completano il quadro delle minacce ai danni degli istituti finanziari.
«La sicurezza informatica è divenuta una delle maggiori preoccupazioni per i direttori delle principali banche e compagnie assicurative. Ciò trova corrispondenza nella crescita verticale dei budget dedicati negli ultimi anni alla tutela dei sistemi informativi» considera Brera.
Seppur già ben attrezzati con soluzioni consolidate, gli operatori finanziari ora devono andare oltre, sfruttando nuovi approcci come l'intelligenza artificiale e le tecnologie analitiche a completamento delle soluzioni in uso al fine di accrescere il proprio livello di sicurezza. In questo modo, gli istituti finanziari possono proteggersi attivamente contro le nuove minacce con cui si confrontano quotidianamente e avanzare fiduciosamente verso una trasformazione digitale di successo. «Ma in un ambito tanto sensibile come quello bancario e assicurativo le aziende devono proteggersi scegliendo tecnologie affidabili, la cui affidabilità e robustezza si riflette nella certificazione e classificazione ai massimi livelli europei» osserva il manager.

Dati al sicuro nel cloud

Sia che si tratti di Industry 4.0 che di Finance o di infrastrutture IT convolte nella trasformazione digitale, un denominatore sempre più comune è il ricorso al Cloud o al Multicloud, e come garantire in un tale contesto la sicurezza dei dati. Il 90 % delle organizzazioni se ne avvale per accedere remotamente ad applicazioni e a dati aziendali, oltre che per migliorare il modo in cui collabora con il proprio ecosistema.
Accedere a informazioni e applicazioni ovunque, in qualsiasi momento e su qualsiasi dispositivo, significa oggi accettare di archiviare dati critici aziendali sul server di qualcun altro, spesso dislocati da qualche parte nel mondo" osserva Brera. Secondo il Computing Cloud Report 2018, quasi il 90% degli intervistati sarebbe preoccupato per le violazioni della sicurezza e la perdita dei dati nell'ambiente Cloud. «Ciò che si nasconde dietro questi timori è semplice in realtà: un solo difetto di sicurezza può portare al furto e alla divulgazione di milioni di informazioni, come abbiamo visto nei casi purtroppo noti di Yahoo e Twitter (solo per citarne alcuni)» spiega Brera. Il concetto di fiducia è, quindi, essenziale.
Quattro anni dopo lo scandalo delle foto delle celebrità rubate e cinque anni dopo le rivelazioni di Edward Snowden, che ha decisamente offuscato la reputazione del Cloud, la fiducia nel Cloud è di nuovo in aumento. Sebbene le minacce non siano scomparse, l'idea che i rischi connessi all'uso del Cloud possano essere gestiti sta iniziando a farsi strada nella nostra coscienza.
Per proteggere applicazioni e informazioni archiviate su server delocalizzati, i responsabili della sicurezza di numerose aziende tendono ad implementare gli stessi strumenti di protezione



adottati nel tradizionale perimetro aziendale, in particolare installando firewall virtuali posizionati all'interno dell'infrastruttura Cloud. Una buona misura, ma non basta, crittografare i dati archiviati online fornisce un'adeguata protezione. "Pur limitando, in taluni a dipendenza della soluzione adottata, alcune funzionalità di collaborazione, la cifratura impedisce qualsiasi accesso illegittimo ai dati in caso di compromissione della sicurezza del fornitore di servizi cloud. Risponde inoltre alla potenziale e di certo indesiderata intercettazione dei propri dati da parte del provider di servizi cloud", conferma Brera.

Se in azienda esiste la necessità di garantire un accesso globale e costante alle informazioni, è sempre opportuno crittografare le informazioni nel Cloud. Soluzioni, come Stormshield Data Security per Cloud e Mobility consentono agli utenti di crittografare i dati memorizzati all'interno di applicazioni fruite in outsourcing, pur mantenendo la propria chiave decrittografica, evitando di utilizzare quelle proposte dal provider Cloud, tutelando quindi la riservatezza dei propri asset digitali come richiesto dal GDPR.

Tecnologie smart per la sicurezza perimetrale

«Anticipare le esigenze future delle aziende in termini di sicurezza è una vera sfida quando ci si confronta con l'esponenziale accelerazione dello sviluppo tecnologico, il Cloud, l'IoT, la crescente richiesta di banda e l'estensione del perimetro aziendale che ne deriva. Una missione di cui Stormshield si è fatta carico con una serie di prodotti che si adattano alle esigenze delle piccole imprese come di aziende di dimensioni medio grandi» commenta Brera.

Per garantire la sicurezza aziendale assistendo le imprese nella loro trasformazione digitale, Stormshield ha sviluppato una specifica gamma di soluzioni con cui si è prefissata di assicurare prestazioni ideali per applicazioni SaaS come per ambienti virtuali PaaS (Platform as a Service) e IaaS (Infrastructure as a Service).

Le soluzioni IPS a marchio Stormshield hanno un ciclo di vita tra i cinque e gli otto anni. Se rapportiamo un tale periodo alla velocità con cui la tecnologia evolve e alla conseguente evoluzione dell'infrastruttura aziendale, non ha senso dotarsi di prodotti difficilmente adattabili alle future esigenze, e che faticano a gestire nel tempo un importante incremento del traffico.

Un paradigma che Stormshield ha fatto proprio non lavorando in ASIC. E' quindi in grado di incrementare esponenzialmente le prestazioni dei propri firewall grazie al continuo lavoro di ottimizzazione del codice. I nuovi dispositivi per la sicurezza perimetrale che ha annunciato di recente beneficiano ad esempio di un'ottimizzazione del controllo del traffico http (+40%) e della VPN IPSec (+50%) necessaria per una comunicazione sicura sul cloud, scevra da colli di bottiglia. Con l'ultima release ha anche raddoppiato il throughput delle soluzioni esistenti.

«Investire in sicurezza significa investire nel futuro dei propri asset critici, tra cui dati e infrastrutture. L'approccio modulare che abbiamo sviluppato, sia come hardware sia in termini di funzionalità e prestazioni, assicura il massimo ritorno sull'investimento per l'intero ciclo di vita dell'infrastruttura informatica implementata nell'ambito di un processo continuo di trasformazione digitale», conclude Brera.

HYPER AVAILABILITY È LA CHIAVE DI VOLTA PER UNA ENTERPRISE E UN'INDUSTRY SMART E ALWAYS-ON

La diffusione di ambienti multicloud aumenta l'esigenza di modificare l'approccio nella gestione del dato e di passare ad uno proattivo basato sull'AI e su analitiche

Albert Zammar, Veeam

Quelli che stiamo attraversando e che dovremo affrontare nel prossimo futuro sono tempi di profondi e impegnativi cambiamenti tecnologici e organizzativi per le aziende e i manager IT.

L'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione del dato passando ad uno proattivo basato sull'Intelligenza artificiale e su analitiche è conseguenza dell'evoluzione del mondo produttivo e delle modalità da parte delle aziende e dei privati a cui erogano servizi di fruire delle applicazioni IT, sempre più basate su ambienti multicloud. Si tratta di realtà che, sia che si parli di reti di sensori IoT inerenti infrastrutture di tipo sanitario, dei trasporti, di grid per l'erogazione di energia che di pubblico servizio, necessitano di essere orchestrate e garantite sia per quanto concerne la loro disponibilità assoluta che per i tempi di risposta in termine di latenza e velocità alle richieste di dati inoltrate.

La risposta a queste esigenze Veeam l'ha data con una vision che concretizza la Hyper-Availability, il cui compito è di abilitare e facilitare l'orchestrazione dei dati guidata dagli eventi anche su infrastrutture multi cloud di grandi dimensioni.

Hyper-Availability: la risposta alle esigenze del business

La Hyper-Availability rappresenta nella vision di Veeam la nuova frontiera nel trattamento del dato e nella sua fruizione per il business.

La piattaforma che abbiamo sviluppato, la Hyper-Availability Platform, già utilizzata da numerose grandi aziende ed operatori mondiali e italiani, costituisce una soluzione completa di Intelligent Data Management che permette di sviluppare e fornire rapidamente e in modo sicuro servizi digitali innovativi.

In sostanza, la protezione e la gestione dei dati pensata come mera salvaguardia attraverso policy reattive appare non più congrua con le nuove esigenze e nella vision di Veeam deve trasformarsi in un sistema che fornisca in modo proattivo valore di business.

Come tutte le evoluzioni, Veeam riconosce che non sempre è però possibile operare partendo da un green field e si deve tenere necessariamente conto della realtà aziendale e delle esigenze di

salvaguardia degli investimenti già attuati in IT e processi di business.
Per questo e per concretizzare una Hyper-Available Enterprise nelle diverse condizioni aziendali abbiamo sviluppato un portfolio ad hoc che permette di evolvere in fasi successive.
Una prima fase interessa il Backup ed è inerente alla salvaguardia di tutti i workload, assicurando che siano sempre ripristinabili.
La seconda è relativa alla Aggregazione ed è volta a garantire la protezione e la disponibilità dei dati in ambienti multi cloud.
Una terza fase interessa la Visibilità, con soluzioni che permettono di migliorare la gestione dei dati in ambienti multi cloud grazie ad un controllo unificato dell'utilizzo, delle prestazioni e operatività, a cui aggiunge monitoraggio, ottimizzazione delle risorse, capacity planning e intelligenza integrata.
La quarta fase è l'Orchestrazione, che tramite un motore appositamente sviluppato permette di movimentare i dati all'interno degli ambienti multi-cloud e assicurara la continuità del business, la compliance, la sicurezza e l'utilizzo ottimale delle risorse.
L'ultimo fase è rappresentata dall'Automazione, con i dati che, tramite la pattern recognition e il machine learning, si auto-gestiscono, imparando a duplicarsi, spostarsi verso il sito più adatto in base alle esigenze di business, proteggersi in caso di attività anomale e ripristinarsi in modo istantaneo.

Veeam DataLabs, il passpartout per il passaggio in produzione

Garantire la sopravvivenza e la disponibilità del dato, tramite anche il ricorso all'intelligenza artificiale, è però solo una delle componenti dell'equazione che porta ad una smart economy e ad un'azienda always-on.
L'altro fattore da considerare è il "Tempo" correlato ai processi produttivi e a cosa necessita a livello di dati per passare dalla formulazione di una idea al suo passaggio in produzione, sia che si tratti di un bene materiale che di un servizio immateriale.
Un aiuto concreto lo diamo con la piattaforma per l'alta disponibilità Veeam DataLabs, una soluzione per la gestione delle copie che permette alle aziende di creare rapidamente e on-demand nuove istanze dei propri ambienti di produzione.
La soluzione abilita casi d'uso che vanno oltre i classici scenari di protezione dei dati, come DevTest, DevOps e DevSecOps, e include test di sicurezza e di analisi forense e sandbox on-demand per le operations IT. In sostanza, rende disponibile un contesto per sperimentare e accelerare l'innovazione, migliorare l'efficienza operativa, ridurre i rischi e ottimizzare le risorse.
Veeam DataLabs si basa sulle funzionalità dei Virtual Labs di Veeam, abilitando istanze di produzione di ambienti virtuali su richiesta.
Queste "sandbox" isolate sfruttano i dati esistenti per accelerare l'innovazione e ridurre il rischio in fase di test di nuove soluzioni.
Non ultimo, in linea con la vision di Veeam volta alla creazione di ambienti aperti, permette di integrarne il software con le soluzioni di storage dei principali partner tecnologici come Cisco, HPE, IBM, NetApp o Pure Storage.

Una vision per la iper disponibilità confermata dal mercato

Come evidenziato, la Hyper-Availability Platform è una soluzione sviluppata per aiutare le aziende ad automatizzare la gestione dei dati e ad assicurarne la disponibilità.
La sua corrispondenza alle esigenze delle aziende è ampiamente confermata dai dati di mercato e dai clienti che l'hanno adottata.
Alla data annovera oltre 307.000 clienti nel mondo, tra cui il 75 percento delle aziende Fortune 500 e poco meno del 60 percento delle aziende Global 2000. L'indice di soddisfazione dei clienti,

pari al 3.5X della media, è tra i più alti di mercato. A questo affianchiamo 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.

Un futuro Multicloud, predittivo, 5G per IoT e M-to-M

L'esigenza di iper disponibiità non è solo un argomento di oggi, ma sempre più costituirà la chiave di volta, una condizione sine qua non, per le nuove infrastrutture smart abilitanti l'evoluzione digitale.

Il problema della gestione, evidenzia una ricerca che abbiamo realizzato, è dei più critici e riteniamo che sia fondamentale per le aziende riconoscere l'importanza dell'Intelligent Data Management per essere sempre un passo avanti e fornire servizi migliori ai propri clienti.

Un report a firma di McKinsey & Company rivela che i dati dalle regioni chiave del Nord America e dell'Europa sono saliti drasticamente a 5.000 – 20.000 Gbps e 1.000 – 5.000 Gbps rispettivamente, rispetto ai 100-500 Gbps e meno di 50 Gbps nel 2005. Con aziende che operano a livello internazionale e l'utilizzo sempre più massiccio di tecnologia, ciò rende quasi inevitabile il ricorso al multi-cloud.

IDC da parte sua stima che nel 2021 le aziende spenderanno 554 miliardi di dollari per il cloud computing e servizi correlati, più del doppio rispetto al 2016.

I dati e le applicazioni on-premise non diventeranno obsoleti, ma i modelli di implementazione dei dati si espanderanno con un mix crescente di on-prem, SaaS, IaaS, managed clouds e private cloud.

Un altro tema è costituito dall'Analisi Predittiva e dal Machine Learning, che si avviano a divenire mainstream e saranno estremamente diffuse.

Ad esempio, cominceremo a vederli realizzati utilizzando firme e impronte digitali, contenenti le configurazioni di best practice e policy, per consentire all'azienda di ottenere più valore dall'infrastruttura implementata.

I Predictive Analytics, o Diagnostics, aiuteranno in sostanza a garantire la continuità operativa, riducendo al contempo l'onere amministrativo di mantenere i sistemi ottimizzati. Questa capacità riteniamo che sia di vitale importanza, in quanto le organizzazioni IT saranno sempre più chiamate a gestire un ambiente ampiamente diversificato, con più dati e con obiettivi di livello di servizio più stringenti.

Un elemento di disruption sarà poi l'arrivo delle prime reti 5G, che prevedibilmente creerà nuove necessità per i CSP che aiuteranno nella raccolta, gestione e archiviazione di maggiori volumi di dati.

Nel corso dei prossimi mesi assisteremo infatti alla diffusione di nuovi tipi di telefoni 5G. Ipotesi realistica è che il 5G venga probabilmente adottato più rapidamente dalle aziende per la comunicazione Machine-to-Machine e l'Internet delle Cose (IoT), mentre per i consumatori la velocità della rete mobile con il 4G sembra già più che soddisfacente per le loro esigenze.

Per i rivenditori e i fornitori di servizi cloud, l'interesse si concentrerà sull'arrivo di nuove opportunità di guadagno sfruttando il 5G o l'infrastruttura per supportarlo.

L'elaborazione di questi maggiori volumi di dati in tempo reale, a una velocità più rapida, i nuovi requisiti per hardware e dispositivi e le nuove applicazioni per la gestione dei dati presenteranno tutte le opportunità da cogliere e aiuteranno a facilitare le conversazioni con l'edge computing, ma richiederanno infrastrutture ad elevatissima disponibilità.

Gestire i dati in modo intelligente migliora l'operatività: Il caso IRI e Telethon

Se a livello funzionale la Hyper-Availability Pla-

tform di Veeam è qualificata dagli analisti al top del mercato, ancor più lo è dal numero elevato di aziende che l'hanno adottata.
Ad esempio IRI, attiva nella fornitura di ricerche di mercato dedicate ai settori del retail e del marketing, ha adottato Veeam Backup & Replication per garantire la disponibilità dei dati e la business continuity.
IRI, nello sviluppo del proprio business al servizio delle aziende, fa leva su quello che evidenzia essere praticamente il più grande patrimonio di informazioni su acquisti, investimenti sul punto vendita, media, shopper loyalty e comportamento dei consumatori, il tutto integrato in piattaforme tecnologiche on demand.
Nelle sue attività la qualità e la disponibilità dei dati e dei sistemi informativi è quindi un aspetto irrinunciabile del proprio business.
La complessa infrastruttura di IRI include per il data center principale per l'Europa circa 350 server virtuali che elaborano circa 1 Petabyte (PB) di dati, che vengono poi erogati on-demand o in tempo reale verso i clienti di IRI attraverso servizi cloud.
E' in questo quadro tecnologico e di esigenze di business che la società ha implementato Veeam Backup & Replication all'interno di una più ampia strategia di sicurezza, per garantire la protezione e la gestione del suo data center europeo, situato in Germania, e assicurare la disponibilità dei dati ivi residenti.
L'approccio di Veeam all'intelligent data management ha consentito una migliore visibilità ed un migliore accesso alle informazioni, e fornito al contempo tecnologie di backup affidabili e flessibili per mitigare ogni potenziale interruzione della continuità operativa.
Fondazione Telethon, una delle principali charity biomediche italiane, ha invece adottato 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, 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 ch assiduamente svolge.
La Fondazione opera in sedi multiple e 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.
Le funzionalità di backup e replication scalabili accelerano le prestazioni di business, oltre a permettere al team di addetti IT di gestire workload scalabili in modo efficiente e più semplice rispetto al passato.
In pratica, 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.
Affidabilità, sicurezza e disponibilità sono essenziali per l'operatività di Fondazione Telethon. La sua priorità è 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 sulla loro meritoria attività.