Cloud & Business

n.87
Gennaio 2020

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

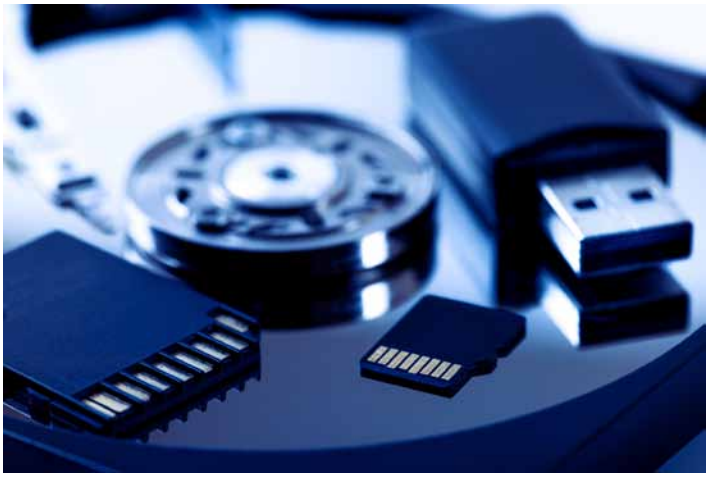
Lo storage dal cloud all'iperconvergenza

di Giuseppe Saccardi

Lo storage sta affrontando profondi cambiamenti per permettere di supportare multi-cloud, edge computing e containerizzazione. La chiave è nella tecnologia flash

A 2020 oramai inoltrato si può cercare di passare dalle previsioni a qualcosa dipiù concreto e meno aleatorio in quelli che sono i settori che appaiono più promettenti ed in evoluzione dell'IT.

Una cosa su cui aziende del settore e soprattutto i dati di società di analisi è la progressiva accettazione e diffusione del modello "as a Service", in sostanza, del continuo passaggio ad un modello IT basato sul cloud e sul multi cloud nelle sue varie combinazioni e declinazioni. In questo quello che fa premio per le



Reportec Cloud&Business - N.87 Gennaio 2020 - società- Editore: Reportec Srl **(www.reportec.it)** - Direttore responsabile: Giuseppe Saccardi
In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

aziende è la semplicità che un tale modello mette a disposizione: mi serve una cosa, la prendo e la pago a consumo senza dovermi preoccupare di avviare progetti per individuare il prodotto più adatto, realizzare impianti pilota onerosi e che implicano tempi lunghi e rischi, installarlo, gestirlo, aggiornarlo nella varie release hardware e software, eccetera.

E' una tendenza che, mutatis mutandi, va di pari passo con la diffusione a livello di piattaforma con le soluzioni iperconvergenti, evoluzione ultima delle soluzioni convergenti apparse sul mercato pochi anni fa e che ora si stanno sempre più imponendo all'attenzione anch'esse a causa della semplificazione che apportano nella realizzazione di infrastrutture aziendali e nella loro gestione.

Serve ad esempio decentrare as livello di edge capacità di calcolo e di storage? .Invece di procedere all'acquisto separato dei diversi componenti e alla loro integrazione prendo un sistema già predisposto con capacità elaborativa, storage e rete e il gioco, entro certi limiti è fatto. E soprattutto ho un unico responsabile a cui rivolgermi se qualcosa non va come dovrebbe.

Verso un modello di business as-a-Service

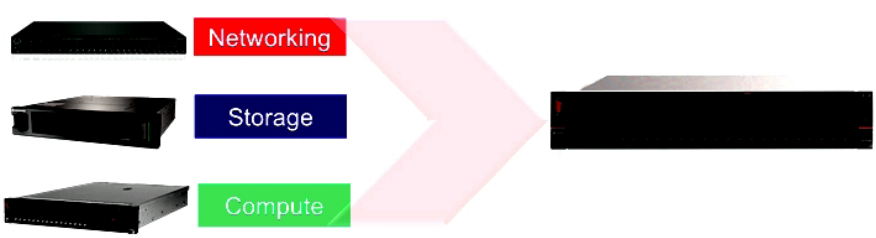
I modelli as-a-Service per l'IT esistono da quando esiste il Cloud, anzi, ne costituiscono la genesi.

Si sono poi andati differenziando a secondo che si parli di cloud, di cloud ibrido o di multi-cloud, una evoluzione che ha richiesto per essere supportata una pari evoluzione del modo di gestire le risorse e di orchestrarle tra fornitori diversi, ad esempio per quanto riguarda la movimentazione trasparente e sicura di dati tra il servizio storage fornito da un provider ed un altro, ad esempio da Microsoft Azure e AWS , o viceversa, o tra questi e lo storage on-premise.

DI qualunque cloud si tratti e con il cloud ibrido o multi-cloud che rappresenta una consolidata realtà quello che gli utenti si aspettano è una semplicità ed una automazione delle infrastrutture on-premise che sia pari di quelle cloud, e di disporre nel cloud degli stessi livelli di controllo e funzionalità di classe Enterprise che si possiedono on-premise , il tutto a partire da un modello di pagamento as-a-Service che sia altamente flessibile.

Nel 2020, con le aziende che stanno spostando gli investimenti verso i costi operativi a scapito di quelli in conto capitale , la richiesta di storage as-a-Service aumenterà ma prevedibilmente la scelta si orienterà verso quei modelli di servizio che più coniugheranno la semplicità operativa con una pari semplicità di quelli di acquisto.

Da un punto di vista operativo gli attributi più importanti includono ad esempio standardizzazione, accesso on-demand, gestione basata su API e, non ultimo, un grado di scalabilità perlomeno potenzialmente illimitata.
Se ci si sposta sul piano dell'utilizzo di un servizio gli elementi qualificanti comprendono invece come condizione che appare sine qua non un modello pay-per-use, alta flessibilità in termini di capacità e la possibilità di far crescere o evolvere i servizi nel tempo garantendosi la business continuity.
La diffusione del cloud è poi alla base di un ritorno di interesse per l'Object Storage, che oramai non viene più percepito come una sorta di storage economico da utilizzare per lo storage di dati poco utilizzati ma bensì visto come una nuova forma di storage primario.
Si tratta di una tecnologia che proprio per la sua capacità di supportare l'accesso parallelo e altamente distribuito ha finito con il divenire una sorta di standard per applicazioni cloud-native. In pratica, mentre le applicazioni vengono sviluppate o riscritte per architetture cloud-friendly, l'Object Storage si prospetta sempre più come una scelta naturale al fine di disaccoppiare e disaggregare le applicazioni e le relative risorse di calcolo da un pool di storage condiviso.



La iperconvergenza mette a disposizione blocchi integrati di calcolo, storage e rete

Questo pattern, osserva un protagonista dello storage come Pure Storage, ha preso piede non solo nello sviluppo personalizzato di software, ma anche presso i grandi vendor di software come Splunk e Vertica.

Dallo storage all'iperconvergenza

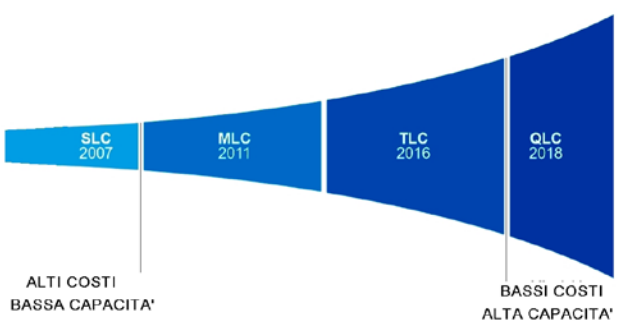
L'adozione di infrastrutture iperconvergenti (HCI) in Italia (e nel mondo) continua ad accelerare a mano a mano che aumenta l'esigenza da parte delle aziende di modernizzare e trasformare in chiave digitale i propri data center.
Il motivo, osserva la società di ricerche IDC, risiede nel fatto che per molte organizzazioni alla ricerca di agilità, facilità di gestione e razionalizzazione dei costi, l'infrastruttura iperconvergente rappresenta oggi la migliore soluzione possibile, come peraltro evidenziano recenti sondaggi condotti dalla società.
Significativo è che il 70% delle imprese italiane vedano nei sistemi iperconvergenti uno dei principali abilitatori della modernizzazione delle infrastrutture IT, con particolare riferimento agli ambienti legacy.
In sé non è del tutto una novità. HCI ha cominciato a diventare popolare una decina di anni fa, ma solo con la recente maturazione della tecnologia ha iniziato a divenire una sorta di standard de facto se non de jure per il consolidamento di data center, la gestione di applicazioni business-critical e l'implementazione di cloud ibridi.
Molte aziende stanno poi implementando HCI

sia per carichi di lavoro tradizionali sia per moderni workload con ordini di grandezza tipici del mondo web.
IDC ritiene in proposito che l'adozione di HCI sia necessaria per poter compiere quel salto generazionale verso architetture software-defined e API-driven in grado di portare vera automazione e intelligenza infrastrutturale nelle aziende, indispensabile o quasi per competere a livello applicativo e quindi di processi e servizi nell'economia digitale.
Sull'onda dell'adozione in aumento, IDC ha stimato il mercato complessivo HCI sviluppatosi nel 2019 essere stato pari a 12 miliardi di dollari. Ma il futuro prossimo appare estremamente promettente.
Le previsioni vedono la spesa HCI crescere con un CAGR annuo superiore al +20% da qui al 2023, con un mercato che proprio nel 2023 arriverà a valere 16,8 miliardi di dollari.

L'impatto crescente della tecnologia Flash

Una forte evoluzione lo sta avendo nello storage, on premise o nel cloud, anche la tecnologia flash. Se se ne analizza l'evoluzione a partire dalla sua introduzione sul mercato, la tecnologia flash è stata sostanzialmente re

Evoluzione della tecnologia SSD



in una prima fase relegata ad applicazioni di Tier1 incentrate sulle prestazioni.
Un passo avanti lo si sta però facendo grazie a nuove tecnologie allo stato solido come quella costituita dalla Storage Class Memory (SCM, riferita anche come Persistent Memory) e QLC (quad-level cells, e cioè celle che possono memorizzare 4 bit pere cella), che permettono di aggiungere nuovi livelli nel settore delle memorie e lasciano presagire come la tecnologia flash sia destinata ad essere impiegata per tipologie di dati del tutto nuove.
Ad esempio, in ambito high-end, con la combinazione di SCM e protocolli ad alta velocità come NVMe-oF (acronimo di NVMe over Fabrics, un'estensione del protocollo di rete NVMe a Ethernet e Fibre Channel che accelera la connettività tra storage e server), gli array a storage condiviso possono garantire alle applicazioni maggiormente sensibili alla latenza, nota Pure, prestazioni simili a quelle dello storage basato su server.
Va osservato che NVMe, acronimo di Non-Volatile Memory Express, è una interfaccia di comunicazione introdotta nel 2013 da un consorzio di aziende leader nel settore dei dischi SSD.
L'introduzione sul mercato delle memorie QLC sta estendendo la tecnologia flash ai tier storage finora principalmente rimasti su disco magnetico. In sostanza, la riduzione dei costi permette a tutte le applicazioni di sfruttare i vantaggi del flash al di là delle prestazioni: semplicità, affidabilità e minor consumo di spazio ed energia nei data center.

Storage e container

I container sono nati con l'obiettivo di rendere il più semplice e leggero possibile il deployment di applicazioni stateless.

Va osservato che il termine Stateless fa riferimento ad una comunicazione client–server tale per cui nessun contesto client è memorizzato sul server e ogni richiesta da ogni client contiene tutte le informazioni necessarie per richiedere il servizio e lo stato della sessione è contenuto sul client, stato che può anche essere trasferito al server attraverso un altro servizio posto a persistere, ad esempio un database.
Tuttavia, poiché la diffusione di Kubernetes e il supporto dei container da parte di VMware sta rapidamente ampliando l'impiego dei container verso applicazioni mainstream, la disponibilità di storage persistente si prospetta sempre più essenziale al fine di movimentare database e applicazioni sui container.
Il 2020 sembra da questo punto di vista costituire l'anno in cui un'ampia percentuale di aziende farà evolvere le proprie piattaforme cloud ibride e private al di là delle VM implementando una strategia container universale comprendente la realizzazione di basi di storage che rendano possibile l'adozione dei container da parte delle applicazioni stateful mission-critical.

I dati della diffusione dell'Iperconvergenza

I dati di mercato confermano il crescente interesse per infrastrutture iperconvergenti. L'adozione di infrastrutture di questo tipo in Italia e nel mondo continua ad accelerare a mano a mano che aumenta l'esigenza da parte delle aziende di modernizzare e trasformare in chiave digitale i propri data center.
Il motivo, osserva la società di ricerche IDC, risiede nel fatto che per molte organizzazioni alla ricerca di agilità, facilità di gestione e razionalizzazione dei costi, l'infrastruttura iperconvergente rappresenta oggi la migliore soluzione possibile, come peraltro evidenziano i più recenti sondaggi condotti dalla società.
Ciò rispecchia anche la situazione nazionale, con il 70% delle imprese italiane che vedono nei sistemi iperconvergenti uno dei principali abilitatori della modernizzazione delle infrastrutture IT, con particolare riferimento agli ambienti legacy.
In sé non è del tutto una novità. HCI ha cominciato a diventare popolare una decina di anni fa, ma solo con la recente maturazione della tecnologia ha iniziato a divenire una sorta di standard de facto se non de jure per il consolidamento di data center, la gestione di applicazioni business-critical e l'implementazione di cloud ibridi.
Mole aziende stanno poi implementando HCI sia per carichi di lavoro tradizionali sia per moderni workload con ordini di grandezza tipici del mondo web.
IDC ritiene in proposito che l'adozione di HCI sia necessaria per poter compiere quel salto generazionale verso architetture software-defined e API-driven in grado di portare vera automazione e intelligenza infrastrutturale nelle aziende, indispensabile o quasi per competere a livello applicativo e quindi di processi e servizi nell'economia digitale.
Sull'onda dell'adozione in aumento, IDC ha stimato il mercato complessivo HCI pari a 12 miliardi di dollari nel 2019.
Le previsioni vedono la spesa HCI crescere con un CAGR annuo superiore al +20% da qui al 2023, con un mercato che proprio nel 2023 arriverà a valere 16,8 miliardi di dollari.

La nuova infrastruttura in OMG garantisce failover e velocità

Una nuova infrastruttura server dedicata ha consentito a OMG di operare con un'elevata affidabilità dei sistemi e agevolare la produttività

OMG è un'azienda italiana che opera da 50 anni su tre linee di business: produzione di carrelli elevatori elettrici standard e custom per la movimentazione di qualsiasi tipo di merce, commercializzazione e manutenzione di chiusure industriali e servizio di verniciatura e sabbiatura industriale.
Le tre aree operative convivono all'interno dell'azienda operando sia all'estero, sia in Italia, dove è presente con quattro stabilimenti.
Nel 2018, dopo aver subito alcuni incidenti informatici a causa di virus che hanno danneggiato i sistemi e le applicazioni aziendali, ha deciso di rivedere l'intera infrastruttura IT, valutando con particolare attenzione le nuove metodologie di virtualizzazione previste per i server.
L'esigenza principale era quella di gestire l'attività di assessment per poter verificare quali fossero le tecnologie di failover che consentissero la massima protezione e sicurezza sia per il backup sia per l'eventuale restore, la scalabilità ottimale per aggiungere o togliere risorse a un server in base al fabbisogno, e il miglior risparmio economico raggiungibile.
Tramite la consulenza di Centro Computer si è arrivati alla definizione della nuova soluzione che è stata implementata nei primi mesi del 2019 ed è basata su server di ultima generazione di server in termini di sicurezza, espandibilità e prestazioni, virtualizzazione, sistema di backup di Veeam con repository NAS e supporto esterno RDX per duplice copia; dispositivi storage e firewall ad alta affidabilità per tutte le sedi.
Sono stati inoltre forniti servizi sistemistici per la migrazione dei sistemi e la definizione della nuova piattaforma informatica per assicurare la connettività VPN tra la sede centrale e le filiali.
«La richiesta principale era quella di ottimizzare i costi dei nostri server, guadagnando sensibilmente in termini di alta affidabilità e sicurezza grazie all'ausilio delle tecnologie di virtualizzazione e siamo più che soddisfatti della stabilità ottenuta dai nostri sistemi che oggi sono più performanti e assicurano una buona velocità delle applicazioni, poiché abbiamo ridotto del 25-30% la latenza di banda», ha commentato i risultati ottenuti **Enzo Falco**, IT Manager di OMG.

Più sicuri gli utenti privilegiati e nel cloud con la biometria

Zero Trust, biometria e provisioning just-in-time si combinano in Alero di CyberArk per permettere ai fornitori di servizi di accedere solo alle applicazioni abilitate

La proiezione di un'azienda verso l'esterno, il dissolversi dei confini di sicurezza tradizionali, la mobilità, il cloud e il multi-cloud sono paradigmi che allo stesso tempo offrono la possibilità di sviluppo aziendale e criticità per chi deve garantire che il tutto debba svolgersi in modo controllato e sicuro.

I benefici derivanti dall'esternalizzare della gestione di un IT sempre più complesso sono di certo molti, soprattutto perché diventa possibile concentrarsi sul proprio core business, ma questo ha come implicazione che le organizzazioni aziendali per gestire sistemi anche critici si debbano affidare a fornitori a loro remoti in base a specifici contratti.

Il dissolversi del perimetro aziendale richiede però che i fornitori remoti di un servizio di gestione dispongano di un accesso ai sistemi di cui necessitano per svolgere il compito loro assegnato e contrattualizzato, sistemi ai quali deve essere permesso di accedere solo quando ne hanno un effettivo bisogno.

Per mitigare i rischi le organizzazioni tengono in genere traccia di chi accede a sistemi aziendali ricorrendo ad un primo livello di autenticazione in cui gli utenti in qualche modo sono tenuti a dimostrare di essere realmente chi o cosa affermano di essere.

Solo al termine della fase di identificazione e autenticazione del fornitore remoto del servizio il processo di abilitare o disabilitare l'accesso ha inizio.

Il problema, osserva però **Andrew Silberman**, senior product marketing manager di CyberArk, risiede nel fatto che l'affidarsi a processi manuali per eseguire abilitazione o disabilitazione dell'accesso nei confronti dei fornitori remoti del servizio contrattualizzato è lungi dall'essere infallibile e introduce molti potenziali problemi.

Questo perché quello siglato con fornitori remoti è un contratto limitato nel tempo e gli stessi non sono in genere parte di Active Directory o servizi di directory equivalenti.

Non ultimo, hanno la necessità di accedere non all'intero panorama dei sistemi IT ma solo ad un loro sottoinsieme e in base al tipo di contratto, alle operazioni da effettuare o alle sessioni richieste al fine di espletare il compito loro assegnato.

I team IT, osserva Silberman, hanno quindi bisogno di un modo per garantire automaticamente che questi dispositivi siano sicuri anche quando

ai sistemi critici accedono da remoto.

I benefici di un approccio Zero Trust e a più fattori

La risposta alle esigenze evidenziate la si trova in quello riferito come "Zero Trust", e cioè un modello di sicurezza basato su un rigido processo di verifica delle identità che prevede che solo gli utenti e i dispositivi autenticati e autorizzati possano accedere a dati e applicazioni.

Zero Trust, in sostanza, focalizza le politiche di sicurezza e i controlli di accesso sull'identità dell'utente e del dispositivo anziché sulla posizione dell'utente o del dispositivo. Ne deriva una forte influenza su quello che costituisce un modello ideale di autenticazione.

Il verificare una identità attraverso l'autenticazione è un processo che può tuttavia assumere molte forme. Esempi classici sono il digitare una combinazione di nome utente e password o metodi più attuali quali i sistemi di riconoscimento biometrico o l'utilizzo di un dispositivo trusted e noto.

Ad alto livello, l'autenticazione in genere assume tuttavia tre possibili forme e si esprime in:

- Qualcosa che sai (e.g. una parola segreta o una combinazione di nome utente e password).
- Qualcosa che hai (e.g. lo smartphone personale o un badge con il nome).
- Qualcosa che sei (e.g. l'impronta digitale o la scansione della retina).

Un approccio generalmente raccomandato, evidenzia Silberman, soprattutto quando si tratta di accedere a risorse critiche, è istituire un ulteriore livello di sicurezza con autenticazione a più fattori, che richiede agli utenti di utilizzare contemporaneamente più di un metodo per dimostrare la propria identità.

Ciò può includere qualcosa che conoscono, come la risposta a una domanda su qualcosa che hanno, ad esempio a un messaggio di testo inviato al telefono cellulare.

Zero Trust e Biometria per una sicurezza ad alto livello

Il problema è che "Qualcosa che sai" e "Qualcosa che hai" sono entrambi metodi che presentano punti ciechi. Il primo espone al fatto che i cyber criminali hanno una esperienza trentennale di cracking di password, il secondo che "Quello che hai" può essere rubato o intercettato.

La criticità insita nei primi due approcci enfatizza la valenza del terzo perché una impronta digitale costituisce un modello unico. L'uso di una retina o delle impronte digitali può perciò bloccare le vie di attacco e migliorare notevolmente la sicurezza. Inoltre, una autenticazione biometrica non può essere rubata, persa o decifrata.

In sostanza, combinando l'autenticazione biometrica con una soluzione di back-end avanzata si dà alle organizzazioni aziendali la possibilità di concedere ai fornitori remoti di servizi esclusivamente l'accesso a quello che loro necessita e di effettuare automaticamente il processo di provisioning e di deprovisioning.

«Questo, è ciò che fa CyberArk Alero, una nuova soluzione di CyberArk fruibile in modalità SaaS. Alero combina l'accesso Zero Trust, l'autenticazione biometrica e il provisioning just-in-time in modo da garantire che i fornitori remoti possano accedere esclusivamente e in modo sicuro ai sistemi loro necessari. E' una soluzione che non richiede la realizzazione di VPN, l'installazione di agenti o password e permette di creare un'esperienza senza soluzione di continuità e sicura per amministratori IT, team operativi e utenti di fornitori remoti», ha evidenziato Silberman.

Un data base nel cloud assicura la protezione degli degli end-point

La soluzione di Endpoint Detection and Response di F-Secure migliora la protezione di utenti e dispositivi con algoritmi di analisi avanzata e il machine learning

Le nuove modalità di lavoro basate su una crescente mobilità, sull'home working o sul co-housing, il ricorso al cloud e al multi cloud hanno accresciuto gli aspetti a cui si deve porre attenzione al fine di garantire la sicurezza di dati e applicazioni. Tra questi, ad esempio, utenti, dispositivi, applicazioni, avvisi, vulnerabilità, patch e non solo.

È un compito oneroso per l'IT, soprattutto nelle aziende più piccole che non hanno la possibilità di tenere sotto controllo le reti IT nell'arco delle 24 ore. Il risultato è che dati riferiti al 2018 evidenziano che circa il 58% delle PMI ha subito una violazione, non poche delle quali hanno portato alla chiusura dell'azienda.

Carmen Palumbo, Country Sales Manager F-Secure Italia

La domanda che ci si pone è: cosa può fare un manager IT che disponga di risorse limitate?

La risposta può consistere nel ricorso alla tecnologia EDR (acronimo di Endpoint Detection and Response). In essenza, si tratta di soluzioni studiate per incrementare la protezione degli endpoint facendo ricorso a funzionalità di rilevamento e risposta altamente efficaci.

Come funziona una soluzione EDR e con quali benefici

Una volta in funzione una soluzione EDR raccoglie un numero enorme di eventi comportamentali relativi ai dati (come esecuzioni di processi, connessioni di rete e operazioni sui file) dalle workstation e dai server dell'organizzazione attraverso sensori endpoint non invasivi.

Questi dati sono estremamente utili per il rilevamento degli attacchi ma, se sono troppi, sono impossibili da gestire per gli analisti.

Utilizzando strumenti di analisi avanzata e con il supporto del machine learning, l'EDR è invece in grado di analizzare questi dati e intercettare gli indicatori di attacco cui corrispondono minacce sia note che nuove. Esempi di cosa una soluzione EDR può fare sono:

- Identificare processi insoliti avviati dalle workstation aziendali.
- Individuare i dipendenti che utilizzano applicazioni sconosciute o dannose.
- Isolare dalla rete i computer e i server compromessi per evitare che un cyber attacco si diffonda.
- Rilevare nuovi tipi di malware nell'ambiente, anche senza firme esistenti.
- Rilevare attacchi malware fileless distribuiti da siti web che contengono codice malevolo, documenti PDF caricati sui browser o macro

incorporate in file di MS Office.
In sostanza, invece di segnalare una miriade di falsi positivi in cui è difficile districarsi, l'EDR è in grado di evidenziare solo i risultati rilevanti. Una volta identificate le minacce, l'EDR supporta poi nell'eseguire ulteriori indagini e rispondere con azioni automatizzate e raccomandazioni.
Questo è un aspetto chiave soprattutto per le PMI che non dispongano delle risorse e delle competenze necessarie per gestire autonomamente i cyber incidenti di un certo rilievo.
«Con una soluzione EDR come F-Secure Rapid Detection & Response, non solo si può scoprire se ci sono problemi sulla rete IT, ma ottenere anche un aiuto concreto per risolverli», osserva **Carmen Palumbo**, Country Sales Manager di F-Secure Italia, azienda specializzata nella sicurezza degli end-point.

La soluzione EDR di F-Secure e come funziona

Come evidenziato, il funzionamento della soluzione EDR di F-Secure si basa su sensori invisibili agli utenti installati nei computer Windows, Mac e nei server in modo da monitorare il comportamento degli utenti. Gli eventi/dati raccolti vengono inviati ad un database in cloud per l'analisi in tempo reale. Il software in cloud esamina i dati raccolti e distingue gli eventi sospetti dalle normali attività degli utenti. Questo avviene con l'analisi comportamentale, reputazionale e dei Big Data, in associazione al machine learning.
A questo punto sulla dashboard di gestione viene visualizzato un elenco filtrato di avvisi e informazioni sugli attacchi. Gli avvisi sono contestualizzati e tengono conto dell'importanza degli host coinvolti, del panorama delle minacce e dei livelli di rischio attuali.
Due le strade che a questo punto si presentano per rispondere a un attacco:
a) Esaminare il problema e rispondere mediante il team IT aziendale, utilizzando le azioni di risposta automatizzate e le indicazioni fornite dalla soluzione.
b) Inoltrare il problema agli esperti di F-Secure in materia di risposta agli incidenti ricorrendo alla funzionalità integrata "Segnalare a F-Secure". Gli esperti eseguiranno un'indagine approfondita sulla minaccia e consiglieranno le misure appropriate per correggerla.

I benefici dell'EDR per manager e azienda

L'EDR è un approccio alla sicurezza che ne migliora la postura e permette di disporre e fornire risposte precise e rapide sul suo stato generale.
Sempre più spesso ai manager IT viene chiesto di segnalarne lo stato ai vertici aziendali e di farlo con il supporto dei dati provenienti dalle piattaforme di gestione delle vulnerabilità e di protezione degli endpoint. Compreso in questo quali tipi di attacchi sono stati riscontrati nei sistemi, se i dipendenti stanno seguendo le linee guida per la sicurezza IT, eccetera.
Nel caso di problemi complessi è possibile ricorrere al supporto di esperti. «Con la funzionalità 'Segnalare a F-Secure', i rilevamenti di minacce più gravi o complesse possono essere inoltrati direttamente agli esperti del nostro centro specializzato nella risposta agli incidenti, le stesse persone che gestiscono quotidianamente la cyber security dei clienti Enterprise - evidenzia Palumbo -. Ma non solo. L'EDR aiuta anche a rispettare il GDPR e a dimostrare alle autorità di avere adottato le misure basilari per proteggere l'ambiente IT. E qualora un attacco riuscisse a penetrare le difese, di raccogliere informazioni per segnalarlo alle autorità entro la scadenza delle 72 ore».

Nuove tecnologie proteggono i dati in modo più efficiente

Far fronte all'esigenza di tracciare i dati e proteggerli è più facile con i nuovi strumenti basati sul machine learning e l'artificial intelligence

La trasformazione digitale in atto obbliga le aziende ad affrontare sfide sempre più impegnative. Le esigenze sono diverse a seconda del core business e del settore di attività ma il denominatore comune è sostanzialmente il medesimo, e cioè sfruttare in maniera strategica le tecnologie presenti sul mercato in modo da trarne un beneficio competitivo e di business.

A 2020 avviato un aiuto nel vedere quali sono le tecnologie che possono dar euna mano epr perseguire questo non facile obiettivo è stato offerto nel corso del Gartner IT Symposium/Xpo di Barcellona, dove sono stati esaminati i "Top 10 Strategic Technology Trends 2020": dall'AI Security al Distributed Cloud, dall'Empowered Edge alla Transparency e Traceability sono molte le tecnologie emergenti a possedere un elevato potenziale strategico e in grado di modificare per sempre il modo di fare business. Una tendenza emerge però precisa, la centralità dei dati «Buona parte dei tech trend individuati da Gartner per il 2020 è strettamente legata alla gestione dei dati. Diventa, quindi, fondamentale affidarsi a soluzioni storage innovative che integrano al loro interno AI e Machine Learning per ottenere elevate prestazioni, affidabilità e scalabilità a costi contenuti con una gestione semplificata e la possibilità di prevedere eventuali malfunzionamenti» osserva in proposito **Donato Ceccomancini**, Country Manager Italia di Infinidat.

Nella sua top ten, Gartner fa riferimento anche all'inizio di una nuova era per il cloud prevedendo un significativo slittamento dal cloud pubblico centralizzato verso un modello distribuito su diversi servizi cloud.

Le previsioni Gartner non sorprendono, osserva inoltre Ceccomancini, perché sono già alcuni anni che, in particolare all'estero, le aziende stanno utilizzando modelli di servizi cloud distribuiti e quello che si sta diffondendo è in sostanza lo spostamento verso uno storage sia in cloud che "on-premise" di tipo software-defined atto ad assicurare una mobilità ottimizzata dei dati nell'ambito del data center e del cloud pubblico.

Il Next-Generation Security Operations Center di Lutech

Lutech rafforza il supporto della digital transformation con il completamento di acquisizioni e l'ampliamento della propria offerta di servizi di cybersecurity

Tullio Pirovano - AD di Lutech

Le aziende si trovano a fronteggiare i problemi posti, nel corso della trasformazione digitale, dal come garantirsi la sicurezza in ambienti multi cloud, nella mobility per quanto concerne gli end point o in applicazioni IIoT, solo per citarne alcuni. La scarsità di esperti e la necessità in un mondo estremamente competitivo di concentrarsi sul proprio core business richiede un ripensamento delle strategie aziendali in termini di investimento. E' una sfida complessa e per aiutare ad affrontarla il Gruppo Lutech ha orchestrato un approccio alle sfide che nel 2020 le aziende dovranno fronteggiare operando su due piani, quello delle risorse umane e del know how, e quello tecnologico.

Una risposta efficace alle sfide della Cyber Security

Sul piano tecnologico la risposta alle esigenze delle aziende per una migliore cyber security si è concretizzata nell'inaugurazione, all'interno del Services Operations Center di Cinisello Balsamo (MI), di un proprio Next-Generation Security Operations Center NG SOC.

Il Services Operations Center di Cinisello, ha evidenziato la società, è da più di 20 anni specializzato nell'erogazione di Servizi Gestiti.

E' su questa base che diventa ora anche un hub di riferimento per la strategia di crescita a supporto della sicurezza aziendale del Gruppo Lutech nell'ambito dei Managed Services.

I numeri che lo caratterizzano da soli evidenziano l'ampiezza del progetto e il ruolo che Lutech ricoprirà per quanto concerne la sicurezza aziendale e dei suoi dati e dispositivi..

Il SOC si sviluppa su 3mila metri quadri di superficie e dispone di 330 postazioni operative attive h24, è dotato di impianti tecnologici ridondati ed è affiancato da due siti secondari situati l'uno a Padova e l'altro a Torino in modo da garantire la continuità del servizio erogato anche in condizioni di disastro.

Il modello di erogazione di tutte le soluzioni è OASI (Outsourcing Advanced Services Integration), in base al quale i servizi vengono gestiti secondo l'approccio Qualitative Full Outsourcing in grado di risolvere tutta la filiera operativa a supporto del cliente.

A livello tecnico, il centro nel suo complesso annovera un team di ingegneri e tecnici certificati in grado di supportare un portfolio di servizi a 360° che comprende Service Desk, Network Operations Center, Cloud Operations Center e Next-Generation Security Operations Center.

Obiettivo Cybersecurity

Obiettivo del nuovo NG SOC è quello di rispondere alla crescente domanda di soluzioni e servizi di sicurezza predittivi e dinamici richiesti dalle aziende indipendentemente dalla dimensione e dal settore e assicurare la gestione della governance e dell'operatività legate alla sicurezza.

«La sicurezza informatica oggi non può più essere solo un elemento per la mitigazione del rischio, ma deve far parte della strategia di crescita delle aziende. È a tutti gli effetti un vantaggio competitivo e garantisce la corretta gestione e protezione dei dati aziendali e la piena aderenza alle norme di compliance» ha dichiarato **Tullio Pirovano**, Amministratore Delegato di Lutech.

Nello specifico, il team del NG SOC comprende esperti di sicurezza ed ethical hacker in grado di progettare servizi dedicati o condivisi, multilivello (L1-L3), in modo da assicurare una business continuity di elevata efficienza, abbinata all'ottimizzazione dei costi e al perseguimento di un TCO ottimizzato.

Un altro elemento chiave del SOC è il fatto di essere dinamico, vendor independent e di aderire al modello CARTA (Continuous Adaptive Risk and Trust Assessment).

In sostanza, i servizi fruibili dal cliente sono modulabili e scalabili in funzione delle specificità dei diversi settori e dei profili di rischio che li caratterizzano. «Il modello scalabile di erogazione dei servizi offerti dal NG SOC offre grande flessibilità e la sicurezza di fruire di servizi dimensionati in base alle esigenze dei nostri clienti, che del nostro NG SOC apprezzano prima di tutto i quindici anni di esperienza. Con il tempo e grazie agli investimenti che il Gruppo Lutech ha fatto, abbiamo costruito un mix di processi, procedure e competenze che ci contraddistinguono, soprattutto per la capacità di gestire volumi elevati con qualità ed efficienza» ha commentato Pirovano.

A sua volta il servizio di Data Center al cui interno si sviluppa il servizio NG SOC, è compreso in un ampio portfolio di servizi e soluzioni ICT erogati tramite oltre 2.700 professionisti. Le competenze specifiche rispondono alle esigenze delle aziende di progettare, realizzare, manutenere e porre in sicurezza e gestire soluzioni di Hybrid Cloud Technology, individuando le architetture innovative, scalabili e flessibili, atte a garantire la continuità operativa.

Competenze rafforzate dalle acquisizioni

Come evidenziato, al rafforzamento del portfolio servizi e tecnologico, si è abbinato quello del patrimonio delle conoscenze.

In particolare, con la recente conclusione del processo di fusione per incorporazione di Sinergy Spa e di NEST2, il Gruppo Lutech si presenta ora sul mercato con una struttura solida e consolidata e un'offerta ICT molto ampia con cui ha inteso rispondere alle esigenze del mercato delle aziende italiane ed europee.

L'operazione è un preciso segnale evolutivo nella direzione di consolidamento del Gruppo e va inquadrato nella sua strategia di sviluppo indirizzata a posizionare il Gruppo Lutech tra le prime aziende ICT italiane e a consolidarne la posizione come player europeo.

Alla data è presente in 9 Paesi nel mondo, conta sulla citata struttura di 2700 professionisti e su insieme di oltre 90 partner che servono circa 1500 aziende clienti.

Ampia anche la tipologia di mercati verticali supportati. In termini di quote di fatturato pari a 435 milioni di euro (Pro forma 2018 incluse attività di M&A al 31/12/19), allo stesso contribuiscono con percentuali diverse il Manufacturing (23%), il Financial Services (22%), il Public Sector & Healthcare (20%), i Telco e Media (18%), il Fashion & Retail (10%) ed Energy & Utilities (7%).

Cloud Azure e Web sicuri con la gestione del servizio

I Servizi di Sicurezza gestita di Radware proteggono le applicazioni nel cloud Azure e bloccano gli attacchi BOTnet che ne inibiscono il funzionamento

Nicola Cavallina - Channel&Alliance Manager per l'Italia di Radware

Per la propria digital transformation le aziende fanno sempre più ricorso alla esternalizzazione dei servizi IT. In questo processo di trasformazione l'esigenza primaria è quella di servizi completamente gestiti, soprattutto per quanto concerne la componente sicurezza, incluso in questo le Web Application Firewall (WAF) e cioè quelle applicazioni che filtrano, monitorano e se previsto dalle policy bloccano il traffico HTTP da e verso un'applicazione Web.

Il crescente interesse per applicazioni WAF deriva dal fatto rilevante che Ispezionando il traffico HTTP è possibile prevenire gli attacchi dovuti a falle nella sicurezza delle applicazioni Web,

L'interesse nel passaggio a servizi in cloud e ancor più nel multi cloud non è però dovuto solamente al desiderio di ottimizzare Capex e Opex ma anche dalla pressione esercitata sui team dediti alla security a causa della velocità con cui si sviluppano nuove applicazioni o si modificano quelle esistenti. Sono tutti eventi che richiedono un assessment continuo e frequente delle policy per la sicurezza e un livello di conoscenza molto elevato che è sempre meno disponibile nell'ambito aziendale, soprattutto nelle PMI.

Nello scenario che ne deriva, la esternalizzazione non si traduce quindi unicamente nel fruire di un servizio di security erogato da un provider, ma anche nella richiesta di quei servizi professionali necessari per configurare e gestire le policy inerenti le applicazioni WAF.

Il servizio Cloud WAF per la sicurezza su Azure

Una risposta alle esigenze connesse alla gestione e alla manutenzione di soluzioni di sicurezza è quella data da Radware (radware.com), che sviluppa e tramite i suoi distributori di canale propone soluzioni che sono completamente gestite da esperti Radware. In particolare, il "Cloud WAF Service" è un servizio h24 completamente gestito da un team di "Emergency Response" di cui fanno parte esperti che si fanno carico di configurare e aggiornare le policy di sicurezza e allo stesso tempo monitorare, individuare, allertare e mitigare in tempo reale gli attacchi apportati a una azienda.

Come tipologia è un servizio di "Security as a Service (SaaS)" di classe Enterprise volto a proteggere le applicazioni nel Cloud Azure di Microsoft, un ambiente cloud in cui opera in modo nativo.

Operativamente, il servizio fa ricorso a tecnologie di nuova generazione per creare e distribuire le firme aggiornate automaticamente che pro-

teggono e bloccano i vari tipi di attacchi, compresi quello molto pericolosi di tipo zero-day.
«Azure Cloud WAF fa ricorso a tecnologie di machine learning per rilevare e bloccare automaticamente i diversi tipi di attacco che possono essere portati su Web. Inoltre, man mano che le applicazioni mutano, provvede ad aggiornare automaticamente le policy in modo da permetterne rapidamente il passaggio in produzione» evidenzia **Nicola Cavallina**, Channel&Alliance Manager per l'Italia di Radware.

Roberto Branz - Division Director Security & Cloud di Arrow ECS

Il servizio, che tramite Azure e Azure Networks opera con una bassissima latenza, fornisce in sostanza una approfondita e esaustiva sicurezza su Azure, accompagnata dal monitoraggio in real-time e dalla fornitura di dati statistici, oltre che alert e un reporting dettagliato degli attacchi bloccati.

Applicazioni sempre disponibili con il servizio di BOT management

Tramite computer infettati con virus possono essere avviati seri attacchi a siti web, noti come Distributed Denial of Service (DDoS). Vengono portati simulando e subissandoli di richieste lecite che ne rallentano anche di molto i tempi di risposta. L'insieme collettivo dei dispositivi in rete coinvolti è riferito come Botnet, acronimo dove BOT è l'abbreviazione di roBOT, riferendosi alla possibilità che ha una macchina intelligente di agire autonomamente.
«Non tutto il traffico Bot è malevolo - osserva Cavallina -, ma lo è circa il 26%, in pratica un quarto del traffico Internet. E in 4 casi su 5 il fornitore dei servizi non è in grado di distinguere il traffico malevolo da quello legittimo».
Una protezione da questo tipo di attacco è fornita da Radware BOT Manager, una soluzione che persegue quattro obiettivi fondamentali nella protezione delle applicazioni e dei siti Web: la protezione da attacchi provenienti dai diversi canali esistenti; blocco proattivo e automatizzato degli attacchi tramite modelli di analisi e apprendimento in profondità del loro comportamento; l'allestimento di un ampio Database delle impronte di Bot mediante attività di intelligence realizzate con i dati raccolti da migliaia di sorgenti; opzioni di installazione delle difese di tipo non intrusivo attuate mediante API che non hanno impatto sullo stack di tecnologie già installate.
«BOT Manager è stato progettato - evidenzia **Roberto Branz**, Division Director Security & Cloud di Arrow ECS (arrow.com/ecs/it/), società che distribuisce e supporta le soluzioni Radware - anche per operare congiuntamente con l'intero portfolio di soluzioni Radware per la sicurezza, e in primis i servizi Cloud, tramite la sua integrazione con Cloud WAF. A questa interoperabilità si aggiunge quella con le soluzioni per mitigare gli attacchi tramite la condivisione e la sincronizzazione delle attività di intelligence».
Per le aziende che non dispongono di personale specializzato o che sono orientate ad esternalizzare il servizio di security è disponibile anche il servizio gestito di Cloud Security, un servizio di classe Enterprise che mira a proteggere da attacchi multi vettore ed a ottimizzare le prestazioni delle applicazioni.
Alla soluzione di affianca anche quella di Bot Analyzer, un servizio di valutazione gratuita per ambienti business che possono essere soggetti ad attacchi Bot e per quegli utilizzatori che desiderano disporre di una miglior comprensione dell'impatto che Bot di tipo malevolo possono avere sulla loro organizzazione.

Ricoh tra i leader nei Managed Print Services

Per l'ottavo anno consecutivo Ricoh ottiene lo status di leader nella stampa gestita per la capacità di rispondere alle esigenze dei moderni ambienti di lavoro

L'edizione 2019 del report Managed Print Services (MPS) Landscape di Quocirca ha confermato Ricoh come leader nel settore dei servizi di stampa gestiti per l'ottavo anno consecutivo.
«Ricoh mantiene la posizione di leadership nel settore MPS anche grazie alla sua strategia multicanale e alla sua copertura internazionale. L'azienda ha sviluppato un'offerta di tecnologie e di servizi che va oltre gli MPS tradizionali, rispondendo così alle nuove esigenze delle imprese. Grazie alla presenza globale e ai servizi erogati in maniera diretta, Ricoh è in grado di supportare le organizzazioni di grandi dimensioni che operano in più Paesi» evidenzia il rapporto.
Va osservato che i MPS fanno parte dell'offerta Ricoh Managed Document Services (MDS). E' un ambito in cui Ricoh lavora insieme ai propri clienti al fine di ottimizzare i processi in modo da riuscire a rendere la gestione delle informazioni più efficiente anche dal punto di vista della sicurezza.
"Ricoh offre un ampio portfolio di soluzioni rivolte sia al mercato Office che a quello della stampa professionale. Tra le caratteristiche che abbiamo in particolar modo apprezzato, vi sono la capacità di includere nella fase iniziale di consulenza anche tecnologie di terze parti, di analizzarle in relazione alla sostenibilità e di erogare servizi di supporto in ambienti multi-vendor. Questi aspetti rendono Ricoh la scelta ideale per le organizzazioni alla ricerca di un unico fornitore in ambito documentale e IT. Ricoh supporta le aziende nella trasformazione digitale mediante soluzioni e servizi che includono ambiti fondamentali come ad esempio cloud, sicurezza e analytics", ha commentato Louella Fernandes, Research Director di Quocirca, il posizionamento attribuito a Ricoh.
Ricoh, ha poi evidenziato Quocirca, fornisce servizi standardizzati a livello globale, ma allo stesso tempo mantiene un approccio flessibile per personalizzare l'offerta in base alle caratteristiche dei mercati locali.
«Siamo orgogliosi di essere stati nominati da Quocirca leader negli MPS per l'ottavo anno consecutivo. Questo dimostra la nostra attenzione verso i clienti. Le soluzioni affidabili, sicure e personalizzabili di Ricoh rappresentano la base per la Digital Transformation. Vogliamo aiutare le aziende ad entrare nell'era digitale per riuscire a cogliere nuove opportunità», ha dichiarato **David Mills**, CEO di Ricoh Europe.

Più sicurezza con Stormshield per le infrastrutture critiche

Stormshield ha rafforzato l'impegno per diventare il riferimento per la sicurezza informatica nelle infrastrutture critiche, dati sensibili e ambienti industrial

Pierre-Yves Hentzen - CEO di Stormshield

Il nuovo orientamento del produttore di soluzioni per la cyber security è il risultato di una riflessione strategica globale dettata da un mercato in rapida trasformazione, che si tratti dell'affermazione di nuove pratiche lavorative o di nuove questioni economiche e geopolitiche nel contesto della sovranità digitale.

In tali condizioni, proteggere le infrastrutture OT e IT critiche diventa una priorità al fine di tutelare la stabilità economica, sociale e ambientale.

Sono questi i moti alla base della decisione che ha portato Stormshield ad incrementare i propri investimenti a sostegno delle aziende e delle organizzazioni dotate di tali infrastrutture.

Pierre-Yves Hentzen, CEO di Stormshield, è in proposito dell'opinione che molte aziende, enti pubblici e fornitori di servizi essenziali stiano prendendo coscienza dell'importanza di mantenere il controllo sui propri dati sensibili e sulle loro infrastrutture critiche.

«IT e OT convergono in ambienti iperconnessi, dilatando la superficie di attacco. Di fronte a queste minacce e alle conseguenze drammatiche che esse comportano per la tutela di beni e persone, le aziende in questione - indipendentemente dalle loro dimensioni - dovranno adottare politiche di sicurezza che si adattino al grado di esposizione dei loro ambienti IT e OT. La nostra missione è sostenerle in questa sfida» ha commentato il manager.

Numerosi i punti di forza che la società può mettere in campo. Tra questi, la forte esperienza nel campo delle tecnologie OT, in portafoglio prodotti per la protezione di ambienti IT/OT, certificazioni dell'Unione Europea e della NATO, una presenza locale che le permette di fornire una consulenza personalizzata e un servizio reattivo.

«Questo progetto coinvolge tutte le nostre equipe e sarà il filo conduttore delle nostre attività nei prossimi anni. Vicinanza al cliente, tecnologie all'avanguardia e personale impegnato a consolidare il nostro nuovo posizionamento sono i pilastri alla base del successo delle nostre ambizioni», ha osservato **Matthieu Bonenfant**, Direttore Marketing di Stormshield.

La nuova strategia volta ad incrementarne lo status quale scelta europea in fatto di sicurezza informatica si basa peraltro su due anni, il 2018 e 2019, caratterizzati da una sua forte crescita dei fatturati, con un più che significativo +57% nel periodo.

Multi Cloud più sicuro e gestione automatica con i servizi SaaS

Il servizio Cloud One di Trend Micro automatizza e semplifica la cloud security delle applicazioni, di container e devops in ambienti ibridi e multicloud

Il progressivo rivolgersi al cloud per tutta una serie di esigenze aziendali che spaziano dalla Business Continuity al Data Recovery, dalle e-Mail all'ERP, dai DevOps allo sviluppo di Container applicativi, sta complicando enormemente il problema di come garantire la sicurezza di un insieme così variegato di applicazioni con esigenze, normative e enti di riferimento per la protezione dei dati e la loro riservatezza anche molto dissimili.

Emblematico è quanto inerente i processi DevOps o di containerizzazione delle applicazioni, processi che permettono da un lato di accelerarne lo sviluppo e il loro passaggio in produzione ma che dall'altro stanno imponendo una accelerazione di passo per quanto riguarda la capacità di adeguare altrettanto velocemente l'architettura di sicurezza e la protezione contro modalità e vettori di attacco che si rivelano sempre più sofisticati.

Salvatore Marcis - Technical Director per l'Italia di Trend Micro

«Il fattore velocità non è però l'unico con cui i manager aziendali e i responsabili della security si devono fronteggiare. Un problema parimenti importante e correlato al precedente è costituito dal come diminuire la complessità derivante dal dover gestire in modo integrato e semplice la sicurezza in complessi ambienti cloud e ancor più multi cloud. E' una sfida a cui abbiamo risposto con lo sviluppo del servizio Cloud One», evidenzia **Salvatore Marcis**, Technical Director per l'Italia di Trend Micro (trendmicro.com), società annoverata tra i principali attori mondiali per la cyber security.

Cloud One è una soluzione ideata per aiutare le aziende a soddisfare le priorità del cloud maggiormente strategiche e per farlo integra una ampia gamma di funzioni di sicurezza in una singola piattaforma. A livello operativo consente di migrare le applicazioni esistenti nel cloud, erogare nuove applicazioni cloud-native e portare ad un alto livello l'operatività nel cloud.

Sicurezza semplificata e automatica

Cloud One è un servizio di sicurezza che è stato sviluppato da Trend Micro per permettere di approcciare in modo olistico e chiaro quanto concerne la sicurezza di un complesso progetto Cloud e di definirne le caratteristiche operative.

Si compone di un insieme di servizi che supportano le principali piattaforme cloud esistenti incluse Amazon Web Services (AWS), Microsoft Azure e Google Cloud. Le diverse piattaforme possono essere integrate direttamente nei processi DevOps e relative "toolchain", e cioè l'elenco di passi che un team di sviluppo può seguire, dalla progettazione alla sua manutenzione, nel processo di rilascio di un nuovo software.
Numerose le esigenze a cui Trend Micro si è posta l'obiettivo di rispondere con lo sviluppo del servizio Cloud One.
Tra queste:

- La migrazione al Cloud e al Multi Cloud: il servizio Cloud One permette di automatizzare il processo di security e di protezione di ambienti cloud privati e pubblici. La protezione si estende sino a comprendere il livello di rete in modo da semplificare e rendere sicuro il processo di migrazione verso il cloud o di sua espansione in ambiti ancor più complessi.
- Rilasci DevOps: Cloud One abilita una protezione automatica per le applicazioni che può essere inserita direttamente nella pipeline CI/CD (Continuous Integration/Continuous Delivery), per assicurarne la protezione, identificare e risolvere più velocemente i problemi di sicurezza che dovessero insorgere e migliorarne le tempistiche connesse al loro rilascio da parte dei team DevOps.
- Containerizzazione: Nello sviluppo e nel ricorso a processi di containerizzazione, Cloud One permette di disporre di una sicurezza in cloud di tipo nativo e integrata con la pipeline CI/CD. La sicurezza nativa è ottimizzata al fine di abilitare la protezione e la scalabilità tra ambienti cloud diversificati. In particolare, permette ai team DevOps di prevenire che immagini che sono state identificate come potenzialmente rischiose per la sicurezza vengano passate in produzione. Il servizio permette altresì di individuare vulnerabilità, malware e dati sensibili quali chiavi e password all'interno delle immagini del container e risolvere le vulnerabilità prima che queste possano essere sfruttate da attaccanti in fase di esecuzione.
- Serverless: abilita la protezione di applicazioni serverless il cui sviluppo si basa su una combinazione di servizi di terze parti tipicamente ospitati in cloud. La protezione opera proattivamente nei confronti di possibili exploit che potrebbero danneggiare i sistemi, i dati e il business ad essi correlato. Il servizio è stato sviluppato in modo da avere un impatto minimo sulle prestazioni e sul codice della applicazione.
- Data Center: il servizio, una volta integrato con l'ambiente fisico e virtuale, abilita l'elevata efficienza operativa richiesta per supportare il funzionamento continuo e sicuro di un modern data center. Tra I compiti svolti da Cloud One è compreso, tramite un numero limitato di agenti, la rilevazione automatica e la distribuzione delle applicazioni di sicurezza. Il servizio permette anche di consolidare gli strumenti per la sicurezza in modo da rilevare, proteggere e rispondere alle vulnerabilità, al malware e alle modifiche non autorizzate del sistema più efficientemente.

«Cloud One sarà disponibile nel corso del Q1 2020 con tre servizi pienamente integrati: workload security, network security e application security. Le altre componenti saranno disponibili come soluzioni singole e verranno integrate con Cloud One entro la fine del 2020. Per fruirne, sfruttando le caratteristiche di AWS Marketplace come SaaS Contract API e le offerte dei partner, le aziende possono stipulare un contratto direttamente con Trend Micro o attraverso un partner», ha evidenziato Marcis.