

# Cloud e Managed Service

An abstract graphic at the bottom of the page features stylized clouds in shades of blue and white. Overlaid on these clouds is a complex network of grey lines and arrows, suggesting data flow and connectivity. The lines and arrows radiate from the bottom left towards the top right, creating a sense of movement and direction.

# OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID (in attesa di conferma).



# INDICE

## 4 La flessibilità del cloud

- 6 L'imprescindibilità del cloud per l'innovazione del business
- 8 Cloud, Hosting ed esternalizzazione dell'IT per far crescere il business
- 10 L'ERP si allarga as a service
- 11 Automium, un servizio SaaS che abilita la cloud transformation
- 12 I servizi che piacciono alle aziende
- 13 La videosorveglianza professionale di aziende e uffici viaggia sul cloud
- 14 Cloud e DevOps semplificano lo sviluppo delle applicazioni business
- 17 Il cloud rivoluziona il modo di gestire le reti

## 19 I servizi gestiti

- 20 L'Operational Outsourcing cambia le regole del gioco
- 24 Il futuro della collaborazione è negli Hosted Phone Systems

## 27 La Data Availability

- 28 Il governo dei data lake inizia dai metadati
- 30 La Hyper Availability è il paradigma per un'azienda a prova di futuro
- 32 La protezione dei dati inizia in locale ma si completa nel cloud

## 34 La sicurezza per il cloud

- 36 La sicurezza incomincia dal team aziendale
- 38 I rischi e i costi di un approccio multicloud
- 40 Identificare gli incidenti di sicurezza del cloud
- 41 Con Managed Endpoint Security la sicurezza si fruisce a consumo
- 44 Dati e ambienti industriali al sicuro con la behavior analysis
- 46 Armonizzare IT, sicurezza e policy compliance... con un pizzico di cloud

Direttore responsabile: Gaetano Di Blasio  
In redazione: Giuseppe Saccardi,  
Gaetano Di Blasio, Paola Saccardi,  
Edmondo Espa  
Grafica: Airmone Bolliger  
Immagini da: Dreamstime.com  
Redazione:  
via Marco Aurelio, 8 - 20127 Milano  
Tel 0236580441 - fax 0236580444  
www.reportec.it  
redazione@reportec.it

Direction Reportec • anno XVI - numero 105

Stampa:  
Media Print Srl, via Brenta 7,  
37057, S.Giovanni Lupatoto (VR)

Editore: Reportec Srl, via Marco Aurelio 8,  
20127 Milano

*Il Sole 24 Ore non ha partecipato alla  
realizzazione di questo periodico e non  
ha responsabilità per il suo contenuto*

Presidente del C.d.A.: Giuseppe Saccardi  
Iscrizione al tribunale di Milano  
n° 212 del 31 marzo 2003  
Diffusione (cartaceo ed elettronico)  
50.000 copie  
Tutti i diritti sono riservati;  
Tutti i marchi sono registrati e di proprietà  
delle relative società.



# LA FLESSIBILITÀ DEL CLOUD

La logica dell'informatica come servizio  
prende piede spingendo l'innovazione



# L'imprescindibilità del cloud per l'innovazione del business

Punto di osservazione privilegiato sull'evoluzione del mercato, i Cloud Data Center di Aruba sono protagonisti della crescita delle imprese e di Internet in Italia

**A**ruba ha iniziato a proporre servizi cloud nel 2011, tra i primi in Italia, e come fornitrice non solo di servizi cloud ma anche di infrastrutture IT e di data center, a partire dal livello più basso, ha conquistato negli anni un buon punto di osservazione, dal quale Stefano Sordi, direttore marketing di Aruba, può testimoniare la maturità del mercato: «In meno di un anno dall'apertura del Global Cloud Data Center di Ponte San Pietro in provincia di Bergamo, i 10mila metri quadrati della prima sala sono stati riempiti, grazie alle molte richieste di operatori nazionali e internazionali». Attualmente, continua Sordi: «si tratta del più grande Data Center Campus d'Italia, nel quale è stato attivato il nuovo PoP del MIX (Milan Internet eXchange), che amplierà le proprie potenzialità come nodo di interscambio. Un ulteriore passo per il cloud provider nato in Toscana, ma ormai proiettato su una dimensione sempre più nazionale e internazionale. La maturità del cloud si manifesta per la crescita e le richieste del mercato, ma anche e soprattutto attraverso la sua evoluzione.

## Come il cloud diventa indispensabile

Fino a poco tempo fa, ci spiega Sordi, il cloud era un mercato relativamente puro: «Si nasceva cloud nativi. Le startup non ci pensano nemmeno a comprare del ferro e sono 100% cloud e anche nelle imprese alcuni progetti, come il disaster recovery erano impostati completamente in cloud. Dall'altro lato c'era, separata dal cloud, la scelta della colocation, cioè aziende che preferiscono installare un data center nelle nostre strutture, per avvalersi delle caratteristiche di sicurezza, infrastrutture, gestione, certificazioni e degli standard che in un centro dati aziendali sono difficili e onerosi da raggiungere e mantenere».

In pratica due mondi separati, le grandi aziende con la propria infrastruttura e alcuni "silos" in cloud e le piccole, che i progetti li pensavano direttamente in cloud. «Oggi si può dire che l'approccio è quasi completamente ibrido: i progetti nuovi presentano una parte in colocation, con hardware proprietario posizionato nel



Stefano Sordi, direttore marketing di Aruba

nostro data center e qualcosa in casa del cliente e una componente cloud ma integrata», spiega ancora Sordi. Il cloud diventa quindi un "mattoncino" sempre presente, talvolta nella parte software, in quella gestionale, nella rete, nelle applicazioni e così via. Talvolta l'infrastruttura è solo cloud, più spesso è mista, ma il cloud è ormai indispensabile.

### I vantaggi per le imprese dal GDPR alle tecnologie emergenti

Per l'imprenditore il vantaggio nell'utilizzo del cloud consiste nel poter demandare una componente infrastrutturale, come la rete, la connettività o la sicurezza, affidandola al provider. Inoltre nel computo del Total Cost of Ownership, che i consulenti di Aruba usano per garantire l'efficienza delle soluzioni, oggi entrano componenti legate alle tecnologie innovative.

Precisa Sordi: «Non si tratta solo di risparmiare o di trasformare capex in opex. I clienti arrivano da noi con un'idea e delle esigenze e ci chiedono di aiutarli a definire un progetto e a svilupparlo nel cloud».

Si tratta di utilizzare le tecnologie emergenti in ambiti come IoT (Internet of Things), analytics, e storage intelligente.

In quest'ultimo caso, per esempio, una forte spinta è arrivata e arriva dall'Agenda Digitale, che ha promosso la dematerializzazione e dalla conformità alla normativa europea GDPR (General Data Protection Regulation).

Oltre alla maggiore autonomia dall'infrastruttura e ai risparmi,

## Soluzione IaaS per SAP HANA

Aruba ha presentato un servizio per le crescenti esigenze degli utenti SAP HANA, fornendo macchine virtuali su hardware certificato o supportato da SAP, su cui è possibile installare ambienti HANA (High-performance Analytic Appliance) in modalità BYOL (Bring Your Own License). Aruba, forte della collaborazione con Dell e VMware, ha sviluppato il servizio, consentendo ai clienti di beneficiare di SAP HANA sul proprio cloud.

«Tra i vantaggi per i clienti SAP: una piattaforma multi tenant disegnata specificatamente per supportare i grandi carichi di lavoro e i big data, assieme alla capacità di offrire affidabilità mission-critical 24x7 di livello enterprise». Aruba fornisce, inoltre un alto livello di flessibilità, come le diverse opzioni ad alta qualità di storage SSD e di macchine virtuali affinché ciascuna azienda possa integrare i propri carichi di lavoro nell'infrastruttura più adatta, senza limitare la scelta a configurazioni pre-installate. A corredo anche un supporto tecnico specializzato, per prevenire eventuali problemi a livello infrastrutturale, così da ottimizzare le performance e ridurre i costi di gestione. Il tutto con le garanzie di sicurezza dei suoi data center.

quello che le imprese hanno finalmente capito e cercano, ci spiega Sordi, è la possibilità di sfruttare la dinamicità del cloud in termini di progettazione e sviluppo. Anche grazie ad API e metodologie quali il coding, le aziende possono rapidamente realizzare soluzioni e provarle per affinarle e portarle in produzione con tempi prima impensabili. In molti casi, evidenzia Sordi, l'IT aziendale c'ingaggia perché se non riesce ad anticipare internamente le esigenze, rischia che le linee di business si arrangino da sole, togliendo all'IT l'ownership del progetto. L'IT deve dunque pensare l'architettura delle soluzioni in modo "cloud by design". Anche questo approccio dal dinamismo elevato, sottolinea ancora Sordi, è una conferma della maturità del cloud, che trova riscontro nelle piccole imprese che comprano soluzioni chiavi in mano "a scaffale".

### Un data center a Roma per la crescita dell'Italia

Aruba, come accennato, intende svolgere un ruolo da protagonista per l'innovazione del Paese e per questo si è mossa in anticipo, annunciando l'accordo per la realizzazione del nuovo Hyper Cloud Data Center, a Roma, «dove siamo stati accolti benissimo» evidenzia con soddisfazione Sordi: «Da Bergamo a Roma, passando per Arezzo e portando infrastrutture al Centro e Sud Italia, che è una miniera d'oro, perché le imprese ci sono e possiamo aiutarle a crescere».

Il nuovo Data Center, che avrà le caratteristiche di quello di Ponte San Pietro, comprese tutte le certificazioni più stringenti in termini di disaster recovery, come l'attestazione dei siti su taglie differenti, sarà aperto, secondo le previsioni, nel 2020. ❁

# Cloud, Hosting ed esternalizzazione dell'IT per far crescere il business

Una rete mondiale di 27 data center di OVH permette di esternalizzare nel cloud la complessità dell'IT e dedicarsi al business in tutta sicurezza

**L**e aziende si trovano a dover rispondere alla continua trasformazione del mercato e alle sue dinamiche, alla mobilità di clienti e dipendenti, alle esigenze di raccogliere e analizzare grossi volumi di dati. In un tale contesto, che si abbina all'esigenza di ottimizzare Capex e Opex, fruire dell'IT sotto forma di servizio come reso possibile dal cloud è universalmente ritenuta la soluzione più immediata e adatta.

La difficoltà sorge, tuttavia, quando si deve scegliere a chi rivolgersi tra decine di fornitori di servizi o di infrastrutture perché, osserva Dionigi Faccenda, Sales Manager Italia e Spagna di OVH e con una robusta esperienza nelle reti e nell'IT maturate in grandi aziende nazionali e internazionali, non tutte le proposte si basano su infrastrutture in grado di supportare applicazioni e utenti con la flessibilità, la sicurezza e un vantaggioso rapporto prezzo/prestazioni.

Tra i punti critici, quando si decide di migrare tutto o in parte l'IT legacy su cloud, si annovera per esempio il problema di come farlo senza interrompere l'erogazione dei servizi business erogati all'interno o ai clienti, il poter fruire di più cloud, la movimentazione dei dati, la corrispondenza alle normative, la disponibilità di connessioni di rete con prestazioni adeguate, la presenza territoriale e, non ultimo, la capacità progettuale e di supporto abbinata a un rapporto costo/benefici che permetta a livello di costi di incidere sensibilmente su Capex e Opex.

Sono alcuni dei temi, evidenzia Faccenda, che fanno la differenza tra un progetto di successo ed uno che non permette di raggiungere gli obiettivi desiderati, che non tutti i provider sono in grado di affrontare e che OVH ha invece considerato nel predisporre la propria piattaforma di infrastrutture e servizi.

## Capillarità territoriale e "Openness"

Due sono i fattori chiave della vision OVH per abilitare la trasformazione digitale: la presenza sul territorio e l'apertura dei servizi offerti che non crea un rapporto vincolante tra cliente e OVH. La presenza territoriale è assicurata da una rete



Dionigi Faccenda, Sales Manager Italia e Spagna di OVH

mondiale di 28 data center distribuiti in 12 siti in 4 diversi continenti collegati da una rete in fibra ottica ad altissima velocità. Qualunque sia la sua distribuzione territoriale un'azienda può contare sulla presenza locale, Italia compresa, di data center OVH che assicu-



OVH nel mondo: 27 Data Center e 3 livelli di cloud

rano prossimità, accesso, sicurezza e rispondenza alle normative.

In quanto proprietaria sia dei data center sia della rete in fibra a larghissima banda che li collega con capacità trasmissiva globale di 15 TB, OVH gestisce direttamente l'intero percorso dal cliente all'host che eroga i servizi cloud. Tre le tipologie di servizi:

- **Soluzioni cloud:** comprende servizi di cloud pubblico, privato e ibrido; connettività e sicurezza; cloud desktop.
- **Web hosting:** spaziano dall'hosting di domini web a servizi di email.
- **Server:** comprende la fornitura di server dedicati; server GPU per applicazioni grafiche o di analytics ad altissime prestazioni; storage di dati o backup.

Come accennato, uno dei punti critici che le aziende si trovano ad affrontare nel passare a un cloud ibrido è quello della migrazione di dati e macchine virtuali. Per garantire la migrazione trasparente OVH ha sviluppato la tecnologia HCX, che permette di migrare le macchine virtuali del cliente senza interruzione di servizio da un data center a un altro o a partire dalla propria

infrastruttura. La trasparenza della infrastruttura di servizi è ulteriormente garantita dall'adozione della piattaforma di virtualizzazione VMware.

### Cloud sicuro e garantito con vRack

Un altro punto critico di una infrastruttura IT basata su cloud è la garanzia della connettività tra le sedi aziendali e di parametri quali il delay o la latenza, parametri che possono impattare negativamente sulle applicazioni business. Per eliminare questi problemi e connettere, isolare o ripartire i servizi scelti dal cliente in modo ottimale OVH ha sviluppato vRack, una tecnologia che permette di mettere in comunicazione in modo sicuro server e servizi distribuiti sul territorio e di interconnettere i servizi OVH all'interno di una o più reti private sicure.

In pratica, le aziende possono creare infrastrutture private complesse grazie a un'architettura distribuita in modalità multi-data center che permette di creare fino a 4.000 LAN virtuali private caratterizzate da prestazioni elevate e affidabilità dei collegamenti.

«Elemento chiave di vRack è che si tratta di una soluzione estremamente flessibile che permette di scegliere tra numerosi servizi di OVH per quanto concerne infrastruttura, storage, big data, private e public cloud. Consente alle aziende di estendere le proprie infrastrutture on premise ai data center

di OVH e creare una propria rete privata collegando le diverse soluzioni OVH di cui dispongono, in modalità ridondante o distribuita» ha evidenziato Faccenda.

### Aderenza alle normative e al GDPR

Per facilitarne il rispetto di quanto previsto dal GDPR, OVH ha integrato nella sua infrastruttura i criteri previsti dalla normativa da poco in vigore, come la trasparenza in merito alla localizzazione dei dati e il rifiuto di ricorrere a un subappalto che implichi l'accesso ai dati archiviati dall'utente. Inglobate nella sua offerta sono anche le linee guida dettate dal Codice di condotta CISPE (Cloud Infrastructure Providers in Europe), che ha l'obiettivo di fornire un quadro di riferimento per l'applicazione della normativa presso i provider e i loro clienti.

OVH è anche parte attiva dell'Open Cloud Foundation, un'iniziativa che riunisce fornitori, utenti, centri di ricerca, organismi pubblici. Il suo obiettivo è garantire soluzioni aperte e alternative alle politiche di chiusura tutt'ora presenti sul mercato. ❁

# L'ERP si allarga as a service

di  
Gaetano  
Di Blasio

**Secondo gli analisti di IDC, entro il 2020 le applicazioni gestionali enterprise saranno in cloud per la massima parte**

**U**na ricerca di IDC sembra sancire la fine di un'epoca e, presto, cominceremo a parlare sempre meno di applicazioni legacy, cioè di quei "monoliti" che sono presenti nei CED (Centri di Calcolo) di una volta e che impongono vincoli all'evoluzione tecnologica.

Disegnati su misura hanno permesso alle imprese di gestire le peculiarità dei mercati verticali di riferimento, compresi gli adeguamenti ai regimi fiscali e legislativi dei diversi paesi in cui ciascuna azienda opera. Lo scotto è sempre stato il costo di questa personalizzazione, che comporta alti costi per ogni singola modifica.

Gli analisti della società di ricerca statunitense, pronosticano, infatti, che entro il 2020 il 40% delle grandi organizzazioni avrà spostato su cloud pubblico il 60% delle applicazioni gestionali. In altre parole, entro due anni, avverrà il sorpasso delle applicazioni ERP (Enterprise Resource Management) in cloud rispetto quelle on premise, almeno in termini di valore.

Più precisamente in IDC utilizzano il termine di Enterprise Resource Management

(ERM), che nella definizione della società di ricerca, include e completa l'espressione ERP). Spostare il software applicativo di tipo core business, affermano gli analisti, sta assumendo un ruolo chiave nel percorso di digital transformation. Un passaggio necessario per poter sfruttare i benefici che il cloud può garantire in termini di accelerazione della trasformazione tecnologica, di agilità aziendale e di razionalizzazione dei costi, evidenziano in IDC.

In effetti, gli studi di quest'ultima, mostrano che l'intero mercato delle applicazioni ha già o sta attraversando una fase di migrazione verso il cloud. In particolare, l'ERM, secondo i dati più aggiornati, si prevede crescerà con un tasso medio (CAGR) del 6,6% fino al 2021,

quando arriverà a valere 77 miliardi di dollari).

Ci sono, però, due trend contrapposti: da un lato le applicazioni su public cloud che cresceranno con un CAGR del +14,8%; dall'altro lato, le applicazioni on-premise che resteranno sostanzialmente stabili, con un CAGR da un risicato +0,1%.

Questo nel 2020, prevedono in IDC, per la prima volta, porterà a un valore del mercato ERM su cloud pubblico maggiore di quello on-premise.

L'ERM su cloud pubblico sarà sempre più apprezzato dalle imprese, proprio perché "crescerà la focalizzazione sui processi di trasformazione e innovazione digitale", sottolineano gli analisti.

I costi associati alle applicazioni legacy sono destinati a scomparire nell'era del digitale, delle API, del coding, della virtualizzazione e del cloud. L'obiettivo, sperando non sia un miraggio è raggiungere la flessibilità e l'ottimizzazione operativa.

In IDC ci credono, evidenziando che un "ERM cloud-enabled permette un maggior grado di configurabilità e scalabilità, può essere aggiornato e implementato più velocemente, è disponibile ovunque e in qualsiasi momento". Soprattutto, concludono gli analisti, consente di stare al passo con i requisiti e la velocità dei clienti, ovvero del front-end.



# Automium, un servizio SaaS che abilita la cloud transformation

di  
Giuseppe  
Saccardi

**Il software di Continuous Deployment di Enter gestisce l'automazione dell'infrastruttura cloud e del deployment applicativo. Semplificata la gestione delle applicazioni**

**L**e architetture a microservizi sono di fatto lo standard per le applicazioni cloud-native. Lo stile architetturale a microservizi è un approccio allo sviluppo di una singola applicazione come insieme di piccoli servizi, ciascuno dei quali viene eseguito da un proprio processo e comunica con un meccanismo snello, spesso una HTTP API. Le parole chiave di questo paradigma sono automazione, API, microservizi e sistemi distribuiti.

Automium, ha spiegato Mariano Cunietti, CTO di Enter, è stato ideato proprio con l'obiettivo di semplificare lo scenario complesso della gestione delle applicazioni e permettere alle aziende di intraprendere la cloud transformation con semplicità lasciando

che sia Automium a gestire le complessità.



Mariano Cunietti, CTO di Enter

Si tratta, in particolare, di un servizio che fa parte di Enter Cloud Suite, un insieme di tecnologie open source che presiedono a tutta la filiera (dalla gestione del codice sorgente fino alla produzione), e che consente di fare DevOps fin da subito, fornendo gli strumenti per costruire la propria pipeline di continuous deployment. È anche una piattaforma di automazione che consente di creare e gestire la propria infrastruttura cloud, e fruirne con facilità sin dal primo momento. In sostanza, può essere visto come un collante che rende accessibili le tecnologie open source di uso più diffuso e consolidato, come Terraform, Ansible, Docker, Kubernetes, Consul, Vault, Golang.

«Vogliamo portare gli utenti a fare un passo evolutivo, facendo loro comprendere che il design architetturale e la comprensione del processo produttivo di un'applicazione sono il loro vero business value, e non la tecnologia che lo concretizza. La tecnologia e

la semantica di ogni tool sono il valore dei provider, non dei clienti - evidenzia Cunietti -. Il nostro business value è gestire questa complessità, selezionare (quindi scartare) e semplificare quello che secondo noi è più utile, e presentarlo ai clienti in modo che lo possano usare, senza bisogno di essere degli esperti del settore. Nascondiamo e riduciamo la complessità, senza limitare la libertà».

L'aspetto chiave della soluzione è che non serve più fare tutto a mano. Sia che si stia costruendo la propria nuova infrastruttura cloud o riprogettando quella esistente in ottica cloud, osserva Cunietti, Automium mette a disposizione i "mattoni" che servono, e permette di partire dal punto in cui ci si trova: si disegna quello che serve e sarà poi Automium ad automatizzare la costruzione e il deployment della infrastruttura direttamente su Enter Cloud Suite, la piattaforma cloud europea multi-region basata su OpenStack di Enter. In linea con il concetto di "cloud portability" Automium è multi-cloud, e in quanto tale può funzionare anche su VMWare, AWS, GCP, Azure ed altri cloud, una apertura che evita il rischio di un lock-in su un fornitore se si dovesse cambiare strategia. ❁

# I servizi che piacciono alle aziende

di  
Gaetano  
Di Blasio

## Un'inchiesta della redazione mette in luce l'apprezzamento verso il cloud e i servizi gestiti

**T**ra i vantaggi del cloud c'è il modello dei costi basato sul pay per use, ma è soprattutto la flessibilità a essere tra le caratteristiche più apprezzate. È quanto emerge da un'inchiesta della nostra redazione, che, premettiamo, non ha alcun presupposto statistico, sia per quantità sia per tipologia del campione coinvolto.

Si tratta, in sostanza di una "prima impressione", ottenute attraverso un breve sondaggio online e una serie di interviste. Un primo punto di vista, a livello macroscopico, mostra che tutte le tipologie di servizi cloud sono utilizzate dai nostri lettori, che almeno una volta hanno usato un servizio Infrastructure as a Service (IaaS), Software as a Service (SaaS) e Platform as a Service. Meno usati questi ultimi, forse perché

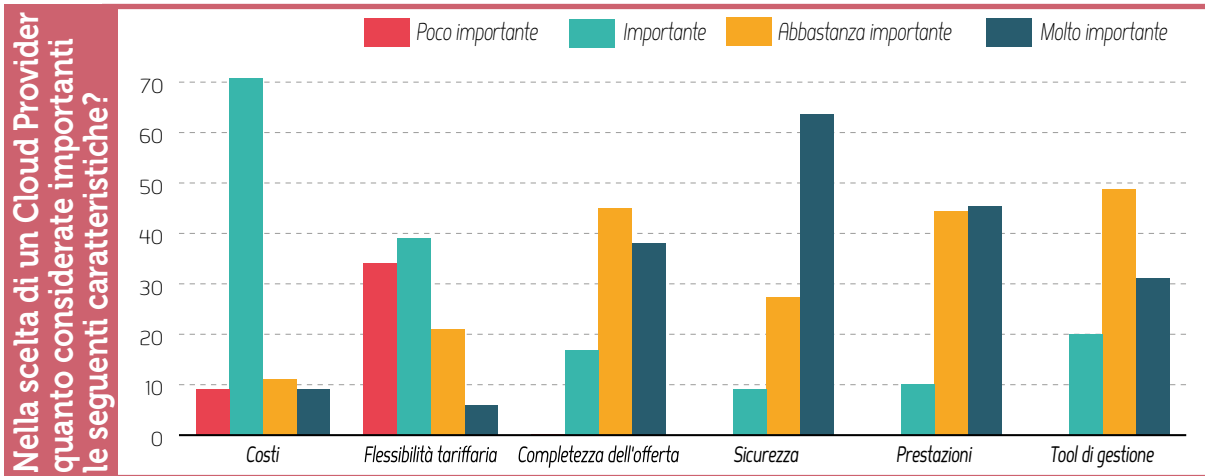
impiegati in sistemi più complessi. Non stupisce, quindi, che lo IaaS più usato sia il noleggio di server. Positivo, riteniamo, l'alto livello di utilizzo di data center as a service, che mostra un'opportunità per le aziende che vogliono concentrarsi sul proprio core business. Nella stessa direzione va letto il dato sui servizi gestiti, in primis l'alto livello di outsourcing completo si potrebbero sviluppare altri servizi, come quelli di rete, ma, forse, il mercato è meno pronto. Più sorprendente lo scarso utilizzo dello storage e piacevolmente interessante l'utilizzo del desktop as a service, forse alimentato dal successo dello smart working,

## Il SaaS in gran spolvero, con qualche pecca

Sui servizi Software as a service non sorprende il primo posto delle applicazioni per il business, che, entrando nel dettaglio sempre con le pinze, vedono un risultato netto nell'uso del cloud privato per le applicazioni gestionali (ERP), ma con numeri interessanti anche per le modalità in cloud pubblico e on premise.

Parità, con un 50% a testa l'attestazione delle soluzioni per i big data e analytics in cloud privato e in cloud pubblico. Quest'ultima, del resto è la più logica organizzazione per l'analisi dei big data, che sempre più devono avvalersi di soluzioni in tempo reale, magari appoggiate a soluzioni di edge computing.

Più in generale sembra che tante imprese stiano spostando applicazioni sul public cloud. Non abbiamo tracciato la dimensione delle imprese coinvolte nella nostra inchiesta, ma numericamente non sarebbero state comunque significative. \*



# La videosorveglianza professionale di aziende e uffici viaggia sul cloud

Le soluzioni video VUpro e VUpoint di RISCO Group permettono, tramite cloud e smartphone, la video verifica live del proprio ambiente di lavoro o smart office

**R**ISCO Group, azienda che sviluppa, produce e commercializza soluzioni di sicurezza integrate e smart home/office, ha risposto alle esigenze del controllo di ambienti di lavoro in tempo reale tramite soluzioni di video verifica e di videosorveglianza professionale. Chiave delle soluzioni è l'utilizzo del cloud e di App per dispositivi mobili che permettono di mantenere sotto controllo, in ogni istante e da ovunque, il proprio ambiente office e di smart working così come una proprietà residenziale o industriale.

VUpoint è una soluzione di video verifica live che permette di integrare alla centrale un numero potenzialmente illimitato di telecamere IP P2P, in grado di fornire video e immagini in alta definizione al verificarsi di un evento potenzialmente pericoloso oppure on demand.

Si integra con sicurezza e smart home nel cloud, con differenti modelli di telecamere da interno o esterno, collegabili in rete con modelli WiFi o PoE; sono plug&play, senza necessità di configurare router o avere IP pubblici. I diversi modelli, anche personalizzabili

nel brand, sono stati progettati per adattare l'installazione ai diversi ambienti e garantire livelli professionali di sicurezza e praticità.

L'infrastruttura cloud di RISCO utilizzata per la comunicazione abilita notifiche, trasmissione di video e immagini e garantisce un percorso ridondato per l'archiviazione. La sicurezza si basa su metodologie che forniscono un doppio livello di protezione, basato sulla cifratura dei dati e su credenziali di accesso variabili. Congiuntamente, i due metodi assicurano che l'accesso alle telecamere avvenga esclusivamente da parte di persone autorizzate.

Sempre grazie al cloud di RISCO, VUpoint è gestibile in modo intuitivo, in qualsiasi momento e ovunque gli utenti si trovino, tramite l'app iRISCO disponibile per dispositivi iOS e Android o tramite una semplice interfaccia web. «Lavoriamo per mettere a disposizione dei nostri utenti le più avanzate tecnologie e siamo da sempre



*Ivan Castellan, Branch Manager di RISCO Group Italia*

impegnati a sviluppare soluzioni che rappresentino lo stato dell'arte del mercato della sicurezza, oltre a fornire nuove funzionalità avanzate che soddisfino al meglio le esigenze in continua evoluzione degli utenti e a potenziare il supporto al canale professionale di RISCO Group», ha dichiarato Ivan Castellan, Branch Manager di RISCO Group Italia.

VUpro è una soluzione professionale TVCC che indirizza le esigenze del settore residenziale, commerciale e industriale. Permette a installatori e distributori certificati RISCO di avere assistenza garantita dall'azienda, oltre a una gestione degli eventi intelligente. Assicura un'elevata qualità delle immagini notturne e diurne con risoluzione di 4 megapixel grazie alle telecamere con funzionalità Wide Dynamic Range (WDR) a 120 dB, agli NRV e alla tecnologia SMART IR.

# Cloud e DevOps semplificano lo sviluppo delle applicazioni business

Per la maggioranza dei CIO la continua e troppo veloce innovazione è un rischio per la customer experience ma cloud e DevOps possono essere di aiuto

---

Il mercato richiede rapidi cambiamenti, ma aderire a questa vision e assecondare (perlomeno troppo) il mercato se non ben organizzato come processo evolutivo potrebbe essere deleterio. Il problema è presto detto: le maggiori organizzazioni rilasciano nuovi aggiornamenti software in media tre volte all'ora, uno scenario in cui quasi due CIO su tre sono costretti a scendere a compromessi tra il perseguire un'innovazione più veloce e il rilascio di applicazioni che siano adeguatamente testati e perfettamente funzionanti.

La cosa non stupisce di certo chi le applicazioni le utilizza, perlomeno nelle loro versioni iniziali prima che i problemi siano corretti, e l'esperienza quotidiana che si vive tra aggiornamenti continui, allarmi per la sicurezza e veri e propri bachi nel software che si utilizza sia in ambito aziendale sia privato ne è una conferma. Una conferma basata su pareri dei diretti interessati viene anche da uno studio basato su un sondaggio condotto da Vanson Bourne su 800 sistemi informativi di tutto il mondo appartenenti a grandi aziende con oltre 1.000 dipendenti, studio che evidenzia come per oltre il 70% delle organizzazioni la necessità di accelerare in innovazione digitale stia mettendo a rischio la customer experience e, in definitiva, ottenere l'effetto contrario a quello che ci si era prefissato di raggiungere.

## Attenti ai compromessi

Lo studio ha rilevato che, in media, a causa delle pressioni della concorrenza e delle crescenti aspettative dei consumatori, le organizzazioni di una certa dimensione rilasciano nuovi aggiornamenti software tre volte ogni ora, un compito che grava sul reparto IT che le deve sviluppare, assicurarne qualità e prestazioni e supportarle su infrastrutture proprietarie, nel cloud o in ambienti ibridi. Nel futuro prossimo la situazione non sembra destinata a migliorare. Quasi il 90% dei CIO ha infatti dichiarato che sarà necessario rilasciare aggiornamenti ancora più velocemente, velocità crescente che non sarà indolore per i budget e che comporterà un costo.

Quasi i due terzi dei CIO ha anche confessato di essere costretti a scendere a compromessi tra un'innovazione più rapida e la necessità di garantire ai clienti un'esperienza software di alto livello.

Il punto critico risiederebbe nel fatto che praticamente ogni organizzazione è diventata un'azienda di software, l'hardware una commodity e si è in presenza di una forte evoluzione verso ambienti software-defined accompagnata da una crescente propensione al servizio. Per esempio, società leader di mercato come Amazon, anche se si tratta di casi limite, rilasciano aggiornamenti sulla base dei secondi, con cicli di sviluppo rapidi e agili in ambienti dinamici e ibridi multi-cloud.

In questa gara ad essere più veloci e ad anticipare i concorrenti chi ne soffre sono gli utenti finali, che invece si aspetterebbero che il flusso costante di nuove funzionalità e aggiornamenti avvenisse con prodotti adeguatamente provati e senza dover scendere a compromessi.

La sfida che l'IT nel suo complesso si trova a dover affrontare e in qualche modo risolvere è quindi offrirli in modo rapido, cosa possibile tramite il ricorso ad architettura native cloud e curando però adeguatamente l'esperienza dell'utente.

Perlomeno sul piano delle risorse e dei costi il ricorso al cloud permette in ogni caso di accelerare gli sviluppi e contenere il Capex dell'IT necessario, nonché di allinearne i costi ai ritorni economici prodotti dai nuovi servizi rilasciati.

## Il problema della collaborazione e il DevOps

Quello dei tempi di sviluppo brevi e del loro impatto sulla qualità del prodotto finale, e sull'impatto che possono avere sul brand aziendale software non adeguatamente testati, non è però l'unico degli aspetti critici evidenziati dallo studio. Un altro problema è posto dalla cooperazione inter-divisionale.

Quasi l'80% dei CIO ritiene che la propria organizzazione abbia subito ritardi in progetti IT, cosa che si sarebbe potuto evitare se i team di sviluppo e quelli operativi fossero stati messi in grado di collaborare più facilmente. A questo si aggiunge il fatto che le iniziative di digital transformation sono spesso finite su un binario sbagliato a causa di (con una media intorno al 50%) interruzioni IT causate da problemi esterni da modifiche interne e della rettifica del codice errato che è stato spinto attraverso la pipeline.

Ma come fare per mitigare questi problemi? Una risposta suggerita è quella del DevOps, vista come approccio allo sviluppo che favorisce e migliora la collaborazione. I dati sostanziano questa posizione, pur con qualche criticità:

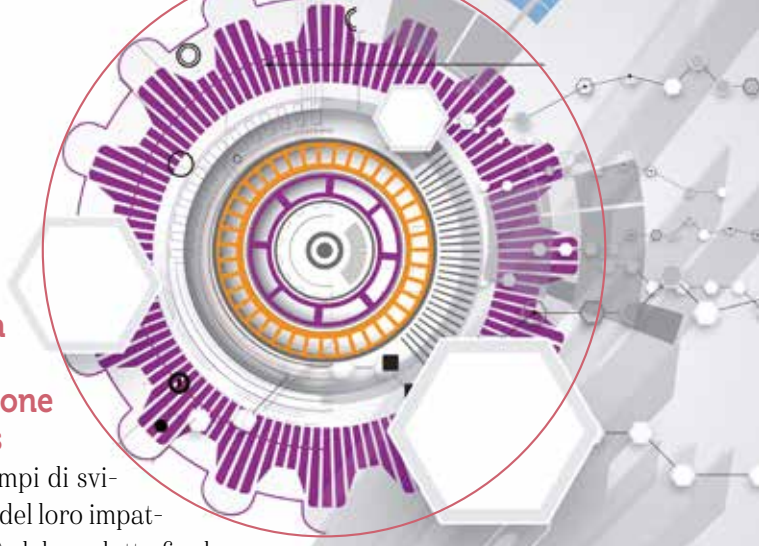
- Il 68% delle organizzazioni ha implementato o sta esplorando le possibilità di una cultura DevOps

per migliorare la collaborazione e promuovere un'innovazione più rapida.

- Il 74% dei CIO ha affermato che gli sforzi DevOps sono spesso indeboliti dall'assenza di dati e strumenti condivisi, il che rende difficile per i team IT ottenere un'unica visione della "verità".

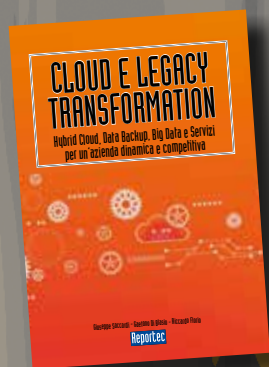
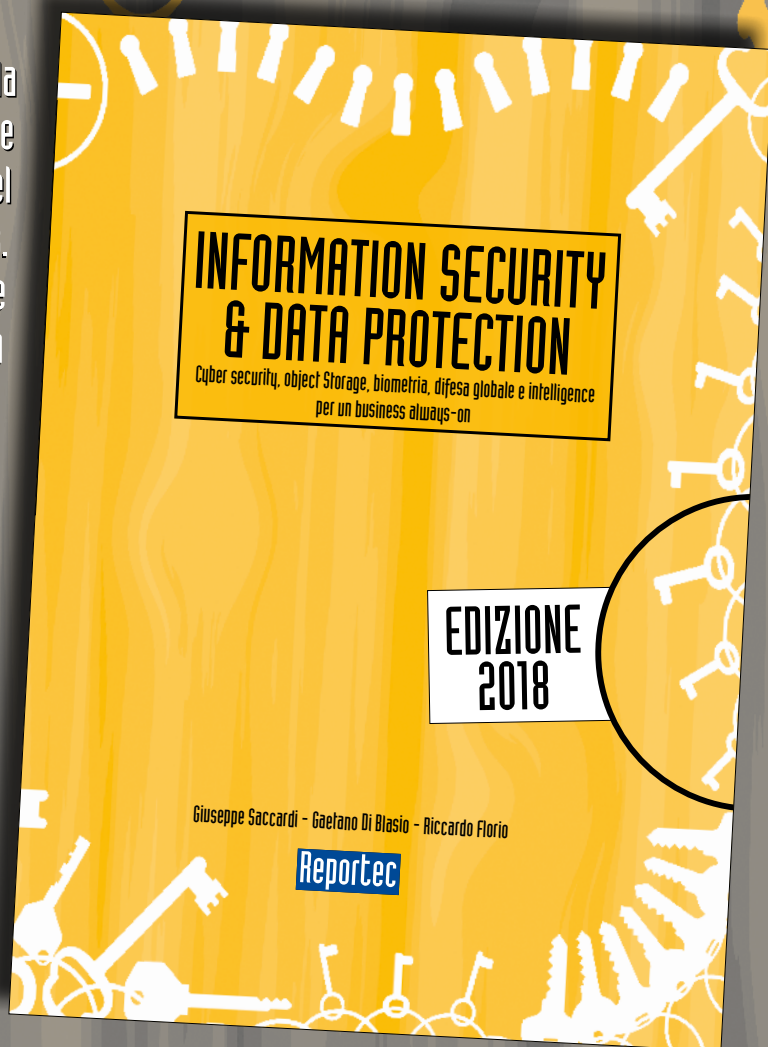
- Il 56% dei CIO ha identificato differenze nelle priorità tra i silos dipartimentali come ulteriore barriera all'adozione di DevOps.

I dati evidenziano come con la maturazione del DevOps le aziende stiano perseguendo in modo crescente la strada dell'automazione e dell'integrazione nello sviluppo software in modo da abilitarne un più veloce rilascio, ma facendolo con una maggior qualità e un minor sforzo manuale. Un aiuto sarà di certo offerto dagli sviluppi consistenti nell'intelligenza artificiale, che è prevedibile ricoprirà un ruolo molto attivo ed importante nella riduzione delle attività manuali e che ci si aspetta permetta di sviluppare software migliori e più verificati, implementare nuove applicazioni più rapidamente e fornire esperienze software di alto livello.



# È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche  
**CLOUD E LEGACY TRANSFORMATION**

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

# Il cloud rivoluziona il modo di gestire le reti

di  
Giuseppe  
Saccardi

## La piattaforma Nebula di Zyxel fa viaggiare la rete fissa e Wi-fi sul cloud e ne automatizza la gestione

Il cloud computing ha ridefinito il modo di fare business e ha coinvolto l'intero mondo ICT in un profondo processo riferito come digital transformation, che vede un numero crescente di aziende rivolgersi al cloud per le proprie applicazioni business o gestionali.

«Perché allora non completare il processo e farlo anche con l'infrastruttura hardware? I motivi di certo non mancano - osserva Valerio Rosano, country manager di Zyxel Italia, società con esperienza trentennale nello sviluppo di soluzioni per infrastrutture IT e di rete -. Tra questi, la riduzione dei costi, l'aumento di flessibilità, scalabilità, efficienza e ridondanza della rete».

Per permettere di chiudere il cerchio del passaggio al cloud applicandone il paradigma anche all'infrastruttura di rete e alla sua gestione, Zyxel ha sviluppato una soluzione specifica denominata Nebula, costituita da dispositivi di rete e da un centro di gestione in cloud, con l'obiettivo primario di ottimizzare la rete stessa e la gestione delle relative risorse.

### Nebula concretizza il cloud networking

Nebula è una soluzione di cloud networking sia wired che

wireless che comprende access point, switch e firewall, tutti gestibili centralmente tramite il Nebula Control Center, che mediante un pannello di controllo permette di monitorare tutti i dispositivi di rete e di gestirli in tempo reale, indipendentemente dalla dimensione topologica e in apparati della rete.

Gli Access Point Nebula, gestiti da cloud, sono stati progettati per supportare carichi elevati e assicurare una copertura Wi-fi affidabile e di qualità Enterprise. Tramite l'interfaccia cloud gli amministratori possono controllarli e configurarli rapidamente, oltre che installarli e monitorarne il comportamento in qualsiasi istante. La piattaforma di rete comprende anche Access Point ibridi che possono operare sia in modalità standalone sia cloud.

Gli Switch Nebula, anch'essi gestibili dal Nebula Control Center, sono gli apparati che forniscono le principali funzionalità layer-2. L'interfaccia cloud permette la loro configurazione e il monitoraggio delle porte di rete. Per semplificare le installazioni, switch



Valerio Rosano, Country Manager Zyxel Italia

multipli della medesima sede possono essere configurati contemporaneamente.

I Firewall Nebula, chiave di volta per la sicurezza della rete, sono configurabili da cloud, con la possibilità di realizzare automaticamente VPN site-to-site che permette alle varie sedi aziendali di comunicare in sicurezza fra loro o con la sede centrale, tramite VPN full Mesh o Hub and Spoke. Gli amministratori hanno anche la possibilità di creare policy di sicurezza per ciascuna sede e monitorare le diverse reti. Di recente è stato rilasciato un aggiornamento gratuito che permette di avere una protezione UTM molto ampia (IDP, Anti Virus, Content Filter e Application Intelligence) per proteggere la rete dalle minacce ransomware.

Per la gestione è disponibile anche l'applicazione Nebula Mobile App che permette di accedere da ovunque e monitorare i diversi siti. Approfondimenti sulla soluzione si trovano sul sito [www.zyxel.it/nebula](http://www.zyxel.it/nebula).





# I SERVIZI GESTITI

Andando oltre il concetto di outsourcing, i managed service forniscono l'ottimizzazione dell'ICT, grazie a una partnership con aziende specializzate

# L'Operational Outsourcing cambia le regole del gioco

I Cloud Managed Service di Hitachi Systems CBT supportano nello sviluppo di servizi per i clienti, la migrazione nel cloud e la gestione sicura h24 su cloud pubblici, ibridi e privati

**L**e aziende sono quotidianamente alle prese con il problema di come ottimizzare Capex e Opex e contemporaneamente incrementare clienti e business. Per farlo devono sviluppare, migrare ed integrare applicazioni specifiche al fine di potersi dedicare al proprio core business ed espanderlo attraverso soluzioni innovative.

È un'esigenza che si scontra sovente con proposte da parte di service provider rigide o confinate all'infrastruttura, quando invece quello che serve è un attore del settore che, operando come partner, coniughi una consolidata capacità progettuale e di sviluppo applicativo con la comprensione delle esigenze aziendali e la disponibilità di infrastrutture che abilitino un'efficace e produttiva migrazione verso il cloud.

Questa è la strada intrapresa da diversi anni da Hitachi Systems CBT, System Integrator europeo del gruppo giapponese Hitachi Ltd, che ha definito un approccio al cloud pragmatico e adattabile alle esigenze aziendali, ai processi e agli obiettivi di business.

«La necessità da parte dei clienti di implementare con il nostro supporto servizi cloud trae origine da diverse esigenze e in primis da quella di potersi concentrare sul core business e trasformarlo. Aiutiamo i nostri clienti ad ottenere il massimo valore dal cloud, configurando le soluzioni coerentemente alle loro necessità di business e partecipando attivamente alla loro trasformazione digitale. Questo risultato viene raggiunto attraverso il nostro modello di Operational Outsourcing, che prevede, una volta definite le reali necessità del cliente, la presa in carico dello sviluppo e della migrazione in cloud. Da quel momento in poi gestiamo l'infrastruttura e le applicazioni mettendo a disposizione le nostre competenze per garantire il servizio in termini di qualità e continuità, mentre il cliente può dedicarsi al proprio core business», ha spiegato Matteo Masera, Sales Director North Italy di Hitachi Systems CBT.



Matteo Masera, Sales  
Director North Italy di  
Hitachi Systems CBT

## Operational Outsourcing al servizio del business

L'approccio descritto da Masera si declina prevalentemente in molteplici scenari di supporto in cui il modello di Operational Outsourcing di Hitachi Systems risponde alle necessità di diverse tipologie di clienti.

Uno scenario è quello delle software house, a cui le aziende si rivolgono per fruire di servizi IT. Per queste Hitachi Systems sviluppa servizi di "Software as a Service" su misura che ne abilitano la trasformazione digitale e l'evoluzione da classica azienda che propone licenze software a fornitore di soluzione SaaS erogate tramite il cloud di Hitachi.

Un esempio è la collaborazione tra Hitachi Systems e OMOOVE, società di Octo Telematics, specializzata nella fornitura di piattaforme SaaS per la gestione del Vehicle Sharing e delle flotte aziendali. Grazie ad un approccio consulenziale evoluto, Hitachi ha effettuato un assessment puntuale delle necessità di business e tecnologiche e ha poi provveduto a migrare i sistemi aziendali sulla propria piattaforma EasyCloud. L'approccio adottato ha portato a un efficace connubio tra cloud privato e pubblico che, unito alle alte performance della piattaforma OMOOVE, permetterà di offrire un servizio ancor più reattivo e scalabile.

Un'ulteriore tipologia di offerta differenziante di Hitachi Systems copre l'esigenza, tutt'ora molto sentita, degli utilizzatori

di applicazioni in ambienti IBM AS400/Power, che devono fronteggiare costi di gestione elevati. Per abilitare un processo di riduzione dell'Opex ha ideato ed eroga un servizio chiavi in mano che permette ai clienti di usufruire di un consolidato, pluriennale e continuamente aggiornato know-how in ambito Ibm.



«Il nostro valore è la capacità di porci al fianco dei clienti e di costruire assieme i servizi di cui necessitano. Nel farlo non operiamo come il classico venditore di "spazio disco", ma disegnando congiuntamente la soluzione per loro migliore. Che si tratti di soluzioni private, ibride, cloud o multi-cloud, quello che forniamo è un "Cloud Managed Service", definito anche outsourcing operativo, che si compone di diverse fasi: dallo sviluppo del servizio alla sua erogazione e alla sua gestione a tutto tondo, grazie ai nostri data center di Roma e Milano e al nostro Service Operation Center che opera h24 e gestisce cloud e on-premise. Attraverso l'Operational Outsourcing siamo in grado di orchestrare le applicazioni migrate sui nostri data center con quelle on-premise presso l'azienda o in altri ambienti cloud, e di accompagnare i

clienti nel loro percorso di digital transformation», ha evidenziato Masera.

## Sicurezza e supporto costante per dormire tranquilli

Attenzione particolare nell'erogazione dei servizi è posta da Hitachi Systems alla sicurezza e alla disponibilità di dati e applicazioni. «Il tema della sicurezza è nel DNA del gruppo Hitachi. In Hitachi Systems abbiamo una Business Unit verticale dedicata alla cyber security e investiamo continuamente nella sicurezza dei nostri data center. Prova di questa continua attenzione è il

conseguimento di un lungo elenco di certificazioni, come la ISO 27001, e l'essere assolutamente compliant con il GDPR. Inoltre, offriamo un'ampia gamma di servizi di back-up e di disaster recovery. Anche in questo caso il ruolo del cliente è centrale, in quanto la soluzione ottimale viene identificata decidendo in un'ottica di co-creation come proteggere i dati, salvarli e garantirne la disponibilità», ha spiegato Masera.

La sicurezza nell'erogazione dei servizi è supportata da una capillare presenza territoriale. L'azienda è presente con quattro sedi situate a Roma, Milano, Venezia e Bologna. Al supporto fornito tramite questi centri si aggiunge quello di primo livello erogato da terze parti distribuite su tutto il territorio nazionale e coordinato con SLA puntuali che garantiscono un'assistenza di alto livello. ❁

# I servizi gestiti per risolvere la sicurezza aziendale

Panda Security fornisce soluzioni che nascono nel cloud e alimentano un ecosistema che accresce il valore aggiunto supportando le imprese a 360 gradi

**G**ianluca Busco Arré, consapevole delle peculiarità che differenziano Panda Security di cui è country manager per l'Italia dal 2015, tiene a sottolineare: «La nostra è un'azienda spagnola, quindi europea, pertanto differente rispetto alle molte aziende statunitensi e russe, che si occupano di sicurezza. Ma ciò che più ci distingue è aver colto una grande opportunità già nel lontano 2007, decidendo di spostare interamente il nostro portfolio in cloud e tuttora possiamo dire di essere l'unico vendor di security ad avere un'offerta di questo genere in termini di sicurezza».

In pratica, sostiene Busco Arré, gli altri vendor hanno ancora nel loro core business tecnologie tradizionali e vedono solo adesso nel cloud un'opportunità, «non avendo investito in tal senso con lungimiranza e permettendoci di essere considerati fra i vendor più innovativi nello sviluppo di tecnologie cloud "native"». In Italia formalmente dal 2015, Panda Security ha oggi due uffici, a Milano e Roma coprendo il territorio italiano attraverso una struttura commerciale, marketing, prevendita e di supporto tecnico. Un assetto considerato strategico per avvicinare il mercato dei servizi gestiti.

## Il cloud nativo

Talvolta quando si parla di tecnologie di cloud security, è importante distinguere fra il prodotto gestito attraverso una semplice interfaccia web, o una dashboard in cloud, da una soluzione progettata e sviluppata per sfruttare i vantaggi di un'infrastruttura completamente cloud. «Panda Security - rimarca Busco Arré - ha spostato il portfolio in cloud, trasformando completamente le tecnologie di sicurezza. In altre parole, per noi, cloud security non è solo una console Web, ma, ad esempio, significa permettere a un partner di sfruttare queste soluzioni per realizzarne un servizio gestito».

Il Managed Service è l'approccio "primario" per Panda Security, perché le imprese hanno necessità di tornare a concentrarsi sul proprio core business e devono poter



Gianluca Busco Arré,  
country manager per  
l'Italia di Panda Security

contare su un partner che diventi un vero e proprio alleato tecnologico, rappresentando il "braccio armato" dell'azienda contro i pericoli del cyber-crime.

«L'intero portfolio delle nostre tecnologie è pensato per poter offrire ai partner gli strumenti per modellare servizi gestiti ad hoc per i loro clienti come ad esempio riallocare le licenze, aggregare la sicurezza, gestire centralmente il reporting», spiega il country manager.

Sono aspetti, continua il manager, che i partner trovano spesso complessi da gestire, anche perché molti vendor di sicurezza realizzano le proprie tecnologie per l'utente finale, ma non si pongono dal lato del partner che, sempre più, si focalizza sull'erogare servizi gestiti come vero fruitore della soluzione. Racconta Busco Arrè: «Una delle grosse sfide che affrontiamo è rappresentata dai clienti che ci chiedono "come può il mio system integrator supportarmi a 360 gradi nella gestione completa della mia struttura di security" e i partner non solo interessati a vendere prodotti, ma più focalizzati e organizzati per aiutare i clienti nella gestione della sicurezza».

### Dall' Endpoint Detection and Response al GDPR

In termini di soluzioni, nel 2015 Panda Security è stata tra i primi vendor ad aver sviluppato una tecnologia di Endpoint Detection and Response (EDR), allora unica azienda europea presente nell'elenco, rilasciato da Gartner, dei fornitori di tali di soluzioni, oggi al



centro dell'attenzione.

Oltre alla cloud security e ai managed services Panda Security, come evidenzia il country manager, ha compiuto importanti passi avanti sul fronte dei data analytics e della correlazione degli eventi di sicurezza, che per un partner è una componente molto interessante, perché consente di fornire un servizio avanzato all'utente finale. Ultimo, ma non meno importante, sottolinea Busco Arrè: «Panda Security ha sviluppato un prodotto ad hoc per il GDPR (General Data Protection Regulation) con la "sensibilità" di un'azienda europea, quindi fortemente interessata alla nuova normativa, di cui tutti parlano, ma a cui nessuno ha dato una risposta puntuale, come la nostra soluzione Panda Data Control, che consente al cliente di controllare e monitorare i dati in suo possesso soggetti al GDPR e di verificare come vengono utilizzati».

Anche questa tecnologia permette ai partner di fornire servizi gestiti in merito al GDPR, che per molti può significare aprire una nuova linea di business. Audit, Advanced Reporting sull'utilizzo dei dati e altri sono gli strumenti messi a disposizione da Panda Data Control, fondamentali per i DPO (Data

Protection Officer), ruoli ufficiali previsti dalla normativa.

### La logica del servizio

Come accennato, i clienti chiedono un supporto a 360 gradi, per questo, in un mercato che Panda Security considera sempre più attivo, è fondamentale creare un ecosistema che risolva i problemi delle aziende, supportando i partner nel creare valore. Su questo il vendor di sicurezza ha fondato il proprio business: «Ovviamente forniamo tecnologia, tipicamente indirizzata a risolvere una problematica di sicurezza, quale una soluzione per evitare i ransomware. La nostra è una tecnologia che offre anche al partner la possibilità di aggiungere valore, come nel caso della soluzione per il GDPR», chiarisce il country manager «Le imprese hanno bisogno di un servizio che si basi sulla tecnologia fornita da Panda Security e che venga corredato dalle competenze che il partner può, di volta in volta aggiungere indistintamente dalla tipologia di cliente».

Con questo approccio e l'utilizzo del cloud le imprese possono contare su un supporto continuo, concentrarsi sul proprio core business, anche a livello internazionale o geografico per le imprese distribuite. Per questo, in particolare, è fondamentale il servizio di Threat Hunting, cioè la ricerca continua sulle minacce e gli attacchi. Se, per esempio, viene rilevato un attacco a una sede in Cina, si può immediatamente attivare una protezione in tutte le filiali nel resto del mondo, senza costi aggiuntivi. ❁

# Il futuro della collaborazione è negli Hosted Phone Systems

I telefoni IP di Snom abilitano l'auto provisioning e la gestione remota e permettono di fruire di servizi UCC efficienti e sicuri con qualità business-class

Indipendentemente dal luogo in cui ci si trova, poter comunicare e collaborare in ogni istante è alla base dell'odierno modo di condurre il proprio business. Le Unified Communications hanno trovato nelle reti IP, nel cloud e nelle reti mobili lo strumento ideale per proiettare l'azienda verso l'esterno, aprirla a nuovi mercati e soprattutto per farlo con investimenti contenuti. Comunicazione IP su reti ottiche e su cloud, videocomunicazione su IP e altri strumenti di collaborazione sono tutti aspetti qualificanti di una moderna soluzione di comunicazione e collaborazione unificata (UCC). Congiuntamente permettono di ampliare la portata del proprio business e allo stesso tempo di ottimizzare Capex e Opex.

Un ulteriore beneficio deriva dal poter installare il software di un sistema telefonico, il PBX, non più su una macchina specializzata ma su un server standard di mercato. Il medesimo server su cui girano per esempio le applicazioni office. La simbiosi che è derivata tra applicazioni UCC e Office costituisce un ulteriore vantaggio e aumenta le modalità di cooperazione, estendendole dalle persone alle applicazioni e all'Internet delle cose.

Tuttavia, osserva Fabio Albanini, Head of Sales South of Europe di Snom, società specializzata nello sviluppo di sistemi e apparati telefonici IP per il mondo business, come tutte le medaglie anche questa presenta il suo rovescio. Se numerosi sono i benefici di un IP PBX installato come software su un server in un data center, un tale approccio apre la strada a criticità e a rischi, soprattutto se connesso a reti mobili esterne, al cloud o a Internet. Importante anche la regolarità degli aggiornamenti della soluzione di UCC, del server su cui gira e, soprattutto, della tutela, qualità e continuità del servizio tramite strumenti business-class.

Rete IP, mobile o il cloud sono elementi critici in termini di qualità del servizio, osserva il manager, perché per assicurare la qualità del parlato intervengono parametri che devono essere rispettati e non sempre facili da implementare con le infrastrutture citate.



Fabio Albanini, Head of Sales  
South of Europe di Snom

## Qualità e sicurezza i punti salienti di una soluzione di UCC

A garanzia della necessaria qualità e sicurezza delle conversazioni business, evidenzia Albanini, i telefoni IP per aziende e provider firmati Snom sono progettati in modo da massimizzare la qualità delle applicazioni di UCC secondo linee guida molto severe in termini di qualità della voce, ritardo nella trasmissione della fonia su IP, interoperabilità, compliance alle normative e, non ultimo, di sicurezza, in quanto come il traffico dati la voce su IP è soggetta alle stesse criticità che interessano lo scambio di dati, passibile di abusi, intercettazioni, dirottamento e attacchi da parte di hacker.

Quello della sicurezza è un problema da non sottovalutare quando si tratta di un PBX virtuale su cui girano applicazioni UCC o di Contact Center. Se usato per attività di collaborazione diventa infatti il punto di scambio di informazioni riservate inerenti progetti, dati amministrativi, dettagli sui clienti, e così via, tutti dati sensibili che in base al GDPR vanno accuratamente protetti. Tenere aggiornata e in sicurezza una soluzione UCC on-premise può tuttavia rivelarsi improbo ed esporre a rischi concreti la continuità di un servizio essenziale per il successo dell'azienda.

La soluzione, particolarmente per aziende della fascia delle PMI che desiderano fruire dei benefici della UCC ma esternalizzarne la complessità gestionale, suggerisce



IP-Phone D785

Albanini, la si trova nell'hosting presso un provider di fiducia del centralino IP che eroga il servizio di UCC.

## PBX in hosting: più servizi meno problemi

Un sistema telefonico fruito in modalità "hosted" prevede che il sistema IP-PBX sia residente presso un service provider che si assume la completa responsabilità del suo esercizio e della gestione del software e dei telefoni IP richiesti dal servizio business desiderato dal cliente. In sostanza, ci si libera della complessità gestionale, si riduce a zero il Capex e si distribuisce e si riduce l'Opex. Ma con in aggiunta il fatto che il provider dispone h24 di personale per la gestione centralizzata e il sistema è inserito in un contesto altamente ridondato che assicura la continuità del servizio molto di più di quanto si potrebbe ottenere con una soluzione on-premise.

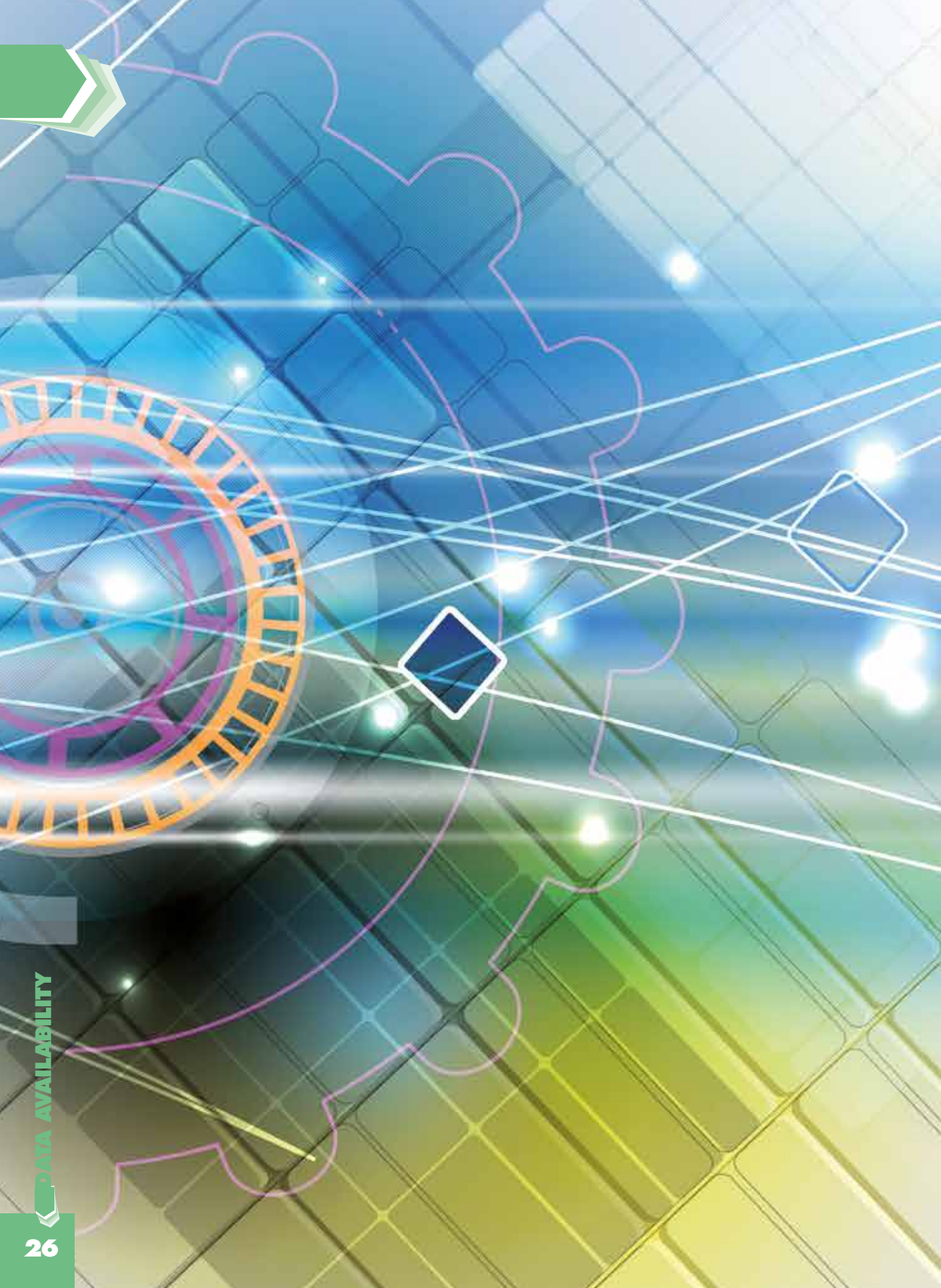
Tutto quanto attinente al suo funzionamento, dalle chiamate alla segnalazione alle funzioni di UCC, è gestito dal server IP PBX presso il provider, che in cambio

provvede a una tariffazione su base periodica, ad esempio mensile, che può comprendere un ammontare massimo contrattualizzato di minuti di conversazione e l'utilizzo di un set di funzionalità.

## La chiave della qualità è nei telefoni IP

Punto chiave nell'ottenere i benefici esposti è la qualità e il set di funzioni dei telefoni IP forniti dall'operatore, o scelti liberamente dall'utente. I telefoni devono disporre di tutte le caratteristiche richieste per garantire la qualità contrattuale, la sicurezza delle conversazioni e la gestione da remoto tramite IP o cloud.

«Nel corso dell'ultimo anno il numero di telefoni IP a marchio Snom venduti in Italia è cresciuto notevolmente dando luogo a un incremento del fatturato di quasi il 50%, anche grazie al consolidamento di importanti collaborazioni siglate con i principali Carrier operanti sul territorio nazionale, indice questo di come i telefoni IP di Snom rispondano in modo ampio alle esigenze della digital transformation», ha commentato Albanini, che ha anche evidenziato come l'aumento degli operatori telefonici che propongono il VoIP e/o piattaforme UC alla clientela business in modalità "as-a-service" coinvolga sempre più frequentemente anche gli installatori telefonici tradizionali. \*



# LA DATA AVAILABILITY

L'importanza della disponibilità  
dei dati e delle infrastrutture  
per l'impresa always on

# Il governo dei data lake inizia dai metadati

Talend ha sviluppato una soluzione che gestisce i dati nella catena del valore, assicura usabilità, governance multi-cloud e predicibilità dei costi connessi alla crescita di dati e risorse

**L**a digital transformation inizia dai dati e dal loro utilizzo intelligente. Se però si passa dall'enunciazione teorica alle considerazioni pratiche la realtà è che quasi la metà dei dati aziendali ha problemi di integrità, l'ottanta per cento del tempo degli analisti è speso nel preparare i dati e oltre la metà dei dati aziendali non è accessibile.

Il porre mano a questi problemi che possono rallentare il processo di trasformazione aziendale, osserva Talend, trova però un forte ostacolo nel fatto che le esistenti architetture dati non sono in grado di tenere il passo con i tempi, le tipologie dei dati, il volume, la distribuzione e le esigenze di analisi in tempo reale. Quello che serve è una soluzione che metta a fattor comune paradigmi quali il multi cloud, i big data, i data lake, gli analytics, e che lo faccia in modo aperto e facile da fruire.

Potrebbe sembrare la classica quadratura del cerchio, ma è quello che ha realizzato Talend, posizionata da Gartner tra i leader nel Quadrante Magico Data Integration Tools, con la soluzione Talend Data Fabric.

La piattaforma, ottimizzata per la gestione di ambienti IT cloud e multi-cloud di classe enterprise, permette di gestire in modo trasparente e sicuro le informazioni aziendali distribuite sulle principali piattaforme pubbliche cloud, e permette di integrare, pulire e analizzare rapidamente i dati ovunque questi si trovino e in aderenza alle specifiche esigenze dei processi di business.

In pratica, la soluzione fornisce alle aziende impegnate nella digital transformation una struttura di governance esaustiva basata sui metadati per la creazione, il controllo, l'attribuzione, la definizione e la gestione delle informazioni aziendali in modo da poter estrarre e diffondere ulteriore valore



*Antongjio Dona, Vice President  
Sales per l'Italia di Talend*

dai dati disponibili.

L'assunto che sta alla base della vision di Talend, per abilitare la digital transformation e colmare il digital divide che si è progressivamente creato tra le esigenze del business e l'architettura IT convenzionale, è che i metadati permettono di riassumere le informazioni di base relativamente ai dati associati, come posizione, formato, semantica, utilizzo e valore. Accedere rapidamente a tali informazioni consente alle aziende di migliorare la condivisione dei dati, il loro riutilizzo, la governance, il controllo dei rischi e avere una migliore valutazione dell'impatto delle modifiche prima che i dati vengano condivisi all'interno dell'azienda.

«La corretta comprensione della struttura, dei limiti, della definizione e della descrizione dei dati consente di proteggersi dagli errori di interpretazione o da un uso improprio. Indipendentemente dalle sue dimensioni, un'azienda può dotarsi di una solida strategia per i metadati che è essenziale in un'epoca in cui l'informazione è fondamentale per il successo delle aziende sul lungo periodo», ha osservato Antongiulio Dona', Vice President Sales per l'Italia di Talend.

## Multi-cloud e big data a fattor comune

Uno degli obiettivi che Talend si è posta con lo sviluppo di Talend Data Fabric è consistito nel dare alle aziende la possibilità di disporre di servizi cloud di diversi provider in modo da offrire un valore aggiunto alle business unit di

un'azienda che si trovano coinvolte in un processo di adozione di piattaforme cloud in base alle specifiche esigenze.

Per evitare il diffondersi dello shadow IT i CIO devono progettare le infrastrutture IT in modo agile e atte a fornire soluzioni ibride e multi-cloud.

Talend Data Fabric permette alle aziende di sviluppare pipeline di dati su una qualsiasi delle principali piattaforme cloud con la consapevolezza che tutto sarà compatibile con il cloud di ultima generazione e con le innovazioni in ambito open source.

La piattaforma mette a disposizione delle aziende un'ampia library di componenti cloud nativi Talend, fruibili mediante strumenti visivi intuitivi per il drag-and-drop, che permettono di creare flussi di big data in grado di funzionare con qualsiasi cloud.

Ampio il supporto di provider, che comprende AWS, Cloudera Altus, Google Cloud Platform, Microsoft Azure e Snowflake. Le funzioni disponibili consentono ad esempio di:

- **Sviluppare pipeline multi-cloud:** è realizzato tramite connettori con i diversi ambienti cloud e funzionalità che permettono di semplificare la costruzione e la distribuzione di pipeline di dati intelligenti.

- **Accelerare la migrazione al cloud:** consente di migrare i dati residenti e disponibili on-premise su cloud e di crearvi data warehouse, alimentare analisi più ricche e velocizzare i tempi di consultazione.

- **Ottimizzazione e portabilità:** permette di sfruttare le attività di sviluppo progettate per una piattaforma cloud e riutilizzarle con altre piattaforme cloud.

- **Data quality e apprendimento automatico:** permette di bonificare e gestire i dati in modo automatico per far fronte alla crescita degli archivi. Il processo si basa su algoritmi di machine learning alimentati da Apache Spark per automatizzare e accelerare la corrispondenza e la bonifica dei dati, migliorare la scalabilità, le prestazioni e l'accuratezza.

## Il supporto per SAP

Talend Data Fabric e tutte le piattaforme intermedie comprendono anche diversi supporti per i dati archiviati nei sistemi SAP.

Le funzionalità sono di ausilio nel gestire in modo semplice e rapido i dati SAP già esistenti e fonti di big data esterne all'azienda, per poi far confluire il tutto in data lake o data warehouse on premise o su cloud.

Per esempio, con l'ultimo e recente annuncio del SAP Bulk Extraction, le piattaforme Talend consentono di estrarre grandi quantità di Big Data batch da SAP Business Suite e SAP S/4HANA e migrarli verso altri sistemi; Business Content Extractor è uno strumento che fornisce viste semantiche delle fonti di dati SAP che ne facilitano l'accesso; SAP HANA Calculation Views consente di lavorare con snapshot compositi ed eseguire calcoli complessi che semplificano il processo di modellazione dei dati. ❁

# La Hyper Availability è il paradigma per un'azienda a prova di futuro

Il business nel cloud richiede soluzioni per l'assoluta disponibilità e sicurezza dei dati. È quello che rende possibile Veeam con la sua Availability Suite

La diffusione di un IT basato su cloud o multi-cloud ha fatto emergere l'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione del dato, passando da uno reattivo ad uno proattivo basato sull'intelligenza artificiale e su analytics.

Si tratta di realtà, sia che si parli di reti di sensori IoT inerenti infrastrutture di tipo sanitario, dei trasporti, di grid per l'erogazione di energia o per servizi pubblici, che richiedono di essere orchestrate e garantite sia per quanto concerne la loro disponibilità assoluta che per i tempi in cui rispondono in termine di latenza e velocità alle richieste di dati inoltrate. Ciò ha portato alla coniazione del nuovo termine di Hyper-Availability, che ha come obiettivo chiave quello di facilitare una orchestrazione dei dati pilotata dal comportamento delle applicazioni su infra-

strutture multi-cloud anche di grandi dimensioni.

«La Hyper-Availability è la nuova frontiera nel trattamento del dato e nella sua fruizione per il business. La Hyper-Availability Platform di Veeam, già utilizzata da numerose grandi aziende ed operatori mondiali e italiani è una soluzione completa di Intelligent Data Management che permette di sviluppare e fornire rapidamente e in modo sicuro servizi digitali innovativi on-premise e nel cloud», ha evidenziato Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam.

La protezione e la gestione dei dati pensata come salvaguardia attraverso policy puramente reattive è in sostanza superata dai fatti e nella vision di Veeam si è concretizzata in un sistema che fornisce in modo proattivo valore di business.



*Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam*

## Cloud ibrido e multi-cloud sempre disponibili con Veeam Availability Suite

La vision per il cloud di Veeam trae la sua genesi dalla considerazione che nell'odierna economia digitale le aziende adottano una strategia multi-cloud per incrementare l'innovazione, accelerare il time-to-market ed ottimizzare i costi, tutti aspetti a cui Veeam ha inteso dare una risposta .

Per supportare le aziende nella esternalizzazione della complessità dell'IT basata sul Cloud la società ha inglobato nella sua soluzione Veeam Availability Suite un insieme di funzionalità che permettono di gestire in pratica la totalità dei dati aziendali e di assicurarne la disponibilità per tutti i carichi di lavoro possibili, virtuali, fisici o nel cloud, il tutto gestendoli da un pannello di controllo Veeam centralizzato.

In sostanza, con la sua soluzione, ha perseguito l'obiettivo di consentire alle aziende in fase di transizione al cloud di sostituire le soluzioni legacy di backup , business continuity e data recovery legacy, che rallentano la business transformation, con un approccio innovativo centrato sul cloud e che assicura la disponibilità dei dati tramite una singola piattaforma ad elevata affidabilità.

Le funzioni di gestione dei dati atte a garantire la "Always-on Availability" per i carichi di lavoro virtuali in ambito premise, comprendono anche il supporto multi-cloud per Microsoft Azure, Azure Stack, Amazon Web Services, IBM Cloud nonché applicazioni SaaS,

ad esempio per quanto concerne il Backup su ambienti Office 365 di Microsoft.

## Al sicuro i dati su Microsoft Office 365

Veeam Backup for Microsoft Office 365 è una funzione che aggiunge un nuovo supporto di scalabilità e multi-tenancy per le implementazioni aziendali e i provider di servizi che offrono servizi di backup gestiti da Office 365. Lanciata in ottobre con la versione, ha già raggiunto più di 25.000 aziende che lo stanno utilizzando, estendendo la protezione dei dati ad oltre 2,3 milioni di caselle postali Office 365.

La positiva accettazione da parte delle aziende trova spiegazione nel fatto che Veeam Backup for Microsoft Office 365 fornisce alle aziende varie opzioni aggiuntive per proteggere i loro dati, oltre alla replica automatica dei dati che Microsoft fornisce nei suoi data center e ai controlli nativi di resilienza disponibili in Office 365. E una combinazione che consente alle aziende di mantenere un controllo completo dei propri dati nel cloud e garantirne la disponibilità ai propri utenti.

Veeam Backup for Microsoft Office 365 v1.5, ha evidenziato l'azienda, ha avuto una massiccia adozione da parte del mercato Enterprise grazie alle sue numerose funzioni per garantire la scalabilità e ad una architettura multi-repository e multi-tenant che consente di proteggere le implementazioni Office 365 di grandi aziende con un'unica installazione.

## Servizi subito in produzione con Veeam DataLabs

L'impegno di Veeam Software nel cloud ibrido o multcloud, come chiave per una digital transformation di successo e la salvaguardia dei dati, si è esteso sino a comprendere il ricorso all'intelligenza artificiale e a quanto necessita per avere una un'azienda che sia sempre always-on.

Per questo, oltre all'elevata disponibilità, entra in gioco anche il fattore tempo correlato ai processi produttivi e a cosa necessita a livello di dati e informazioni per passare dalla formulazione di un'idea al suo passaggio in produzione, sia che si tratti di un bene materiale sia di un servizio immateriale.

Un aiuto concreto Veeam Software si è proposta di darlo tramite lo sviluppo della piattaforma per l'alta disponibilità denominata Veeam DataLabs, una soluzione per la gestione delle copie di dati che permette alle aziende di creare rapidamente e on-demand nuove istanze dei propri ambienti di produzione.

La soluzione, ha spiegato Albert Zammar, 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. \*

# La protezione dei dati inizia in locale ma si completa nel cloud

Il servizio C2 Backup di Synology abbina il salvataggio dei dati in locale con il loro backup su cloud e garantisce la loro protezione e disponibilità

**L'**entrata in campo della normativa GDPR per quanto concerne il trattamento dei dati ha profonde implicazioni sul come i dati stessi vengono protetti. Ma non basta proteggerli, si deve anche averli disponibili e garantire la loro conservazione a termine e nei termini di legge.

In sostanza, memorizzarli su qualche supporto fisico e tenerne la copia in ufficio in qualche cassetto non è più sufficiente. Comportamento che, peraltro, va anche contro il comune buon senso, che suggerisce di conservarne più copie a distanza di sicurezza e su supporti robusti e ridondati.

Una soluzione al problema è stata ideata da Synology, una società che sviluppa dispositivi storage connessi alla rete locale (NAS: Network Attached Storage), di sorveglianza su rete IP e apparecchiature di rete, tutte soluzioni con cui si è proposta di essere di ausilio nel gestire e salvare i dati facendo leva anche sul cloud.

Abbinare salvataggio in locale con loro copie nel cloud, evidenzia la società, è un sistema economico, efficiente ed estremamente sicuro per garantirsi la protezione e la disponibilità dei dati.



*NAS Synology per la protezione locale e nel cloud*

## C2 Backup: la simbiosi tra locale e cloud

Un esempio di piattaforma sviluppata da Synology per la protezione del dato è C2 Backup, una soluzione integrabile con i NAS dell'azienda (ma utilizzabile anche come prodotto indipendente) che consente

di gestire backup multi-versione sul cloud con elevate garanzie in termini di flessibilità, efficienza e sicurezza. Va osservato che già di per sé un apparato NAS è un dispositivo che nasce per conservare i dati in maniera sicura grazie a funzionalità quali quella RAID che replica copie di file su più dischi.

A questo la soluzione C2 Backup, che diventa un'altra destinazione del salvataggio dei dati, aggiunge un ulteriore livello di sicurezza sul cloud, appoggiandosi a server veloci allocati in Germania.

Ideato per rispondere alle esigenze sia di un'utenza professionale sia privata

(ad esempio di home working), C2 Backup è un servizio di backup in cloud che si integra con l'interfaccia dei dispositivi di storage NAS di Synology e con l'applicazione di salvataggio dei dati installata, Hyper Backup.

Peraltro, osserva la società, per fruire di servizi non è precondizione disporre di un NAS Synology perché i dati oggetto del backup sono accessibili e gestibili da qualunque piattaforma e con qualsiasi tipo di dispositivo.

A livello pratico, consente di pianificare le attività di backup e dispone del supporto multi-versione, che permette di mantenere molteplici versioni degli stessi file consentendo il recupero di versioni precedenti, anche in caso di incidenti, per esempio quando si scopre che da una certa data in poi dei virus hanno infettato un file.

La soluzione è disponibile in due versioni. La prima prevede un Backup giornaliero con la conservazione di fino a 11 versioni di backup nel corso degli ultimi 30 giorni e capacità di storage di 100 GB, 300 GB e 1 TB. La seconda prevede piani di backup flessibili, policy di conservazione personalizzabili, deduplica dei dati per l'ottimizzazione dello storage e capacità dell'ordine dei Terabyte.

## Proteggere i dati di business in Office 365

Synology ha dato una risposta anche alle esigenze di salvaguardia dei dati degli utenti di Microsoft Office 365. La versione "Active Backup for Business" consente il salvataggio del pc sul NAS e permette

NAS Synology in tecnologia flash



di garantire la disponibilità dei dati per workload sia negli ambienti fisici sia virtuali.

«Cresce sempre più il numero di aziende e imprese che lavorano tramite piattaforme fisiche, virtuali e in cloud. Questo fenomeno costituisce una sfida notevole per i reparti IT che devono garantire la sicurezza dei dati in crescita in questo ambiente su diverse piattaforme», ha osservato Jia-Yu Liu, Director of Application Group presso Synology Inc. «Per risolvere il problema, Synology ha sviluppato una soluzione all-in-one che integra software e hardware per aziende di diverse dimensioni».

Active Backup for Office 365 è un'applicazione che utilizza una tecnologia a singola istanza che oltre a supportare le aziende nella gestione e disponibilità dei dati su Office 365, riduce sensibilmente lo spazio occupato dai backup. In particolare, la funzione di ricerca dei contenuti è specificamente ottimizzata per le ricerche della posta e degli allegati, e consente agli utenti di identificare nel più breve tempo possibile il messaggio da recuperare. A questo aggiunge funzionalità chiave quali:

- **Il supporto per svariati endpoint Office 365:** Office 365, Office 365 Germany, Office 365 gestito da 21Vianet.
- **La protezione centralizzata:**

con il backup di OneDrive per Business, dati di posta, contatti, e calendario su un NAS Synology e gestione ottimizzata delle copie da una singola interfaccia.

- **Ripristino dal portale self-service:** la funzione di ricerca nei contenuti permette di applicare filtri tramite parole chiave. È possibile trovare l'e-mail desiderata, ripristinare un singolo file, messaggio di posta, allegato, contatto o uno specifico evento del calendario.
- **Efficienza di archiviazione e backup:** la singola istanza trasferisce e archivia soltanto i file con contenuti unici tramite una funzione di deduplica.

Active Backup for Business è invece una soluzione che integra diverse tecnologie e dispone di funzionalità che includono per esempio la protezione di pc e server tramite un agente software che permette di completare i backup per proteggere i workload dei server o dei pc Windows.

In base allo scenario, gli utenti possono decidere di ripristinare un singolo file dal portale di ripristino, optare per un ripristino dell'intero sistema o eseguire direttamente un backup su Virtual Machine Manager per recuperare i dati dell'applicazione e provvedere alla disponibilità della stessa. ❁



# LA SICUREZZA PER IL CLOUD

Dal GDPR alla protezione dalle  
minacce, soluzioni e strategie  
per la security





# La sicurezza incomincia dal team aziendale

di  
Giuseppe  
Saccardi

Garantire la sicurezza nel cloud o nel cloud ibrido è un compito che spetta al security team. CyberArk aiuta le aziende a verificarne la reattività

---

**C**on il crescente ricorso ai servizi cloud pubblici, come AWS, Azure e simili, a servizi infrastrutturali (IaaS) e di piattaforma IT (PaaS), le aziende si trovano ad affrontare due problemi: chi ne è responsabile e come garantirne la preparazione.

Sebbene i provider pubblici come la citata Amazon o Google enfatizzino tatticamente che il loro uso, per quanto concerne la sicurezza dei carichi di lavoro, deve intendersi a responsabilità condivisa, gli utilizzatori tendono a considerare l'aspetto sicurezza come di competenza del fornitore del servizio.

È indubbio, osserva CyberArk, ai primissimi posti in una classifica mondiale di 500 fornitori di soluzioni di sicurezza e specializzata nella protezione degli account privilegiati su end-point e nel cloud, che le organizzazioni che fanno conto esclusivamente sulla sicurezza garantita dai cloud provider espongono la propria azienda a concreti rischi, e fatti recenti lo hanno dimostrato ampiamente.

L'asserzione è particolarmente vera per quanto concerne la riservatezza delle credenziali, che in ambienti cloud tendono a proliferare. Create automaticamente ed utilizzate per fornire, configurare e gestire migliaia di macchine e di micro servizi, se compromesse offrono ad un attaccante un accesso laterale a rete, dati e applicazioni e la successiva possibilità di accedere ad asset aziendali ancor più critici.

Espandere la propria infrastruttura IT nel cloud o nel multi cloud è quindi un approccio che, seppur pagante in termini di riduzione di Capex e Opex, va realizzato con estrema attenzione.

## Cloud al sicuro con CyberArk Red Team

Il cloud ha apportato al problema sicurezza nuove sfide. Con il cloud, la superficie per un attacco si è fatta notevolmente più ampia e complessa e interessa numerosi aspetti sistemistici e organizzativi quali gli ambienti ibridi, DevOps, SaaS e applicazione Web, solo per citarne alcuni.

Quello che in un tale scenario fa la differenza dal punto di vista di un'azienda è la capacità del suo team di sicurezza di individuare rapidamente la superficie disponibile per un attaccante e l'abilità nel bloccarlo.

Per aiutare le aziende nel passaggio al cloud, mantenendo un efficace controllo

dell'infrastruttura e dei servizi IT, ovunque questi siano allocati, CyberArk ha sviluppato "Red Team Cloud Security Services", un insieme di servizi che permettono alle aziende di verificare la propria posizione in termini di sicurezza e valutare se e come l'organizzazione è in grado di difendersi quando l'IT o una sua parte viene spostata nel cloud pubblico.

I servizi Red Team sono stati ideati per fornire ai team dediti alla sicurezza un modo sicuro per verificare la propria abilità nel difendere efficacemente e in profondità l'ambiente cloud aziendale, comunque esteso, da attacchi cibernetici.

Le verifiche si basano su simulazioni di attacchi che includono molteplici tattiche, tecniche e procedure (TTP) che sono state sviluppate da CyberArk specificamente per ambienti cloud pubblici e ibridi.

I TTP si basano su quanto avviene nel corso di un attacco reale e l'obiettivo è quello di individuare le vulnerabilità insite nell'infrastruttura cloud complessiva di un'azienda, verificare la qualità delle procedure di sicurezza e individuare le aree dove questa deve essere migliorata.

L'approccio adottato dai servizi Red Team, che effettuano i test senza impattare sull'ambiente controllato, simula in sostanza il comportamento di un potenziale attaccante reale e mette alla

prova la capacità del team di sicurezza nel rispondere ad attacchi avanzati.

### Attacchi al cloud conosciuti e sconosciuti

Una volta definiti gli obiettivi da perseguire, l'azienda può optare per la verifica della capacità di individuare attacchi conosciuti o sconosciuti:

- **Attacchi conosciuti:** in questo scenario è verificata la capacità



di individuare minacce già comprese in uno specifico modello di attacco.

- **Attacchi sconosciuti:** è uno scenario in cui il Red Team sviluppa strumenti personalizzati che vengono ideati con lo scopo di penetrare le difese dell'ambiente on-premise o cloud sotto test, di muoversi trasversalmente all'interno della sua rete e di esfiltrare dati sensibili. È un servizio ideato da CyberArk per verificare la capacità effettiva di individuare e rispondere ad attacchi avanzati senza introdurre rischi per il business.

Per valutare la qualità delle risposte agli attacchi, nel corso delle attività di test realizzate il Red Team

mette in atto tecniche di evasione nei confronti degli strumenti di sicurezza di cui è dotato il cliente e per rimanere nascosto il più a lungo possibile all'interno della sua rete.

Con il proseguire dell'attività di test gli attacchi si fanno progressivamente più complessi e sono portati sempre più in profondità in modo da verificare e misurare quali tipi di attacchi il team di sicurezza è in grado di individuare e quali non è in grado di rilevare, in modo da quantificare la postura corrente in termini di sicurezza dell'organizzazione.

### I benefici del servizio

Tra i benefici che il servizio permette di ottenere, osserva CyberArk, oltre ad

evidenziare cosa è opportuno fare per migliorare la sicurezza, vi è la comprensione di quanto risulti facile o difficile per un attaccante esterno o interno l'entrare in possesso di dati sensibili e di valore come ad esempio credenziali privilegiate, rilevare le debolezze delle difese, valutare l'impatto sul business di vulnerabilità sconosciute e definire la priorità degli interventi da apportare. Nessuna organizzazione è completamente a prova di attacco. Tuttavia, evidenzia CyberArk, simulando attacchi e facendone esperienza i team operativi possono migliorare la propria capacità di risposta e diventare più efficaci nella caccia alle minacce e nel rilevare vulnerabilità. ✨

# I rischi e i costi di un approccio multcloud

di  
Gaetano  
Di Blasio

**Security Fabric di Fortinet automatizza gestione delle connessioni software defined e protezione di infrastrutture riducendo i costi aziendali**

Il cloud, per le imprese, è come il nettare per le api, perché dà opportunità di business, facilità di sviluppo e accelerazione del time to market, con grandi vantaggi rispetto al passato. Per questo, ci spiega Antonio Madoglio, Director Systems Engineering di Fortinet per l'Italia: «Le imprese per lanciare un nuovo servizio o rinnovare la manutenzione di un'applicazione, per prima cosa valutano la possibilità di erogare lo stesso servizio nel cloud».

Un'opportunità che «però nasconde molte insidie per quanto riguarda la gestione della sicurezza, a cominciare dal sapere chi accede a quel servizio/applicazione», evidenzia l'esperto di Fortinet, aggiungendo: «Il cloud service provider, normalmente, forniscono impostazioni per una sicurezza di primo livello, che non ha caratteristiche come quelle che le imprese impostano on premise».

## Un'infrastruttura tra le nuvole

A un basso di security si somma il tema del multcloud che complica molto la situazione, perché le aziende si trovano a dover gestire servizi ubicati presso luoghi e cloud provider differenti, il che, spesso, non facilita l'ottenimento di una visibilità end to end complessiva e per i Ciso (Chief Security Officer) è complicato dover interagire di volta in volta con diversi cloud service provider. Il risultato, conclude Magoglio: «è che il perimetro dell'azienda non è più quello delle mura di un castello protetto, ma si allarga tra le nuvole, impedendo la visione omni-comprendiva di tutta l'infrastruttura e quindi, anche per il Ciso o l'IT manager nelle aziende più piccole è difficile gestire e, soprattutto, dimostrare il livello di sicurezza e protezione della propria infrastruttura».

## La rete che rischia di imbrigliare il business

Altro tema caldo è quello delle reti SD-WAN, che ciascuno interpreta con un approccio diverso, ma, in sostanza, ci spiega l'esperto di Fortinet, consiste in uno strato software che astrae la gestione delle connessioni geografiche, siano esse su Internet o sul protocollo MPLS usato dalle grandi imprese. L'SD WAN permette di vedere le diverse connessioni a disposizione dell'azienda come se fossero un unico "tubo", anche se invece sono servizi proprietari e noleggiati presso diversi provider. Tutti questi insiemi di connettività possono essere astratti anche



Antonio Madoglio,  
Director Systems  
Engineering di Fortinet  
per l'Italia

a livello di gestione e di configurazione e visti come un unico link, che il software gestisce in modo trasparente per l'amministratore. Quest'ultimo deve solo definire delle regole che permettono di indirizzare al meglio il traffico aziendale. Per esempio possono esserci regole che indirizzano il traffico più pregiato per l'azienda sui link più veloci o su quelli più affidabili in termini di latenza, che, se alta, non rende intelleggibili le chiamate Voip. Tutto si complica se si considerano le dinamiche di sicurezza e non solo quelle di fruibilità delle applicazioni, perché si dovranno proteggere le connessioni dalle minacce provenienti da Internet.

### Un esempio concreto

Madoglio ci spiega in che senso occorre gestire le regole delle SD-WAN e l'uso del multicloud per ottimizzare la connessione, così modo da supportare nel modo più consono i vari servizi e perché una gestione unificata significa maggiore sicurezza, più efficacia e fa risparmiare molti costi.

Pensiamo, tenendo presente che per una media impresa cambia poco o nulla, a una grande azienda distribuita, con molte sedi sul territorio in Italia o all'estero, ciascuna con diverse connessioni, anche presso provider differenti.

Essendoci, come accennato, la propensione delle aziende a spostare i servizi nel cloud, possiamo immaginare un utente che deve accedere alla propria posta elettronica in cloud da una sede remota. La fruizione della posta non

avverrà attraverso la connessione che porta alla sede principale, perché il server è in cloud, quindi verrà utilizzata la connessione Internet locale. In questo caso, l'infrastruttura di SD-WAN e quella per la sicurezza, dovranno capire che quell'applicazione è la posta elettronica e, mentre la SD-WAN deve scegliere il cammino più consono, (che in questo caso sarebbe la connessione a Internet magari sul provider primario) al tempo stesso la struttura di sicurezza, deve proteggere la connessione dagli attacchi che arrivano tipicamente da Internet.

Si tratta di una situazione classica che richiede sia le capacità di una SD-WAN, cioè la capacità di scegliere il cammino migliore, sia le capacità di protezione, che è auspicabile siano quelle di sicurezza next generation firewall, cioè allo stato dell'arte.

Un modo per gestire i due processi è quello di realizzare in azienda centri specializzati NOC/SOC (Network Operation Center e Security Operation Center), come si è spesso fatto in passato. Ma queste strutture costano, ci spiega Madoglio, precisando: «Il costo della gestione nel day by day ha un forte impatto.

Tali centri prevedono reperibilità delle persone, risorse competenti, continua formazione, la gestione dell'evoluzione, cioè delle richieste del business, con applicazioni che nascono e muoiono ogni giorno. Quindi vanno gestite in modo dinamico le attività di configurazione dell'SD-WAN, della sicurezza e del cloud.

### Un tessuto per un vestito unificato su misura

Afferma Madoglio: «Il nostro approccio permette di avere una gestione unificata della security, come nell'esempio su descritto, e, più in generale, su situazioni che vedono le imprese avere soluzioni installate e gestite nel data center aziendale e sistemi e servizi acquistati in cloud. Che poi sia cloud singolo o multiplo, ibrido o privato poco importa, riusciamo comunque ad avere una gestione semplice dei diversi ambiti, pur in una situazione molto complessa». Lo strumento che Fortinet mette a disposizione delle imprese «per raggiungere quanto descritto da Madoglio è il Fortinet Security Fabric. Fabric, in inglese "tessuto", è il framework che, come un "tessuto di sicurezza", serve per «costruire un vestito cucito ad hoc per ogni cliente, cui dà visibilità sul traffico di rete e sulla situazione della sicurezza», spiega l'esperto, che aggiunge: «Quindi se un'applicazione è soggetta a un attacco, per esempio sul service provider 1, quello stesso attacco viene notificato alla console di gestione centralizzata che si attrezza per contrastare lo stesso attacco, anche su applicazioni ubicate presso altri provider».

Inoltre, conclude Madoglio, la facilità di gestione permette di definire una policy coerente con le policy di sicurezza aziendali e di attivarla in ogni ambiente, in modo trasparente rispetto all'ubicazione nell'infrastruttura e della situazione frastagliata che potrebbe presentarsi».



# Identificare gli incidenti di sicurezza del cloud

di  
Gaetano  
Di Blasio

## Dalla Cloud Security alliance le indicazioni per l'affidabilità del cloud

**L**a sicurezza del cloud è uno dei temi più dibattuti e la domanda da cui si parte generalmente è: «Fino a che punto i fornitori di servizi cloud possono essere considerati affidabili per proteggere i dati dei clienti, mantenere l'integrità e garantire che siano disponibili quando i clienti devono accedervi?».

Luca Bondimani, membro del Consiglio direttivo di AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica (aperta a chiunque abbia a che fare con la protezione dei dati e con la Privacy), evidenzia che l'ENISA (European Network and Information Security Agency) conteggia oltre 35 rischi del cloud con diverse probabilità di verificarsi e importanza d'impatto per l'organizzazione colpita.

Sette di questi rischi, per esempio, sono relativi alle politiche di utilizzo e all'organizzazione. Qui il rischio maggiore è quello del "block in", cioè la difficoltà o, nel caso peggiore l'impossibilità di trasferire i propri dati e/o applicazioni e servizi da un provider a un altro.

Un'altra tipologia di rischi riguarda la tecnologia: mentre in un cloud completamente

privato si può avere un controllo totale dei sistemi utilizzati, nelle altre soluzioni è possibile che l'infrastruttura utilizzata per fornire il servizio cloud sarà utilizzata, quindi acceduta, da molti utenti e da una vasta gamma di organizzazioni, incluse quelle concorrenti. Ciascun cliente, infatti, avrà le proprie macchine virtuali, queste gireranno su hardware comune, su una rete comune e useranno storage fisico condiviso.

Qui il rischio maggiore, evidenzia Bondimani, corrisponde nel non riuscire ad assicurare l'isolamento della struttura. L'esperto di AIPSI ricorda, per esempio, un caso del 2011, quando l'FBI sequestrò dei server "ospitati presso la società di Digital One. Su quei server si trovavano anche alcuni siti, estranei agli illeciti che avevano portato al sequestro, che scomparvero.

Altro esempio famoso, riporta Bondimani, è quello relativo alla violazione della PlayStation

Network di Sony: per l'attacco furono utilizzati server residenti nel cloud di Amazon che furono, almeno in parte, sequestrato (non è ancora chiaro come le forze dell'ordine possano coordinare il sequestro di tutti i server in una distribuzione globale, ammette il membro di AIPSI, che spiega: « Il cloud è una forma di outsourcing in cui il servizio è una merce, e i rischi non possono essere gestiti attraverso i tradizionali controlli di outsourcing. Di conseguenza, stabilire la sicurezza (che significa fiducia dei clienti) è diventata una sfida fondamentale per i fornitori di servizi Cloud».

Qui entra in gioco il lavoro della Cloud Security Alliance (CSA), che ha definito un insieme di controlli preposti a coprire la riservatezza e l'integrità delle informazioni memorizzate, elaborate e trasmesse dal sistema. L'efficacia dei controlli deve essere dimostrata attraverso valutazioni e audit.

✱



# Con Managed Endpoint Security la sicurezza si fruisce a consumo

Costi per la sicurezza predeterminati e flessibili con le soluzioni Endpoint Protection e Total Control Business a canone mensile di G DATA

**T**rasformare applicazioni in “SaaS” e i servizi di gestione del parco installato in “Managed Services”, è un approccio che permette di esternalizzare la complessità dell’IT ottimizzando Capex e Opex e che spinge sempre più spesso le aziende e i rivenditori specializzati di cui si avvalgono, a valutare nuove modalità di erogazione e fruizione dei servizi di sicurezza.

Servono però soluzioni che oltre a fornire flessibilità ed economicità possano integrarsi nell’infrastruttura esistente in modo trasparente e sicuro. È quello che ha realizzato G DATA con il rilascio di Managed Endpoint Security (MES), un servizio caratterizzato da una formula “a consumo” che risponde all’esigenza di abbattere gli investimenti e i costi operativi necessari per realizzare e mantenere un’adeguata tutela dell’infrastruttura IT.

Fondata nel 1985 a Bochum, G DATA è annoverata tra i principali fornitori di soluzioni per la sicurezza IT e sviluppa e commercializza soluzioni di sicurezza aderenti alle normative europee sulla protezione dei dati di aziende di qualsiasi ordine e grado, oltre ad applicazioni rivolte all’utenza consumer.

«Managed Endpoint Security permette alle aziende che non dispongono di uno staff dedicato alla sicurezza IT di non scendere a compromessi in termini di protezione e monitoraggio quotidiano della propria infrastruttura. La formula MES consente di affidare tale compito al proprio fornitore di servizi IT senza che lo stesso debba trovarsi presso l’azienda. Il servizio bilancia in modo ideale la convenienza e la comodità dei servizi gestiti e integra tutti i benefici delle soluzioni business di fascia alta di G DATA in un pacchetto “all-inclusive” fruibile sia da aziende che da partner», ha evidenziato Giulio Vada, Country Manager di G DATA per l’Italia.



Giulio Vada, Country Manager di G DATA per l’Italia

## Parco gestito con un click e costi trasparenti

La piattaforma MES (la cui versione tradizionale è disponibile a partire da 250 licenze) consente di gestire da una singola console centralizzata, ospitata nel proprio data center o nel cloud, l’intero parco installato. Aspetto chiave del servizio è che le funzioni centralizzate che permettono di configurare le policy e i filtri che si desidera applicare a singoli client, gruppi o all’intera azienda, la distribuzione



delle patch e il monitoraggio in tempo reale dello stato operativo dei sistemi, sono fornite in modo del tutto trasparente per quanto concerne i costi. Qualora si renda necessario aggiungere ulteriori client, l'operatore deve solamente inserire le nuove licenze nella sua dashboard per avviare il processo di fatturazione mensile.

Il processo automatizzato elimina l'eventuale rischio di overhead dovuto all'acquisto di licenze non necessarie in previsione di una crescita dell'azienda, o al contrario, di sottodimensionamento.

A tutela delle aziende che per fruire del servizio si rivolgono a un partner tecnologico, un aspetto chiave della piattaforma è che la console di gestione MES è nativa multitenant, garantisce quindi una netta separazione tra i diversi clienti serviti, consente di visualizzare report per ogni singola azienda gestita e di adottare misure di sicurezza e costi ad hoc per ciascuna di esse.

«Le organizzazioni che fruiscono

delle soluzioni G DATA Endpoint Protection e G DATA Total Control Business in modalità MES, beneficiano di una gestione professionale e quotidiana della sicurezza IT da parte del proprio fornitore e della serenità di avvalersi di suite dotate di tecnologie di nuova generazione per la tutela contro malware, ransomware, dirottamento di sessioni e transazioni bancarie, vulnerabilità ed exploit su qualsiasi client di rete, sia esso Windows, Mac, Linux, Android, iOS, il tutto in base al reale consumo», ha osservato Vada.

### **Il servizio MES disponibile su Azure**

Una recente espansione del servizio MES è la sua declinazione per Microsoft Azure, una piattaforma cloud sempre più diffusa tra aziende e professionisti. Con la versione Azure, G DATA consente a qualsiasi rivenditore di avvicinarsi al mondo della sicurezza gestita e ai Managed Service Provider con clienti di alto profilo, che già

fruiscono del cloud Microsoft, di beneficiare a loro volta della formula MES. Inoltre, con G DATA Managed Endpoint Security per Azure, il produttore rende fruibili i vantaggi della formula originale già a partire da un parco installato complessivo di sole 50 licenze.

Semplice la modalità di attivazione. Accedendo al G DATA Action Centre e acquistando la licenza per il management server multitenant, il sistema crea automaticamente il server virtuale su piattaforma Azure attraverso cui sono distribuite le applicazioni client sulle macchine da gestire, si configurano le policy e tutti i parametri per i diversi clienti seguiti dall'operatore.

«A differenza della formula MES tradizionale, che prevede l'attivazione o disattivazione delle licenze a consumo con cadenza mensile, con il G DATA MES powered by Azure il rivenditore può disattivare i servizi in tempo reale con un click. È una tutela aggiuntiva ideata per gli operatori di canale che desiderano abbattere quanto più possibile il proprio rischio economico affacciandosi a un nuovo mercato, indipendentemente dal tipo di clientela a cui erogano i propri servizi», ha commentato Vada.

La conformità alle nuove normative europee sulla protezione dei dati per applicazioni ospitate nel cloud è un ulteriore beneficio della suite MES powered by Azure. Questa è infatti ospitata nel nuovo data center Microsoft in Germania, progettato per soddisfare i rigorosi requisiti di protezione dei dati e certificazioni dell'Unione Europea: l'accesso fisico e logico

ai dati viene gestito esclusivamente da un Trustee tedesco. La stessa Microsoft non ha accesso alle informazioni che vi sono archiviate. Cura G DATA l'ha posta anche nel rendere semplice ed economica la fruizione del servizio MES powered by Azure, che include nel costo della licenza per utente anche il costo di Azure.

### Ampia scelta tecnologica e tutto incluso

In pratica, osserva Vada, l'offerta MES ha come presupposto fondamentale l'assenza di qualsiasi investimento economico a priori. Il fornitore di servizi di sicurezza gestita attiva il servizio e la

fatturazione in base alle effettive esigenze dei propri clienti e riceve le fatture solo a partire dal mese successivo. Una proposta che l'MS-SP può a sua volta valorizzare con ulteriori servizi a valore di proprio sviluppo in modo da creare un'offerta ancor più interessante.

Ampie le modalità di utilizzo sotto il profilo tecnologico. Il Managed Service Provider può erogare i servizi sottoscritti tramite una propria infrastruttura, oppure può appoggiarsi a data center esterni, così come può optare per l'offerta MES powered by Azure e fruire dell'infrastruttura messa a disposizione da Microsoft.

«Un concreto beneficio di MES

powered by Azure è che permette di controllare in maniera dettagliata il servizio senza la necessità di accedere alla piattaforma Azure. Tramite i wizard del nostro portale web GDATA Action Center, è possibile creare, installare ed attivare il workload necessario per l'infrastruttura da dedicare ai propri clienti. Il partner può creare la sua server farm virtuale e tramite essa abilitare e disabilitare servizi, controllare l'andamento della fatturazione delle licenze, abilitare e disabilitare clienti e intervenire capillarmente su ogni aspetto del servizio erogato», ha evidenziato il country manager di G DATA. \*



# DE gustare

alla scoperta dei sapori d'Italia

**giornalisti, enologi, chef, nutrizionisti, esperti alimentari vi promettono un'esperienza nuova**

[www.de-gustare.it](http://www.de-gustare.it)



# Dati e ambienti industriali al sicuro con la behavior analysis

Le soluzioni Stormshield per la protezione di cloud, device e ambienti produttivi fanno leva sull'analisi comportamentale e garantiscono un ambiente di lavoro protetto e sicuro

**S**tormshield è un brand del gruppo Airbus Defence and Space e sviluppa soluzioni per la cyber security, sia per ambienti office sia per ambienti di fabbrica in evoluzione verso l'Industry 4.0. La qualità delle soluzioni di cyber security e la loro rispondenza alle esigenze di mercato, ha osservato Alberto Brera, country manager Italia, è testimoniata dalle centinaia di migliaia di sue soluzioni installate nella sola Europa.

Come parte di un grande gruppo europeo con oltre 170.000 dipendenti, per le sue soluzioni pone particolare attenzione alle certificazioni europee, a cui si aggiungono quelle di stati quali USA, Russia e Cina. Attenzione che le ha permesso di ottenere per i suoi prodotti certificazioni di rilievo quali la EU Restricted, la NATO Restricted o la ANSSI EAL 4+.

## Reti protette on-premise e nel cloud

Cloud e mobility sono due dei paradigmi che hanno fatto svanire i confini aziendali e richiedono nuove soluzioni per la sicurezza di reti, sistemi IT o end point, siano essi tablet, notebook o smartphone.



Alberto Brera, country manager Italia di Stormshield

Per quanto concerne le infrastrutture di rete la soluzione nel portfolio Stormshield, evidenzia Brera, è costituita dalla linea di appliance SNS (Stormshield Network Security), costituita da dispositivi di firewalling per la prevenzione delle intrusioni (IPS) che, in linea con la progressiva virtualizzazione dell'IT, sono disponibili sia in versione fisica sia come istanza virtuale.

Nella interpretazione virtuale, che presenta le medesime funzionalità di quella fisica, è una soluzione particolarmente adatta per installazione in cloud pubblico o privato o per il controllo dei

perimetri aziendali virtuali. Sempre nell'interpretazione virtuale le soluzioni Stormshield possono essere installate come software in ambienti Microsoft, VMware o Citrix, con inoltre la possibilità di poterle acquisire, nell'ambito di migrazione dell'IT a un cloud pubblico, direttamente da provider quali Microsoft Azure o AWS.

«Quello che contraddistingue i dispositivi SNS è il loro funzionamento. Non si basano sul riconoscimento delle firme che caratterizzano gli attacchi, un approccio reattivo che appesantisce il funzionamento e non garantisce la protezione, ma su un motore di analisi comportamentale dell'infrastruttura da proteggere che rileva comportamenti anomali e non conformi e li blocca sul nascere» ha evidenziato Brera.

La linea di firewall comprende anche soluzioni specifiche per la protezione di ambienti industriali quali quelli SCADA. Sono soluzioni hardware robuste agganciabili alle barre DIN, con alimentazione a 48 Volt e con il supporto di range estesi di temperatura, umidità, vibrazione e campi elettromagnetici. «Una peculiarità molto gradita in ambito SCADA è che le soluzioni interpretano tutti e 12 i protocolli standard per ambienti SCADA. Siamo quindi in grado di rendere disponibili a chi programma le policy di sicurezza dei registri i contenuti dei protocolli in modo da creare delle finestre di funzionamento per bloccare gli eventi con parametri non congrui con tali policy, ad esempio un comando che

blocchi le ventole di un apparato in funzione» ha spiegato Brera.

### Con SDS dati al sicuro e sotto chiave

Connesso al cloud è anche il problema del come garantire la sicurezza dei dati, un tema affrontato da Stormshield con la sua piattaforma SDS (Stormshield Data Security), costituita da soluzioni di classe Enterprise per la protezione dei dati tramite la loro robusta criptazione a standard DES256.

Stormshield Data Security permette di creare un ambito aziendale all'interno del quale i membri di un team, dislocati anche in luoghi diversi, possono collaborare e condividere dati in modo trusted, sia che li scambino su cloud sia tramite un server remoto. La soluzione provvede a criptare e a decriptare i dati ogni volta che sono ricevuti o inviati in rete, con l'intero processo di protezione che avviene in modo trasparente per l'utente.

In pratica, osserva Brera, viene risolta la criticità del punto debole della catena costituito dal fattore umano. Nel caso i dati fossero esportati in modo non corretto, risulterebbe in ogni caso impossibile risalire al loro reale significato. SDS costituisce quindi una soluzione di "data leakage protection" che garantisce la riservatezza dei dati e permette in quanto tale di ottemperare anche a quanto previsto dal GDPR.

### Sicurezza end-point basata sul comportamento

Una terza linea di soluzioni per la protezione aziendale è la

Stormshield Endpoint Security (SES), una piattaforma client-server costituita da un software da installare su un server centrale e da software per dispositivi portatili.

La soluzione permette l'hardening dei sistemi operativi degli end-point in termini di sicurezza e non richiede che il dispositivo su cui è installata sia dotato di connettività a Internet o al cloud o a una rete pubblica per funzionare correttamente, come invece avviene per altre soluzioni di sicurezza. Questo perché SES si avvale esclusivamente dell'analisi comportamentale monitorando la legittimità di tutte le chiamate a sistema, e, in quanto tale, oltre a poter operare come protezione in ambienti chiusi quali quelli industriali SCADA, è in grado di rilevare attacchi non a semplice livello di exploit (ad esempio il classico virus) ma a livello di vulnerabilità globale.

«Gli usuali sistemi di rilevazione degli attacchi puntano essenzialmente a individuare i virus tramite le loro firme. Il problema è che una vulnerabilità presente in un sistema può essere sfruttata da centinaia di virus diversi e difficili da individuare e bloccare tutti in modo tempestivo. SES permette invece di chiudere la vulnerabilità risolvendo di fatto il problema alla radice. Si tratta inoltre di una protezione dinamica che tiene conto dell'ambiente di utilizzo di un dispositivo, aumentando automaticamente le difese se sono all'esterno del perimetro aziendale e allentandole se sono al suo interno», osserva Brera. \*

# Armonizzare IT, sicurezza e policy compliance... con un pizzico di cloud

La piattaforma cloud di Qualys permette di valutare lo stato della sicurezza e della conformità dell'azienda, identificare le risorse compromesse e ridurre l'Opex

**S**toricamente, IT e sicurezza nelle aziende non sono mai stati grandi amici. La crescente sofisticazione di attacchi e il diffondersi di data breach ha portato il Legislatore a emettere regole e linee guida, alcune delle quali soggette a sanzioni per assicurarne il rigoroso rispetto, come il GDPR. La recente tendenza all'adozione massiva di ambienti di sviluppo e operation basati su cloud ha certamente aggiunto complessità e opacità a questo quadro, riducendo la visibilità e il conseguente livello di sicurezza di un perimetro talmente elastico da non meritare più nemmeno di essere chiamato tale. Come combinare le molte difficoltà e i conflitti di interessi che la situazione appena descritta comporta? Come unire compliance e controlli di security identificando le affinità elettive, senza creare o esacerbare i conflitti tra i responsabili IT, security e compliance? Alcuni suggerimenti li offre Marco Rottigni, CTSO di Qualys per l'area EMEA, azienda tra i leader nelle soluzioni di sicurezza e conformità basate sul cloud che consentono di assicurare visibilità, sicurezza end-to-end e compliance per le risorse IT.



Marco Rottigni, CTSO di Qualys per l'area EMEA

## Il denominatore comune

Le necessità di IT, security e compliance hanno un minimo comune denominatore: l'accesso a informazioni che sono per la maggior parte le stesse, solo viste da utenti e prospettive molto diversi. In passato i fornitori di soluzioni di sicurezza hanno fatto sforzi importanti per fornire soluzioni puntuali e locali che rispondessero a queste esigenze; ciò ha portato all'adozione di una pila importante di tecnologie, che però generano una quantità ancora più importante di allarmi, informazioni, log, console di amministrazione e così via.

Uno dei concetti fondanti, evidenzia Rottigni, è stata l'elaborazione centralizzata dei dati raccolti da una varietà di sensori, che avrebbe prodotto una visibilità adeguata, un'aggregazione adeguata dei dati per diverse

tipologie di utenti, una velocità di risposta adeguata nell'interrogazione di questi dati. Questo paradigma all'inizio si chiamava "on demand computing", mentre oggi si è evoluto verso un concetto moderno e innovativo di "cloud based

computing" e tale visione si combina bene con un processo IT tipico di un numero sempre crescente di aziende chiamato Digital Transformation, spesso abbreviata in DX. Ci sono molte definizioni possibili di DX, tutte semplificabili in:

“adozione delle più moderne tecnologie e best practice per digitalizzare tutti i processi di business e non, sia interni che esterni di un'azienda e dei propri business partner”.

In questo processo di trasformazione la sicurezza non può essere posta in secondo piano o implementata a posteriori, ma l'agilità, la flessibilità e la velocità della DX rappresentano ostacoli spesso importanti per la security, tipicamente fondata su analisi, esame forense, rilevamento preciso e altri termini che suonano quasi come un ossimoro se combinati con le caratteristiche di una DX.

In sostanza, quello che appare necessario è comprendere a fondo gli aspetti IT della DX (inclusi gli ambienti cloud), gli aspetti di security della DX (inclusi gli ambienti cloud) e non ultimi gli aspetti di compliance della DX (inclusi gli ambienti cloud).

«Qualys ha deciso di dedicare gruppi di ricerca e sviluppo e risorse di product management ad ognuna di queste aree, di stringere partnership con molti clienti per capire meglio i casi utente da una prospettiva di business, tecnica e di processo. Questo ci ha fornito la giusta prospettiva per sviluppare un insieme di cloud App a indirizzare le esigenze illustrate nel modo migliore. Non ultimo, ci ha dato la visibilità necessaria su trilioni di eventi, di scansioni IP, di metadati e informazioni per aiutare i nostri clienti ad ottenere il meglio da questi big data, nel massimo rispetto della privacy», ha osservato Rottigni. ❁

## Qualys Cloud Platform

La vision per la sicurezza di Qualys si è concretizzata nella Qualys Cloud Platform, una soluzione che ha come obiettivo primario quello di consentire la valutazione costante dello stato globale di sicurezza e di conformità dell'azienda, l'identificazione delle risorse compromesse, la messa in sicurezza del processo di Digital Transformation e di ridurre sensibilmente i costi. La soluzione include 18 App, che condividono in modo nativo i dati acquisiti per l'analisi e la correlazione in tempo reale, distinte per:

- **Gestione delle risorse:** È un insieme di App che comprende l'Asset Inventory, volto a garantire una estesa visibilità delle risorse IT distribuite in ambienti ibridi, e il CMDB Sync, che sincronizza le risorse nel database delle configurazioni. La Cloud App Container Security consente inoltre di monitorare la sicurezza dei container, partendo dall'interno dei cicli DevOps fino alle implementazioni applicative.
- **Sicurezza IT:** Comprende il Vulnerability Management per il rilevamento e la protezione contro gli attacchi e i moduli Threat Protection e Continuous Monitoring, che consentono di localizzare le minacce critiche e prevedono avvisi in tempo reale sulle irregolarità di rete.
- **Sicurezza delle applicazioni web:** Del set fa parte la Web Application Scanning, volta ad assicurare la protezione end-to-end delle applicazioni web, e il Web Application Firewall, che prevede il blocco degli attacchi e relativa applicazione virtuale delle patch per le vulnerabilità delle applicazioni web.
- **Monitoraggio della conformità:** Comprende i moduli Policy Compliance e PCI Compliance per la valutazione, l'automazione e il conseguimento delle configurazioni richieste per essere conforme alle normative. A questi si aggiungono i moduli Security Configuration Assessment per la valutazione automatica delle configurazioni delle risorse globali e il Security Assessment Questionnaire, per ridurre la gestione del rischio dei fornitori.

