

# DIRECTION Reportec 94

SOLUZIONI SERVIZI E TECNOLOGIE ICT

## LA MOBILITY AL CENTRO DELLA DIGITAL TRANSFORMATION

### TECHNOLOGY

IBM Cognitive Systems,  
intelligenza artificiale nel data center

Lenovo protagonista nella  
Digital Transformation

### INTERVIEW

I vantaggi dell'IOT

### TRENDS & MARKET

Investire nel digitale per  
sopravvivere alla concorrenza

### CASE HISTORY

Microsoft House: ispirata  
dalle logiche di smart working

### SPECIALE

Threat prevention, intelligence e resilienza

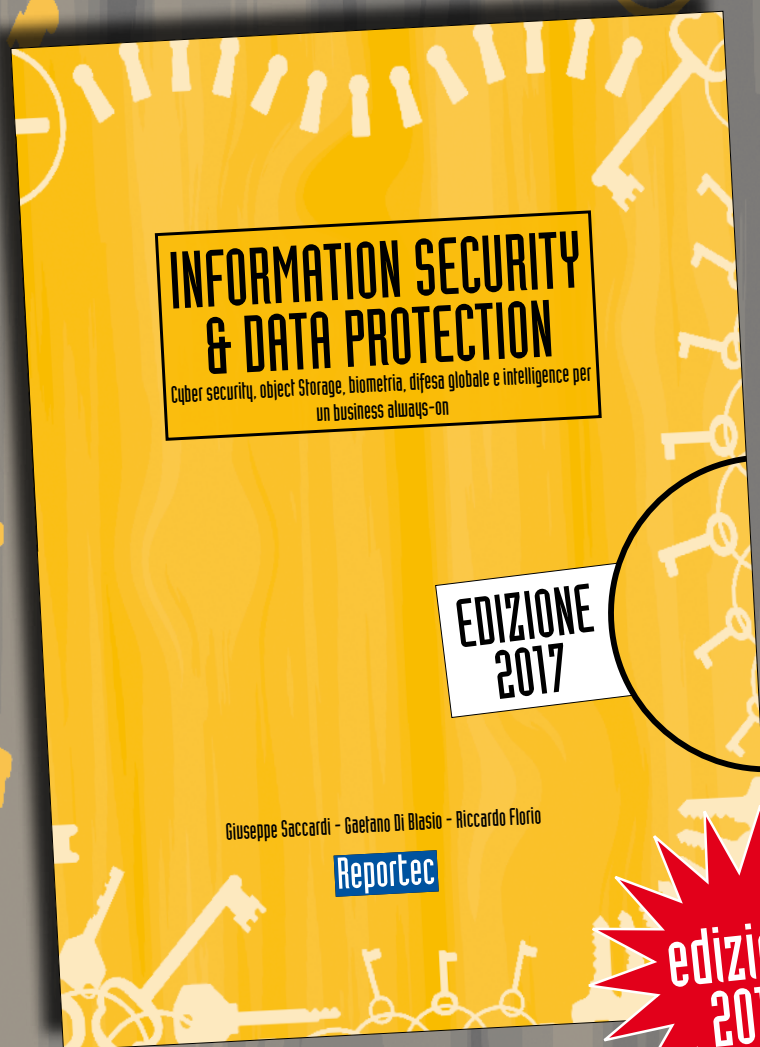
### CYBER ATTACK

La sicurezza è la prima preoccupazione del cloud  
F5: l'Application Security al centro della protezione

### SOLUZIONI

HPE Security Arcsight:  
"intelligence" di sicurezza alla massima velocità

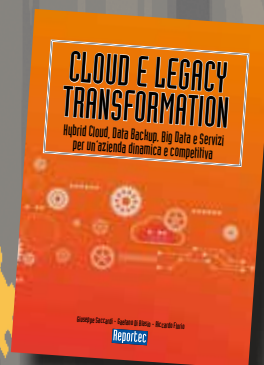
# È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



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 48 euro (più IVA 22%) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

Direction Reportec  
 anno XV - numero 94  
 mensile gennaio-febbraio 2017

Direttore responsabile: Riccardo Florio  
 In redazione: Giuseppe Saccardi,  
 Gaetano Di Blasio, Paola Saccardi,  
 Daniela Schicchi  
 Ha collaborato: Gian Carlo Lanzetti  
 Grafica: Aimone Bolliger  
 Immagini da: Dreamstime.com

Redazione:  
 via Marco Aurelio, 8 - 20127 Milano  
 Tel 0236580441 - fax 0236580444  
 www.reportec.it  
 redazione@reportec.it

Stampa:  
 A.G. Printing Srl, via Milano 3/5  
 20068 Peschiera Borromeo (MI)

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

Presidente del C.d.A.: Giuseppe Saccardi  
 Iscrizione al tribunale di Milano  
 n° 212 del 31 marzo 2003  
 Diffusione (cartaceo ed elettronico)  
 12.000 copie

Tutti i diritti sono riservati;  
 Tutti i marchi sono registrati e di proprietà  
 delle relative società.

FOCUS ON

<b>La digital transformation passa per la Mobility</b>	<b>4</b>
<b>VMware rafforza la gestione della mobilità</b>	<b>9</b>
<b>Huawei X Labs: il futuro della ricerca mobile</b>	<b>10</b>
<b>ToughBook e ToughPad: nuovi modelli 2-in-1</b>	<b>12</b>
<b>Il pc 2-in-1 di HP per chi lavora in mobilità</b>	<b>14</b>

INTERVIEW

<b>I vantaggi dell'IoT</b>	<b>16</b>
----------------------------	-----------

TECHNOLOGY

<b>Emerson Network Power ora è Vertiv e si prepara a nuove sfide</b>	<b>18</b>
<b>IBM Cognitive Systems, intelligenza artificiale nel data center</b>	<b>20</b>
<b>Lenovo: protagonista nella Digital Transformation</b>	<b>23</b>
<b>Nasce Delinda, e-commerce beauty che vuol fare la differenza</b>	<b>32</b>
<b>Lexmark porta il document management alla PMI</b>	<b>34</b>
<b>NetApp: i trend per l'IT in trasformazione</b>	<b>36</b>

CASE HISTORY

<b>Microsoft House: ispirata dalle logiche di smart working</b>	<b>27</b>
<b>Fincantieri rinnova il modo di progettare navi con IBM Cloud</b>	<b>30</b>

TREND

<b>Investire nel digitale per sopravvivere alla concorrenza</b>	<b>39</b>
---	-----------

**La Mobility si conferma uno dei più dibattuti e solidi paradigmi dell'attuale momento evolutivo dell'ICT. La trasformazione digitale che stanno affrontando le aziende e la società nel suo complesso, nella sua essenza, si basa in buona parte sulla crescente mobilità di beni materiali e persone fisiche, nell'ambito di un processo volto nella sua globalità a ottimizzare i processi di business, a ridurre Capex e Opex e a facilitare la collaborazione e la comunicazione tra dipendenti e tra questi e i clienti.**



**La digital transformation passa per la Mobility**



**U**n ruolo fondamentale nell'evoluzione verso il digitale lo giocano, oltre ad aspetti organizzativi, le tecnologie che favoriscono la mobility e i dispositivi di utente, insieme a quanto correlato in termini di gestione e sicurezza. Vediamo di approfondire i diversi aspetti che intervengono quando si parla di mobilità della forza lavoro di un'azienda.

### **I fattori tecnologici della Mobility**

I fattori tecnologici coinvolti nel processo di trasformazione di un'azienda in chiave mobile giocano naturalmente un ruolo primario nella sfida per una maggior e proficua mobilità aziendale e di business. L'importanza di strumenti di ultima generazione e pensati specificatamente e in modo nativo per il business, dal tablet al portatile allo smartphone, costituisce un fattore primario nella sua positiva accettazione in azienda e lo è soprattutto per assicurare alle ultime generazioni che entrano nel mondo del lavoro, quelle riferite come native digitali, quella qualità e indipendenza nel modo di lavorare che hanno ampiamente sperimentato e metabolizzato con i dispositivi consumer, non di rado più all'avanguardia di quelli in uso nelle aziende. Il problema posto dalle nuove generazioni di worker nativi digitali è di importanza critica per le aziende che vogliono attrarre giovani la cui creatività apporti un reale beneficio e riuscire a trattenerli una volta che sono stati formati.

Se la qualità dei dispositivi è importante per garantire il successo di una trasformazione in chiave digitale e mobile di un'azienda, parimenti lo è il farlo in sicurezza. Qui il punto è più dolente perché mentre le generazioni "più datate" sono abbastanza attente, meno lo sono quelle più recenti abituate a navigare su Internet e a chattare.

Quando si parla di ambienti mobili di tipo business la sicurezza non è però una opzione che può essere fruita o meno a piacere, ma è un obbligo di legge e ancor prima è un modo per garantire che il patrimonio aziendale non venga intaccato mediante il trafugamento di informazioni riservate o che se divulgate possono causare un serio d'anno al brand ancor prima che economico. La sicurezza, allo stato attuale della evoluzione del settore, può basarsi su una serie di strumenti fortemente progressivi che vanno dai più semplici software on board per il controllo dell'accesso sino alla verifica biometrica dell'utilizzatore, o a policy che permettano l'uso del dispositivo solamente in certi momenti, che controllino il tipo di applicazioni fruito, sino al virtual desktop che facendo risiedere il controllo dell'accesso e i dati su un sistema centrale permette di applicare politiche forti che possono comprendere anche la robusta cifratura dei dati, che è molto utile anche per l'invio e la ricezione di informazioni quando si opera tramite reti pubbliche o il cloud.

## Il cloud e le reti di trasporto

Un ruolo primario e lo status di efficace abilitatore alla diffusione di dispositivi mobili lo hanno le reti di nuova generazione e il cloud, che in definitiva, non sono altro che una rete che nel caso di ambienti pubblici è di tipo aperto (e cioè condiviso) e sta via via sostituendo, o meglio, sovrapponendosi, alle reti a pacchetto tradizionali aggiungendovi uno strato di virtualizzazione molto spinto derivato dalla diffusione del Software Defined Networking.

Nella mobility la qualità della rete gioca un ruolo primario perché deve garantire quella immediatezza nella cooperazione e collaborazione tra corrispondenti con caratteristiche e un feeling che non deve essere molto dissimile da quanto si sperimenta operando dal proprio desktop connessi a reti locali dalle decine e centinaia di megabit.

Le reti di quarta e quinta generazione che si affacciano all'orizzonte hanno proprio questo obiettivo, quello di abbattere le barriere e le differenze ancora esistenti tra reti fisse e mobili. Che poi questo avvenga e in che tempi, e soprattutto su che aree e con che costi del servizio, è da vedersi. Intanto un aiuto sta venendo dalla diffusione e dalla modernizzazione delle reti di operatore e di quelle dei service provider, che stanno procedendo alla sostituzione sia degli apparati di backbone al fine di assicurare maggior banda agli utenti o ad operatori locali. Oltre al backbone

numerosi sono gli operatori che stanno anche rinnovando lo strato di accesso con dispositivi periferici (quelli riferiti come CPE o virtual CPE nella loro interpretazione più recente) che permettono di garantire un'elevata flessibilità nell'erogazione delle applicazioni e minor costi di esercizio, oltre a un miglior controllo della rete e della qualità del servizio erogato.

Siccome a queste dorsali fisse, generalmente in fibra ottica, e allo strato di accesso fa riferimento la distribuzione locale di servizi a dispositivi mobili, la qualità di questa parte dell'infrastruttura diventa essenziale sia per garantire la qualità richiesta per un servizio business sia per la diffusione territoriale capillare di un servizio.

### **Gestire la mobilità**

Un aspetto non meno importante quando si parla di dispositivi mobili, o meglio, di flotte di dispositivi, è quello della loro gestione, soprattutto quando ci si muove in uno scenario di dispositivi di tipo BYOD.

La diffusione di soluzioni di virtual desktop permette indubbiamente di centralizzare il controllo dei dispositivi, consentirne l'uso solo a chi è effettivamente autorizzato, applicare policy non solo di sicurezza ma anche relative all'allineamento immediato ed omogeneo delle versioni delle applicazioni, e l'accesso controllato ai silos informativi. Si tratta tuttavia di una realtà che copre solo una ridotta parte dei casi che, il più delle volte,





# VMware rafforza la gestione della mobilità

## Novità per AirWatch Unified Endpoint Management e nuovi servizi disponibili

**V**Mware ha annunciato una serie di novità rela-

tive ad AirWatch Unified Endpoint Management (UEM), la soluzione software che consente di unificare Mobile and Desktop Management, pensata per migliorare l'esperienza lavorativa, aumentare la sicurezza e ridurre i costi e la complessità della gestione degli endpoint rispetto ai metodi tradizionali. Le novità riguardano il supporto esteso per Windows 10, con nuove funzionalità per controlli granulari di aggiornamento del sistema operativo, un nuovo cruscotto per avere visibilità in tempo reale delle patch installate e l'integrazione con Windows Store for Business per accedere più facilmente alle licenze on-line. Grazie a una più stretta integrazione di Google Play AirWatch Unified Endpoint Management contribuirà a rafforzare l'adozione di Android in azienda, favorendo la distribuzione delle applicazioni, l'automazione delle autorizzazioni e delle configurazioni per gli utenti finali. La soluzione AirWatch



La console di AirWatch UEM

si integrerà con VMware TrustPoint per migliorare ulteriormente la sicurezza degli endpoint in ambiente Windows, così da automatizzare il rilevamento delle minacce e le azioni di ripristino dinamico su dispositivi compromessi. Infine è stato introdotto un

nuovo motore di regole che consente di automatizzare le azioni a distanza indirizzato per dispositivi specializzati utilizzati nei depositi, negli impianti di produzione, nelle piattaforme petrolifere e negli ospedali che utilizzano endpoint "rugged".

VMware ha anche annunciato la disponibilità dei VMware AirWatch Mobility Services come servizio gestito attraverso il Programma VMware vCloud Air Network per consentire ai Communications Service Provider (CSP) di fornire servizi differenziati, a valore aggiunto. Questa iniziativa mette a disposizione dei CSP la soluzione chiavi in mano di Enterprise Mobility Management AirWatch, che permette la gestione di dispositivi aziendali, dei modelli BYOD e dei dispositivi line-of-business, compresi i pc in ambiente Windows 10: tutto ciò senza doversi dotare di una propria infrastruttura applicativa EMM. ✱

# Huawei X Labs: il futuro della ricerca mobile



**H**uawei con i suoi "X Labs" sale in cattedra e indica le direzioni da dare alla ricerca sui modelli di collaborazione e la fornitura di risorse in ambito mobile. I laboratori X Labs, creati nel 2016, si propongono di fornire una piattaforma di innovazione aperta e promuovere la comunicazione e la collaborazione integrata all'interno di un ecosistema intersettoriale. Quattro le aree strategiche individuate da Huawei, in aree apparentemente sorprendenti, in base al presupposto che, in futuro, tutti i servizi saranno fruibili attraverso applicazioni mobili e questo creerà nuove e numerose opportunità di sviluppo nell'ambito video, delle soluzioni smart per abitazioni e di specifici settori verticali.

La prima area è quella dei droni connessi, poiché questi dispositivi svolgono un ruolo sempre più importante in diversi settori tra cui la logistica, la sicurezza e i media e Huawei ritiene che sarà essenziale approfondire la ricerca sull'uso di reti wireless per regolare in modo efficace i voli di aerei senza pilota e gestire attività automatizzate da remoto.



**Nel corso del Mobile World Congress 2017 il vendor delinea le aree cruciali di sviluppo tecnologico in ambito mobile**



Il progressivo passaggio su cloud di servizi e contenuti legati alla Realtà virtuale e aumentata dovrà mettere in guardia gli operatori di telefonia mobile che si devono preparare, secondo Huawei, ad affrontare questo cambiamento.

Il terzo tema è quello della robotica wireless ovvero delle connessioni wireless tra robot intelligenti nelle fabbriche che costituiscono un fattore chiave dei modelli Industry 4.0 e della produzione "intelligente" del futuro. Anche il settore dei robot per la casa rappresenta un'area in

crescita, soprattutto in vista del progressivo invecchiamento della popolazione e dell'aumento dei consumi.

La quarta direzione di sviluppo della ricerca riguarda i veicoli connessi. Sfruttando le reti mobili di ultima generazione, X Labs si concentrerà sulla connettività di piattaforme per veicoli connessi, sulla possibilità di questi oggetti di comunicare tra loro e su uno sviluppo concreto della loro capacità di analisi, con l'obiettivo di sviluppare di soluzioni end-to-end che creeranno nuove opportunità di business sia per il settore automobilistico che per l'ICT. ✱



# ToughBook e ToughPad: nuovi modelli 2-in-1

La famiglia di dispositivi 2-in-1 di Panasonic per la forza lavoro mobile si arricchisce del modello fully rugged CF-33 e del semi rugged FZ-Q2. Punti di forza l'elevata affidabilità e la personalizzazione.

**F**esteggia 20 anni la gamma di notebook "rinforzati" ToughBook/ToughPad, una delle famiglie di prodotti di riferimento all'interno della divisione AVC Network di Panasonic che contribuisce per il 14% alle vendite complessive della multinazionale nipponica. Un compleanno segnato dall'annuncio di due nuovi modelli che saranno disponibili sul mercato italiano a partire da maggio 2017.

## ToughBook CF-33



Il primo dei due è il ToughBook CF-33, un dispositivo "fully rugged" caratterizzato da un fattore di forma "detachable" 2-in-1 con la possibilità di distaccare dalla tastiera il display touch screen da 12 pollici, con ri-

soluzione QHD (2160 × 1440) e caratteristiche di anti-riflesso e alta luminosità (fino a 1200 cd/m<sup>2</sup>) che lo rendono ottimale per la visualizzazione all'aperto. Questo modello rappresenta il successore del CF-31 che resterà in commercio ancora per almeno un anno. Come è nella tradizione di questi dispositivi, il CF-33 dispone delle più stringenti certificazioni in merito a robustezza e affidabilità: resistenza a cadute da 120 cm grazie alla scocca in magnesio, alla polvere e all'acqua intesa come pioggia forte (non immersione ma, peraltro, è difficile immaginare un utilizzo subacqueo).

Il nuovo ToughBook rappresenta il primo pc "detachable" di tipo "fully rugged" ed è pensato per adattarsi alle differenti tipologie di lavoro.

Dispone del sistema operativo Windows 10 Professional ed è dotato di un processore Intel Core i5-7300U vPro, 3 porte USB 3, 1 porta USB 2.0, con 8 Giga-byte di RAM e un disco a stato solido

(SSD) da 256 Gigabyte. Il peso di 2,76 Kg (1,53 kg in modalità tablet), considerando le caratteristiche di robustezza, è da considerare molto contenuto.

Il punto di forza di questi notebook è l'estrema flessibilità offerta dalle innumerevoli opzioni di personalizzazione che Panasonic mette a disposizione. Il CF-33 è, infatti, progettato per poter installare lettori di codice a barre, porta seriale nativa (ancora utilizzatissima per il collegamento di strumenti industriali), lettore di smart card (anche di tipo contactless), lettore di impronte digitali, GPS dedicato, scheda di rete wireless WAN con GPS, fotocamera posteriore da 8 Megapixel (in aggiunta a quella frontale standard da 2 Megapixel). Inoltre permette di alloggiare due batterie per consentire un'autonomia fino a 10 ore, che salgono a 11 ore quando viene utilizzato nella modalità separata dalla tastiera. Il touch screen è stato pensato per operare in modo efficiente anche in condizioni estreme come, per esempio, in situazioni di pioggia intensa. Disponibile anche un replicatore di porte per abbinare l'attività sul campo a quella d'ufficio.

### **Panasonic ToughPad FZ-Q2**

Il secondo modello annunciato da Panasonic è il ToughPad FZ-Q2, che rappresenta la quarta generazione della serie FZ.

Si tratta di un dispositivo semi rugged 2-in-1 con schermo staccabile, leggermente più pesante di un notebook consumer (complessivamente

1,93 Kg, mentre la componente display separata pesa 1,09 Kg) ma con caratteristiche di robustezza molto superiori. È fornito con sistema operativo Windows 10 Pro, ma offre la possibilità di effettuare il downgrade a Windows 7 Professional, per le situazioni in cui è necessario garantire la compatibilità certificata con software preesistenti. Disponibile con opzione 4G e munito di processore è Intel m5-6Y57 vPro, il Panasonic ToughPad FZ-Q2 prevede uno schermo "detachable" IPS multi-touch da 12,5 pollici di diagonale, con risoluzione Full-HD (1920x1080) e ad alta luminosità. È certificato per resistere a cadute da 76 centimetri (lo standard europeo di altezza per le scrivanie da ufficio) e offre innumerevoli opzioni di personalizzazione, inclusa la possibilità di integrare un lettore di smart card (anche contactless).

Progettato per l'uso in movimento, il nuovo dispositivo 2-in-1 è dotato di una maniglia che può anche essere utilizzata per impugnarlo con una mano. Inoltre, è possibile utilizzare un "hand-strap" opzionale con rotazione a 360 gradi per facilitare il lavoro con

il tablet in modalità verticale o orizzontale. Non è ancora stato definito il prezzo ufficiale italiano, ma per la versione standard del ToughBook CF-33 dovrebbe aggirarsi attorno a 3400 Euro mentre per il ToughPad FZ-Q2 a poco meno di 2000 Euro. ✱





Interessanti le funzionalità di sicurezza che includono un lettore di smart card integrato, un disco SSD estraibile, la suite per la protezione dei dati HP Client Security Suite Gen3 e la disponibilità opzionale di un lettore di impronte digitali e del sensore Near Field Communications.

La presenza di una cover rimovibile, di un cavalletto e la possibilità di una manutenzione aziendale per il pannello del display rispondono alle esigenze di un utilizzo prettamente aziendale su un ciclo di vita suggerito da HP compreso tra 3 e 5 anni.

Questo pc è attualmente disponibile in differenti configurazioni con processori Intel di settima generazione, con prezzi a partire da € 899.

«Oggi oltre il 60% dei Millennial lavora da più posti differenti - ha osservato Benoit Bonnafy, vice president, Business Personal Systems EMEA, HP Inc. - ed entro il 2020 questa categoria demografica rappresenterà la maggioranza della forza lavoro. Vogliono dispositivi mobili dal design accattivante, che rispondano al loro stile di lavoro in mobilità, e i responsabili IT delle aziende hanno bisogno che questi dispositivi siano gestibili e sicuri. Solo HP sta riuscendo a unire questi form factor innovativi a funzionalità di sicurezza e gestione dei flussi di lavoro verticali integrate, con un Total Cost of Ownership ridotto».

HP Pro x2 612 G2

## Accessori per lavorare in mobilità



Per i propri dispositivi delle serie x2 e x3 HP ha recentemente rilasciato i seguenti accessori pensati per supportare i professionisti in mobilità.

- HP Elite x3 Mobile Scanning Solution: un lettore di codice a barre integrato adatto per l'healthcare e il retail, utilizzabile per controllare i prezzi, accedere all'inventario e alle informazioni del sistema CRM direttamente dal palmo della mano.
- HP Pro x2 612 G2 Rugged Case: un "case" di protezione che consente di utilizzare il pc in ambienti di lavoro estremi, dotato di cinturino girevole a 360 gradi, tracolla, portastilo e porta spine opzionale.
- HP Elite USB-C Dock: la dock station per trasformare il proprio dispositivo HP in un desktop e collegarlo a display e dispositivi esterni mentre è in carica.
- HP MX12 Retail Solution: combina il Pro x2 con l'HP Retail Case 12 per creare una soluzione portatile che consenta di vendere ed effettuare transazioni in mobilità sul punto vendita. Collegando la soluzione mobile all'HP Retail Expansion Dock per Pro x2, questa funziona come un tradizionale sistema POS.
- HP USB-C Travel Hub: per disporre di connettività "pass-through" per il display e i dispositivi USB e la ricarica per il Pro x2, l'Elite x2 o l'Elite x3 mentre il pc viene usato. ❁

# I vantaggi dell'IoT

**P**aolo Valcher è il direttore della divisione Software Asset Management e Tutela Diritto d'Autore di Microsoft che ha recentemente assunto la carica di presidente del Comitato italiano di BSA | The Software Alliance, l'organizzazione multi-vendor nata per favorire la Digital Transformation e sviluppare relazioni istituzionali e allinearle con le aree d'intervento della Pubblica Amministrazione, delle istituzioni e delle aziende software membri dell'Associazione stessa, a livello nazionale e internazionale.

**Qual è la visione strategica di BSA Italia sull'IoT e come incardinate questa tecnologia nella evoluzione dell'innovazione digitale?**  
IoT è una soluzione di avanguardia che permette di

**Intervista a Paolo Valcher, neo presidente del Comitato italiano di BSA | The Software Alliance**



pensare a nuovi modelli di business: una nuova Digital Transformation dell'azienda che offre inedite opportunità di business. IoT aiuta a pensare dei

modelli d'azione nuovi e decisamente "disruptive". Inoltre, sfruttando le potenzialità che il Cloud offre è possibile sviluppare tali soluzioni all'avanguardia anche affrontando costi accettabili persino per realtà aziendali di dimensioni contenute.

**Avete prodotto studi vostri su questa tendenza?**  
No, al momento non abbiamo ancora prodotto studi specifici come BSA a livello globale, ma esistono diversi studi realizzati da singole società aderenti all'associazione.

**Perché considerate l'IoT come un pilastro del piano Industry 4.0 o comunque di programmi per la conversione della produzione industriale e anche agricola verso il nuovo che avanza?**

Il Governo italiano e in particolare il Ministro Calenda si sono molto spesi ed impegnati sul Piano Industria 4.0. Riteniamo che il Piano possa essere un punto di partenza importante: sotto questo profilo, ad esempio, una opportunità come l'iperammortamento è davvero decisiva per rilanciare anche il settore del software.

**Cosa proponete alla politica di fare per dare spazio all'IoT e cosa suggerire alle industrie per approcciare in modo corretto questa tecnologia e inserirla in modo efficiente nei loro processi?**

Le aziende devono iniziare a pensare in logica digitale tutti i processi della loro filiera di lavorazione: quest'evoluzione di logica d'approccio potrà costare uno sforzo all'inizio, ma i vantaggi in termini di efficienza e produttività lo ripagheranno largamente, perché i dati strutturati e connessi fra loro hanno un valore incomparabile rispetto a dati (per quanto abbondanti) isolati e non comunicanti.

### **La normativa può fungere da acceleratore?**

Sicuramente: secondo l'On. Davide Baruffi, relatore dell'indagine in materia di contrasto della contraffazione via web intervenuto al nostro evento sull'IoT, è necessario aumentare la responsabilità in capo agli Internet Service Provider per contrastare la pirateria online, un problema che sta entrando nell'agenda politica con sempre maggior urgenza; e poi Baruffi ha inoltre sottolineato l'urgenza di rivedere la normativa europea per aumentare la cooperazione tra Stati Membri.

### **Quali sono i cantieri digitali che secondo BSA maggiormente impatteranno sullo**

### **sviluppo dell'IoT e anche sulla applicazione di questa tecnologia a livello di customer experience?**

Come ha detto sempre al nostro convegno romano Antonello Busetto, Direttore Assinform, i cantieri digitali che si preparano ad ridefinire il mercato attuale saranno quelli della Mobilità, del Cloud computing, dei Big data, dei Social media e, appunto, dell'IoT, di cui Busetto ha sottolineato l'importanza della formazione per fare il prossimo passo, ossia "dal dato alla filiera".

### **Siete al corrente di qualche progetto di IoT in Italia meritevole di evidenza?**

Al convegno di Roma dello scorso primo dicembre, Luigi Mastrobuono, Direttore Generale Confagricoltura, ha esposto per esempio alcuni esempi di IoT applicati all'agricoltura: come l'Azienda Agricola Pontevecchio, la prima ad inaugurare una stalla completamente computerizzata, o il caso della App "iCow", che permette a 11.000 allevatori kenyoti di semplificare i procedimenti di produzione e vendita del latte con un efficientamento

delle spese. Mentre ancora Antonello Busetto, ha portato esempi di IoT come i droni molecolari per la medicina del futuro, videosorveglianza, pagamenti digitali nelle Smart City etc., che miglioreranno decisamente la vita dei cittadini. Marcello Gamberale Paoletti poi, Presidente e fondatore di Viveat, ha ricordato come la sua azienda già impiega tecnologie (dall'RFID al QR Code) che consentono una piena tracciabilità del prodotto (il cosiddetto product passport), già in adozione nelle filiere produttive agro-alimentare e del fashion, e che consentono al contempo la tutela del brand, avanzate forme di CRM, di customer engagement e di mobile communication.

### **IoT e software: quali legami e quali implicazioni?**

Il software rimane sempre il cuore intelligente delle soluzioni innovative in campo di IoT. Ogni applicazione in questo campo esprime la propria potenzialità attraverso appositi software sviluppati per gestire il funzionamento degli oggetti e consentire il dialogo fra essi e l'intelligenza al centro di

qualsiasi processo: in particolare quella dell'uomo, che riceve (meglio e più rapidamente) le informazioni, siano esse sulle merci in transito alle dogane, sulla filiera produttiva di un alimentare o sulla produzione agricola come si diceva sopra, quindi valuta e ordina al sistema le azioni più opportune in funzione dei dati raccolti appunto via internet.

**Cosa pensate andrebbe fatto per ridurre il tasso**

**di illegalità nel settore del software e come l'IoT potrebbe aiutare, se può?**

Come Associazione pensiamo fermamente che la collaborazione con le altre Associazioni di categoria dei titolari di diritti e la possibilità di ampliare gli orizzonti saranno importanti per contrastare la contraffazione a tutti i suoi livelli e spiegarlo all'opinione pubblica, benché l'evento che BSA ha organizzato a Roma presso la

Camera dei Deputati non avesse in verità solo lo scopo parlare di illegalità del software. BSA infatti ha voluto porre attenzione in modo trasversale sul modello IoT come motore d'innovazione nei confronti del controllo e del monitoraggio dei processi, dei prodotti e quindi anche della qualità degli stessi. Ciò significa anche un migliore controllo della contraffazione dei prodotti di ogni settore merceologico. ✱

di Gaetano Di Blasio

TECHNOLOGY

# Emerson Network Power ora è Vertiv e si prepara a nuove sfide

*Il completamento dello spin off da Emerson, da vita a una nuova struttura che promette maggior dinamismo e massima flessibilità, per imporsi nei settori emergenti*

**G**iordano Albertazzi, presidente Europe Middle East e Africa di Vertiv, per presentare la nuova azienda nata dallo spin off di Emerson Network Power da Emerson ha scelto l'Italia, non perché sia italiano, ma perché in Italia sono stanziate risorse e strutture importanti, che ne fanno la

principale country europea sia per mercato sia, soprattutto, per progettazione e produzione.

Nel nostro Paese si trovano 2 dei 4 customer center Emea: a Castel Guelfo, vicino Bologna e a Piove di Sacco, vicino Padova.

Sembra superata, dunque, la crisi che aveva portato a considerare dei licenziamenti nel 2014 e il nuovo assetto, con il passaggio a un capitale privato, mette al riparo dalle oscillazioni di borsa donando maggiore flessibilità.

La nuova Vertiv al futuro guarda con entusiasmo (sceglie proprio questo termine Albertazzi) perché la separazione da Emerson porta grandi vantaggi, a cominciare da un maggior dinamismo e la già citata flessibilità, che significa, per esempio garantire la possibilità d'investire dove occorre per supportare un cliente in un'espansione internazionale. Sono, afferma Albertazzi, elementi necessari per competere in un settore affollato di concorrenti e caratterizzato da clienti molto esigenti, a partire dalle principali telco, i



*Antonio Carnassale, country manager di Vertiv Italia*

cloud provider, le utility e imprese del settore energy & oil, tra i quali Vertiv conta clienti come America Movil, Apple, AT&T, China Mobile, Ericsson, Facebook, Microsoft, Verizon, elencati in rigoroso ordine alfabetico. La nuova azienda punta anche sulle nuove tendenze del mercato. Una delle principali, afferma Antonio Carnassale, country

manager di Vertiv Italia, parte dallo sviluppo del cloud, che in Italia è e sarà per i prossimi tre o cinque anni ibrido, favorendo la realizzazione di piccoli data center locali.

Ma il cloud significa anche nuove architetture, come quelle che devono supportare applicazioni fruite as a service, eliminando la latenza, oppure, semplicemente devono sostenere la densità delle macchine chiamate a gestire maggiori carichi di lavoro e traffico, con tutte le ripercussioni in tema di power e cooling.

Altresì l'ambito della sicurezza informatica sta portando cambiamenti nei data center, il che non sorprende, considerando che il dato è l'obiettivo finale del cyber criminale. Lo studio "Cost of Data Center Outages" effettuato nel 2016 da Ponemon Institute e sponsorizzato da

Emerson Network Power, ha rivelato che il 22% delle interruzioni dell'attività dei data center prese in esame è rappresentato da cyber attacchi.

Vertiv è già pronta per le sfide dei nuovi mercati. ❁



*Giordano Albertazzi, presidente Europe Middle East e Africa di Vertiv*

# IBM Cognitive Systems, intelligenza artificiale nel data center

*Una nuova divisione e una focalizzazione verso l'intelligenza artificiale per portare tutta la potenza di Watson sui System z*

**S**i amplia l'offerta di IBM con nuovi annunci che riguardano tecnologie e soluzioni a supporto del processo di evoluzione verso la Digital Transformation sia sul versante server e storage. Elementi centrali dei nuovi annunci sono l'aspetto infrastrutturale e il tema dell'intelligenza artificiale.

«IBM sta ripensando l'infrastruttura - osserva Marco Utili, Director Systems di IBM Italia - per renderla elemento abilitante di un processo di trasformazione che vede il passaggio dalla focalizzazione sull'aspetto transazionale dei dati (system of record) a quello che si basa sull'analisi e l'estrazione di valore da dati di ogni tipo (insight system). L'infrastruttura a supporto di questo passaggio è di tipo ibrido e coniuga cloud privato, machine learning, risorse on-premise e cloud pubblico. Questo approccio IBM intende portarlo all'interno di tutti i componenti dell'infrastruttura».

A supporto di questa visione strategica IBM ha creato una nuova divisione denominata Cognitive Systems per portare le tecnologie di machine learning e di intelligenza artificiale a ogni azienda (non solo a quelle di grandi dimensioni) che voglia intraprendere questo percorso.



Marco Utili,  
Director Systems di IBM Italia

Tra le prime soluzioni veicolate dalla nuova divisione vi è Power AI (Artificial Intelligence) un framework pacchettizzato per le aziende che combina l'hardware dei processori Power ottimizzato per sfruttare i sistemi di accelerazione hardware di Nvidia (NVLink),

IBM Italia -. Il machine learning che viene inserito all'interno di System z tramite IBM Machine Learning for z/OS automatizza il processo di interazione tra l'analista e il sistema, delegando al sistema molti aspetti di gestione. Questo approccio consente di accelerare molto il processo sollevando il Data Analyst da molto del lavoro che dovrebbe svolgere».

IBM evidenzia innumerevoli mercati in cui il machine learning creerà nuove opportunità. In ambito retail, per esempio, potrà essere utilizzato per la previsione delle vendite basandosi sui trend di mercato attuali, mentre nel settore finanziario sfruttato dagli advisor finanziari o dai broker per fornire suggerimenti basati su trend e movimenti di mercato aggiornati in tempo reale.

All'interno del settore "healthcare", il machine learning apre la strada a offerte di assistenza medica personalizzate, realizzate utilizzando dispositivi connessi tramite Internet of Things per raccogliere dati sui comportamenti e le interazioni delle persone e delle macchine.

*Andrea Negro, server solutions sales manager di IBM Italia*



## **Storage più flessibile, performante e versatile**

IBM evidenzia come, anche nello storage, l'infrastruttura assuma un'importanza fondamentale a supporto dell'intelligenza artificiale. L'esigenza di analisi delle informazioni in tempo reale rende, infatti, essenziale poter differenziare la componente infrastrutturale di memorizzazione per scegliere quella più adatta alla differente natura dei dati, conseguendo maggiori prestazioni e riducendo i costi. «Dopo avere attraversato il primo decennio del 2000 all'insegna dei processi di consolidamento, ci si torna ora a concentrare sul tema delle distribuzione dei dati

con tecnologie software di autoapprendimento (Deep Learning).

Un'altra importante proposta di IBM Cognitive Systems è la disponibilità del machine learning all'interno del mainframe IBM (ovvero dei server della famiglia System z) con la possibilità per i clienti IBM di integrare all'interno del loro data center tramite private cloud alcune componenti tecnologiche derivate da Watson, finora accessibili unicamente tramite cloud pubblico.

«Il processo tradizionale di apprendimento si basa su un'analisi dei dati in cui la maggior parte dell'attività viene svolta manualmente dai Data Analyst - ha spiegato Andrea Negro, server solutions sales manager di

- sottolinea Francesco Casa manager storage solutions di IBM Italia -, in base al presupposto che i dati devono poter essere memorizzati in modo differenziato in base al loro valore e alla loro natura».

La flessibilità di scelta resta l'elemento centrale nella strategia storage di IBM che, attraverso l'offerta Spectrum, già da tempo consente all'utente finale di scegliere la modalità di memorizzazione preferita.

«L'offerta Spectrum - ha continuato Casa - è disponibile come soluzione

*Francesco Casa, Manager Storage Solutions di IBM Italia*



*IBM Storwize V5030F*

interamente software adatta a ogni tipo di hardware, come appliance, in modalità cloud come servizio erogato sull'infrastruttura IBM SoftLayer e anche come servizio cloud nativo sull'infrastruttura cloud di terze parti». Nel 2016 la gamma Spectrum si è ampliata con l'introduzione di due nuove tasselli. Il primo è Spectrum CDM, un cruscotto per visualizzare e gestire funzioni di Copy Data Management in-place. La seconda novità riguarda l'offerta object storage, che IBM ha portato anche sul cloud con IBM Cloud Object Storage. Per il 2017 alcune delle soluzioni Spectrum saranno

rese disponibili in modi sempre più versatili. In particolare, IBM Spectrum Virtualize e IBM Spectrum Scale potranno "girare" anche su Container o Virtual Machine non IBM, mentre IBM Spectrum Archive sarà disponibile anche come servizio cloud.

Sul versante hardware viene aggiornata l'intera offerta IBM Storwize con modelli nativamente All Flash contraddistinti dalla sigla F (V5030F e V7000F) e dal 10 gennaio anche i sistemi storage di fascia enterprise della serie DS8000 sono disponibili come sistemi nativamente All Flash (DS8884F, DS8886F, DS8888F). ❁

Dai sistemi di intrusion detection all'analisi comportamentale per rilevare le tecniche di evasione, continua la rincorsa alle minacce di ultima generazione mentre si aprono scenari apocalittici con lo sviluppo dell'IoT e gli attacchi DDoS di massa.

L'attenzione alla sicurezza dell'identità digitale e l'avvento delle tecniche basate su analytics e machine learning **pag. 10**

# malware

**SPECIALE  
THREAT PREVENTION**

## UNA RUBRICA SULLA SICUREZZA DIGITALE CURATA DA AIPSI

Da questo numero di Security&Business inizia la pubblicazione della rubrica mensile di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, che tratterà temi e strumenti sulla sicurezza digitale. Si rafforza la partnership con Reportec, con attività online. **pag. 3**



## CYBER ATTACK

### LA SECURITY FABRIC DI FORTINET ORCHESTRA I FIREWALL

Una ricerca di Check Point rivela le preoccupazioni sulla sicurezza che rendono critiche le scelte nel cloud. Un'indagine di F5, invece affronta il tema dell'application security e della delicata questione delle identità digitali. **pag. 8**

## IN QUESTO NUMERO:

### AIPSI

pag. 3-5

- Una rubrica sulla sicurezza digitale curata da AIPSI

### CYBER ATTACK

pag. 6-7

- La sicurezza resta la prima preoccupazione del cloud

pag. 8-9

- F5 mette l'Application Security al centro della protezione

### SPECIALE

pag. 10-13

- Threat Prevention, intelligence e resilienza

pag. 14-15

- La protezione dal ransomware e oltre con Kaspersky Lab

### SOLUZIONI

pag. 16-17

- HPE Security Arcsight: intelligence di sicurezza a massima velocità

pag. 18-19

- Proteggere i sistemi SCADA per non fermare la produzione

# SICUREZZA COSTANTE, INTELLIGENTE

**E PUOI AVERLA SUBITO.**

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

**Visita [www.fortinet.it](http://www.fortinet.it) per maggiori informazioni.**

**FORTINET®**

**Sicurezza senza compromessi**

# UNA RUBRICA SULLA SICUREZZA DIGITALE CURATA DA AIPSI

*Da questo numero di Security&Business inizia la pubblicazione della rubrica mensile di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, che tratterà temi e strumenti sulla sicurezza digitale.*

*di Marco Bozzetti*

**A**IPSI ([www.aipsi.org](http://www.aipsi.org)) è il capitolo italiano di AISSA ([www.issa.org](http://www.issa.org)), l'associazione internazionale no-profit di professionisti ed esperti praticanti, focalizzata nel mantenere la sua posizione di "Global voice of Information Security". Più precisamente, si tratta, grazie all'attiva partecipazione dei singoli soci e dei relativi capitoli in tutto il mondo, della più grande associazione non-profit di professionisti della sicurezza (vanta oltre diecimila associati a livello mondiale).

L'organizzazione di forum e di seminari di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, la formazione per le certificazioni europee eCF per la sicurezza informatica (normato in Italia come UNI 11506), oltre all'interazione fra i vari professionisti della sicurezza, contribuiscono concretamente a incrementare le competenze e la crescita professionale dei soci, oltre che promuovere più in generale la cultura della sicurezza ICT e della sua gestione in Italia. L'appartenenza al contesto internazionale ISSA, permette ai soci AIPSI di interagire con gli altri capitoli

europei, americani e del resto del mondo.

Numerosi i benefici per i Soci AIPSI, sintetizzati nel Box 1.

## **La strategia AIPSI 2017-18**

AIPSI è una associazione di singole persone, non anche di aziende ed Enti, che professionalmente si interessano e/o operano nell'ambito della sicurezza digitale. Quindi un'associazione di liberi professionisti e dipendenti lato domanda e lato offerta ICT, specialisti tecnici e manager della sicurezza digitale, professionisti e manager di altri settori che si occupano anche saltuariamente di sicurezza digitale. Tipici esempi di questa ultima tipologia di soci includono svariati settori e ordini professionali, dalla sanità alla finanza, dall'industria ai servizi, dagli avvocati ai commercialisti, dai consulenti manageriali ai fornitori di servizi ICT, dai progettisti agli sviluppatori di software, dai gestori di risorse umane ai responsabili degli acquisti.

Come per ogni libera associazione, l'obiettivo primario è la continua crescita dei Soci. Per questo

occorre far conoscere AIPSI e le sue qualificate attività al più ampio bacino possibile di potenziali soci, oltre che realizzare per essi servizi reali e utili nell'ottica primaria della loro crescita professionale. Per ottenere tali risultati AIPSI in particolare, per il biennio 2017-8:

- ha recentemente rifatto il proprio sito web quale portale dei servizi digitali per i propri Soci e come punto di informazione e promozione delle proprie attività per tutti i potenziali interessati alla sicurezza digitale;
- collabora e promuove OAD, Osservatorio Attacchi Digitali in Italia, e la sua diffusione, oltre ad altre indagini relative alla sicurezza digitale in Italia;
- supporta i Soci nelle qualificazioni e certificazioni professionali, in primis l'europea eCF;
- fornisce lo scambio di informazioni su opportunità professionali e di business tra i Soci;
- favorisce e contribuisce all'aggiornamento continuo delle competenze sulla sicurezza digitale con convegni, workshop, seminari e nel prossimo futuro con corsi di formazione e sensibilizzazione in aula e a distanza (elearning), anche grazie alle numerose iniziative di ISSA e all'ISSA Journal;
- presidia vari tavoli istituzionali fornendo un proprio autorevole contributo.

### **Iniziative AIPSI 2017**

Per il 2017 AIPSI ha in cantiere varie iniziative, alcune delle quali in collaborazione con Reportec, che è il suo primo Media Partner.



Un'iniziativa attualmente in corso è l'indagine sugli attacchi agli applicativi informatici, il cui questionario, completamente anonimo, è online all'indirizzo <http://vm2538.cloud.seeweb.it/lime/index.php/survey/index/sid/258122/newtest/Y/lang/it>.

Si invitano tutti i lettori di Security&Business a compilarlo quanto prima possibile, dato che l'indagine è in fase di chiusura: bastano pochi minuti, sono solo 14 domande con le risposte tra cui scegliere preimpostate.

Come riconoscimento dell'aiuto fornito con la compilazione del questionario online, alla fine i rispondenti potranno scaricare un numero della rivista mensile ISSA Journal, che rappresenta uno dei principali benefici per i soci in termini di aggiornamento e di reale trasferimento di know-how.

**Il Rapporto 2016 OAD è scaricabile gratuitamente da** [http://www.malaboadvisoring.it/index.php?option=com\\_sfg&formid=43](http://www.malaboadvisoring.it/index.php?option=com_sfg&formid=43), inserendo i pochi dati richiesti e il codice coupon AIPSI: ABmi5VmTIH (attenzione a non inserire caratteri blank prima o dopo il codice!).

L'elenco dei Convegni e workshop a calendario è riportato nella pagina <http://www.aipsi.org/eventi/calendario-eventi-2017.html>.

L'elenco è "corrente", man mano si aggiorna. Alcune manifestazioni sono effettuate in collaborazione con altri Enti e associazioni, e per talune deve ancora essere fissata la data precisa. Alle iniziative italiane si affiancano quelle internazionali di

ISSA, che sono di elevata qualità e di forte interesse, specialmente i webinar riservati ai soci, il cui calendario sarà quanto prima pubblicato online.

Dal 2015 è stato costituito in ISSA un gruppo di lavoro dei referenti dei capitoli europei, per cooperare su possibili comuni iniziative e migliorare lo scambio di informazioni inerenti l'ambito europeo.

### **I principali benefici nell'essere socio AIPSI**

- Ricevimento di ISSA Journal, la rivista mensile di ISSA.
- Accesso/ricevimento newsletter di ISSA e newsletter italiana di AIPSI.
- Partecipazione ai webinar ISSA.
- Trasferimento di conoscenza e formazione continua sulla sicurezza per l'aggiornamento e la crescita professionale dei soci.
- Corsi per le certificazioni professionali per le competenze sulla sicurezza, in particolare per eCF.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Accesso e sconti a seminari, conferenze, training a carattere nazionale e internazionale.
- Pubblicazione di articoli e contenuti nel sito web AIPSI.
- Possibilità di redigere articoli per conto di AIPSI/ISSA.
- Pubblicazione e ricerca di curricula vitae per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web ISSA.
- Visibilità nazionale e internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare a seminari e conferenze come operatore per conto di AIPSI/ISSA.
- Nel prossimo futuro la rappresentanza dei soci professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate.

## LA SICUREZZA RESTA LA PRIMA PREOCCUPAZIONE DEL CLOUD

*Una ricerca di Check Point evidenzia i timori e gli accorgimenti dei professionisti IT legati ai processi di migrazione dei dati nel cloud* di Riccardo Florio

Il tema della sicurezza è da sempre una variabile centrale in tutti i progetti cloud.

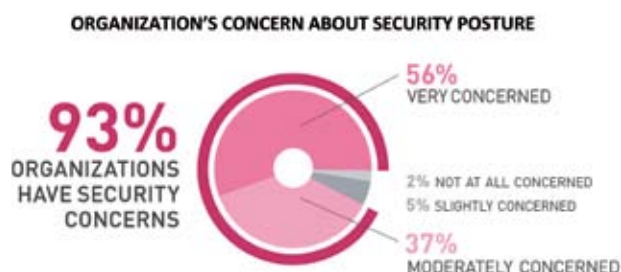
Le aziende, nel corso degli anni, hanno dovuto imparare a superare la barriera psicologica di aprire la propria infrastruttura all'esterno verso clienti e partner. Il cloud, però, richiede un passo in più perché la natura stessa con cui i dati vengono memorizzati e "backuppati" rende più difficile (e qualche volta impossibile) sapere sempre dove questi si trovano fisicamente e riduce, pertanto, la percezione di controllo da parte dell'azienda.

Mettere i dati critici sul cloud significa affidare a un'organizzazione esterna e alle sue procedure interne operative, di gestione e di sicurezza il futuro della propria azienda.

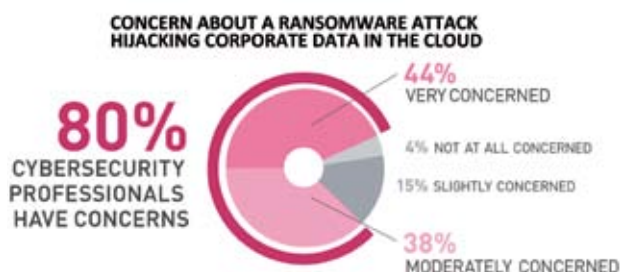
Per queste ragioni, nonostante gli investimenti nel

cloud continuano ad aumentare guidati dalla ricerca di modi per ridurre i costi, aumentare l'agilità e migliorare il supporto al business, la sicurezza di dati, applicazioni e sistemi critici all'interno del cloud resta una barriera importante che rallenta la diffusione dei servizi cloud. La percezione di una sicurezza insufficiente rappresenta il principale singolo contributore al rallentamento nell'adozione del cloud computing.

A questo tema Check Point ha dedicato un survey condotto a novembre 2016, coinvolgendo oltre 200 professionisti dell'IT e della sicurezza per evidenziare le preoccupazioni e i fattori di rischio correlati alla migrazione nel cloud e per individuare i controlli di sicurezza e le best practice adottate dagli esperti in cyber security nel passaggio al cloud.



*Livello di preoccupazione per la sicurezza*



*Livello di preoccupazione riguardo agli attacchi ransomware*

*Dall'alto:  
Le minacce maggiori agli ambienti cloud.  
Capacità di sicurezza per incrementare la  
fiducia in ambienti cloud.  
I 5 metodi più efficaci per proteggere  
i dati nel cloud.*

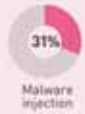
Il primo dato evidente che è emerso è l'elevato grado di preoccupazione per la sicurezza mano a mano che sempre più dati vengono spostati nel cloud. Il 93% è mediamente o molto preoccupato di questo aspetto. Un altro elemento di preoccupazione è rappresentato dalle principali minacce che possono colpire i dati nel cloud. Tra queste innanzitutto il ransomware che preoccupa l'80% dei professionisti della cyber security, a cui si aggiungono, nell'ordine, l'accesso non autorizzato (67%), il data leakage (65%) e gli attacchi del tipo Denial-of-Service (52%).

Le funzionalità di sicurezza su cui si fa affidamento per ridurre i rischi legati al cloud sono innanzitutto legate alla possibilità di ottenere visibilità, report e controllo costante sugli eventi di sicurezza esteso attraverso tutte le piattaforme cloud (74%), di riuscire a mappare i controlli di sicurezza delle applicazioni installate localmente nei confronti dell'infrastruttura cloud (51%) e l'utilizzo di policy efficaci e consistenti (48%).

La tecnologia di sicurezza e controllo considerata più efficiente per proteggere i dati nel cloud è la cifratura dei dati e del traffico, seguita dalle soluzioni di controllo dell'accesso (56%), monitoraggio a livello di rete (53%) e l'uso di sistemi di Intrusion prevention (44%).

Alle specifiche esigenze di sicurezza nel cloud Check Point indirizza vSEC, una soluzione di protezione dalle minacce caratterizzata da scalabilità dinamica, "intelligent provisioning" e controllo dell'accesso esteso attraverso reti fisiche e virtuali.

## THE BIGGEST CYBER THREATS TO CLOUD ENVIRONMENTS



Share memory attacks 21% | Lateral movement of threats (east-west traffic) 17% | Other 6%

## SECURITY CAPABILITIES TO INCREASE THE CONFIDENCE IN ADOPTING CLOUD ENVIRONMENTS



74%

VISIBILITY, REPORTING, AUDITING AND ALERTING ON SECURITY EVENTS ACROSS ALL CLOUD PLATFORMS



51%

EFFECTIVE MAPPING OF SECURITY CONTROLS FOR INTERNALLY-HOSTED APPLICATIONS TO THE CLOUD INFRASTRUCTURE



48%

CONSISTENT SECURITY POLICIES AND ENFORCEMENT ACROSS CLOUD PLATFORMS



Other 5%

## TOP 5 MOST EFFECTIVE METHODS TO PROTECT DATA IN THE CLOUD



- Data leakage prevention 41%
- Firewalls / NAC 36%
- Endpoint security control 38%
- Patch management 38%
- Security information and event management (SIEM) 34%
- Anti-virus / anti-malware 28%
- Sandboxing 25%
- Content filtering 20%
- Other 7%

## F5 METTE L'APPLICATION SECURITY AL CENTRO DELLA PROTEZIONE

*Il 72% degli attacchi mira all'identità digitale degli utenti e alle applicazioni, ma il 90% degli investimenti in sicurezza è focalizzato sulla protezione di un perimetro che non esiste più*

*di Gaetano Di Blasio*

La sicurezza informatica è tradizionalmente basata sulla protezione del perimetro aziendale, ma quest'ultimo non esiste più o, più precisamente, non è più definibile come un confine tra un esterno insicuro e un interno dove sistemi e dati sono al sicuro. Maurizio Desiderio, country manager di F5 Networks, lo spiega chiaramente tracciando le attività quotidiane di un information worker, che accede alla propria mail e a una serie di applicazioni, come, cita per esempio il dirigente, Office e SharePoint, Dropbox, Concur, ServiceNow, Workday, Webex. Solo alcune delle quali appartenenti alla categoria del cosiddetto "shadow IT", cioè non controllate dall'IT aziendale.

«Tutte attività che non richiedono alcun accesso al perimetro di rete aziendale», continua Desiderio, che poi aggiunge: «Viviamo in un mondo application centric», mostrando i risultati tratti da una recente ricerca svolta negli Usa, secondo la quale oltre il 54% delle aziende utilizza in media più di 201 applicativi. Il 31% conferma di adoperare anche un numero superiore alle 500 applicazioni.



*Maurizio Desiderio, country manager di F5 Networks*

I dati sono relativi a 406 rispondenti, estrapolati da un campione di 3000 interviste in tutto il mondo. Aldilà della rappresentatività statistica, il dato qualitativo è poco confutabile e appare coerente con altre analisi che certificano il massiccio utilizzo di strumenti "esterni" all'azienda, come i device mobili spesso usati con pratiche BYOD (Bring Your Own Device) o il cloud.

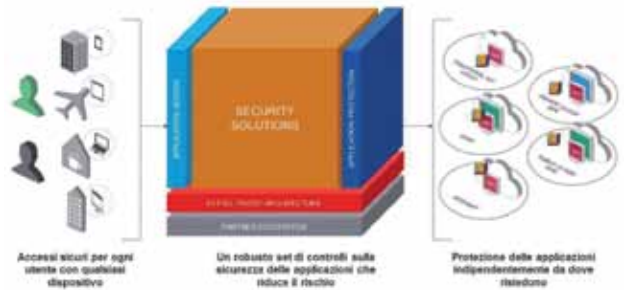
«Tutte le aziende, a prescindere dal settore merceologico, erogano servizi tramite applicativi. Le applicazioni sono il cuore dell'azienda e la rappresentano in termini di brand e reputazione sul mercato», evidenzia il manager e il pensiero non può che andare alle app protagoniste della cosiddetta digital

transformation. I processi aziendali, compresi quelli rivolti verso l'esterno, per esempio nelle relazioni con la clientela, si basano sulle applicazioni, che, quindi, «devono essere sempre disponibili, veloci e sicuri», afferma ancora il country manager di F5.

I cyber criminali, hanno da tempo compreso che non è necessario bucare un firewall o eludere un IPS (Intrusion Prevention System), ma può



*Proteggere le applicazioni ovunque risiedono*



*Application Security integrata*

essere più facile ottenere le credenziali di accesso o sfruttare vulnerabilità degli applicativi.

Secondo dati in possesso di F5 solo il 25% degli attacchi informatici è rivolto verso il tradizionale perimetro della rete aziendale, mentre ben il 72% delle minacce mirano alle identità digitali e alle applicazioni per guadagnare un "comodo" accesso. Ciononostante, il 90% degli investimenti per la sicurezza informatica è dedicato alla protezione del perimetro.

Uno squilibrio che va corretto con un cambio d'approccio, spiega Desiderio dopo aver così introdotto l'azienda: «F5 Networks è stata fondata nel 1996. Nel 2015 ha registrato un fatturato di 1,92 miliardi di dollari e annovera tra i suoi clienti aziende di fama mondiale, comprese le prime 10 telco e le prime dieci case automobilistiche».

Di fatto una specialista "storica" di Internet che oggi propone un set completo di soluzioni per la protezione, integrate in un sistema di controllo unico, ideato per fornire l'accesso sicuro di ogni utente, con ogni dispositivo, a qualsiasi applicazione, ovunque essa risieda, spiega il country manager.

Questo comprende soluzioni realizzate grazie alla collaborazione con Microsoft per Azure, come, per esempio, il servizio F5 SharePoint Online, che rende sicuro l'uso di SharePoint da mobile, poiché la directory rimane in azienda e tutto il resto è gestito nel data center di F5.

Come detto, la sicurezza proposta da F5 si concentra sulla protezione dell'identità e delle applicazioni. Per la prima è necessario poter effettuare controlli incrociati, per esempio sulla posizione dell'utente e sul tipo di dispositivo che sta utilizzando. C'è ovviamente differenza se quest'ultimo dispone o meno di un sistema biometrico o di altre funzioni per una strong authentication. Anche la "salute", cioè lo stato d'aggiornamento del dispositivo, richiede considerazioni adeguate.

Le principali funzionalità comprendono identity e access control, e SSL inspection.

Sul fronte applicativo, F5 dispone di un'ampia gamma di funzionalità, perché non è sufficiente proteggersi solo dalle vulnerabilità. Per questo il portfolio F5 comprende firewall, Web Application Firewall, sicurezza del DNS (spesso preso d'assalto con gli attacchi DDoS), Web Fraud protection.

Come s'intuisce, concentrarsi su accesso e applicazioni sembrerebbe portare a trascurare i controlli tradizionalmente legati al perimetro, come l'anti-malware, ma permette di arrivare a controllare il livello 7 della "vecchia" pila OSI. Significa anche realizzare le protezioni nel data center aziendale e anche nel cloud, quando si ha a che fare con l'hybrid cloud, ormai la condizione predominante presso le imprese.

## THREAT PREVENTION, INTELLIGENCE E RESILIENZA

***Dai sistemi di intrusion detection all'analisi comportamentale per rilevare le tecniche di evasione. Continua la rincorsa alle minacce con analytics e machine learning***

*di Gaetano Di Blasio*

**A**gli albori di Internet, le principali minacce erano rappresentate dalle vulnerabilità che consentivano a malintenzionati di penetrare nei sistemi informatici attraverso la rete. Ben presto i firewall dimostrarono la loro inadeguatezza e nacquero i sistemi di intrusion detection, prima, e intrusion prevention dopo. La differenza tra rilevamento e prevenzione stava (e sta) tutta nel tempo di risposta, cioè nella capacità di correlare i diversi dati relativi alla sicurezza per bloccare un attacco prima che andasse a buon fine.



Oggi questo approccio è ancora utilizzato anche se i sistemi preposti al rilevamento non possono più limitarsi all'analisi del traffico, perché devono considerare più tecniche di penetrazione e non solo quelle basate su exploit in grado di sfruttare vulnerabilità. Si sono, infatti, diffuse anche tecniche di mascheramento, che consentono di bypassare buona parte dei controlli tradizionali e di annidare dei codici maligni, il cui scopo è studiare il sistema, il più "silenziosamente" possibile per preparare successivi attacchi.

È ormai frequente, inoltre, che l'attacco abbia inizio con un errore umano, dovuto alla scarsa preparazione "culturale": è il caso, per esempio, dell'ingenuo click su un link in una mail di spear phishing. Questo tipo di mail sono ormai sempre più sofisticate e scritte in un ottimo italiano ed è facile essere tratti in inganno.

Per accelerare il tempo di risposta, considerando anche che le minacce riescono a fare il giro del mondo in pochi minuti, se non secondi, sono stati sviluppati nuovi meccanismi per mantenere aggiornati i sistemi di protezione. Tali meccanismi si basano sul cloud e sulla condivisione delle cosiddette informazioni di "intelligence", che, in buona parte alimentate da soluzioni di sandboxing. Queste ultime consistono in software di analisi che verificano in una zona protetta (la scatola di sabbia) il funzionamento di un codice sconosciuto, prima di inoltrarlo all'interno del sistema informativo.

Data la rapidità con cui le tecniche e le modalità di attacco si susseguono, si è storicamente assistito

a un continuo rincorrersi tra minaccia e rimedio. L'ultima tendenza è quella di integrare le soluzioni di protezione in un unico sistema, che si potrebbe denominare Universal Threat Management o UTM 2.0, prendendo spunto dalle appliance nate una decina d'anni fa che semplicemente racchiudevano in una scatola soluzioni diverse, senza, però, condividere l'intelligenza dei vari controlli.

I sistemi integrati, oggi, devono consentire l'interazione di tutte le soluzioni preposte a controllare traffici, codici e anomalie, in modo da avere la maggiore visibilità possibile su ciò che sta accadendo sulla rete.

### **Condivisione, analytics e machine learning**

Per accelerare ulteriormente i controlli, in modo da reagire in tempo reale si stanno impiegando tecnologie nate in altri contesti, come la business intelligence, al fine di riuscire ad analizzare il più rapidamente possibile i miliardi di dati provenienti dai sistemi di sicurezza, anche quelli installati dall'altra parte del globo.

Attenzione: stiamo parlando di una prevenzione ancora una volta basata sulla velocità di reazione. Considerando che i mezzi economici dei cyber criminali sono superiori a quelli dei "buoni" o quandanche



si confidasse di sostenere il confronto, sarebbe comunque una sfida a chi arriva prima.

La vera sfida è ottenere una vera prevenzione, cioè essere in grado di vedere prima cosa sta per accadere. Per questo alle soluzioni di security analytics si stanno abbinando sistemi di machine learning, che possano riconoscere i prodomi di un attacco e bloccarlo prima che sia pronto.

### Resilienza, governance e incident response

Finora si è illustrato il punto di vista del "soldato" che sul fronte protegge la patria, ma è tempo di capire che le minacce informatiche non costituiscono un problema tecnico, bensì un rischio economico che deve essere gestito nell'ambito della governance aziendale. Un passaggio epocale reso maturo dal ransomware.

Da Cryptoloker in poi, gli imprenditori hanno violentemente compreso che la violazione del sistema informatico ha un impatto economico diretto sull'azienda. Come ci ha recentemente evidenziato Rik Ferguson, vice President Security Research di Trend Micro, il ransomware ha avuto e avrà ancora per molto successo perché mette in relazione il cyber criminale e la vittima senza intermediari,

rendendo semplice al criminale la monetizzazione, al contrario, per esempio, di una frode economica che richiede una forma di riciclaggio del denaro.

Come si è accennato, è facile essere tratti in inganno da una mail o un altro tipo di messaggio, ancor di più se questo

ci raggiunge attraverso uno smartphone, sul quale è più "facile" cliccare su: "se non visualizzi correttamente clicca qui". Questo faticoso clic può innescare un processo drammatico. Il link apparentemente non funziona e l'utente viene rassicurato da un messaggio "riprova più tardi", ma in realtà viene scaricato un malware, che troverà la strada per passare dallo smartphone al sistema informatico (magari insieme ai file delle foto via USB o tramite un servizio cloud gratuito). Arrivato nel punto giusto, il malware comincerà a crittografare i backup, per poi passare agli storage di produzione e, infine, presenterà una



richiesta di riscatto: "paga o non recupererai più i tuoi dati".

Praticamente tutti pagano, ma solo pochi riottiranno i dati. Ecco perché, anche strutturando sistemi di threat prevention è opportuno partire dal presupposto che, prima

o poi, si sarà colpiti. Le strutture e le strategie di incident response, anche se talvolta non riescono a fare piena luce sulle origini dell'attacco, consentono di ridurre il costo della violazione ai dati, come dimostra il rapporto sui costi dei data breach pubblicato ogni anno dal Ponemon Institute.

Queste strategie, infatti, riducono drasticamente i tempi di ripristino. È il concetto di resilienza, cioè della capacità tipica in natura di molte specie di ritornare alla posizione di riposo o di stabilità. In questo caso, in quello di stabilità.

Con questo spirito e avendo compreso che la



sicurezza informatica è un fattore di business, le imprese ne stanno rivedendo i processi guidandone l'evoluzione che «si esprime in termini di: governance, per la tutela degli asset-chiave delle organizzazioni (sempre più immateriali); controllo, come monitoring del corretto disegno e dell'efficacia ed efficienza del sistema IT; Trasformazione, ovvero delle capacità di continuo aggiustamento correttivo ed evolutivo del sistema di controllo; prevenzione degli attacchi e degli incidenti, intesa come capacità di monitorare trend e comportamenti interni ed esterni alle organizzazioni allo scopo di prevenire la costituzione degli attacchi; gestione degli incidenti, come capacità tecnologiche di rilevare tempestivamente l'evento- incidente, filtrarlo rispetto a logiche di analisi in grado di scartare gli eventuali falsi positivi, innescare i processi di comunicazione, escalation e reazione, predisporre i relativi piani di rientro». Come scrivono nel focus "Dalla Sicurezza Informatica alla Protezione aziendale: nuovi modelli di prevenzione e di gestione degli incidenti" contenuto nel Rapporto Clusit 2016, Federico Santi e Danilo Benedetti, rispettivamente Security Principal e Security Solutions Architect di Hewlett Packard Enterprise.



# LA PROTEZIONE DAL RAMSONWARE E OLTRE CON KASPERSKY LAB

*La nuova versione di Kaspersky Small Office Security prelude allo sviluppo dell'offerta per la protezione delle Pmi e delle aziende enterprise con soluzioni avanzate*

*di Gaetano Di Blasio*



La principale minaccia per ogni impresa, ma in particolare per quelle più piccole, è rappresentata dal ransomware, le cui campagne s'intensificano vieppiù. Una recente ricerca condotta da Kaspersky Lab ha rilevato come il 42% delle microimprese sia preoccupata dal fenomeno dei crypto-malware. Ne hanno ben donde, considerando che secondo il Kaspersky Security Network (KSN) le piccole imprese hanno subito un numero di attacchi ransomware otto volte superiore nel terzo trimestre del 2016 rispetto a quello del 2015. Più precisamente, Kaspersky Small Office Security ha individuato e fermato 27.471 tentativi di blocco all'accesso ai dati aziendali, rispetto a 3.224 attacchi simili nel medesimo periodo dell'anno precedente.

Il ransomware blocca tutte le operazioni o cripta i dati importanti per le aziende finché non viene pagato un riscatto. La perdita economica può essere significativa, anche considerando la totale mancanza di scrupoli dei cyber criminali, che non sono più i programmatori, magari un po' nerd che producono il software maligno, ma veri e propri delinquenti che affittano il malware e intendono massimizzare i guadagni.

Nell'indagine di Kaspersky Lab Corporate Security Risks 2016, oltre metà (55%) degli intervistati di piccole imprese ha dichiarato che, in seguito a un attacco, ci sono voluti diversi giorni per ripristinare l'accesso ai dati crittografati.

Il problema è che non sempre ci si riesce, anche perché il pagamento del riscatto non garantisce il recupero della chiave per decriptare i dati, come evidenzia Morten Lehn, General Manager Italy di Kaspersky Lab, che aggiunge: «Per assicurare la protezione contro ransomware e altri tipi di attacco, le imprese devono implementare soluzioni di sicurezza up-to-date affidabili come misura preventiva». I requisiti minimi di sicurezza dovrebbero includere la formazione dei dipendenti su come resistere ai tentativi di social engineering e di phishing, la creazione di backup dei dati critici e copie degli stessi, l'aggiornamento costante dei software e, infine, l'implementazione di soluzioni per la sicurezza delle piccole imprese.

Per questo Kaspersky Lab ha preparato una nuova versione del proprio software Kaspersky Small Office Security, che comprende una funzionalità anti-ransomware potenziata, una migliore protezione delle

transazioni finanziarie online e un monitoraggio dedicato dello status della sicurezza. Inoltre la funzionalità anti-ransomware inclusa nella componente System Watcher, oltre a bloccare i tentativi nocivi di cifratura, avvia anche il backup e il ripristino automatico.

### Safe Money e monitoring

Tra le novità della nuova versione troviamo l'aggiornamento della funzionalità Safe Money, che protegge l'accesso all'home banking e la sua operatività. Di fatto, spiega Kaspersky, le transazioni sono protette anche dagli screenshot o dall'utilizzo della funzione appunti, su cui normalmente si basano i cyber criminali per rubare informazioni aziendali e asset finanziari. Kaspersky Small Office Security fornisce anche una semplice modalità per monitorare lo stato della sicurezza. Mediante una console di monitoraggio dedicata, basata su cloud, le aziende ottengono una visione completa del livello di protezione relativo a ciascun dispositivo interno al proprio network: server, pc notebook e qualsiasi device. Il portale online permette di accedere a queste informazioni ovunque e in qualsiasi momento, modificare le impostazioni di protezione.

Kaspersky Small Office Security è progettato per aziende con un numero di computer tra 5 e 25, ma in termini di funzionalità, afferma ancora il responsabile della filiale italiana, è una soluzione completa che consente di affrontare le problematiche cui deve rispondere anche la grande impresa. «Abbiamo investito in una nuova piattaforma per potenziare la formazione, non solo verso le aziende del canale, ma anche verso gli utenti finale», racconta Lehn,

*Morten Lehn, General Manager Italy di Kaspersky Lab*



precisando: «La piattaforma ci consente di creare scenari realistici e simulare gli attacchi. Sono convinto che insegnare a capire che un link è malevolo, sensibilizzare gli utenti sui rischi, risolva più dell'80% dei problemi». La piattaforma sarà anche a disposizione dei rivenditori.

Nel 2017 Kaspersky Lab festeggia vent'anni tutti dedicati alla sicurezza e con l'occasione porterà sul mercato un'importante serie di novità, spiega il general manager: «Eugene (in dizione inglese il fondatore Evginij Kaspersky) intende rimanere alla guida dell'azienda che ha fondato ancora a lungo ed è alle sue intuizioni che si devono gli sforzi in ricerca e sviluppo degli ultimi tre anni». Sforzi che hanno portato ad allargare il portfolio di soluzioni e servizi. La rinnovata soluzione per gli ambienti SCADA e, più in generale, per il mondo industrial è un esempio, cui vanno aggiunti il nuovo sistema operativo, le soluzioni per gli ambienti virtualizzati, i servizi gestiti.

Questi sono stati immessi sul mercato nell'autunno scorso e comprendono attualmente Kaspersky Endpoint Security Cloud, Kaspersky Endpoint Security for Business Basic e Kaspersky Security for virtualization. Importanti gli sforzi effettuati sulla componente d'intelligence che fornisce una protezione estesa a

un'ampia varietà di sistemi IT con novità importanti quali l'Anti Targeted Attack Platform (per gli attacchi mirati). A questo si aggiungono due soluzioni: una per la protezione da attacchi DDoS, e l'altra per la sicurezza del data center (con un motore di scansione che interagisce direttamente con i NAS) Da citare, inoltre, la rinnovata soluzione per ambienti virtuali, la prevenzione dalle frodi e la citata sicurezza per gli ambienti industriali.

## HPE SECURITY ARCSIGHT: INTELLIGENCE DI SICUREZZA A MASSIMA VELOCITÀ

*La famiglia di soluzioni di HPE permette di fronteggiare le esigenze di analisi dei Big Data della sicurezza e di rispondere agli APT. In arrivo ArcSight Investigate per effettuare analisi ancora più velocemente.*

*di Riccardo Florio*

Il numero enorme di potenziali minacce e rischi ha alimentato la proliferazione delle tecnologie di protezione dando origine veri e propri Big Data correlati agli eventi di sicurezza. L'approccio basato sull'uso di applicazioni di business intelligence per estrarre informazioni utili dalla grande quantità di dati grezzi manifesta, sempre più, le proprie difficoltà nel riuscire a essere nel contempo efficace e rapido.

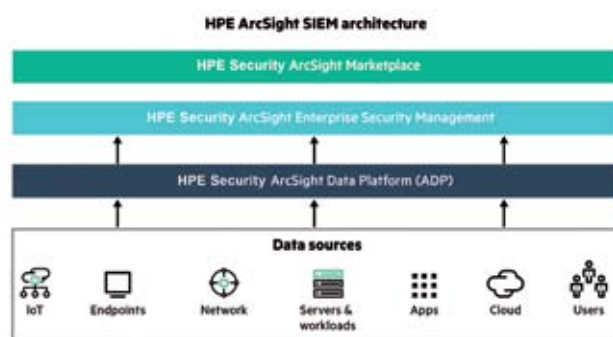
A queste esigenze si indirizza HPE Security ArcSight, una famiglia di soluzioni avanzate di System Information and Event Management (SIEM) per effettuare in tempo reale, attraverso l'intera infrastruttura enterprise, il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da scansioni di vulnerabilità, analisi intelligenti delle minacce, firewall, IDS/IPS, applicazioni legacy e altre applicazioni di sicurezza. Il componente centrale e abilitante della soluzione SIEM di HPE è il motore per la gestione di minacce e rischi HPE Security ArcSight Enterprise Security Management (ESM), le cui capacità di correlazione consentono di identificare, all'interno del complesso scenario fatto da miliardi di eventi di sicurezza, le reali minacce e di definire in modo accurato e automatizzato le priorità di intervento.

Il secondo componente fondamentale è HPE Security

ArcSight Data Platform (ADP), una piattaforma che raccoglie dati di sicurezza provenienti da qualsiasi fonte (inclusi log, sensori, flussi di rete, apparati di sicurezza, Web server, applicazioni custom, social media e servizi cloud), li memorizza, effettua ricerche e produce report con prestazioni compatibili con le esigenze di gestione dei Big Data: è in grado di ricevere fino a un milione di eventi per secondo e di comprimere e archiviare fino a 480 TB di dati di log.

### Difesa efficace contro gli APT

L'approccio offerto da HPE Security ArcSight si dimostra particolarmente efficace per contrastare gli attacchi APT (Advanced Persistent Threat) che sono caratterizzati da una serie di fasi di attacco in successione. Grazie all'uso di tecnologie di "stateful security



*L'architettura della soluzione SIEM sviluppata da HPE*

## **HPE Security ArcSight riconosciuta come migliore soluzione SIEM**

La soluzione di HPE Security ArcSight da 13 anni di seguito viene inserita da Gartner tra i Leader all'interno del Magic Quadrant per le soluzioni SIEM e di recente ha ottenuto il premio SC Awards 2017 come migliore soluzione SIEM, da un gruppo di selezionati professionisti del settore della sicurezza, scelti dal team editoriale di SC Media. Il prestigioso riconoscimento è stato attribuito ad HPE nel corso della RSA Conference di San Francisco.

«La categoria 'Trust Award' è una delle più attese della premiazione agli SC Award - ha detto Illena Armstrong, vice presidente di SC Media - perché rappresenta la voce delle persone che stanno veramente utilizzando i prodotti e i servizi. HPE Security ArcSight ha vinto come migliore soluzione SIEM per la sua capacità di soddisfare le esigenze e di superare le aspettative dei propri clienti».

context", la soluzione di HPE è in grado di capitalizzare sulle attività di correlazione svolte in precedenza utilizzandole come input da associare ai nuovi log di eventi. Questo permette di ridurre notevolmente il carico elaborativo del motore di correlazione che non deve preoccuparsi, a ogni sospetto di attacco, di analizzare l'intero storico dei log di sicurezza, con il risultato di fornire risultati più affidabili in minor tempo. HPE Security ArcSight User Behavior Analytics, attraverso la combinazione di tecniche di machine learning e sofisticati algoritmi di rilevamento delle anomalie, fornisce un'aggiunta naturale che migliora la capacità della soluzione SIEM di HPE di individuare minacce potenzialmente sconosciute all'interno dei

registri di eventi, senza presupporre alcuna conoscenza preliminare dei dati. Altri punti di forza della soluzione proposta da HPE nella difesa contro le nuove minacce sono la possibilità di aggiungere in tempo reale dei metadati ai log di sicurezza, per migliorare l'attività di analisi e distinguere eventi provenienti da ambienti in cui l'indirizzo IP viene assegnato dinamicamente (DHCP) e in cui il medesimo IP può risultare, nel tempo, associato a differenti "host name".

## **HPE Security ArcSight Investigate**

HPE Security ArcSight Investigate è un nuovo prodotto di indagine che andrà ad aggiungersi al portafoglio ArcSight a partire dal secondo trimestre del 2017. Questo prodotto mette a disposizione degli utenti funzioni di analisi di sicurezza di nuova generazione e costituisce un passaggio importante nel processo evolutivo della "vision" di HPE per le Intelligent Security Operations. In particolare, HPE Security ArcSight Investigate garantisce funzioni di ricerca più veloce utilizzando HPE Vertica come database incorporato in grado di elaborare enormi volumi di dati a grande velocità. HPE Security ArcSight Investigate è completamente integrato con gli altri prodotti della famiglia ArcSight e consente un'esperienza di ricerca particolarmente intuitiva grazie all'utilizzo di cruscotti personalizzabili. Prevede, inoltre, un algoritmo contestuale di sicurezza in grado di comprendere le parole chiave e suggerire query in modo dinamico, in modo tale che l'utente ha la possibilità di effettuare interrogazioni in linguaggio naturale anziché dover utilizzare un linguaggio tecnico e complesso. L'integrazione diretta con Hadoop come archivio di dati a lungo termine, consente l'accesso a una gamma completa di dati storici, per cercare e analizzare i dati di qualsiasi periodo di tempo da una singola interfaccia utente.

## PROTEGGERE I SISTEMI SCADA PER NON FERMARE LA PRODUZIONE

*Cloud e IoT migliorano la produzione ma espongono a dei rischi che rendono necessario investire in sicurezza. Il perchè lo spiega Paolo Emiliani di Positive Technologies*

*di Giuseppe Saccardi*

La diffusione dell'IoT e i problemi di sicurezza recentemente segnalati mettono in guardia contro i rischi che si corrono sia per i dati inerenti le tipiche attività IT sia contro i rischi che si possono correre a livello industriale. In quest'ultimo campo un potenziale elemento critico sono i sistemi SCADA. Il termine è l'acronimo dall'inglese di "Supervisory Control And Data Acquisition" (traducibile in controllo di supervisione e acquisizione dati), e si riferisce ad un sistema informatico, dall'architettura tipicamente distribuita e con gestione centralizzata, utilizzato per il monitoraggio e controllo elettronico dei sistemi industriali.

I sistemi da un lato monitorano i sistemi fisici, inviando segnali per controllare e gestire da remoto i macchinari e tutti i processi industriali, dall'altro acquisiscono dati per tenere sotto controllo il funzionamento dei macchinari ed inviare segnali nel caso di problemi.

La svolta per quanto concerne questi sistemi di controllo industriale si è registrata con l'avvento delle applicazioni cloud prima e dell'Internet



*Paolo Emiliani -  
Industrial Security  
Lead Expert di Positive  
Technologies*

of Things più di recente, che li stanno rendendo di più facile fruizione. Ma come in tutte le medaglie il rovescio è costituito dall'aumento dei rischi.

L'interconnessione dei sistemi SCADA, mette in guardia Paolo Emiliani, Industrial Security Lead Expert di Positive Technologies, costituisce da un lato un beneficio per tante applicazioni industriali, consentendo accessibilità maggiore, dall'altro espone le debolezze e le vulnerabilità dei sistemi, che in passato rimanevano confinate all'interno d un sicuro perimetro, a rischi molto più elevati.

«Per questo motivo è necessario affidarsi a produttori qualificati in grado di effettuare un'analisi globale della postura di sicurezza dell'intero sistema ora evoluto in eco-sistema, non limitandosi ad analizzarlo ma verificando ogni interconnessione o componente e identificandone le rispettive vulnerabilità ed il relativo impatto che queste possono avere sui processi produttivi. In gergo definito come Comprehensive threat modelling», mette in guardia Emiliani.





orario 9:00 - 20:00

## Security Summit Milano - IX edizione 14-15-16 marzo 2017

**ATAHOTEL EXPO FIERA** - via G. Keplero, 12 - Pero (MI)

Quanto l'innovazione tecnologica può incidere sulla cultura e quanto quest'ultima può influire sull'innovazione tecnologica e ispirare anche dei principi base della sicurezza informatica?

Lo scopriremo insieme nel nuovo programma serale "parallelo" del Security Summit!

Tre serate, a partire dalle 18.00, con ospiti e iniziative per riflettere sulla connessione tra cultura, innovazione tecnologica e sicurezza informatica.  
#seratesummit #CulturaAISummit

L'agenda di Security Summit Milano 2017 prevede **7 tavole rotonde**, **18 sessioni formative**, **7 seminari** e **28 atelier tecnologici**, che si svolgeranno con il contributo di **oltre 100 relatori**.

**LA PARTECIPAZIONE È GRATUITA, PREVIA REGISTRAZIONE  
SUL SITO [WWW.SECURITYSUMMIT.IT](http://WWW.SECURITYSUMMIT.IT)**

Organizzato da



# Lenovo: protagonista nella Digital Transformation

*L'azienda cinese rafforza le proprie armi nell'arena del data center e promuove una ricerca per valutare il livello di prontezza delle aziende enterprise nell'affrontare le sfide della Digital Transformation*

**I**l valore della diversità come ricchezza è da sempre un tratto distintivo dell'approccio di Lenovo al mercato, riassunto nel suo motto "different is better". Non sorprende, quindi, che in un momento in cui il mercato guarda alle opportunità della trasformazione digitale, l'azienda cinese punti a ritagliarsi uno spazio da protagonista anche nel segmento di fascia più alta, sviluppando valore sulle soluzioni per il data center risultate dall'acquisizione della tecnologia x86 di IBM.

Alessandro de Bartolo, country manager in Italia di Lenovo data center Group, osserva come: «L'ambito Data Center, sviluppatosi a seguito dell'acquisizione delle tecnologie x86 da IBM, costituisce uno dei motori di crescita globale di Lenovo. Le infrastrutture data center sono da tempo in costante trasformazione e questo, nel tempo, ha causato una "stratificazione" di isole di

gestione eterogenee. Nel percorso verso la Digital Transformation ci si muove, quindi, sempre più verso modelli di tipo software-defined in cui la componente server, punto di forza dell'offerta di Lenovo, continua a crescere per importanza e numero di compiti svolti assumendo un ruolo primario anche all'interno del networking e dello storage. A ciò si

aggiunge che Lenovo ha stabilito partnership con le aziende leader del mondo software (tra cui SAP, Nutanix e Red Hat. N.d.R.)». Tra i componenti tecnologici che, secondo Lenovo, avranno una grande influenza nel processo di Digital Transformation, de Bartolo sottolinea, accanto al software defined, anche le infrastrutture iperconvergenti lasciando

*Alessandro de Bartolo,  
country manager in Italia di  
Lenovo Data Center Group*





## ThinkAgile è il brand per l'iperconvergenza

Lenovo ha raccolto all'interno del brand ThinkAgile la sua offerta di infrastrutture preintegrate e prevalidate con cui inserisce nell'arena in fase di costruzione dell'iperconvergenza. Alla fine di ottobre 2016 Lenovo ha rilasciato le soluzioni ThinkAgile CX Series che

combinano i sistemi storage ibridi e all flash prodotti dal partner Nimble Storage, con le soluzioni server in formato rack e blade di Lenovo e una serie di switch "top-of-rack". Queste soluzioni convergenti si affiancano alle appliance iperconvergenti HX Series introdotte a seguito della partnership con Nutanix e che raggruppano capacità di elaborazione, storage, funzionalità di networking e di management. A breve dovrebbero anche vedere la luce in Europa le appliance Lenovo ThinkAgile indirizzate agli utenti che utilizzano tecnologia cloud OpenStack (commercializzate sul mercato cinese con la denominazione ThinkCloud AIO) che utilizzano la sempre più diffusa tecnologia storage open source Ceph.

intendere il forte interesse del vendor per questo segmento di mercato.

Tra le novità previste nel primo semestre 2017 ci sarà anche il lancio di un nuovo brand, denominato ThinkAgile, all'interno del quale confluiranno tutte le componenti IT per il mercato business, così da rafforzare ulteriormente la posizione e la dedizione di Lenovo verso questo mercato.

## Una ricerca per testare il livello di progresso nella Digital Transformation

Per definire meglio le esigenze dei professionisti IT in merito al processo di trasformazione digitale in atto, Lenovo ha recentemente promossa la ricerca Next Generation Enterprise Business Report, condotta a livello EMEA coinvolgendo 1400 aziende enterprise con oltre mille dipendenti, di cui 250 italiane. La ricerca ha interessato tutte

le principali funzioni IT, per valutare lo stato di fatto sul progresso delle aziende nell'affrontare le nuove sfide di trasformazione.

Tra i risultati più interessanti che sono emersi si evidenzia come l'87% dei manager IT (percentuale che sale al 91% nel caso delle sole aziende italiane) senta su di sé la responsabilità di guidare la propria azienda nel percorso verso la digital transformation.

Il 22% degli IT manager europei intervistati ritiene però che il proprio hardware tecnologico sia inadeguato

a supportare le applicazioni di nuova generazione e, in particolar modo, inadatto per affrontare le sfide dell'IoT. Inoltre, le funzioni IT lamentano la preoccupazione di non riuscire a controllare nel modo desiderato la proliferazione di macchine virtuali all'interno della rete aziendale.

Un quarto del campione lamenta come limite principale una carenza di budget e questo porta i CIO a chiedere maggior potere di negoziazione. Il 25% degli intervistati sottolinea, altresì, come i dipendenti

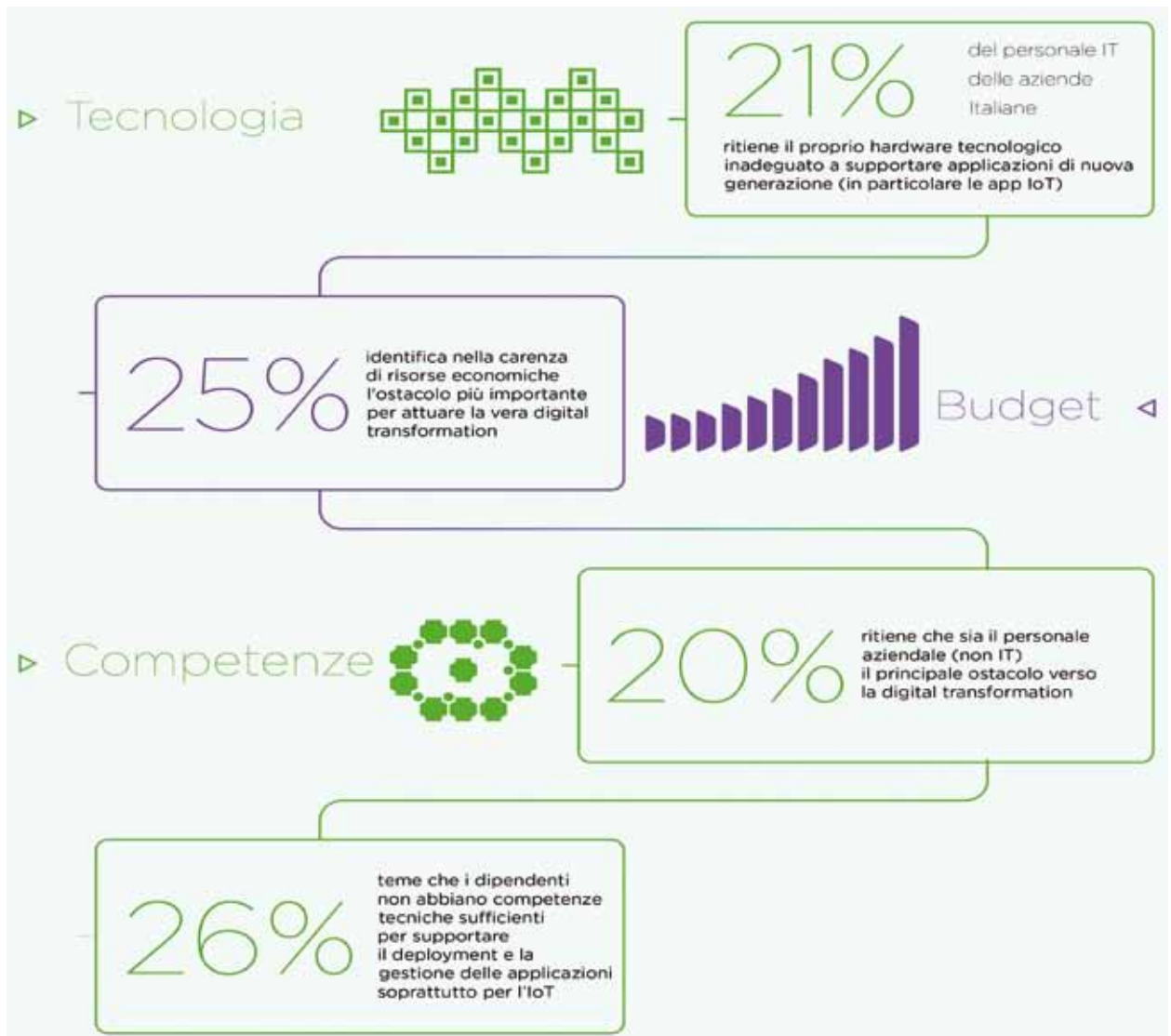
non dispongano delle competenze tecniche sufficienti per sostenere lo sviluppo di applicazioni innovative, soprattutto quelle orientate all'IoT, ponendo l'accento sull'importanza degli investimenti in formazione.

Anche in Italia il 20% degli IT manager afferma che l'ostacolo più grande alla trasformazione digitale sono le competenze tecniche del

personale, mentre il 25% degli intervistati individua il principale ostacolo nella scarsità di risorse economiche.

«In Italia, come si evince dalla ricerca - osserva de Bartolo - la fiducia nelle infrastrutture e nelle persone IT è elevata, nel quadro di una strategia IT che si evolve continuamente in linea con i requisiti di business. Le

lacune attuali sono legate alle competenze insufficienti per garantire questa trasformazione, nonché di budget per consentire ai reparti IT di investire nel futuro digitale. Per questo, Lenovo intende supportare il mercato sia con lo sviluppo di tecnologie allo stato dell'arte adeguate alla Digital Transformation, sia con competenze e conoscenze».





Questa volta  
siamo noi  
a chiedere aiuto  
a voi.

**Fai un'offerta per una nuova ambulanza.**

Servizio emergenza/urgenza 118 - auto medica - trasporto ammalati - trasporto organi - corsi di formazione di primo soccorso per aziende e per la popolazione - stazionamento ad eventi di massa - spettacoli e manifestazioni sportive - 37 sezioni in tutta la Lombardia - 100 anni storia.

Questo è quello che possiamo offrirti, tutti i giorni 365 giorni all'anno. Adesso tocca a te.

DONACI IL TUO 5 x mille: C.F. 03428670156, oppure puoi fare una donazione detraibile  
(IBAN It43u0326801603000866949890)

Visita [www.crocebianca.org](http://www.crocebianca.org) e scoprirai come poterci aiutare.

# Microsoft House: ispirata dalle logiche di smart working

*La nuova sede di Microsoft Italia a Milano è uno spazio aperto alla collaborazione tra persone, aziende e cittadini in cui i dipendenti operano all'insegna della massima flessibilità*



**A**pertura, collaborazione, flessibilità e innovazione: questi i pilastri alla base della Microsoft House, la nuova sede di Microsoft Italia a Milano fortemente ispirata dalle logiche di smart working. L'edificio di 7500 metri quadrati con 832 vetrate, si sviluppa in sei piani fuori terra (di cui tre sono aperti alla città) che sono idealmente collegati dall'innovazione: dalla reception virtuale a sistemi avanzati di video conferencing,

dalla domotica a sensori IoT fino a nuovi strumenti di collaborazione.

Dal secondo al quinto piano si trovano le aree riservate a dipendenti e collaboratori dell'azienda in cui la flessibilità gioca un ruolo essenziale per favorire la conciliazione delle esigenze personali e professionali.

Le aree di lavoro sono open space e non prevedono postazioni dedicate: non è previsto un ufficio riservato neppure per l'amministratore delegato che utilizza gli stessi spazi dei dipendenti. L'idea è che ognuno si muova a seconda delle necessità, trovando spazi di supporto adatti alle differenti esigenze di ogni specifica giornata lavorativa. In base alle logiche di smart working, Microsoft ha identificato sette diverse tipologie di postazioni lavoro, differenziate in base alle diverse esigenze:

- Scrivanie in open space, dotate di pannelli per garantire l'isolamento acustico e in alcuni casi anche di monitor fissi, laddove si preveda un utilizzo del computer prolungato o un



tipo di attività che richieda un maggior confort visivo e acustico.

- Atelier, spazi trasparenti disegnati per un lavoro individuale di breve durata.
- Creative Garden ovvero spazi per le attività di collaborazione e brainstorming,

realizzati all'interno di strutture di legno arredate con piante.

- Smart Platform, aree per le attività che richiedono maggiore concentrazione collocate all'interno di strutture di metallo isolate acusticamente e dotate di lavagne scorrevoli.
- Smart Flowers, aree pensate per svolgere lavori di tipo individuale.
- Garden Tables, elementi circolari strutturati per favorire sia il lavoro individuale che quello di team, grazie a un meccanismo con cui le piante decorative al centro del tavolo possono essere sollevate per garantire la privacy o abbassate per creare un piano di lavoro unico e collaborativo.





La nuova sede di Microsoft a Milano



· Touch down Area, zone strutturate in tavoli alti e concepite per brevi momenti di lavoro, per esempio nel passaggio tra una riunione e un'altra. «Microsoft House riflette la nostra missione di aiutare le persone e organizzazioni ad ottenere di più dal digitale»,

ha commentato Carlo Purassanta, Amministratore Delegato di Microsoft Italia. «Entrare nel cuore di Milano, in un'area dinamica e facilmente connessa con il resto dell'Italia, aprire metà dell'edificio al nostro ecosistema di clienti, consumatori, partner e studenti

è l'impegno che come Microsoft Italia abbiamo intrapreso con il progetto Microsoft House, che vuole essere il nuovo indirizzo per l'innovazione in Italia. Dalle grandi aziende fino alle startup, dagli studenti fino al mondo delle NGO, passando dai nostri partner, Microsoft House rappresenta un nuovo luogo per innovare, collaborare, trovare idee e fare ecosistema: solo insieme si possono fare grandi cose per far crescere l'Italia». ✨

# Fincantieri rinnova il modo di progettare navi con IBM Cloud

*Il principale costruttore navale occidentale si dota di un'infrastruttura cloud di tipo ibrido distribuita a livello globale per conseguire una differenziazione competitiva e rendere più efficienti le attività di progettazione e costruzione*

**I**n oltre 230 anni di storia della mariniera il Gruppo Fincantieri ha costruito più di 7mila navi ed è oggi il principale costruttore navale occidentale, con un portafoglio clienti che annovera i maggiori operatori crocieristici al mondo, la Marina Militare e la US Navy, oltre a numerose Marine estere.

L'attività del Gruppo in questo periodo risente positivamente della crescente domanda globale da parte degli armatori alimentata dalla richiesta di crociere che, secondo i dati di Cruise Lines International Association (CLIA), è aumentata del 68% negli ultimi 10 anni generando ricavi nel 2016 per oltre 39 miliardi di dollari.

Il desiderio di conseguire una differenziazione competitiva, di fornire servizi a valore aggiunto agli armatori e di



rendere più efficienti le proprie attività di progettazione e costruzione, ha portato Fincantieri alla decisione di dotarsi di un'infrastruttura IT globale per il suo sistema Integrated Ship Design and Manufacturing, che consente di gestire in modo integrato il processo di progettazione e costruzione di navi.



Si tratta di un processo particolarmente sensibile alla variabile temporale e che richiede anche funzionalità di provisioning rapido, elevata elasticità e sicurezza. Per rispondere a questa esigenza, al termine di un'analisi di mercato che ha coinvolto un ampio numero di fornitori, Fincantieri ha selezionato IBM Cloud.

«Fincantieri ha sempre considerato l'innovazione tecnologica di prodotto e processo uno strumento fondamentale per rispondere e continuare a fornire gli elevati standard di eccellenza raggiunti - ha osservato Gianluca Zanutto, CIO

di Fincantieri -. Ci siamo affidati al cloud di IBM per ridisegnare la nostra infrastruttura IT e per avere una piattaforma estremamente sicura e scalabile in grado di soddisfare le nostre necessità di fronte a una forte crescita della domanda armatoriale e una conseguente maggiore complessità nel settore della cantieristica navale».

IBM Cloud permette a Fincantieri di predisporre un'infrastruttura ibrida in grado di collegare 13 data center di Fincantieri (privati e distribuiti) con il data center IBM Cloud di Milano. Il risultato è un cloud ibrido

con gli elevati livelli di servizio in termini di disponibilità, affidabilità e sicurezza richiesti dal mondo enterprise.

«Il network globale di data center cloud di IBM consente a Fincantieri di soddisfare la crescente domanda di costruzioni navali - ha dichiarato Stefano Rebattoni, General Manager Global Technology Services, IBM Italia -. Saremo, inoltre, in grado di aiutare l'azienda a integrare agevolmente le altre società controllate e le nuove acquisizioni che contribuiranno a espandere in tutto il mondo la presenza della società».





DELINDA



DELINDA



DELINDA



DELINDA

*Chi segue il mercato sa che le alternative non mancano, ma Delinda fa una scelta di campo fuori dal coro e promette di distinguersi dai competitor*

## Nasce Delinda, e-commerce beauty che vuol fare la differenza

**N**asce dopo mesi di riflessioni, studi di mercato e valutazioni, Delinda. Il nuovo sito di e-commerce che si pone come innovativo punto di riferimento per gli acquisti beauty online. Le alternative, come dicevamo, non mancano. Di siti che offrono, sul mercato, cosmesi e bellezza ce ne sono molti e ben strutturati.

Cosa avrà, dunque, di diverso, Delinda, per portarlo sul mercato italiano con la convinzione di poter davvero funzionare? Intanto il periodo. «Non potevamo non spingere l'acceleratore sul periodo natalizio per un lancio, in un mercato come quello del beauty, che durante il Natale potrà farsi conoscere ampiamente, anche grazie ai massicci investimenti in comunicazione e pubblicità - tradizionale e digitale - che abbiamo stanziato», ha dichiarato Christian D'Acquisto, co-founder di Delinda.

### La premessa sono i numeri

Secondo una ricerca condotta da Human Highway, nel 2015, gli italiani, hanno acquistato online beni e servizi per 20,9 miliardi di euro e a fine 2015 gli acquirenti online sono cresciuti fino a quota 18,8 milioni, di cui 12,8 milioni sono acquirenti online abituali (cioè persone che acquistano con frequenza di almeno mensile). 21 acquisti online ogni 100, in Italia, sono originati da un dispositivo mobile. La quota di acquisti via tablet è rimasta stabile negli

ultimi mesi mentre quella da smartphone ha conosciuto una forte accelerazione, dall'8% di febbraio 2015 al 13,5% dell'anno successivo. Il valore degli acquisti online di cosmetica nel 2015 ha raggiunto 175 milioni di euro ed è cresciuto del 22% rispetto all'anno precedente. Gli acquirenti online di prodotti cosmetici sono stati 4,7 milioni nel 2015, di cui due milioni non saltuari (hanno acquistato più di una volta nei sei mesi). Inoltre, il 16,1%

degli acquirenti di cosmetica esclusivamente tradizionali è un prospect dell'online, ha cioè intenzione di fare il primo acquisto online di cosmetica nei prossimi sei mesi. Il tasso di riacquisto, nell'e-commerce, di prodotti beauty, in generale, è pari al 62,5% e indica che l'esperienza di acquisto online si sta trasformando da prima esperienza a riproduzione di un'esperienza già compiuta in passato. Il tasso di riacquisto nella cosmetica è invece pari al 45,2% e conferma che gli acquirenti stanno scoprendo la nuova modalità di acquisto via Internet in ritardo rispetto ad altri settori. La decisione di acquisto online è guidata dalla ricerca sul web e dalla pubblicità in misura maggiore rispetto alla media dell'e-commerce di prodotti. Infine, tra i motivi che spingono ad acquistare cosmetica online ci sono aspetti legati a considerazioni di convenienza, quali risparmio e offerte oltre a questioni legate alla disponibilità; prodotti difficili da trovare nel mercato fisico tradizionale un ampio catalogo e la presenza di prodotti naturali, bio e vegan.

“The way I am” è il pay off e la



promessa che Delinda vuole condividere, con il suo pubblico, appassionato di bellezza. «Vogliamo offrire una possibilità di acquisto slegata da ogni vincolo sociale, economico, culturale, cercando di non subire - da un lato - l'esclusività di un ambiente troppo di nicchia, dall'altro di far sentire le persone a proprio agio in un universo che propone con semplicità e immediatezza soluzioni allineate alle proprie esigenze, per vivere bene con se stesse ogni giorno» ha concluso D'Acquisto. ❁

# Lexmark porta il document management alla PMI



*Zeendoc for Lexmark è la piattaforma documentale sicura e il sistema di ricerca istantaneo delle informazioni pensato per le esigenze del mercato SMB e caratterizzato da semplicità d'uso e basso costo*

**I**l 2016 è stato un anno record per Lexmark. Pietro Renda, channel and supplies sales director di Lexmark Italia, illustra con orgoglio i dati forniti da IDC Research relativi al mercato italiano dei sistemi di stampa Laser (dispositivi in formato A3 A4, bianco e nero e colore, sia mono sia multifunzione) che assegnano a Lexmark un numero di unità vendute pari a 73.171, con un incremento del 95% rispetto alle 37.397 unità vendute nel 2015. Un dato che alimenta l'obiettivo ambizioso di arrivare nel 2017 a vendere 100mila unità e di guadagnare un +10% di quota di mercato. Si tratta di risultati ottenuti tramite un modello di vendita completamente indiretto costituito da sei distributori (Computer Gross, Esprinet, LDM, Datamatic, Tech Data e Ingram Micro), che trattano sia i prodotti hardware sia i consumabili, e da oltre 4mila rivenditori, di cui 150 partner Silver, 30 partner Gold e

20 Diamond. I 150 partner Silver sono seguiti da un gruppo di tele vendita di Lexmark, mentre i 50 partner con certificazioni Gold e Diamond hanno la possibilità di usufruire di un supporto diretto di Lexmark nel processo di vendita presso i clienti.

Nell'offerta maggiormente a valore Lexmark si affida a 12 business solutions leader che si suddividono il territorio senza interferire tra loro e che, da oggi, hanno a disposizione una soluzione in più da proporre ai loro clienti.

## **Zeendoc for Lexmark**

Si tratta di Zeendoc for Lexmark, una piattaforma per il document management e la ricerca delle informazioni, integrata con i sistemi multifunzione Lexmark, risultato di una partnership con l'azienda franco svizzera Sage Informatique.

La partnership con Zeendoc mette a

disposizione dei clienti di Lexmark un'unica piattaforma documentale sicura e un sistema di ricerca istantaneo delle informazioni, integrato con i suoi dispositivi multifunzione. La soluzione permette di scandire i documenti attraverso un click sul touch-screen dei dispositivi MFP Lexmark e inviarli a Zeendoc grazie alla tecnologia Lexmark Solution Composer. La soluzione è già presente sul mercato francese e svizzero dove ha fornito nel 2016 ottimi risultati.

All'aspetto tecnico si abbina una collaborazione a livello commerciale e di marketing, che prevede l'integrazione della soluzione nel catalogo Lexmark e la predisposizione di azioni commerciali congiunte e promozioni per rivenditori e clienti.

«Zeendoc for Lexmark è una soluzione pensata appositamente per il segmento small business - ha precisato Jean-francois Guiderdoni, international development di Zeendoc - concepito da una PMI per le PMI. Innanzitutto si tratta di una soluzione di semplice utilizzo, dotata di un'interfaccia "Google-like", che è possibile cominciare a utilizzare immediatamente e che si integra senza

problemi all'interno dell'ambiente aziendale esistente. Risolve i problemi relativi a una gestione documentale ad ampio spettro, tenendo conto degli aspetti di sicurezza, garantendo elevata rapidità di accesso alle informazioni e fornendo la capacità di estrapolare e riutilizzare le informazioni. Il tutto a un costo allineato con la capacità di spesa delle PMI».

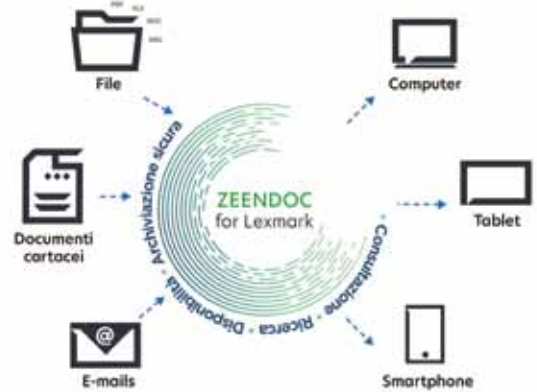
La soluzione supporta un numero illimitato di utenti sfruttando un approccio Software as a Service che prevede la memorizzazione dei documenti in tre formati (di cui uno è il pdf/a) su tre data center a elevata disponibilità. Il trasferimento dei dati avviene su un canale sicuro SSL-https o ftps e i documenti sono cifrati con AES e sottoposti a controlli regolari di integrità dei documenti (MD5).

Zeendoc for Lexmark è in grado di interagire con altri tool quali SAP e tutte le funzioni sono incluse nell'offerta entry level, comprese le tecnologie avanzate di Enterprise Content Management come la capacità di

autoapprendimento.

«La partnership con Zeendoc porta a Lexmark una soluzione ECM focalizzata sul settore SMB, costituito

Acquisizione • Elaborazione • Condivisione



da aziende fino a 500 dipendenti, e veicolata tramite Canale - ha osservato Etienne Maraval, marketing director for Southern Europe di, Lexmark -. L'abbiamo scelta sia per il suo valore tecnologico sia per il fatto di adattarsi molto bene al nostro canale di business solutions dealer, grazie a un modello d'offerta del tipo "pay per documenti flow". Rappresenta per noi un'opportunità per arruolare nuovi dealer anche fuori dal settore printing e un modo, per i dealer, di compensare la riduzione del costo per pagina potendo offrire un elemento di differenziazione all'interno dell'offerta MFP e un modo per aumentare il livello di fidelizzazione».

# NetApp: i trend per l'IT in trasformazione

*L'azienda delinea le direzioni di evoluzione del mercato storage e annuncia due nuovi sistemi All Flash di fascia entry e high end*



Mark Bregman, CTO di NetApp

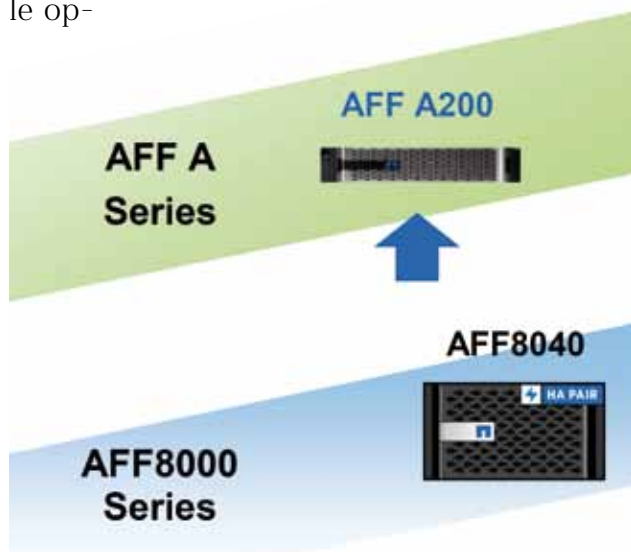
**I**n questo periodo di profonda trasformazione tecnologica, NetApp identifica sei trend che guideranno l'innovazione nel settore dello storage. A delinearli è Mark Bregman, CTO di NetApp, che sottolinea prima di tutto l'importanza dei dati, che continua ad aumentare poiché raccogliere e gestire l'informazione è ormai diventato "il" business e non un meccanismo a supporto del business. Gli esempi a sostegno di ciò non mancano: da Uber a Airbnb, che sono entrambi società costruite sul controllo di una rete di risorse.

Una seconda aspettativa è l'arrivo di nuovi modelli perché la focalizzazione sui dati richiede nuovi servizi integrati e interoperabili per risolvere problemi complessi di ogni tipo i quali, a loro volta, contribuiranno a generare un cambiamento nelle piattaforme tecnologiche e nell'ecosistema a loro supporto. A

sostegno di questo punto di vista NetApp richiama la diffusione di Amazon Web Service come esempio di una nuova piattaforma che è diventata elemento abilitante di nuovi servizi e motore per un nuovo ecosistema di partner.

Il terzo trend è il cloud, che sta diventando catalizzatore e acceleratore del business anche in Ita-

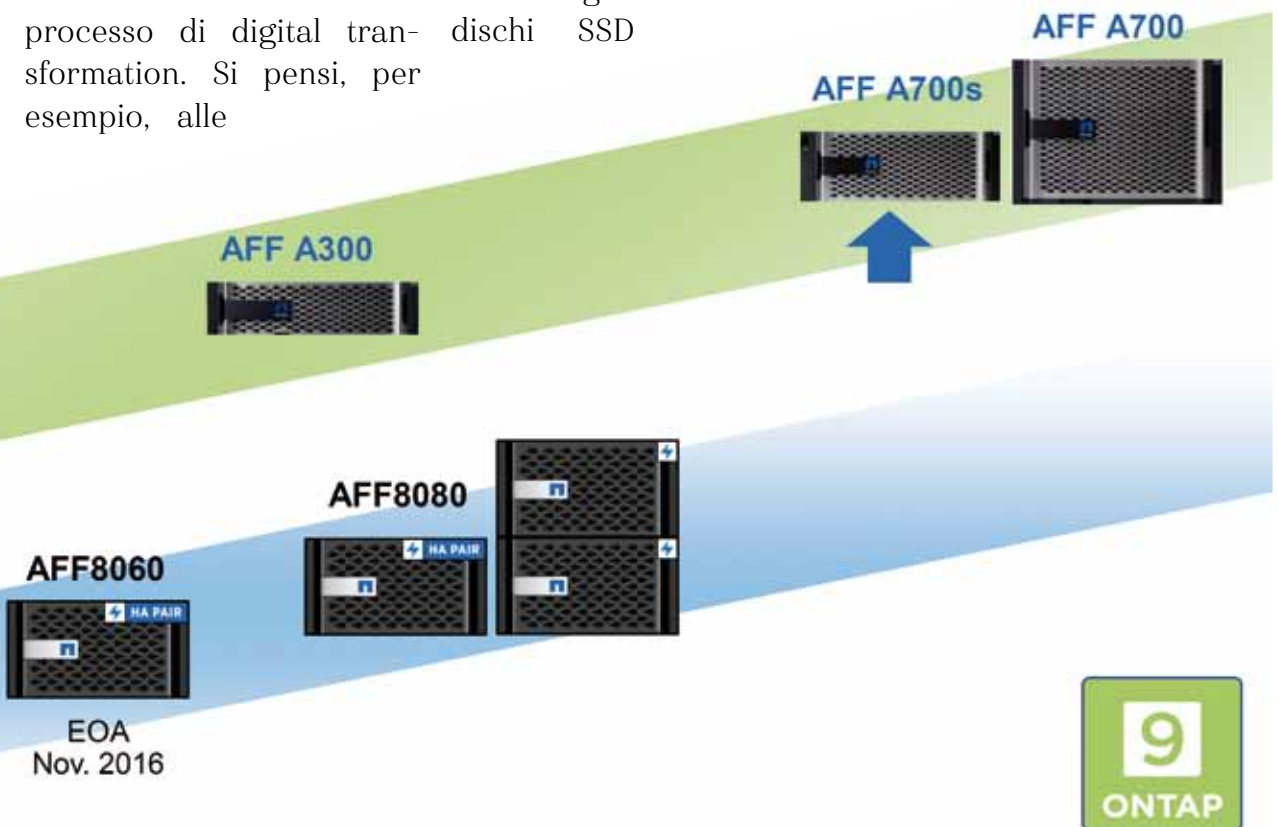
lia, dove sempre più azienda scelgono di spostare i loro workload nella nuvola. «Tra i nostri clienti osserviamo molto fermento - sottolinea Roberto Patano, senior manager Systems Engineering di NetApp - per comprendere in che modo sfruttare le op-



portunità del cloud per operare processi di trasformazione aziendale. Questo ha un'importante ricaduta sullo storage in aspetti quali, per esempio, il backup. A tale riguardo, vorrei ricordare che NetApp ha da poco annunciato un servizio per effettuare anche in locale il backup dei dati di Office 365, indirizzato alle aziende che vogliono poter mantenere anche in casa i propri dati». Un altro trend riguarda la progressiva affermazione di nuove tecnologie che puntano a diventare standard "de facto" mano a mano che ci si addentra all'interno del processo di digital transformation. Si pensi, per esempio, alle

tecnologie DevOps con modelli di propagazione basati su micro servizi e "mashup" così come all'ormai diffusissimo supporto di Open Stack o all'affermazione delle tecnologie Docker. Si amplia, diversifica e si fa più flessibile la disponibilità di tecnologie storage e di data management. Tra queste vi è, innanzitutto, lo sviluppo che stanno avendo i dischi a stato solido in termini di capacità e prestazioni, mentre il costo si riduce. Un tema tecnologico importante sarà quello di creare le condizioni per sfruttare gli IOPS forniti dai dischi SSD

perché il collo di bottiglia, secondo NetApp, è tornato a essere sui server che non riescono a mettere a disposizione un canale di comunicazione sufficientemente veloce. D'altronde, NetApp sottolinea come la sua soluzione all flash AFF A700 sia in grado di fornire oltre 2milioni e 400mila IOPS in un tempo medio di risposta di 0,69 millisecondi (dati: Storage Performance Council SPC-1 Result). Vi è e poi il tema dell'iperconvergenza , rispetto al quale l'attesa è per le soluzioni di seconda



Il portafoglio d'offerta NetApp di sistemi storage All-Flash FAP Serie A

generazione che promettono di affrontare in modo più strutturato la Quality of Service, garantendo prestazioni accuratamente misurabile, a supporto delle esigenze aziendali e dei Service Level Agreement.

Il sesto e ultimo trend è quello della consumerizzazione dell'IT; si tratta di un processo avviato da tempo, che NetApp vede in prosecuzione e che porterà a una maggiore integrazione di servizi e soluzioni pensati per semplificare al massimo l'esperienza d'uso.

«NetApp - ha spiegato Patano - grazie al processo di trasformazione attuato negli ultimi due anni, non è più solo un'azienda che sviluppa sistemi storage, ma vanta una strategia e un portfolio per la data fabric che mette a disposizione l'intera infrastruttura a supporto della memorizzazione e gestione dei dati: file, storage e a blocchi e a object, software-defined, apertura al cloud, gestione, virtualizzazione, hardware e commodity. Un intero ecosistema che permette ai nostri clienti di scegliere. A ciò si aggiungono gli accordi a largo spettro con i principali vendor software».

## Due nuovi sistemi storage All flash

NetApp ha rilasciato due nuovi sistemi storage che completano la famiglia All Flash FAS (AFF) Serie A, affiancandosi ai modelli AFF A300 (midrange) e AFF A700 (high end) annunciati lo scorso settembre. Si tratta dei sistemi AFF A200 e AFF A700s che hanno la caratteristica di poter ospitare anche dischi interni.

Il primo dei due modelli è un sistema entry level di dimensioni 2U dotato di un processore a 12 core (lo stesso utilizzato dal modello AFF 8020) e con una capacità di memoria fino a 64 GB. Per ogni controller prevede 2 porte 10GbE per le applicazioni di Cluster interconnect, 4 porte UTA2 (16Gbps FC oppure 10 GbE) per la connettività verso l'host e 2 porte da 12Gb mini-HD SAS per la connessione di storage esterno.



*Roberto Patano, senior manager Systems Engineering di NetApp*

Il sistema storage AFF A700s è una soluzione di fascia alta, di dimensioni 4U, pensata per applicazioni aziendali esigenti, analytics e integrazione cloud, che dispone di CPU a 72 core, di una capacità di memoria fino a 1024 GB (come il modello AFF A700) e dotata di 4 porte 40 GbE QSFP.

Come tutti i sistemi della famiglia AFF, anche i due nuovi modelli sono pensati per potersi connettere a cloud pubblici come AWS, Azure, IBM Cloud e altri, pur garantendo la massima visibilità e controllo dei dati attraverso il cloud e su ambienti on-premise. «L'array AFF A200 è una soluzione che sono convinto avrà molto successo nel mercato italiano - ha osservato Patano - e tra le piccole e medie aziende che non potevano permettersi una soluzione All-flash ma che, in questo modo, potranno accedere a una soluzione ad alte prestazioni con una scalabilità elevatissima. AFF A700s è una soluzione adatta per chi deve crescere soprattutto in modo orizzontale ovvero alle applicazioni che non richiedono una straordinaria capacità di memorizzazione ma, invece, prestazioni molto elevate».



# Investire nel digitale per sopravvivere alla concorrenza

*Una ricerca di Red Hat mostra i benefici che le aziende possono ottenere investendo in tecnologie per la digital transformation, un percorso non proprio veloce e che coinvolge diverse funzioni aziendali. I vantaggi maggiori però li hanno i nativi digitali*

**S**i sente di frequente parlare di trasformazione digitale delle aziende e dei benefici che derivano dall'adozione di nuove tecnologie come, per esempio, il cloud computing e gli analytics, ma per molte aziende il percorso di innovazione non è una strada semplice anche se ne riconoscono i benefici.

Secondo una ricerca condotta da Red Hat, fornitore di soluzioni tecnologiche open source, e Bain & Company, società di consulenza strategica aziendale, molte aziende tradizionali si trovano ancora all'inizio del loro cammino digitale e le strategie e gli investimenti sulla digital transformation sono ancora in uno stadio iniziale. La ricerca pubblicata dalle due società, dal titolo "For Traditional Enterprises, the Path to Digital and the Role of Containers", ha coinvolto quasi 450 tra executive, decisori e specialisti

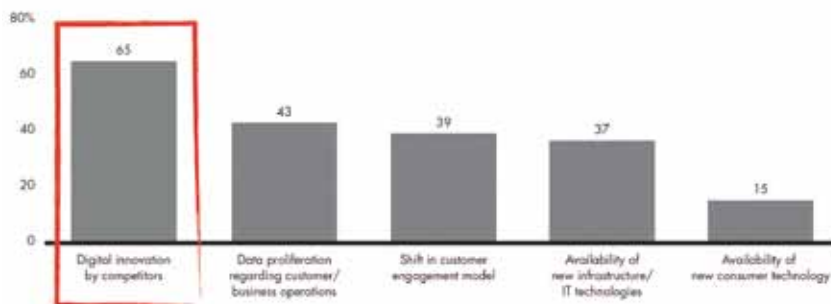
IT di diversi settori negli Stati Uniti e ha mostrato come le aziende che riconoscono il potenziale di una rivoluzione digitale investono in nuove tecnologie, tra cui il cloud computing e lo sviluppo di applicazioni moderne, per avere benefici che vanno da una maggiore flessibilità e capacità di offrire nuovi servizi ai clienti alla riduzione dei costi.

## **I vantaggi della digital transformation**

La dinamicità che caratterizza attualmente il mercato sta mettendo le aziende di fronte alla necessità di sapersi adattare velocemente alle nuove richieste dei clienti e quindi di avere una struttura agile, flessibile e tecnologicamente più avanzata. Per questo motivo la digital transformation riveste un ruolo importante nella strategia di business e molte

On a scale of 1 to 5 (1=not impactful, 5=very impactful), how important have the following forces been in driving digital changes?

Percentage rating 4 or 5



aziende stanno percorrendo questa strada, sfruttando tecnologie come il cloud computing, gli advanced analytics o il mobile per restare competitive.

La ricerca di Bain e Red Hat ha evidenziato i principali benefici che le aziende intervistate hanno riscontrato grazie all'utilizzo delle tecnologie che trasformano il business in digitale.

In particolare è emerso che le aziende che stanno già investendo nel percorso di trasformazione digitale riescono a far crescere la propria quota di mercato di otto volte rispetto a quelle che si trovano a un livello iniziale di adozione.

Un'azienda che utilizza le nuove tecnologie riesce a distinguersi dai competitor anche per la capacità di rispondere velocemente alle esigenze del mercato e quindi di offrire i prodotti più richiesti in modo tempestivo. Questo grazie al fatto che possiede processi

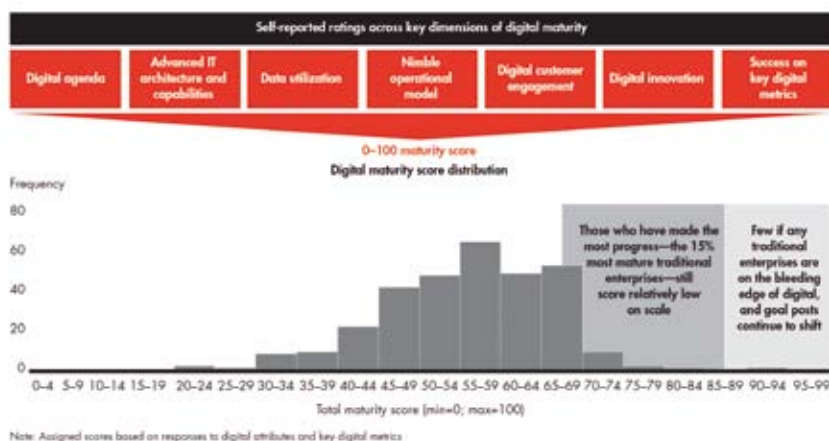
di sviluppo più efficaci e un'infrastruttura più flessibile che consente un time to market più veloce. Inoltre è possibile anche utilizzare la tecnologia dei container per lo sviluppo applicativo. I container consentono di creare ambienti autonomi grazie ai quali è possibile pacchettizzare e isolare le applicazioni con tutte le loro correlazioni a livello di runtime, tutti i file necessari per operare su un'infrastruttura cluster e scale-out. I container sono macchine logiche isolate tra loro che non necessitano di un hypervisor e girano sul medesimo sistema

operativo, grazie all'aggiunta di un componente software, il docker, che permette l'esecuzione delle applicazioni.

Dalle risposte ottenute nella ricerca risulta che le aziende che stanno utilizzando la tecnologia dei container riescono a ottenere concreti vantaggi architetturali come una maggiore flessibilità e, in particolare, si registra una riduzione del 15-30% dei tempi di sviluppo. In più la ricerca indica anche un risparmio del 5-15% legato alla produttività.

## Verso il digitale

Intraprendere la strada verso la trasformazione digitale non è un processo che si sviluppa in poco tempo, ma richiede una strategia continuativa che va distribuita su più anni. I risultati ottenuti dalle aziende che intraprendono questo percorso possono essere diversi e variare a



seconda del contesto di business in cui operano, delle concrete necessità IT e del generale atteggiamento verso la tecnologia. Da notare che, come evidenzia la ricerca, si registrano risultati inferiori nelle aziende tradizionali che hanno intrapreso un percorso di innovazione digitale rispetto alle start-up e alle realtà emergenti che hanno adottato le nuove tecnologie fin dalla nascita, ossia i cosiddetti nativi digitali. In particolare si nota che le aziende che ottengono un avanzamento più importante nell'ambito della digitalizzazione sono quelle che non si limitano a considerare il digitale all'interno di una singola funzione aziendale, ma bensì lo concepiscono come una strategia più estesa che va a includere diverse funzioni e cambiamenti anche in diversi settori del business, come quello organizzativo, di approccio ai processi e allo sviluppo dei prodotti, alle strategie e così via.

Lo ribadisce Jeff Taylor, partner della Technology Practice di Bain e co-autore del report che afferma: «Dando uno sguardo più profondo sulle aziende che abbiamo interpellato, abbiamo visto che quelle che avanzano in



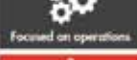
modo più deciso e veloce sulla curva di adozione non si limitano a trattare il digitale come una singola funzione o attività. Lo vedono come una trasformazione estesa, che tocca più funzioni, apportando una serie di cambiamenti a livello di leadership, organizzazione, approccio e processi di sviluppo dei prodotti, strategia e investimenti IT, data governance, strumenti ed altro ancora... Creare capacità digitali sufficienti a generare i risultati desiderati non è una cosa immediata. Il successo richiede un'attività continuativa, distribuita su più anni».

La ricerca ha mostrato che sebbene il 63% delle aziende interpellate abbia costruito processi per rispondere ai trend digitali, solo il 19% considera l'innovazione rapida una priorità. Inoltre, per il 65% circa degli intervistati, il motivo principale che guida

le proprie iniziative digitali è rappresentato dalle attività intraprese dalla concorrenza che rappresenta quindi una spinta a restare competitivi sul mercato. Dimostrano quindi di avere un atteggiamento più di tipo reattivo che proattivo.

La ricerca ha anche valutato la maturità digitale delle imprese tradizionali attraverso attributi chiave e metriche di business come l'uso del digitale per migliorare la capacità di analisi dei dati e la rapida innovazione. In più è stata considerata anche l'agilità, l'adattabilità e la scalabilità della loro architettura IT. Considerando questi fattori risulta che le imprese tradizionali si trovano in situazioni molto variabili rispetto al proprio percorso verso la trasformazione digitale.

Tuttavia, anche tra quelle che hanno fatto i maggiori progressi, il 15% delle imprese

Traditional enterprise segments	
 Digital differentiators	Companies in <b>dynamic industries</b> with innovative/disruptive competitors that see digital innovation as an <b>opportunity to deliver new capabilities and grow markets</b> .
 Shivers	Companies that acutely perceive <b>changes in how customers engage</b> and that <b>invest heavily</b> to keep up.
 Staged and secure	Companies in <b>security-focused industries</b> (e.g., financial services) that use <b>digital platforms and channels</b> but proceed cautiously given security concerns.
 Focused on operations	Companies in moderate growth industries that have been <b>less affected by digital</b> but are using digital to drive <b>operational excellence</b> —often in business-to-business or manufacturing-focused industries.
 Digital skeptics	Companies in industries that have less obvious disruption and/or market forces at play limiting impact (e.g., declining industries)—these companies <b>regard digital as a lower priority</b> and view IT as a back-office function.

più mature, il livello di sviluppo del digitale resta relativamente basso rispetto a quello che ci si aspetterebbe per degli innovatori digitali. All'interno del segmento delle imprese più tradizionali, la ricerca ha anche messo in evidenza cinque segmenti distinti, intersettoriali che emergono a vari livelli di maturità. Ci sono quelli che vengono definiti "digital differentiators", ossia quelle aziende che operano in settori dinamici con concorrenti innovativi che vedono l'innovazione digitale come un'opportunità per offrire nuove funzionalità e crescere nei mercati. Poi ci sono gli "strivers" che percepiscono fortemente i cambiamenti nel modo in cui i clienti vengono ingaggiati e che investono pesantemente per tenere il passo. Quelle che, invece, vengono definite come "staged and secure companies" rientrano nelle

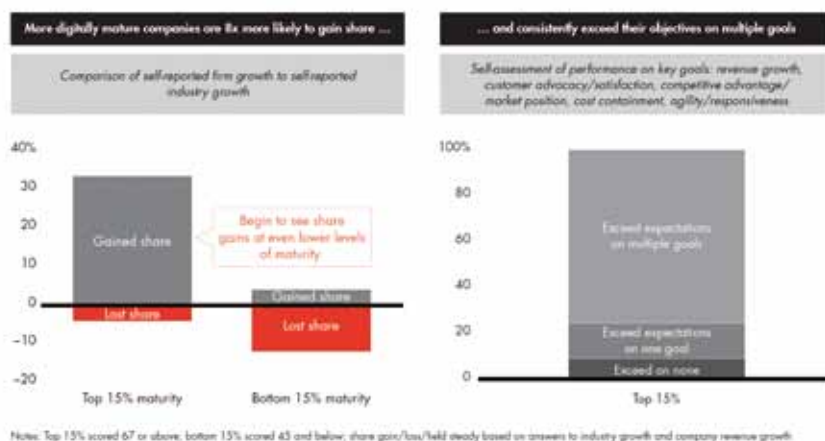
industrie focalizzate sulla sicurezza (per esempio dei servizi finanziari) che utilizzano le piattaforme digitali, ma preferiscono procedere all'adozione con cautela.

Poi ci sono le imprese in settori di crescita moderata che sono state colpite meno pesantemente dal digitale per quanto riguarda la capacità di mantenere un buon livello di operatività e appartengono solitamente al settore B2B oppure all'industria manifatturiera.

Infine c'è il segmento delle imprese ancora "skeptical" (scettiche) che appartengono a settori con meno evidenti disagi o dove le forze di mercato in gioco stanno limitando l'impatto del digitale. In questi casi l'innovazione non rappresenta una priorità e l'IT viene ancora considerato come una funzione di back-office.

Resta evidente che le aziende

che hanno raggiunto un livello più avanzato di maturità digitale riescono a raggiungere risultati maggiori rispetto ai concorrenti e, secondo il report, quelle che si trovano più in alto sulla curva di adozione del digitale hanno una probabilità di 8 volte superiore di guadagnare una maggiore quota di mercato e del 15% di superare costantemente gli obiettivi rispetto alle aziende meno avanzate nell'adozione del digitale. Inoltre quelle più mature investono di più in tecnologie di nuova generazione perché all'infrastruttura è richiesta una maggiore capacità di risultare adattabile, scalabile e agile. In ogni caso, quello che le aziende tradizionali e più mature nel percorso di trasformazione digitale stanno ottenendo è una maggiore adattabilità, resistenza, velocità, capacità di analisi e coinvolgimento dei clienti. Il report mostra, infatti, che se si considera una scala da 1 a 5 il 69% dei dirigenti valuta il suo punteggio tra 4 e 5 quando si tratta di investire in capacità per sviluppare e distribuire rapidamente applicazioni, mentre solo il 12% delle imprese tradizionali meno mature da una valutazione di 4 o 5.



# DOVE TROVI L'INNOVAZIONE PER LA TUA AZIENDA



A partire dalle specifiche esigenze di innovazione, Smau accompagna le imprese nel **percorso verso la scelta dei giusti partner per il loro business**. Per ciascuna tappa del suo Roadshow Smau propone un programma di momenti formativi gratuiti, presentazioni e incontri dove i protagonisti dell'innovazione del nostro Paese possono stringere la mano ai decisori aziendali delle principali aziende italiane.

## IL ROADSHOW 2017

PADOVA, 30-31 MARZO

BOLOGNA, 8-9 GIUGNO

BERLINO, 14-15-16 GIUGNO *internazionale*

MILANO, 24-25-26 OTTOBRE *internazionale*

NAPOLI, 14-15 DICEMBRE

## SMAU IN PILLOLE (dati 2016)



# ABBONATI TI REGALIAMO LA SICUREZZA E IL CLOUD



**DIRECTION**

*la rivista per i professionisti dell'ICT*



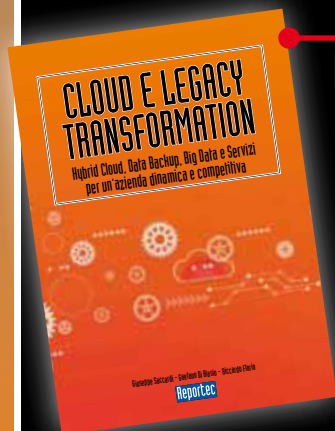
**PARTNERS**

*la rivista per il Canale ICT a valore*

**ABBONATI SUBITO A DIRECTION O PARTNERS  
A SOLI 61 EURO**

**RICEVERAI I 10 NUMERI DEL 2017 E,  
IN OMAGGIO,  
2 LIBRI**

**DEDICATI ALLA SICUREZZA IT  
E AL CLOUD,  
DEL VALORE DI 100 EURO**



vai su

**[www.reportec.it/abbonamenti](http://www.reportec.it/abbonamenti)**  
e compila il modulo di abbonamento