

## LA SOLUZIONE CHIAVI IN MANO DI EXTREME NETWORKS PER IL RETAIL

Grazie a pacchetti basati sulla tecnologia cloud si elimina la complessità della gestione delle reti nel settore del retail.

a pag.08



## TREND MICRO DELINEA IL NUOVO PANORAMA DELLE MINACCE

Trend Micro ha realizzato il nuovo report dal titolo "La nuova normalità: previsioni Trend Micro sulla sicurezza per il 2020" presentato nel corso della quinta edizione del suo Security Barcamp, un evento organizzato per fare luce sulle tendenze per il nuovo anno.

Lisa Dolcini, marketing manager della società in Italia, ha introdotto alla platea presente gli ospiti sul palco, tra i quali Rik Ferguson, Vice President Security Research di Trend Micro e Gastone Nencini, Country Manager di Trend Micro Italia. Al loro fianco anche la Polizia postale e il Politecnico di Milano. Le minacce saranno sempre più complesse avranno la tendenza a combi-



nare i rischi tradizionali con le nuove tecnologie, come l'intelligenza artificiale che verrà utilizzata per compiere truffe aziendali.

a pag.03

## TECH DATA DISTRIBUISCE LA SICUREZZA DI CHECK POINT

Il vendor di sicurezza si affida al distributore per supportare l'adozione delle proprie soluzioni e in particolare in ambito cloud

a pag.05



## SOMMARIO

- Le previsioni di Trend Micro elencate in breve pag.04
- Qualys nomina il nuovo Chief Marketing Officer pag.05
- DotForce sigla un accordo con ExtraHop Networks pag.06
- Servizi gestiti e cyber security trainano i risultati di NovaNext pag.06
- Cresce la richiesta di infrastrutture iperconvergenti pag.07
- UCC all'avanguardia in Moustache Bikes con i telefoni IP Snom pag.09
- Più sicurezza con il Next-Generation Security Operations Center di Lutech pag.10

Partners Flip  
anno IX - numero 252 - quindicinale

Direttore responsabile: Gaetano Di Blasio

In redazione: Giuseppe Saccardi, Paola Saccardi, Edmondo Espa.

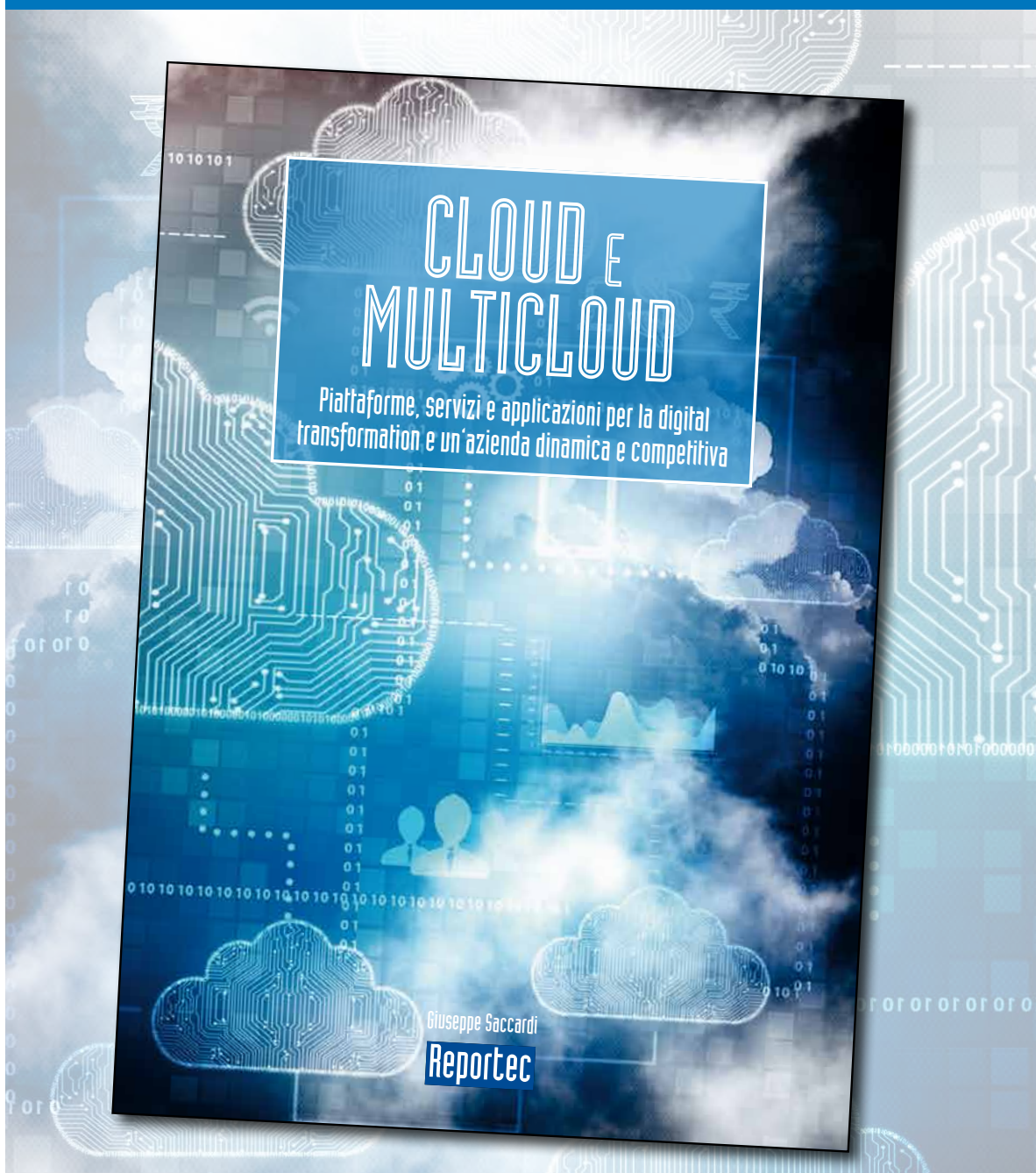
Redazione: via Marco Aurelio, 8 - 20127 Milano  
Tel 0236580448 fax 0236580444 www.partnersflip.it

Proprietà: Reportec srl, via Gian Galeazzo 2, 20136 Milano

Iscrizione al tribunale di Milano n°514 del 13/10/ 2011

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

È disponibile il nuovo libro  
**CLOUD e MULTICLOUD**



**ORDINA E RICEVI SUBITO LA TUA COPIA DEL LIBRO!**

AL COSTO DI **35 EURO** (Iva e spedizione inclusa!)

chiamaci allo 02.36580441  
oppure scrivi a [info@reportec.it](mailto:info@reportec.it)

# Trend Micro delinea il nuovo panorama delle minacce

*Le minacce alla sicurezza non calano, anzi, aumentano con la diffusione delle nuove tecnologie. Lo rivela il Report 2020 della società*

di Paola Saccardi

Da 32 anni Trend Micro si impegna per contrastare le minacce informatiche, a partire dall'antivirus per arrivare alle minacce più complesse che riguardano infrastrutture IT in continua evoluzione e con minacce che si evolvono.

Oggi si assiste a un'ampia varietà di applicazioni, servizi e piattaforme e tutto va protetto. Le minacce sempre più complesse avranno la tendenza a combinare i rischi tradizionali con le nuove tecnologie, come l'intelligenza artificiale che verrà utilizzata per compiere truffe aziendali. Restano sempre presenti alcune minacce che si ripetono da anni, come estorsioni e phishing, ma i rischi maggiori arriveranno dalle migrazioni cloud e dagli ambienti DevOps, che esporranno le organizzazioni a rischi anche di terze parti.

Con questo scenario in corso Trend Micro ha realizzato il nuovo report dal

titolo *“La nuova normalità: previsioni Trend Micro sulla sicurezza per il 2020”* presentato nel corso della quinta edizione del suo Security Barcamp, un evento organizzato per fare luce sulle tendenze per il nuovo anno.

**Lisa Dolcini**, marketing manager della società in Italia, ha introdotto alla platea presente gli ospiti sul palco, tra i quali **Rik Ferguson**, Vice President Security Research di Trend Micro e **Gastone Nencini**, Country Manager di Trend Micro Italia. Al loro fianco anche la Polizia postale e il Politecnico di Milano.

Rik Ferguson ha ricordato che 7 anni fa veniva presentato il Project2020, un documento che portava alla luce le previsioni sul futuro della tecnologia. Ferguson, che ha commentato i trend in corso, ha ironizzato: «Ora che siamo nel 2020 possiamo vedere cosa abbiamo indovinato e

cosa è andato diversamente» riferendosi per esempio alla

diffusione dell'augmented reality di cui si era previsto un maggiore utilizzo e potenziali pericoli. Il ricercatore ha anche sottolineato che il mondo online e quello reale sono sempre più “vicini” tanto che in futuro gli hacker potranno riuscire a «minacciare la percezione della realtà delle persone».

Gastone Nencini, invece, ha ricordato l'importanza di fare informazione alle persone, ai cittadini, per istruirle sui potenziali rischi informatici. Trend Micro in questo senso si sta impegnando in Italia per diffondere questa cultura, anche tra i giovani attraverso un programma di volontariato presso le scuole.

La Polizia postale ha sottolineato come il fenomeno



Da sin: Salvatore la Barbera, Gastone Nencini e Rik Ferguson

della truffa si basi spesso sulla falsificazione e simulazione. «Un soggetto che finge di essere un altro, solitamente tramite e-mail rubate, per ingannare qualcuno che opera all'interno di aziende o istituti bancari» ha spiegato **Salvatore La Barbera**, dirigente della Polizia Postale di Milano, con una vasta esperienza nel settore della criminalità, che lo ha portato ad occuparsi di financial hacking, frodi telematiche su larga scala, uso fraudolento dei mezzi elettronici di pagamento e attacchi informatici. La Barbera ha spiegato che la Polizia postale ha intrapreso un progetto con il mondo bancario per raccogliere informazioni sui destinatari delle frodi e per inserire all'interno di

un'apposita banca dati gli iban che risultano sospetti e verso i quali vengono a priori congelati i trasferimenti di denaro, per evitare possibili truffe.

La tecnologia è sempre più pervasiva e abbraccia tutti i settori, da quello aziendale, a quello bancario, ai cittadini privati alla pubblica amministrazione, perché consente evidenti vantaggi, ma allo stesso tempo non è immune da possibili attacchi informatici.

### **Dove sono i rischi**

Con la diffusione del cloud computing in un numero

sempre maggiore di aziende, ma non solo, soprattutto in quelle di dimensioni minori che grazie al cloud possono ottenere vantaggi prima insperati, i rischi per la sicurezza saranno in aumento.

Lo studio di Trend Micro evidenzia che i cyber criminali cercheranno di impadronirsi sempre più dei dati custoditi nel cloud, attraverso attacchi basati su immissioni di codice che prenderanno di mira sia i cloud provider sia le librerie di terze parti.

Secondo quanto suggerito dal report, il maggior utilizzo di codice di terze parti

che alimenta la cultura DevOps farà aumentare i rischi. I componenti compromessi dei container e delle librerie utilizzate in architetture serverless e di microservizi, fanno aumentare la superficie dell'azienda esposta ai rischi e i metodi di difesa tradizionali faranno fatica a tenere il passo.

Un altro settore a rischio è quello dei Managed Service Provider, che i criminali informatici sarebbero interessati a colpire per raggiungere altre organizzazioni e non soltanto per rubare i dati critici, ma anche per installare mal-

ware e sabotare fabbriche intelligenti oppure estorcere denaro attraverso il ransomware.

Infine, un altro ambito in cui bisognerà fare attenzione sarà quello della supply chain. Spesso i lavoratori si connettono da remoto attraverso reti Wi-fi poco protette oppure creando dei potenziali rischi alla sicurezza ma anche le aziende che inter-scambiano i dati in modo digitale. Anche le vulnerabilità nei dispositivi domestici connessi potranno essere utilizzate come punto di accesso alle reti aziendali.

## **LE PREVISIONI DI TREND MICRO ELENcate IN BREVE**

### **Il futuro è complesso**

- Gli attaccanti non avranno problemi ad aggirare patch incomplete e applicate in modo affrettato
- I cybercriminali utilizzeranno le piattaforme blockchain per le transazioni clandestine
- I sistemi bancari saranno nel mirino con open banking e malware per bancomat
- I deepfake creati con l'intelligenza artificiale saranno la nuova frontiera delle frodi aziendali
- I Managed Service Provider saranno colpiti per distribuire malware e scatenare attacchi supply chain
- Gli attaccanti approfitteranno dei bug trasformabili in worm e deserializzazione

### **Il futuro è esposto**

- I cyber criminali utilizzeranno dispositivi IoT per azioni di spionaggio ed estorsione
- Chi adotterà il 5G dovrà mettere al sicuro le reti

software-defined

- Le infrastrutture critiche saranno colpite da ulteriori attacchi e fermi della produzione
- Gli ambienti home office e di lavoro da remoto ridefiniranno gli attacchi supply chain

### **Il futuro è mal configurato**

- Le vulnerabilità dei container saranno tra i principali problemi di sicurezza per i team DevOps
- Le piattaforme serverless aumenteranno la superficie di attacco a causa di errori di configurazione e codici vulnerabili
- Errori di configurazione da parte degli utenti e il coinvolgimento di terze parti non sicure, aumenteranno i rischi nelle piattaforme cloud
- Le piattaforme cloud saranno preda di attacchi basati sulle loro vulnerabilità come gli SQL injection, attraverso librerie di terze parti

# Tech Data distribuisce la sicurezza di Check Point

*Il vendor di sicurezza si affida al distributore per supportare l'adozione delle proprie soluzioni e in particolare in ambito cloud*

di Paola Saccardi

Tech data ha annunciato un nuovo accordo di distribuzione per le soluzioni di sicurezza end-to-end di Check Point Software Technologies. Le soluzioni Check Point offrono una protezione completa degli attacchi informatici e forniscono una prevenzione uniforme e in tempo reale contro le minacce note e sconosciute.

Roberto Pozzi, Regional Director Southern Europe, Check Point Software Technologies ha dichiarato: «Abbiamo scelto di stringere un accordo di collaborazione con Tech Data a livello italiano con il fine di rafforzare ulteriormente la leadership di Check Point in ambito cyber security grazie alle competenze tecnologiche di questo distributore. Siamo particolarmente orgogliosi di iniziare questa nuova partnership a valore che rappresenta un ulteriore step per raggiungere risultati strategici importanti soprattutto in ambito cloud, che continua a

restare una delle principali sfide della sicurezza informatica».

Tech Data offre diverse tipologie di servizi gestiti in ambito cyber security. Con la suite di servizi del distributore, RECON Security Managed Services, i reseller possono offrire soluzioni specifiche per next generation firewall, endpoint, identity e servizi supplementari quali monitoring e reporting. Grazie all'accordo con Check Point verranno disegnati ulteriori nuovi servizi per il canale, sempre garantendo elevata competenza, SLA in linea con le esigenze di mercato e costi competitivi, fa sapere il distributore.

Vincenzo Bocchi, One Software and Next Generation Technologies Director Tech Data ha commentato: «L'accordo di oggi rappresenta un passo importante nel percorso di trasformazione del canale perché con un brand di sicurezza a portfolio come Check Point possiamo guidare i nostri

partner nell'adozione nel campo della security di nuovi modelli di business ed architetturali, in linea con quanto ci chiedono cloud ed IoT, che ancora oggi vedono la security portata sul mercato in maniera tradizionale. E' un investimento in competenze ed innovazione che sia noi sia Check Point stiamo portando in Italia per offrire una value proposition importante per i nostri partner». Massimiliano Bossi, Channel and Territory Sales Manager Italy, Check Point Software Technologies, ha aggiunto: «Siamo entusiasti di questa nuova alleanza strategica e siamo convinti che riuscirà ad accelerare il consolidamento e l'espansione dei nostri obiettivi di business in ambito cyber security sul territorio italiano. Riteniamo Tech Data uno dei principali player sul mercato in grado di supportare lo sviluppo dell'ecosistema Check Point, garantendo un percorso di reciproca soddisfazione».

## Qualys nomina il nuovo Chief Marketing Officer



Il fornitore di soluzioni di sicurezza e compliance basate su cloud, Qualys, ha annunciato una nuova carica per **Dan Barahona** in qualità di Chief Marketing Officer (CMO) per agevolare le nuove fasi di crescita della società. Dan dirigerà a livello internazionale il team di marketing dell'azienda e supervisionerà le strategie, il brand, le comunicazioni aziendali, le attività di lead generation e tutte le altre iniziative di go-to-market.

Con una carriera di oltre 20 anni alle spalle, il manager ha acquisito esperienza in diverse posizioni nel settore della sicurezza informatica. In precedenza, è stato Chief Marketing Officer per Anomali, società che si occupa di soluzioni di intelligence sulle minacce, e prima ancora ha ricoperto il ruolo di Executive Vice President Worldwide Field Operations per Qualys. A questo si aggiunge anche l'expertise maturata nelle attività commerciali e nello sviluppo di prodotti per organizzazioni come ArcSight e WatchDox.

# DotForce sigla un accordo con ExtraHop Networks



DotForce, distributore con sede a Vimercate (MI) specializzato in soluzioni di cyber security per il mercato enterprise, ha siglato una nuova partnership con ExtraHop Networks, una società di Network Traffic Analysis con sede a Seattle.

Da 13 anni il distributore si occupa di selezionare attentamente le tecnologie più innovative da introdurre sul mercato italiano per la difesa preventiva. La piattaforma di ExtraHop Networks, Reveal(x), è una soluzione di analisi dei dati di rete che fornisce informazioni cruciali sulle mi-

nacce, machine learning e automazione delle indagini, a supporto dei team di sicurezza. «Con ExtraHop ci rivolgiamo agli operatori professionali (VAR, Systems Integrator, Service Provider) che lavorano con grandi aziende nei più svariati mercati verticali - spiega **Fabrizio Bresani**, Managing Director di DotForce -. A differenza di altre soluzioni, Extrahop Reveal(x) si basa sull'unica fonte completa di informazioni: la rete stessa. La piattaforma è in grado di analizzare in tempo reale le informazioni che provengono da ogni livello di

rete (dal L2 al L7), fornendo informazioni critiche sia sulle performance sia sulla security».

La tecnologia ExtraHop, spiegano, è progettata per soddisfare le esigenze delle infrastrutture enterprise ibride moderne, dal core al cloud, con grande scalabilità. Permette di eliminare i punti ciechi nell'infrastruttura e il rumore di fondo generato da falsi alert, offrendo un'analisi del traffico di rete in tempo reale e tecniche di machine learning in grado di garantire visibilità approfondita per attivare risposte immediate.

L'analisi in tempo reale

consente di rilevare e classificare tutti i dispositivi e le risorse sulla rete, mappare tutte le connessioni e le dipendenze e monitorare il flusso di traffico fino a 100 Gbps per singola appliance (incluse le sessioni crittografate SSL o PFS), rilevando e analizzando le anomalie, a livello di singolo pacchetto. La visibilità in real time su tutta l'azienda ibrida include anche il traffico cloud.

La tecnologia ExtraHop può essere implementata on-premise oppure in servizi di cloud pubblico come Amazon Web Services (AWS) e Microsoft Azure.

# Servizi gestiti e cyber security trainano i risultati di NovaNext

NovaNext, system integrator italiano che progetta e realizza servizi e soluzioni ICT a supporto del business, ha annunciato i risultati relativi alla chiusura dell'anno fiscale 2019.

L'anno, ha evidenziato l'azienda, è stato caratte-

rizzato da una forte crescita sia a livello economico che di organico, oltre che dal lancio di importanti iniziative mirate allo sviluppo e al perseguimento dell'eccellenza operativa. A livello finanziario il fiscal year 2019 si è chiuso con ricavi pari a 34,8 milioni di

euro, con una crescita del 27% sull'anno precedente e con un CAGR sugli ultimi 5 anni di oltre il 17%.

La crescita, come osservato, non è stata solo a livello di fatturato. Anche per quanto concerne le risorse umane NovaNext ha registrato una forte crescita,

ed alla data conta 150 dipendenti, un +20% sull'anno precedente, ed è alla ulteriore ricerca di talenti per rafforzare ancor più il proprio organico.

Alla crescita del personale si è abbinata nel 2019 anche quella degli investimenti, a partire dall'aper-

tura della nuova sede aziendale di Roma con spazi dedicati agli uffici di commerciali e tecnici per il territorio del Centro Italia ed aule per i percorsi formativi.

E' poi stata potenziata anche la business unit CyberNext dedicata ai servizi di

cyber security.

«La nostra continua crescita è la conferma della validità del nostro modello di business, incentrato nell'offrire alle aziende italiane soluzioni affidabili ed innovative che le affianchino nel loro percorso verso la Digital Transfor-

mation. La partnership con NovaNext, si traduce in sostanziale crescita del loro business nella sicurezza dell'operatività, grazie ai servizi gestiti della nostra piattaforma CyberNext - ha commentato i più che lusinghieri risultati **Giovanni De Giovanni**, CEO

di NovaNext -. Il potenziamento della business unit CyberNext, interamente dedicata a fornire servizi in ambito cyber security, rappresenta un ulteriore passo nel proteggere il business dei nostri clienti e rendere più sicura e affidabile la loro struttura ICT».

## TENDENZE

# Cresce la richiesta di infrastrutture iperconvergenti

*Le infrastrutture iperconvergenti sono sempre più adottate nella modernizzazione dei data center e per ambienti cloud ibridi. I dati di mercato di IDC*

di Giuseppe Saccardi

L'adozione di infrastrutture iperconvergenti (HCI) in Italia e nel mondo continua ad accelerare a mano a mano che aumenta l'esigenza da parte delle aziende di modernizzare e trasformare in chiave digitale i propri data center.

Il motivo, osserva la società di ricerche IDC, risiede nel fatto che per molte organizzazioni alla ricerca di agilità, facilità di gestione e razionalizzazione dei costi, l'infrastruttura iperconvergente rappresenta oggi la migliore soluzione possibile, come peraltro evidenziano i più recenti sondaggi condotti dalla società.

Ciò rispecchia anche la situazione nazionale, con il

70% delle imprese italiane che vedono nei sistemi iperconvergenti uno dei principali abilitatori della modernizzazione delle infrastrutture IT, con particolare riferimento agli ambienti legacy.

In sé non è del tutto una novità. HCI ha cominciato a diventare popolare una decina di anni fa, ma solo con la recente maturazione della tecnologia ha iniziato a divenire una sorta di standard de facto se non de jure per il consolidamento di data center, la gestione di applicazioni business-critical e l'implementazione di cloud ibridi.

Molte aziende stanno poi implementando HCI sia per



carichi di lavoro tradizionali sia per moderni workload con ordini di grandezza tipici del mondo web.

### **HCI abilita un salto generazionale**

IDC ritiene in proposito che l'adozione di HCI sia necessaria per poter compiere quel salto generazionale verso architetture software-defined e API-driven in

grado di portare vera automazione e intelligenza infrastrutturale nelle aziende, indispensabile o quasi per competere a livello applicativo e quindi di processi e servizi nell'economia digitale.

Sull'onda dell'adozione in aumento, IDC ha stimato il mercato complessivo HCI pari a 12 miliardi di dollari nel 2019.

# La soluzione chiavi in mano di Extreme Networks per il retail

*Grazie a pacchetti basati sulla tecnologia cloud si elimina la complessità della gestione delle reti nel settore del retail*

di Paola Saccardi

**E**xtrême Networks ha annunciato l'offerta di pacchetti Extreme Retail Select, progettati per eliminare i costi e le complessità legate all'installazione e gestione dei servizi di rete nelle strutture retail.

I pacchetti si basano su un ambiente cloud dedicato per il retail e un'offerta pre-selezionata di hardware e servizi che permettono alle organizzazioni centrali di implementare e supportare i punti vendita periferici da ogni postazione remota. In pratica si tratta di una soluzione chiavi in mano, che automatizza il setup dei nuovi store.

## I pacchetti disponibili

I pacchetti Extreme Retail Select, già disponibili attraverso i reseller, sono stati ottimizzati per le esigenze del settore retail, quindi offrono una connettività trasparente e per gli utenti lo stesso livello di servizio e personalizzazione che possono avere online. È possi-

bile scegliere tra sei configurazioni, che vanno dalle esigenze di una connettività di base fino ad ambienti di rete ad alte prestazioni. I pacchetti di base comprendono gli strumenti necessari per connettere i clienti, i dipendenti e tutti gli apparati sul punto vendita e integrano strumenti di analisi. I pacchetti avanzati offrono funzionalità per il monitoraggio dei prezzi in tempo reale, la gestione intelligente degli scaffali e il digital signage, e la gestione distribuita degli ordini. Questi pacchetti sono ulteriormente segmentati per le esigenze di punti vendita di varie dimensioni.

## Installazione e gestione

**L**e configurazioni includono l'accesso a un cloud dedicato per il retail 'ExtremeCloud IQ for Retail' e sono pacchettizzate con i nuovi access point Wi-Fi 6, gli switch PoE e i router SD-WAN.

ExtremeCloud IQ è l'archi-

tettura cloud di terza generazione che sfrutta sia machine learning che intelligenza artificiale. La combinazione di hardware, software e servizi, spiega il vendor, permette di realizzare una rete flessibile basata sul cloud, in grado di scalare per adeguarsi alle oscillazioni della domanda del settore retail. Inoltre, permette di contenere i costi di procurement riducendo il numero delle soluzioni.

## Analisi e monitoraggio

Grazie al pannello di controllo è possibile avere visibilità completa sui clienti e sulla rete per tutti i clienti, le applicazioni e gli apparati IoT, insieme a un'analisi delle prestazioni del punto vendita a confronto quelle delle altre location. I responsabili di negozi o aziende hanno visibilità dei KPI come il tempo di permanenza, i flussi e la fide-

lizzazione.

Gli utenti IT hanno, invece, visibilità sui tempi di risposta, l'utilizzo delle applicazioni in rete e gli allarmi. Una visione a 360 gradi degli utenti e della rete offre il vantaggio al team responsabile di avere a disposizione un'analisi avanzata per sfruttare la presenza e la prossimità dei clienti, e fare comparazioni.

## Sicurezza

Un altro aspetto non meno importante riguarda la sicurezza. Grazie alla conformità PCI gli amministratori possono garantire i dati degli utenti e dell'azienda, e al tempo stesso proteggerli grazie alla segmentazione e al controllo granulare che isolano il traffico dei clienti da quello del punto vendita. ExtremeCloud IQ for Retail è certificato ISO/IEC 27001.



# UCC all'avanguardia in Moustache Bikes con i telefoni IP Snom

*Moustache Bikes, produttore di bici elettriche, ha adottato i telefoni IP di SNOM, interoperabili con la piattaforma UCC di 3CX e dotati di ampie funzionalità*

di Giuseppe Saccardi

Specializzata nella produzione di e-bikes, Moustache Bikes è una società francese che è stata fondata nel 2011. Con sede nei Vosgi, Moustache Bikes ha un organico di 100 persone, nel 2018 ha prodotto 25.000 biciclette e dispone di un portfolio prodotti con oltre 65 modelli di biciclette, da quelle elettro assistite alle classiche mountain bikes per piste sterrate.

Nel corso del trasferimento in locali più grandi, dislocati in diversi edifici geograficamente distribuiti, l'azienda ha deciso di rinnovare il proprio impianto telefonico. Su consiglio del suo System Integrator di fiducia, l'azienda ha adottato la soluzione UC di 3CX, un centralino basato sullo standard aperto SIP.

Nell'ambito delle operatività quotidiane la soluzione di UCC di 3CX consente all'azienda di avvalersi di applicazioni compatibili con i diversi tipi di termi-

nali e sistemi operativi presenti in uffici e fabbriche quali Mac, PC o laddove ne fruisce tramite browser in modalità SaaS.

Tramite l'utilizzo di iPhone compatibili in toto con le funzionalità della soluzione di UCC gli addetti hanno la possibilità di fruire delle funzioni di telefonia e collaborazione, tra cui anche la programmazione di conferenze audio o video o la creazione di gruppi di chiamata.

«Lato terminali abbiamo optato per i prodotti Snom perché pienamente compatibili con il 3CX. Abbiamo scelto Snom ([www.snom.com](http://www.snom.com)) dopo un periodo di valutazione durante il quale abbiamo testato altri terminali, palesatisi non all'altezza delle esigenze. Volevamo dotarci di telefoni IP che consentissero di beneficiare di funzionalità semplici come, per esempio, una directory e una rubrica condivisa. Il periodo di validazione è durato



quasi 6 mesi e alla fine è stato Snom a soddisfare tutti i nostri requisiti grazie alla sua piena compatibilità con il centralino 3CX. Il livello di prezzo equiparabile a soluzioni della concorrenza ha ulteriormente favorito la nostra scelta» ha spiegato **Ludovic Vilderdmuth**, IT Manager di Moustache Bikes.

Per quanto concerne l'architettura, Moustache Bikes ha optato per installare la soluzione 3CX on premise su server Debian virtualizzato.

L'installazione on-premise è stata adottata non solo per mantenere il pieno controllo della soluzione e delle sue evoluzioni, ma anche per garantire la conformità al GDPR in termini

di tutela dei dati.

Per quanto riguarda i telefoni, la parte più interessante dell'installazione coinvolge circa una ventina di dipendenti che si avvalgono dei terminali IP Snom presso una sede in cui la mobilità tra uffici, officine e magazzini è essenziale.

Con 20 telefoni IP cordless DECT Snom M65, cinque stazioni base DECT multicella Snom M700 e due terminali per conferenze telefoniche gli utenti dispongono, ha spiegato l'azienda, degli strumenti necessari per svolgere le proprie mansioni, terminali che hanno permesso di creare un ambiente di lavoro agile che risponde all'esigenza di dinamicità dell'azienda e del mercato.

# Più sicurezza con il Next-Generation Security Operations Center di Lutech

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

di Giuseppe Saccardi

Le aziende si trovano a fronteggiare la necessità di sicurezza di fronte alla trasformazione digitale e all'utilizzo di diverse tecnologie, come per esempio, il cloud o gli endpoint nella mobility.

La scarsità di esperti e la necessità in un mondo estremamente competitivo di concentrarsi sul proprio core business richiede un ripensamento delle strategie aziendali in termini di investimento.

È una sfida complessa e per aiutare ad affrontarla il Gruppo Lutech ha orchestrato un approccio alle sfide che nel 2020 le aziende dovranno fronteggiare operando su due piani, quello delle risorse umane e del know how, e quello tecnologico.

## Una risposta alle sfide della sicurezza

Sul piano tecnologico la risposta alle esigenze delle aziende per una migliore cyber security si è concre-

tizzata nell'inaugurazione, all'interno del Services Operations Center di Cinisello Balsamo (MI), di un proprio Next-Generation Security Operations Center NG SOC.

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

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

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

Il SOC si sviluppa su 3 mila metri quadri di superficie e dispone di 330 postazioni operative attive h24, è dotato di impianti tecnologici ridonati ed è affiancato

da due siti secondari situati l'uno a Padova e l'altro a Torino in modo da garantire la continuità del servizio erogato anche in condizioni di disastro.

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

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

«La sicurezza informatica oggi non può più essere solo un elemento per la mitigazione del rischio, ma deve far parte della



Tullio Pirovano - AD di Lutech

strategia di crescita delle aziende. È a tutti gli effetti un vantaggio competitivo e garantisce la corretta gestione e protezione dei dati aziendali e la piena aderenza alle norme di compliance» ha dichiarato **Tullio Pirovano**, Amministratore Delegato di Lutech.

Oltre al rafforzamento del portfolio servizi e tecnologico la società ha ampliato anche il patrimonio delle conoscenze.

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