Cloud & Business

n.73
Settembre 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

CRESCE LA TELEFONIA IP "AS A SERVICE" GRAZIE A TERMINALI IP

Telefonia as a service sempre più diffusa. Un ultimo esempio è un ambiente universitario che ha adottato una piattaforma ridondata e telefoni VoIP flessibili e soprattutto sicuri

I ritmi della telefonia sono stati sempre più lenti di quelli dell'IT, e per ragioni oggettive. Cambiare un sistema telefonico non è mai stato semplice come cambiare un server o un Pc. I fattori da analizzare sono tanti, non ultimo il piano di ammortamento, la confidenza degli utenti con i dispositivi a disposizione, i servizi forniti, il supporto specializzato, eccetera.

Per queste a numerose altre ragioni quando scadono i contratti di manutenzione della piattaforma di telefonia, a volte ancora di tipo proprietario, gli IT manager si trovano di fronte a un bivio: rinnovare l'impianto esistente o sostituirlo con

Telefono IP Snom D765

Reportec Cloud&Business - Numero 73- Settembre 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 - Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

Università di Greifswald

soluzioni aperte, più al passo con i tempi a livello funzionale e meno impattanti in termini di TCO. Tertium non datur.

Per quanto concerne soluzioni aperte, ad esempio, si sta diffondendo Asterix, una piattaforma Open Source utilizzabile per realizzare centralini telefonici (PBX- Private Branch Exchange) VoIP. La piattaforma è molto ricca funzionalmente per quanto concerne a telefonia e supporta anche il video H.263 e H.264.

A questo aggiunge funzionalità Fax, Email con supporto Smtp, funzionalità di Instant Messaging (compreso Instant Messaging server, configurazione via Web, interconnessioni con Yahoo, MSN Messanger, e altri sistemi), a cui aggiunge il supporto LDAP

Il ricco set di funzioni e il fatto di essere aperta ha portato all'adozione della soluzione di telefonia basata su Asterix (o altre piattaforme più o meno aperte) sia a livello universitario che delle piccole aziende, che hanno optato per nuove soluzioni di proprio sviluppo adattate in qualche modo alle proprie esigenze, corredandole di telefoni IP che erogano stabilmente quanto meno le funzionalità di base.

Ma non tutto è oro ciò che luccica o, detto altrimenti, il diavolo si nasconde nei dettagli, e questo dettaglio, si fa per dire, è costituito dal problema sicurezza. In alcuni casi, osserva Snom, non solo per l'IT Manager aziendale ma anche nelle Università, la sicurezza delle comunicazioni e l'inviolabilità dei terminali IP ha la priorità sull'investimento di risorse e tempo investito in attività di sviluppo del centralino, a fronte di esigenze particolarmente articolate e di un numero elevato di interni da servire con funzionalità avanzate.

Telefonia IP e cloud sicuro all'Università di Greifswald

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

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

L'obiettivo era garantire che solo i terminali autorizzati potessero accedervi. Misure simili di protezione di porte specifiche sono impiegate di norma solo in reti che presentano particolari criticità lato sicurezza. La sfida per gli attori coinvolti (l'operatore di telefonia, l'Università di Greifswald e il produttore dei terminali) era automatizzare il processo di trasferimento protetto della chiave di sicurezza ai numerosi telefoni. Una prima inizializzazione e configurazione identica della porta dati dei terminali condotte in locali protetti e, una volta collocati i telefoni nei vari reparti, l'attivazione tramite IEEE 802.1x e EAP-TLS, hanno azzerato la necessità di interventi manuali durante l'installazione.

E' un processo che garantisce, ha osservato Snom, che in caso di furto l'intero parco instal-

lato di terminali Snom possa essere dotato rapidamente di nuove chiavi di sicurezza, rendendo quella presente sul telefono trafugato quasi immediatamente inutilizzabile, vanificando in sostanza qualsiasi tentativo di estrazione dei parametri di cifratura.
Al momento, ha spiegato Snom, sono circa 2000 i telefoni Snom D765 attualmente installati presso l'Istituto Universitario da oltre un anno e mezzo. Optare per la telefonia "as a Service" fruita con terminali di nuova generazione ha dato già i suoi frutti sia in termini di sostituzione dei vecchi apparati, realizzata in circa 2 mesi senza interruzione dei servizi di telefonia, sia in termini di flessibilità.
Ma quello della sicurezza non è un fattore oramai inderogabile nella scelta di un telefono o di un servizio di telefonia su IP che è limitato alle università.
Esigenze di qualità e sicurezza come quelle dell'Università di Greifswald assumono un'importanza crescente anche presso le piccole e medie aziende.
Per questo, Snom si aspetta che un crescente numero di terminali IP supporti progressivamente in maniera sempre più diretta processi di distribuzione protetta delle chiavi di cifratura contribuendo alla creazione di una sorta di standard in questo senso. Di crescente importanza secondo il produttore sono inoltre anche le procedure di autodiagnosi dei terminali per un'analisi centralizzata degli errori.

UNA NUOVA PIATTAFORMA DI BT FACILITA L'ADOZIONE DI SD-WAN

La nuova soluzione per l'automazione velocizza l'adozione di SD-WAN e migliora la visibilità e la gestione delle infrastrutture di rete ibrida

BT ha annunciato il lancio di una nuova Service and Network Automation Platform (SNAP) progettata per aiutare i clienti a innovare attraverso le più recenti tecnologie di Software Defined Wide Area Networking (SD-WAN) e di Network Functions Virtualisation (NFV).

La piattaforma, che BT evidenzia essere unica nel suo genere, è allocata nel cuore della rete globale di BT. Si basa su una architettura flessibile che consente a BT di integrare le soluzioni dei partner, come ad esempio i controller SD-WAN di Cisco e Nuage Networks di Nokia.
La SNAP funziona anche con il Network Services Orchestrator di Cisco, con cui consente a BT di fornire ai clienti una scelta di servizi gestiti SD-WAN e NFV come BT Connect Services Platform.
BT prevede di estendere l'orchestrazione dal proprio core network ai principali data center cloud di terze parti, fino alle LAN (Local Area Network) dei clienti e alle LAN dei data center (DC-LAN),

in modo da consentire la visibilità, il controllo e la configurazione in cloud delle applicazioni end-to-end dai laptop e dai dispositivi dei clienti fino ai server.
Per garantire la compatibilità tra tecnologie e alti livelli di automazione, SNAP è stato realizzato utilizzando software open source e linguaggi standard del settore, tra cui YANG per modellare la rete e TOSCA per la definizione del servizio.
Le azioni di configurazione e di gestione possono anche essere trasferite a cascata attraverso i sistemi di BT, ed avere effetto in pochi minuti.

Supporto a disposizione dei clienti

Per supportare i clienti nell'implementazione dei futuri progetti di rete, BT ha riunito le sue expertise SD-WAN e NFV e le competenze chiave in un nuovo Centro di Eccellenza (CoE). Il CoE supporta l'intero ciclo di vita dei servizi SD-WAN o NFV dei clienti, collaborando dalla progettazione e implementazione fino alle operations.
Il team integrato è supportato da un programma di investimenti in formazione e in tool come YANG, Netconf e TOSCA – che richiedono nuove competenze ancora poco diffuse..
Il CoE, ha evidenziato BT, situato nei principali centri di sviluppo e assistenza clienti di BT, sarà in grado di monitorare in modo univoco l'intera rete ibrida di un cliente fornendo una singola visione integrata che sfrutta i più recenti tool basati su AI e machine learning.

Keith Langridge -
vice presidente dei servizi
di rete di BT

Il CoE utilizza un approccio simili a quello implementato nello sviluppo di applicazioni cloud, come "DevOps", in cui vengono creati team con tutte le competenze e le capacità necessarie per l'intero ciclo di vita di un servizio. Si allinea anche con il cloud "Serverless", in cui la progettazione, il provisioning e il funzionamento dell'infrastruttura che supporta un'applicazione sono completamente esternalizzati ai provider di servizi cloud gestiti.
«Stiamo investendo per rendere più semplice per i nostri clienti sfruttare le più recenti tecnologie di rete e cloud. La nostra nuova piattaforma per l'automazione della rete e dei servizi e il Centro di Eccellenza aiutano i clienti a sfruttare al meglio il nostro know-how e la nostra esperinza in SDN e NFV. Abbiamo creato un ambiente unico in cui i clienti possono implementare i più recenti servizi software insieme alle tecnologie di rete sottostanti. Questo trasforma la loro esperienza di adozione di SD-WAN, rendendo realtà la promessa di servizi software defined», ha commentato Keith Langridge, vice presidente dei servizi di rete di BT.

CON PANDA PATCH MANAGEMENT PIÙ SEMPLICE GESTIRE LE PATCH

La nuova soluzione aiuta nel prevenire gli attacchi, ne riduce la superficie e permette di apportare le modifiche, gli aggiornamenti e le patch in tempo reale

Panda Security, multinazionale attiva nel campo della sicurezza informatica, ha annunciato il rilascio di Panda Patch Management, una soluzione con cui si è proposta di ridurre la complessità della gestione delle vulnerabilità e degli aggiornamenti sui sistemi operativi e su applicazioni di terze parti.

La soluzione deriva dalla considerazione che ad oggi la maggior parte degli attacchi ed exploit sfrutta vulnerabilità già note in vecchi sistemi. Secondo uno studio di Gartner, si prevede che entro il 2020 il 99% delle vulnerabilità che causano incidenti di sicurezza sarà noto prima che si verifichi un attacco e ciò significa che un aggiornamento tempestivo può essere sufficiente a impedire che ciò accada.

Il rischio di violazione tramite sfruttamento di vulnerabilità, oltre alla possibilità che questa sia l'accesso di un indesiderato attacco zero-day, è aggravato dalla difficoltà di mantenere i sistemi aggiornati. I punti di debolezza principali sono la trasformazione digitale, l'aumento della complessità e dei numeri di endpoint, sistemi e app vulnerabili, il decentramento delle organizzazioni e la loro gestione su strumenti non collegati a sistemi di sicurezza.

In questo scenario ed esigenze si inserisce Panda Patch Management, una soluzione utilizzabile per gestire le vulnerabilità con i relativi aggiornamenti e patch, sia per sistemi che per le applicazioni.

Gli aspetti chiave di Patch Management

La soluzione, ha evidenziato Panda, presenta molteplici benefici. Tra questi:

- Scopre, programma, installa e monitora: fornisce visibilità sullo stato degli endpoint in tempo reale, in termini di vulnerabilità, patch o aggiornamenti in sospeso e software non più supportati (EoL).
- Verifica, monitora e stabilisce le priorità per gli aggiornamenti su sistemi operativi e applicazioni. Aggiornato in tempo reale, offre una visibilità aggregata dello stato delle patch e degli aggiornamenti in sospeso per sistemi e centinaia di app di terze parti.
- Previene gli incidenti, riducendo sistematicamente la superficie di attacco creata dalle vulnerabilità del software. La gestione di patch e aggiornamenti avviene con strumenti di gestione in tempo reale di facile utilizzo, che permettono alle aziende di superare gli attacchi di vulnerabilità.

- Contiene e mitiga gli attacchi, correggendo immediatamente uno o più endpoint: la piattaforma collega minacce rilevate ed exploit a vulnerabilità sconosciute. Il tempo di risposta è ridotto al minimo e ciò permette di contenere e correggere immediatamente gli attacchi con il rilascio veloce di patch dalla piattaforma web.
- Riduzione Opex: implementazioni o aggiornamenti non sono necessari in quanto la componente è già presente sugli endpoint..
- Aiuta a rispettare il principio di responsabilità: molte normative, come GDPR, HIPAA e PCI, impongono alle organizzazioni di adottare misure appropriate per garantire la protezione dei dati sensibili sotto il loro controllo. Panda Patch Management aiuta a rispettare questo obbligo.

Ampliamento dell'architettura Panda

Più in generale, la soluzione è proposta da Panda anche come un ulteriore elemento dell'architettura di sicurezza flessibile di Panda Adaptive Defense 360.

Oltre a rafforzare la capacità di prevenzione contribuendo a ridurre la superficie di attacco agli endpoint, facilita una risposta rapida, isolando i dispositivi compromessi e apportando aggiornamenti in tempo reale.

"Con Panda Patch Management stiamo andando oltre alla massimizzazione della prevenzione e del rilevamento automatico, come abbiamo fatto per anni con Panda Adaptive Defense 360 e le sue tecnologie di machine learning, in continua evoluzione e basate sul cloud. Le organizzazioni necessitano di strumenti di gestione integrati e semplici da usare, che permettano di ridurre la superficie di attacco aperta e rispondere immediatamente agli incidenti di sicurezza, correggendo tutti i dispositivi vulnerabili con un solo clic, da una singola piattaforma di sicurezza e gestione", ha commentato Vázquez, Product Marketing Manager di Panda Security.

Il prodotto si integra con altri diffusi strumenti DevOps come ad esempio Ansible, Jenkins, Docker, Chef e Puppet, tutti tool che tramite Conjuar hanno la possibilità di accedere ed utilizzare le credenziali gestite da CyberArk Conjur.

Si integra anche, ha evidenziato la società, con le piattaforme Platform-as-a-Service leader di mercato, comprese tra queste Red Hat OpenShift, Kubernetes (K8S), Pivotal Cloud Foundry (PCF) e Cloud Foundry (CF).

«Con CyberArk Conjur, segreti e credenziali possono essere gestiti in modo consistente attraverso l'ambiente DevOps indipendentemente dalle capacità di loro gestione degli strumenti DevOps originali o della piattaforma, che può variare in modo anche molto significativa e non essere della classe Enterprise adatta. Ad esempio, alcuni tool non dispongono della rotazione delle credenziali o di funzioni di audit. Non ultimo, Conjur elimina le "isole di sicurezza" che si creano quando strumenti DevOps individuali non possono condividere segreti tra loro in modo sicuro», ha commentato Walsh.

CON TALEND MACHINE LEARNING PIÙ SEMPLICE

Talend semplifica le implementazioni Apache Spark e Machine Learning con una sandbox che crea pipeline di dati intelligenti ad alte prestazioni

Ashley Stirrup, CMO di Talend

Talend, società attiva nello sviluppo di soluzioni di integrazione cloud, in occasione della Strata Data Conference di New York ha annunciato una nuova sandbox che mette a disposizione di sviluppatori e data engineer tecnologie per l'apprendimento automatico, in modo che possano facilmente creare pipeline più intelligenti di dati.
In particolare, ha osservato la società, tramite la soluzione Talend Big Data and Machine Learning Sandbox, i data engineer possono seguire una "guida" passo passo che include proof of concept prestabiliti e utilizza Apache Spark, la Library Machine Learning Spark (MLlib) e Spark Streaming in pochi minuti senza attività di codifica.
«Esiste un enorme divario di competenze per cui sviluppatori e data engineer faticano a implementare big data e apprendimento automatico quali elementi strategici e funzionali al business delle aziende», ha affermato Ashley Stirrup, CMO di Talend. «Le integrazioni Big Data con codifica manuele sono spesso causa di inefficienze quando si entra in fase di produzione, tra cui costi elevati di manutenzione, attività di integrazione manuale e reimplementazione degli algoritmi di machine learning. Con Talend Big Data and Machine Learning Sandbox, i team sono in grado di sfruttare l'apprendimento automatico in pochi minuti e passare più rapidamente dalla fase pilota a quella di produzione». Inclusi nella soluzione vi sono quattro proof of concept predefiniti per l'apprendimento automatico contenuti in una "guida passo passo" insieme a Talend Big Data and Machine Learning Sandbox.
In sostanza, l'obiettivo datosi da Talend nello sviluppo della sua nuova soluzione è stato quello di permettere a sviluppatori e data engineer di poter iniziare rapidamente con un ambiente di elaborazione Spark completamente configurato e fruibile in modalità drag-and-drop, e scoprire informazioni dettagliate per il business utilizzando gli scenari di Talend pronti per l'uso. Tra questi, in particolare, la società ha evidenziato:

- **Motore di suggerimenti:** automatizza l'offerta del film migliore con l'utilizzo dell'apprendimento automatico.
- **Motore di valutazione dei rischi in tempo reale:** diminuisce i rischi con la previsione dei prestiti in tempo reale.
- **Manutenzione predittiva IoT:** ottimizza le prestazioni e il ciclo di vita dei distributori automatici utilizzando i dati del sensore.
- **Ottimizzazione del data warehouse:** porta l'elaborazione dei dati su Spark per una visione più rapida e approfondita, a un costo inferiore.

«La nuova Sandbox consente ai professionisti IT di lavorare in modo più intelligente grazie ad apprendimento automatico e data integration rendendo facilmente operativi i modelli di machine learning creati dagli esperti di Data Science. Tramite un abbonamento Talend, i clienti godranno della massima portabilità per eseguire progetti sandbox su cloud privato, multi-cloud (AWS, Google, Azure), ibrido, Talend Cloud o ambienti on-premise» ha commentato la società.

PIÙ SICUREZZA CON I NUOVI FIREWALL ATP DI ZYXEL

Sfruttando il sandboxing cloud la serie ATP, pensata per le PMI, blocca gli attacchi zero-day in tempo reale

Valerio Rosano, country manager Zyxel

Zyxwel ATP Family

Zyxel Communications, diretta in Italia dal country manager Valerio Rosano, ha annunciato la disponibilità di una nuova serie di firewall ideata con l'obiettivo primario di permettere alle PMI di proteggere le loro reti e i loro dati anche da attacchi zero-day, che non sempre vengono intercettati e bloccati da sistemi di sicurezza convenzionali.

La serie firewall ATP è, nello specifico, una soluzione gateway all-in-one che integra soluzioni di sandboxing cloud con molteplici livelli di sicurezza aggiuntivi per rilevare e bloccare minacce note e sconosciute.

«I numerosi attacchi ransomware dello scorso anno hanno dimostrato che non è necessario gestire informazioni sensibili o ingenti somme di denaro per essere presi di mira», ha commentato l'annuncio Dean Shih, AVP senior di Zyxel's Gateway SBU. «Il pericolo principale è rappresentato dalle minacce sconosciute. Queste non possono essere intercettate e bloccate da soluzioni di sicurezza convenzionali e stanno crescendo rapidamente (+40% solo nella seconda parte del 2017). Fino ad oggi, la tecnologia all'avanguardia necessaria per respingere queste minacce implicava investimenti ingenti - se non proibitivi - per la maggior parte delle piccole e medie imprese».

A livello funzionale, tramite il sandbox che esegue pacchetti di dati sconosciuti e potenzialmente pericolosi in un ambiente sicuro e circoscritto, è possibile determinare se sono affidabili prima di lasciarli entrare o meno all'interno della rete.

Le minacce note non arrivano comunque alla sandbox. Anche gli ATP, come la maggior parte delle soluzioni di sicurezza Zyxel, valutano i pacchetti di dati in entrata controllando l'integrità della loro firma. Ma oltre a ricevere regolarmente aggiornamenti delle signature appena segnalate da fonti attendibili come Bitdefender o Cyren, i firewall ATP ricevono anche un flusso continuo 0-day di aggiornamenti per ogni nuova minaccia identificata da ogni altro firewall ATP in tutto il mondo.

A livello operativo gli ATP Zyxel, per il primo anno di utilizzo, includono anche il Gold Security Pack. Della famiglia, l'ATP200 è proposto come adatto ad aziende di piccole dimensioni, mentre l'ATP500 può soddisfare le esigenze anche delle medie imprese, contando su un throughput rispettivamente di 1.800 e 2.600 Mbps e utenze raccomandate di 1-50 e 50-100.

IL "SOC AS A SERVICE" DI AXITEA PROTEGGE AZIENDE E PMI

Maurizio Tondi, CTO Axitea

I servizi di sicurezza gestita di Axitea integrano tecnologia di nuova concezione e competenze specializzate per garantire una protezione h24

Axitea, Global Security Provider specializzata nella gestione della sicurezza fisica e cyber, ha espanso la propria offerta di sicurezza con il servizio SOC as a Service, che abbina intelligenza artificiale e umana per fornire un monitoraggio h24 in real-time dei log, dell'incident management (in ambito security) per quanto riguarda eventi che accadono sulla rete, sui dispositivi di sicurezza, sistemi o applicazioni.

Il servizio deriva dalla considerazione della società che gli attacchi informatici sono sempre più evoluti e le tecniche utilizzate per colpire aziende e utenti sono così sofisticate da riuscire a oltrepassare le barriere di protezione di rete e infrastrutture di un'azienda. Il timore di subire violazioni dei dati e relativi danni economici, di produttività e di reputazione, porta a dotarsi di soluzioni di sicurezza senza però competenze specialistiche e strumenti adeguati. E' un approccio che, evidenzia l'azienda, non consente di raggiungere un livello di protezione ottimale, con investimenti senza ritorno in soluzioni non implementate correttamente o addirittura non utilizzate.

Per supportare le aziende nella gestione della sicurezza in modo appropriato Axitea ha per questo messo a punto un nuovo servizio gestito: SOC as a Service, che opera in modo trasversale e congiunto per combattere attacchi informatici e individuare eventuali comportamenti anomali.

In pratica, Soc as a service si integra nell'offerta di soluzioni di sicurezza informatica gestita, che comprende anche i servizi di protezione malware (Full Protection) e raccolta e archiviazione log (Incident Recorder).

Il servizio fornisce il monitoraggio continuo degli eventi e l'individuazione e la gestione degli incidenti. L'integrazione di machine learning, threat intelligence e big data dà informazioni utili agli analisti informatici di Axitea per formulare risposte per la risoluzione di incidenti e mitigazione dei rischi. Permette di individuare, ad esempio, possibili attacchi di tipo brute force per scovare password, attacchi provenienti dall'interno, ovvero dipendenti con intenti malevoli, oppure per tracciare sistemi infetti o compromessi da malware. «I vantaggi garantiti sono numerosi. Le aziende che decidono di affidare la propria sicurezza ad Axitea possono focalizzarsi sulle attività di core business, con la garanzia di avere una protezione gestita in modo ottimale da tecnici esperti IT che monitorano la loro infrastruttura h24», ha osservato Maurizio Tondi, CTO di Axitea.

Nella sua essenza, è un servizio modulare e scalabile che consente di ottimizzare i costi legati alla sicurezza perché non è necessario sostituire le soluzioni esistenti di protezione (ad es. firewall, antivirus, etc.) ma è sufficiente collegarle al SOC di Axitea. Data la sua configurazione si propone come una soluzione particolarmente adatta per le piccole e medie imprese, che spesso non hanno figure interne dedicate alla sicurezza, e possono fare affidamento agli esperti Axitea per ottenere la massima protezione.

RISCO GROUP E SICURITALIA PARTNER PER GLI IMPIANTI SPECIALI

La centrale di controllo della sicurezza fisica e logica di Sicuritalia

La gamma ibrida, i sensori e le centrali di RISCO Group ampliano l'offerta di Sicuritalia per la sicurezza fisica e logica e la sua gestione centralizzata

RISCO Group, azienda indipendente operante a livello internazionale nel settore della sicurezza e specializzata nello sviluppo di soluzioni di sicurezza integrata, ha siglato un accordi di partnership con Sicuritalia, società attiva in Italia nel campo della Sicurezza con 8000 dipendenti ed oltre 60000 clienti.

L'accordo interessa gli impianti speciali e prevede una partnership strategica che permetterà a Sicuritalia di fornire ai propri clienti le soluzioni di RISCO, in particolare la gamma ibrida, in modo da ottenere una maggiore efficienza operativa.

Il Gruppo presieduto da Lorenzo Manca ha scelto la partnership con RISCO Group con il duplice scopo di far evolvere la propria offerta di prodotti, e allo stesso tempo di collaborare con RISCO allo sviluppo e alla realizzazione di future soluzioni.

Dall'analisi compiuta da Sicuritalia, infatti, la partnership permetterà una maggiore efficacia nella gestione delle richieste dei clienti finali e una razionalizzazione della gamma. Grazie alle caratteristiche della gamma dei prodotti RISCO, Sicuritalia sarà in pratica in grado di offrire ai propri clienti sistemi di sicurezza ad elevate prestazioni, in tempi più rapidi e a condizioni migliori.

"La qualità e l'affidabilità dei prodotti RISCO ci permette di essere più vicino ai nostri clienti e questo rende la nostra offerta ancora più competitiva." ha commentato Alessandro Turco, Sales Director di Sicuritalia.

La gamma di prodotti interessata

In base all'accordo RISCO fornirà a Sicuritalia tutta la gamma ibrida, i sensori e le centrali Radio. Tra i prodotti più interessanti per Securitalia sono da annoverare ProSYS Plus e LightSYS 2, entrambi nativamente integrati con Video Verifica, Smart Home e programmabili via Cloud.

Nello specifico dei prodotti, ProSYS Plus è una soluzione progettata per essere adattabile a svariate tipologie di installazione che è conforme agli standard di Grado 3. Nell'ultima versione il numero di zone di base della centrale è salito a 128 e include un firmware per la gestione dei nuovi moduli di comunicazione e nuovi sensori.

LightSYS 2 è invece un sistema di sicurezza ibrido progettato per il mercato residenziale e delle piccole e medie imprese e che permette di gestire fino a 50 zone.

Va poi considerato, ha osservato RISCO, che utilizzando il Cloud RISCO e l'App iRISCO disponibile per iOS e Android, LightSYS2 permette di disporre di un livello di sicurezza e di controllo

molto elevato grazie alla possibilità di installare e configurare un numero illimitato di telecamere IP per interno e per esterno, che tramite VUpoint abilitano la video verifica in tempo reale e consentono di ottenere immagini in caso di allarme in corso o su richiesta.
Per Sicuritalia, RISCO ha anche messo a punto un servizio di cloud personalizzato, una soluzione ad hoc per la gestione da remoto dei sistemi di sicurezza, in grado di operare in sinergia con la piattaforma delle loro Centrali Operative.
«Questo accordo sottolinea il valore della nostra gamma di prodotti, e premia la nostra costante ricerca di innovazione e evoluzione. In particolare, la richiesta di realizzare un cloud personalizzato dimostra la nostra leadership in ambito tecnologico e la nostra forza nell'offrire non solo soluzioni, ma interi sistema di controllo personalizzati» ha commentato Ivan Castellan, Branch Manager di RISCO Group Italia.

SI AMPLIA IL PORTFOLIO CLOUD DI ITALTEL E HABBLE

Le due aziende hanno sviluppato una piattaforma di servizi cloud per migliorare la Customer Experience dei telco manager

Daniela Martino, Head of Marketing & Management Telco&Media Product/Solution Unit di Italtel

Italtel, società multinazionale dell'Information & Communication Technology che insieme a Exprivia rappresenta un attore nazionale e internazionale nella progettazione e sviluppo di soluzioni e servizi per la trasformazione digitale, ha annunciato una partnership con Habble centrata su una piattaforma cloud per il monitoraggio in tempo reale e l'ottimizzazione delle comunicazioni provenienti da rete fissa, mobile e dati delle aziende attraverso algoritmi di analytics evoluti.
La partnership fa leva sulle competenze distintive che Italtel ha maturato presso i grandi carrier internazionali e le large enterprise in ambito telco e su quelle di Habble nell'ambito delle piattaforme web-cloud.
I due partner intendono proporre la soluzione sia agli operatori di telecomunicazioni sia alle grandi aziende per mettere a disposizione un prodotto per migliorare la Customer Experience del cliente finale. «La partnership con Habble – ha commentato Daniela Martino, Head of Marketing & Management Telco&Media Product/Solution Unit di Italtel – ci permette di consolidare ed ampliare anche a livello internazionale l'offerta di soluzioni cloud based innovative rivolte ai mercati Telco e Large Enterprise. Crediamo che la soluzione Habble, già oggi integrabile con le nostre tecnologie proprietarie, possa migliorare l'efficienza operativa, contribuire al successo del business delle imprese ed offrire ai Service Provider l'opportunità di migliorare la customer satisfaction dei loro clienti».

La soluzione permette ai carrier di creare valore in base alla maggior visibilità delle esigenze specifiche dei clienti ottenuta attraverso la raccolta e l'analisi dei dati di traffico da rete fissa e mobile.
Sarà possibile, ha spiegato Italtel, monitorare e prevenire picchi anomali di traffico e i relativi costi, per esempio in caso di roaming, e anticipare o prevenire eventuali reclami e/o contenziosi con una conseguente riduzione dei costi legati alle attività di customer care.
Le imprese possono sfruttare i vantaggi della soluzione cloud based per migliorare la gestione e il controllo delle comunicazioni tra l'azienda e il mondo esterno.
Il controllo centralizzato dei dati abilita funzionalità di analytics e rendicontazione personalizzabili con una possibile riduzione fino all'80% del tempo impiegato per la gestione e l'analisi dei dati.
Attraverso un sistema di configurazione la soluzione permette di impostare alert per verificare il corretto funzionamento ed utilizzo dei telefoni aziendali.

NUVIAS SUPPORTA RIVERBED STEELCENTRAL ATERNITY

La partnership tra Nuvias e Riverbed si rafforza sul mercato italiano con la soluzione Riverbed SteelCentral Aternity

Nuvias ha consolidato la partnership con Riverbed distribuendo anche in Italia Riverbed SteelCentral Aternity, una piattaforma per il monitoraggio della End User Experience (EUE).
Congiuntamente a SteelCentral, Nuvias, osserva la società, permette ai rivenditori di disporre di una ampia visibilità end-to-end che comprende la gestione delle reti, delle applicazioni e degli utenti.
A livello funzionale, SteelCentral permette di monitorare, identificare e risolvere problemi sul singolo dispositivo, siano essi legati a problematiche di rete, di infrastruttura, al mondo cloud, nonché alle applicazioni, sia su dispositivi mobile che desktop.
In particolare, osserva Nuvias, SteelCentral Aternity, costituisce una soluzione focalizzata sul business e sugli utenti e il suo obiettivo è di ridurre i rischi durante le migrazioni applicative, anche in ambienti cloud e permettere alle aziende di monitorare i risultati reali di tale operazioni, e di effettuare il troubleshooting su rete e infrastruttura. «In Italia stiamo riscontrando grande interesse dalle aziende per la soluzione Riverbed SteelCentral Aternity - ha sottolineato Piera Loche, Managing Director di Nuvias Italia - perché assicura una tecnologia comprovata che aiuta le aziende a visualizzare l'intera User Experience per ogni applicazione in esecuzione su qualsiasi dispositivo. Contestualmente, Riverbed SteelCentral Aternity fornisce un'analisi che, molti degli strumenti disponibili sul mercato per il monitoraggio delle prestazioni della rete o delle applicazioni a corto raggio, oggi non riescono a fornire. Trasformando efficacemente ogni dispositivo - fisico, virtuale e mobile - in una piattaforma di auto-monitoraggio consapevole dell'esperienza dell'utente, le aziende possono così disporre di funzionalità di gestione IT proattive e incentrate sugli utenti, che riducono drasticamente le interruzioni del business e aumentano la produttività dei team di lavoro».