OTTOBRE 2014 - ANNO 4 N. 14

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

Standard ONVIF nel controllo accessi: ecco il Profilo C

Sicurezza informatica in azienda? Non c'è più tempo da perdere

Business intelligence, big data e videosorveglianza

Cloud: cosa può fare l'utente finale per la sicurezza dei propri dati

www.ipsecuritymagazine.it

SOMMARIO

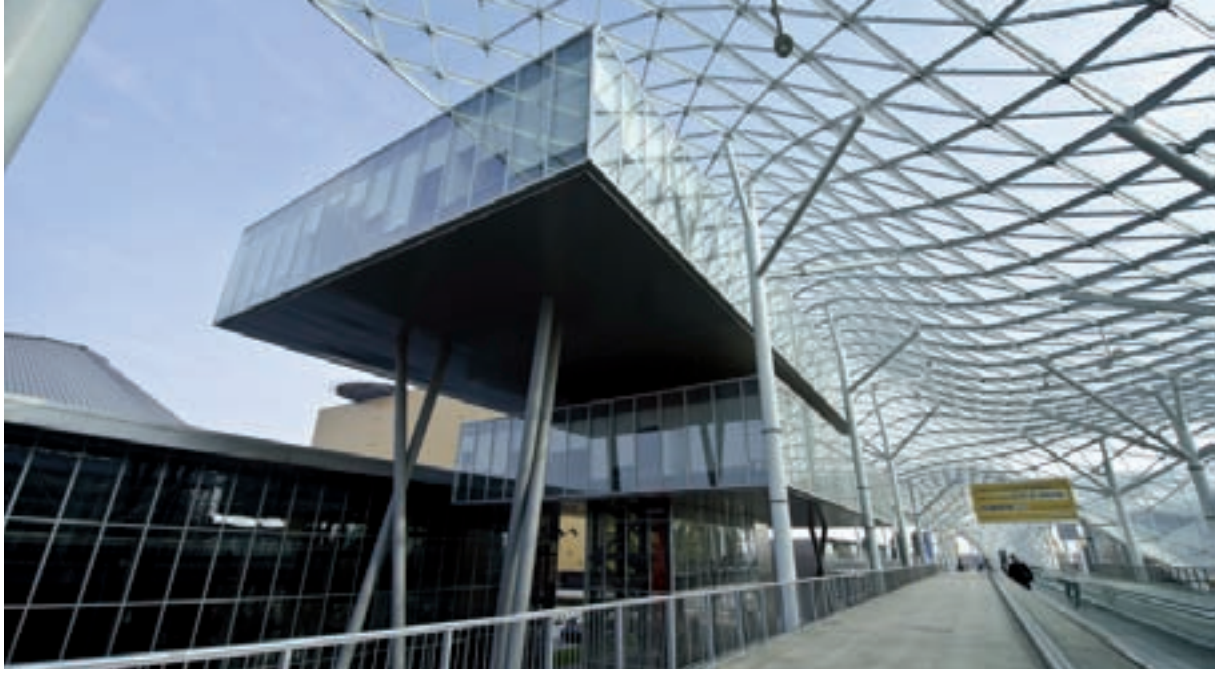
OTTOBRE 2014 - ANNO 4 - N. 14

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

guarda ascolta scarica



Un Novembre di Sicurezza a 360 gradi

Un autunno di grandi attese per il mondo IT e per il mondo della security fisica, con due appuntamenti imperdibili a brevissima distanza l'uno dall'altro, quasi a voler indicare una via ormai solcata della convergenza tra sicurezza logica e sicurezza fisica.

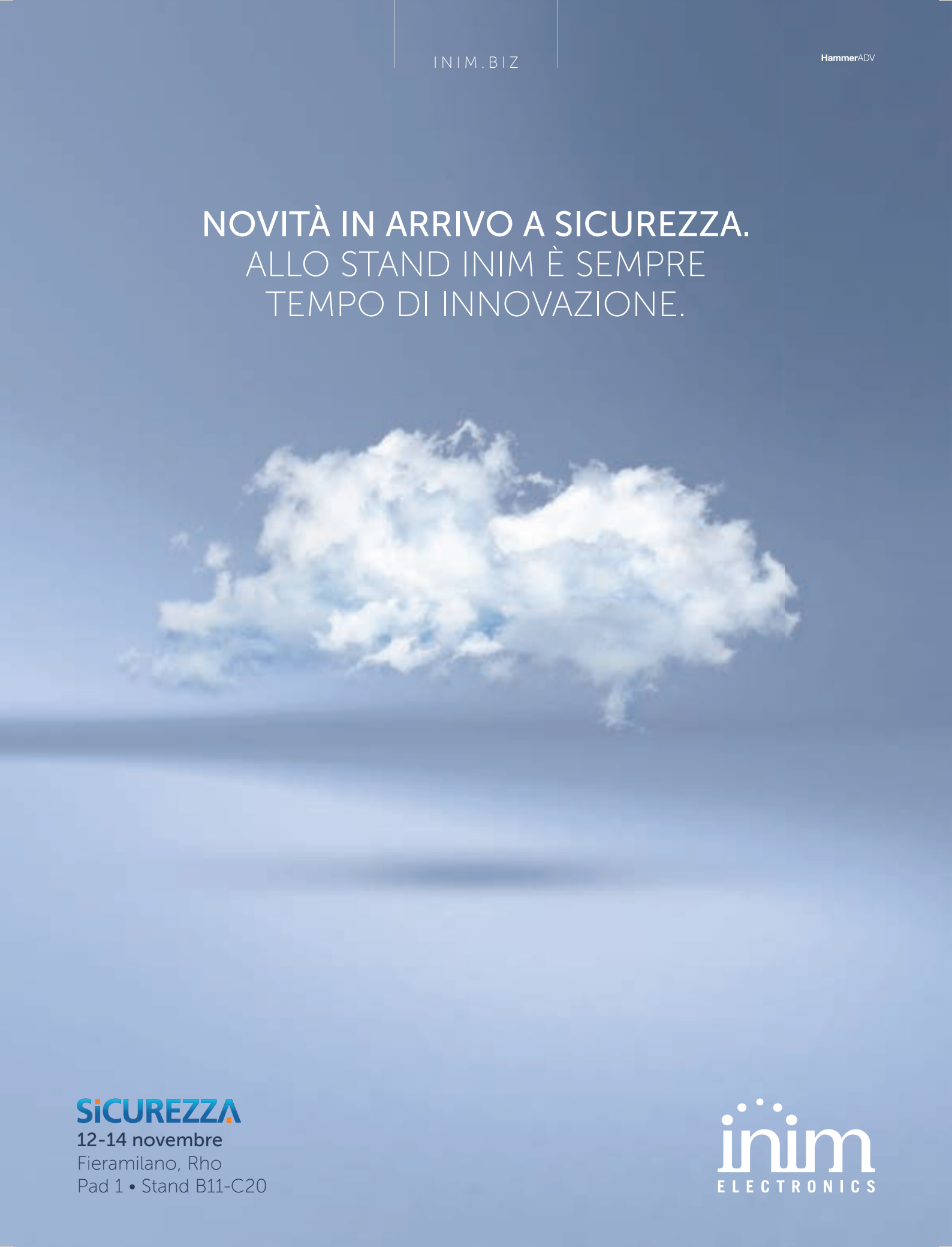
I due eventi si chiamano **festival ICT**, di scena il prossimo 6 Novembre al Palaforum di Assago (MI), e **SICUREZZA 2014**, rassegna biennale di Security & Fire Prevention, che aprirà i battenti dal 12 al 14 Novembre presso i padiglioni 1 e 3 della Fiera di Milano-Rho.

Due appuntamenti che cominciano a richiamare un pubblico sempre più vicino e integrato: da un lato c'è il pubblico che si occupa di proteggere la rete, la sua infrastruttura, i dati che circolano dentro e fuori dal network, e dall'altro c'è il pubblico che vuole impedire l'accesso fisico a determinate aree, che non vuole più subire furti, che vuole avere il controllo di casa e della sua attività.

Due target egualmente professionali e profilati, per una tipologia di visitatore che ormai si interessa di entrambi gli aspetti della sicurezza: quella fisica e quella logica.

Doppio appuntamento a Milano, dunque, per un Novembre dedicato alla sicurezza a 360°.

NOVITÀ IN ARRIVO A SICUREZZA.
ALLO STAND INIM È SEMPRE TEMPO DI INNOVAZIONE.



SICUREZZA
12-14 novembre
Fieramilano, Rho
Pad 1 • Stand B11-C20

inim ELECTRONICS

Baldvin Gislason Bern(*)

Standard ONVIF nel controllo accessi: ecco il Profilo C

ONVIF è un organismo aperto dedicato allo sviluppo di uno standard globale per l'interfaccia dei prodotti di sicurezza fisica a base IP. Fondata nel 2008, l'ONVIF ha l'obiettivo di raggiungere una reale interoperabilità tra i dispositivi di sicurezza IP, efficiente e che non limiti le singole performance operative. Se già moltissimi prodotti adottano la specifica ONVIF per l'area video, con l'ultima release del Profilo C entra in campo anche il controllo accessi fisico (physical access control - PAC). Terzo per ordine di sviluppo, il Profilo C permette infatti la progettazione di un sistema di controllo accessi IP-based. Il Profilo S copre lo streaming video e audio e il Profilo G permette storage, ricerca, retrieval e playback di dispositivi e client che supportino registrazione e storage a bordo. Ma facciamo un passo indietro.

(*) Baldvin Gislason Bern è stato chairman del comitato di lavoro ONVIF dedicato allo sviluppo del Profilo C ed è un esperto R&D di Axis Communications. **www.onvif.org**

Ai tempi dell'analogico, i dispositivi video di diversi produttori potevano essere resi interoperabili solo con la combinazione di prodotti di diversi brand. Con l'avvento della tecnologia IP, ogni brand ha creato un proprio linguaggio con lo sviluppo di tecnologie e protocolli proprietari. Questo rendeva complessa l'interoperabilità tra prodotti: la risposta dell'industria al problema è stata l'interfaccia API (application programming interface), che permetteva ai prodotti di sicurezza fisica IP-based di comunicare tra loro. Ebbene, mentre il video ha migrato all'IP piuttosto rapidamente, il controllo accessi ha invece proceduto *en ralenti*. E la limitata interoperabilità tra prodotti di marche diverse ha condannato a lungo l'intero comparto sicurezza al ruolo di *mercato proprietario*, limitando pesantemente la libertà di scelta tecnologica per consulenti, system integrator e utilizzatori finali del settore. A questo punto è entrata in gioco l'ONVIF. Obiettivo: sviluppare un linguaggio comune che rendesse interoperabili i prodotti di sicurezza. Con la crescita dei prodotti ONVIF compliant, si susseguirono poi aggiornamenti ed estensioni delle specifiche per includere sempre più versioni: questo purtroppo generò una certa confusione su quali versioni fossero conformi e quali no. Inoltre, per la notevole flessibilità delle linee guida di implementazione, alcune caratteristiche chiave incluse nella specifica risultarono con l'essere diverse di dispositivo in dispositivo. Risultato: alcuni apparecchi non lavoravano assieme in perfetta sintonia.
L'ONVIF passò quindi al concetto di Profilo.

IL PROFILO C

All'inizio ci si concentrò sul video streaming con il Profilo S, che ora assomma circa 3.500 prodotti compliant. Come logica estensione, ONVIF identificò la registrazione e i sistemi di controllo accessi quali aree chiave per lo sviluppo di ulteriori standard globali di interoperabilità.
A differenza del Profilo S, spinto in gran parte dalla rivoluzione digitale nella videosorveglianza e dalla relativa industria, il Profilo C è il risultato di un approccio di più ampio respiro e a lungo termine. Quando il controllo accessi ha infatti cominciato a migrare verso tecnologie network-based, il processo di transizione non è stato né rapido né dirompente come quello avvenuto nella videosorveglianza. Per accelerare il processo e ridurne gli ostacoli più rilevanti, l'ONVIF ha quindi stilato il Profilo C.

Per le realtà operative in area video, esiste ora un'interfaccia globale di rete che permette ai produttori di estendere le funzionalità dei loro prodotti a quelle del controllo accessi utilizzando lo stesso backbone ONVIF che governa la loro videotecnologia. Ciò permette di integrare i propri prodotti con un'ampia gamma di door controller e client e dispositivi di controllo accessi.

Lato utente finale e system integrator, Profilo C significa poi liberarsi dai vincoli hardware e software di uno dei segmenti più proprietari che ci sia (il controllo accessi, appunto), e quindi libertà di scelta nella tecnologia, minori costo totale di proprietà e di integrazione del sistema. E ancora: niente più costose e defatiganti personalizzazioni per il system integrator e massima libertà di scelta per l'utilizzatore finale, che potrà disporre di una centrale di controllo che integra diversi sistemi di controllo accessi senza dover ripetere il training del personale. Lats but not least: integratori e utenti finali potranno con estrema facilità migrare verso una piattaforma integrata IP-based di video e controllo accessi.

E veniamo alla vera novità. Mentre il controllo accessi ha sempre avuto dei sottoinsiemi di standard (tipicamente l'interfaccia Wiegand e la OSDP tra il lettore di carte e il controller delle porte), l'interfaccia tra il controller e il software di gestione del controllo accessi è invece sempre stato basato su protocolli proprietari di comunicazione. Ebbene, con il Profilo C, gli IP door controller di diverse marche saranno per la prima volta tra loro compatibili.

Il Profilo C in sostanza detta una linguaggio comune che permette agli IP door controller di supportare dispositivi, creare una lista di lettori e connessioni e adattarsi a lettori di carte ed eventi. Lo stesso profilo potrebbe essere anche utilizzato per controllare gli output del sistema, come l'apertura/chiusura dei dispositivi di rete.

Il Profilo C agevola anche la configurazione di un sistema di gestione che sovrintenda alle telecamere, agli altri dispositivi video di rete e agli IP door controller: permette infatti di individuare e di gestire un dispositivo o un evento, mentre il sistema di gestione riceve ininterrottamente eventi di motion dalle telecamere ed eventi relativi agli accessi dagli IP controller. I sistemi di controllo accessi integrati con dispositivi video di rete useranno questo standard per posizionare correttamente il PTZ di una telecamera dome per registrare una tessera magnetica su una specifica porta, per attivare la registrazione video su una tessera invalida o per controllare e coordinare permessi e diritti di un sistema integrato video + controllo accessi.

SERVE UN ESEMPIO?

Rappresentiamo ora uno scenario applicativo nel quale il client e i dispositivi C-compliant possono essere utilizzati. Pensiamo ad una guardia giurata la cui centrale operativa sovrintenda ad un ampio palazzo uffici, con svariate porte e punti d'accesso. Se il sistema di controllo accessi è conforme al Profilo C, la guardia potrà svolgere da remoto varie funzioni chiave: innanzitutto disporre di una lista di tutte le entrate e dei punti di accesso, delle aree coperte e del rapporto tra controller e porte (es. quale punto d'accesso controlla una specifica porta d'ingresso). La guardia potrà quindi controllare tutte le porte, aprirle e chiuderle, assicurare un accesso provvisorio, bloccare permanentemente una porta e tenere alcune porte chiuse (e altre aperte) per periodi predefiniti. Ancora: la guardia potrà ottenere informazioni sullo stato delle porte anche con strumenti visuali (con uno snapshot del video) e potrà sapere se ciascuna di esse risponde ai parametri precedentemente settati (es. se una porta che doveva essere chiusa è realmente tale o da quale accesso proviene un allarme appena scattato). Infine la guardia potrà modificare lo status dei vari punti d'accesso e disabilitarne alcuni, in modo che le credenziali presentate non vengano più lette. Ma non finisce qui: con un sistema di controllo accessi integrato video + accessi conforme al Profilo C, l'operatore potrà interconnettersi con il sistema di videosorveglianza e rispondere tempestivamente ad un evento verificando a mezzo video chi è presente/vicino ad una certa porta ed utilizzando il controllo accessi per aprire/chiudere/sbloccare la porta.

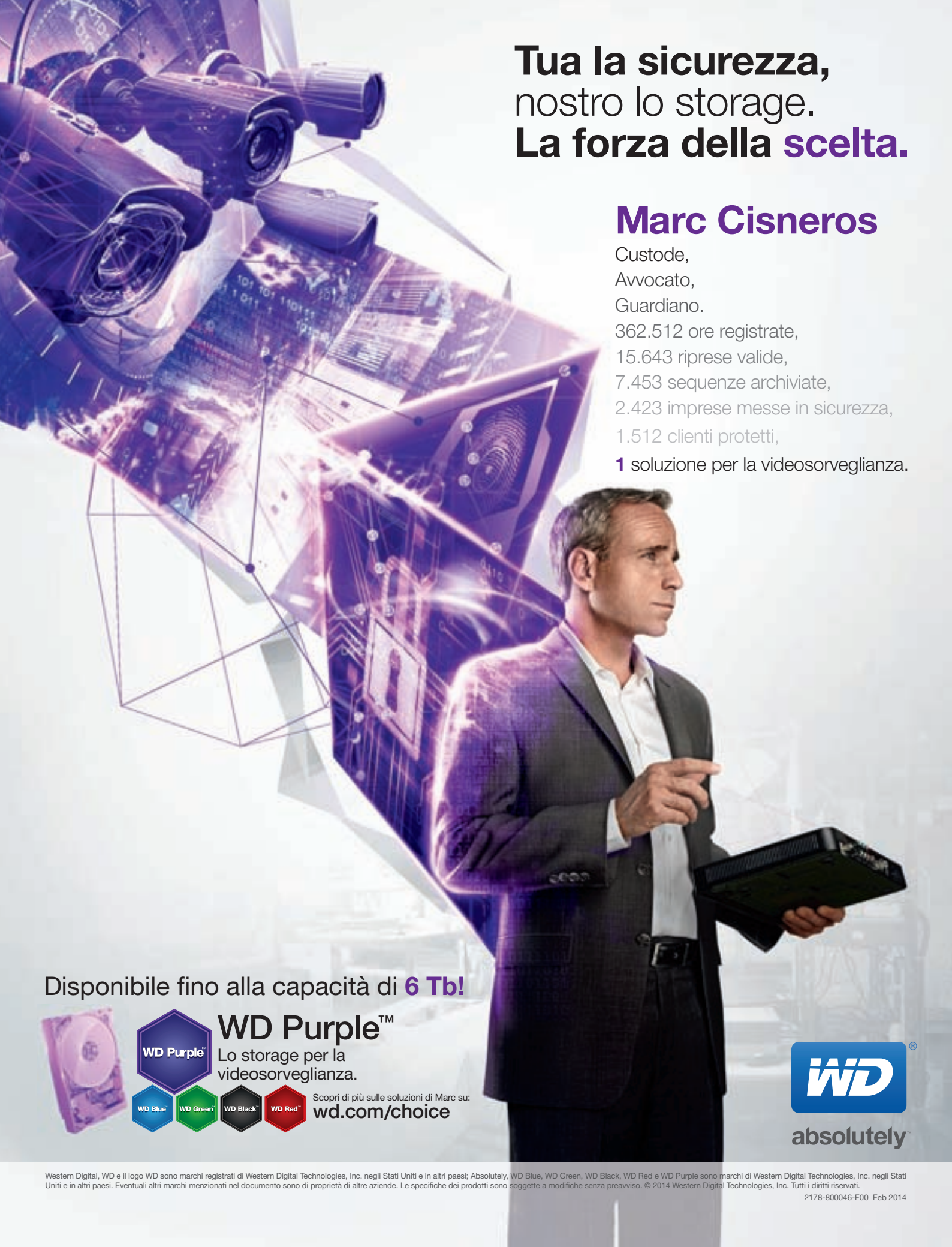
IN PROGRESS

Il Profilo C condivide alcune funzioni con il Profilo S, come si è visto nell'esempio, e anche con il Profilo G. Se pure un dispositivo non disporrà delle tante possibilità offerte dal Profilo C nella sua interezza, lo stesso fatto di disporre anche solo delle funzioni base sarà comunque un grande beneficio, perché porrà le basi per un dialogo comune tra tecnologie diverse. Il Profilo C è del resto solo uno dei tanti passi dell'ONVIF, volti ad anticipare le esigenze dell'industria del settore rendendo la produzione di sicurezza sempre più *a prova di futuro* con prodotti che lavorano assieme. Ora e negli anni a venire.

Tua la sicurezza,
nostro lo storage.
La forza della scelta.

Marc Cisneros

Custode,
Avvocato,
Guardiano.
362.512 ore registrate,
15.643 riprese valide,
7.453 sequenze archiviate,
2.423 imprese messe in sicurezza,
1.512 clienti protetti,
1 soluzione per la videosorveglianza.



Disponibile fino alla capacità di **6 Tb!**

WD Purple™
Lo storage per la videosorveglianza.

WD Blue™ WD Green™ WD Black™ WD Red™

Scopri di più sulle soluzioni di Marc su:
wd.com/choice

WD®
absolutely™

2178-800046-F00 Feb 2014

Wieland Alge(*)

Sicurezza della rete & competitività: questione di firewall

Intercettazione delle comunicazioni aziendali, furto e manipolazione dei dati, fughe di informazioni corporate cruciali per il business: da quando le reti esterne sono entrate in azienda, i firewall hanno avuto il compito di proteggerle da queste minacce onde evitare impatti negativi e rischiosi sui processi interni. Storicamente, quindi, i firewall sono identificati come garanti della sicurezza, ma si tratta davvero solo di questo? Se usati abilmente, infatti, non si limitano a separare le reti di fiducia da quelle non affidabili, ma possono essere uno strumento capace di migliorare produttività e performance, rendendo l'organizzazione più competitiva. Ecco qualche esempio pratico.

(*) VP & General Manager EMEA di Barracuda Networks
www.barracuda.com

Le interruzioni di rete non dipendono sempre da un attacco informatico, molto spesso sono causate da errori del provider, eventi atmosferici, ritardi nei pagamenti dei fornitori e persino da “lavori in corso”. I firewall possono essere utilizzati facilmente per capire la causa dell’arresto e instradare il traffico attraverso percorsi alternativi. Proprio come bravi vigili urbani, non si limitano a individuare il motivo dell’ingorgo e gli autori dell’irregolarità, ma trovano una soluzione per riavviare la circolazione. Non solo: un uso sapiente del firewall consente alle aziende di risparmiare tempo.

RISPARMIARE TEMPO

Quando più imprese sono chiamate a cooperare, a seguito di fusioni e acquisizioni, i firewall permettono alle differenti infrastrutture di rete di essere utilizzate congiuntamente in modo molto rapido ed efficace. Ciò si traduce in un risparmio di settimane e talvolta anche mesi di lavoro dedicato all’integrazione tra le diverse architetture. In un mondo globale, dove il fattore tempo è ormai l'elemento più prezioso e critico per la stessa competitività aziendale, risparmiare del tempo è un valore aggiunto particolarmente apprezzabile.

E IN FUTURO?

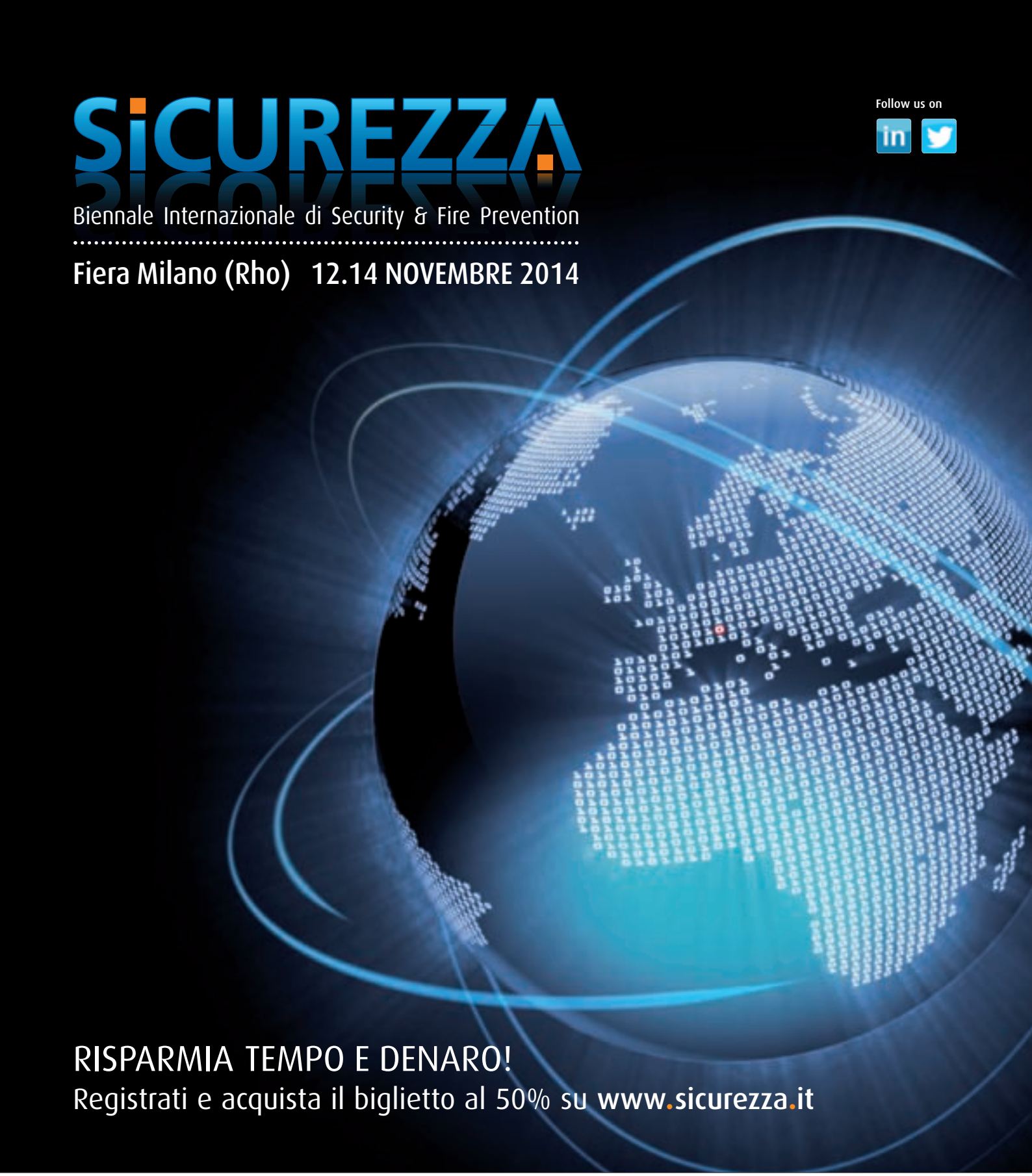
In futuro, il ruolo dei firewall potrà allargarsi sempre più. Oggi le aziende sono chiamate a rispondere a tre sfide principali: l’*empowerment* degli utenti, meno controllabili a livello centrale, l’aumento dei servizi basati su cloud e l'affermarsi dell’internet delle cose (IoT), che implica l’introduzione in azienda di dispositivi non IT connessi alla rete. Questo significa che la rete interna, in precedenza controllata e separata da quelle esterne, potrà trasformarsi in una zona totalmente incontrollata. I firewall dovranno garantire, allora, che questa trasformazione possa procedere senza intoppi, assicurando la disponibilità di dati e applicazioni, senza esporre l’organizzazione al rischio di minacce. Ecco perché è probabile che in futuro useremo più firewall presso le sedi distaccate, gli uffici domestici, nelle infrastrutture cloud-based e in luoghi che prima ritenevamo impensabili.

SICUREZZA

Biennale Internazionale di Security & Fire Prevention

Fiera Milano (Rho) 12.14 NOVEMBRE 2014

Follow us on



RISPARMIA TEMPO E DENARO!

Registrati e acquista il biglietto al 50% su **www.sicurezza.it**

THE INTERNATIONAL NETWORK

EXPOSEC
San Paolo - Brasile 13.15 Maggio 2014

XX FISP
San Paolo - Brasile 08.10 Ottobre 2014

EXPO MILANO 2015

FIERA MILANO

Official Partner

Luca Collacciani(*)

Sicurezza informatica in azienda?

Non c'è più tempo da perdere

È stato un anno intenso sul fronte della sicurezza informatica. Come individuato da Akamai nell'ultimo Rapporto Prolexic sugli attacchi DDoS (Q2 2014), non solo nel 2014 si sono verificati più attacchi informatici rispetto al 2013, ma sono anche state rilevate nuove tattiche e nuovi strumenti a disposizione dei criminali informatici meno "esperti" e, quindi, potenzialmente più pericolosi. Per troppi anni, gli investimenti in sicurezza informatica sono stati considerati dalle aziende troppo costosi e difficilmente misurabili. Fortunatamente, a causa di queste tendenze, questo atteggiamento nei confronti dei sistemi di protezione sta cambiando.

(*) Regional Manager Akamai Italia
it.akamai.com

È vero: alcune delle falle più conosciute sono state risolte, ma esiste ancora una quantità enorme di siti web vulnerabili causati da processi e aggiornamenti ai sistemi non effettuati adeguatamente. E non solo siti web: anche le applicazioni web necessitano di azioni di difesa urgenti. Moltissime, infatti, presentano delle falle di sicurezza molto serie, che possono facilmente essere utilizzate come porte di accesso a dati sensibili o sfruttate per azioni criminose come il furto di dati e lo spionaggio industriale. In caso di attacchi informatici, le aziende rischiano moltissimo: non solo danni contingenti ma anche danni permanenti all'immagine del brand.

RISCHIO ELEVATISSIMO

Purtroppo, nonostante questo scenario e queste premesse, in termini di sviluppo dei sistemi di sicurezza informatica, le aziende sono molto indietro. Di particolare rischio sono alcuni processi, in particolare quelli mirati a ottenere rapide soluzioni web, come ad esempio l'unione di software esistenti con nuovi codici di programmazione.
Cosa succede? Volendo creare un'applicazione troppo velocemente si rischia di dimenticarsi di implementare anche un appropriato livello di sicurezza. E gli hacker sono sempre alla ricerca di opportunità come questa per colpire.

TROPPO LASCIATO AL CASO

Inoltre, quando si tratta di sicurezza IT, troppo viene ancora lasciato al caso. Molto spesso, ci si affida a singole soluzioni che risolvono solo alcune problematiche, come soluzioni specifiche contro i virus, soluzioni per la gestione delle password e delle identità o strumenti per la crittografia di dati aziendali sensibili. Non solo, nelle aziende ci sono tante persone che si occupano di proteggere questo o quell'aspetto, ma raramente vi è una persona responsabile per tutte le attività di sicurezza IT. Il risultato? Un patchwork.

UNA PRIORITÀ

La sicurezza IT deve diventare una priorità per le aziende. E' fondamentale sviluppare strategie olistiche di sicurezza informatica che prendano in considerazioni qualsiasi processo. Sarebbe meglio che fosse previsto, come succede già in altri Paesi, una figura specifica – in particolare uno Chief Security Officer - responsabile dell'implementazione ma anche degli aggiornamenti. Singole soluzioni che risolvono singoli problemi ormai non sono più sufficienti. Le aziende devono agire adesso se vogliono giocare in anticipo e prepararsi a mitigare altri attacchi informatici.

Maurizio Moroni(*)

Cloud: cosa può fare l'utente finale
per la sicurezza dei propri dati

Cloud: un dibattito riemerso con prepotenza dopo i recenti episodi che hanno visto numerosi furti di immagini private. L'articolo fa il punto su potenzialità e limiti del Cloud, individuando alcune strategie che l'utente finale può mettere in atto per assicurarsi un godimento pieno della tecnologia, ma in sicurezza. Perché è bene tenere a mente che i principali vantaggi del Cloud (flessibilità, accessibilità e ottimizzazione dei costi) possono essere vanificati se non vengono posti efficaci sbarramenti all'accesso.

(*) Responsabile Divisione Security di Partner Data.
www.partnerdata.it

Partiamo dai vantaggi, e in particolare dall'**ottimizzazione dei costi**. Sappiamo che uno dei maggiori benefici del Cloud è la possibilità di tagliare la spesa in termini di gestione e manutenzione dell'hardware in house. Il Cloud, infatti, è in grado di combinare allo stesso tempo convenienza economica e prestazioni di alto livello, affidabili e ridondate. Ecco perché i primi a trovare conveniente l'adozione del Cloud sono tutte quelle piccole e medie realtà solitamente non equipaggiate con robusti sistemi di disaster recovery (a volte del tutto inesistenti), che si servono del Cloud al fine di ridurre al minimo le interruzioni lavorative. Per avere un assaggio della **flessibilità** offerta dal Cloud, basti invece pensare a quanto sarebbe anti-economico, per una piccola impresa, implementare, gestire e manutenere sistemi informatici complessi che possano garantire solide performance. Grazie all'**accessibilità** tipica del Cloud, inoltre, diventa possibile semplificare la collaborazione tra utenti interni ed esterni ai propri uffici, grazie a dispositivi fissi o portatili, ed utilizzare qualsiasi tipo di applicazione senza doversi preoccupare dell'hardware necessario.

CRITICITÀ

Il Cloud, tuttavia, presenta anche degli aspetti critici che è bene non sottovalutare: sebbene da un lato questa tecnologia permetta a chiunque di estendere l'affidabilità del proprio sistema IT e la capacità di condividere le informazioni, bisogna sempre ricordare che queste ultime vanno a finire, inevitabilmente, nelle mani del fornitore di servizi. Il fornitore dovrebbe essere di comprovata affidabilità perché è a lui che l'utente finale demanda, oltre che il supporto tecnico, sia la protezione fisica dell'infrastruttura che la protezione telematica da attacchi esterni. Come è noto, inoltre, affidarsi al Cloud significa dipendere al 100% dalla connettività: se la rete dovesse andare offline, si verrebbe irrimediabilmente tagliati fuori, incapaci di connettersi ai servizi chiave per lavorare o leggere file importanti.

E L'UTENTE CHE FA?

I recenti fatti di cronaca, che hanno visto furti di immagini private di personaggi celebri, hanno fatto riemergere con prepotenza il dibattito sulla sicurezza del Cloud, stavolta mettendo in luce anche la possibile responsabilità dell'utente stesso. Non si finirà mai di ricordare infatti che il Cloud non rappresenta necessariamente un passo avanti… se non si presta la dovuta attenzione! Bisogna essere coscienti che, una volta entrati nella nuvola, i propri dati transitano nei server di qualche fornitore, il quale potrebbe farne uso per scopi propri o commerciali o potrebbe addirittura non essere adeguatamente preparato ad affrontare minacce informatiche. Sicuramente è necessario prestare sempre la massima attenzione nella selezione e nella scelta del servizio, leggendo attentamente le policy: i server e l'intera infrastruttura del fornitore devono rispondere ai requisiti minimi di sicurezza imposti dalla EU e godere della massima trasparenza in termini di gestione delle informazioni. Purtroppo però alcune volte questa accortezza non basta.

FURTO DI DATI SENSIBILI

Come recentemente sottolineato dalla Cloud Security Alliance, infatti, al primo posto nella classifica dei 9 pericoli del Cloud computing c'è il furto di dati sensibili. La classifica offre lo spunto per riflettere su come molte delle best practices utilizzate in passato non abbiano più senso in ambito Cloud e, per questo, il modo più efficace per proteggersi sia il **controllo degli accessi alla fonte**, ovvero l'identificazione certa dell'utente e l'amministrazione dei diritti di accesso al singolo dato. Per fare questo, oltre allo scegliere password che non siano troppo semplici, potrebbe essere d'aiuto fare affidamento su una "sicurezza aggiuntiva" gestita dall'utente finale: la crittografia. I prodotti per la cifratura dei dati sul Cloud attualmente in commercio, infatti, rendono i dati sensibili assolutamente illeggibili a chi non sia stato precedentemente autorizzato. Tuttavia anche una soluzione di crittografia, per quanto fortemente consigliata, non rappresenta l'unico step necessario per essere al sicuro, dal momento che in rete le insidie sono molte e sempre più spesso difficili da notare. È buona norma, pertanto, dotarsi anche di sistemi operativi costantemente aggiornati con le pacthes dei rispettivi fornitori, utilizzare sistemi antivirus e adottare "comportamenti responsabili". Ad esempio la scelta di una password robusta e la massima attenzione ad eventuali episodi di email phishing possono sicuramente mettere al riparo l'utente da situazioni spiacevoli. Quello che spesso non viene detto è che anche la scelta della password può rivelarsi meno semplice di quello che si pensa, soprattutto nei casi in cui i dati da proteggere sono di grande importanza. Anche in questo caso è di nuovo la tecnologia a soccorrere l'utente, che può fare ricorso a strumenti generatori di password casuali e utilizzabili una sola volta (come accade nei pagamenti online) o a strumenti di rilevazione biometrica, come i lettori di impronta.

23–26 SEPTEMBER 2014

The World's Leading Trade Fair for

Security & Fire Prevention

THE NUMBER ONE FOR 40 YEARS

Meet exhibitors and safety experts from over 100 nations at the global marketplace. Discover new safety trends, exciting innovations and top-class forums. Seize your opportunity for know-how, networking and business!

MESSE ESSEN
Place of Events

www.security-essen.de

40 YEARS
security essen 2014
THE NUMBER ONE

Mario Vento(*)

La motion detection è video analisi intelligente?

Motion detection è video analisi intelligente? E prima ancora: cosa significa intelligenza?
Quando si parla di video analisi intelligente ci si avvicina ad un territorio i cui confini sono vaghi e imprecisi: sarà che il termine intelligente è abusato, che sul suo significato non vi è un'unitarietà di interpretazione, che faccia scena inserirlo per aggettivare il nome di un prodotto, che un po' di intelligenza non guasti mai. Quindi cosa significa intelligenza?

(*) CEO di A.I. Tech srl

Dal punto di vista tecnico, mi piace dare la definizione che offro ai discenti del corso di Visione e Modelli per la Visione Artificiale da me tenuto all'Università degli Studi di Salerno. «Se desideriamo appurare se un software sia intelligente e contiamo di poter applicare il test di Turing, ci fermiamo prima di partire!». Per chi non lo sapesse, in via semplificata, il test di Turing ha successo per un software allorquando, mettendo dietro una tenda un essere umano e un software, questi risultino indistinguibili a un utente che porge domande e riceve risposta da uno o dall'altro. Affascinante? Coinvolgente? Certo, ma l'utilità pratica del test è decisamente limitata, e non è difficile comprenderlo. E ancora «una video analisi è intelligente quando il relativo software è realizzato con metodologie non procedurali». Paroloni da accademia? Forse sì, ma non vi spavento. I software moderni usano tecniche risolutive che, mediante reti neurali o altre diavolerie informatiche, apprendono da esempi. Un attimo di pazienza e vi offro un esempio che spero possa farci uscire dal vago. Se desideriamo imparare a riconoscere funghi mangerecci da quelli velenosi possiamo procedere in due modi: un esperto ci insegna le proprietà da osservare per capire, passo dopo passo, se un fungo di identità ignota sia velenoso o meno - questo modo di procedere è quello che è realizzato nel software tradizionale, che è guidato da un algoritmo. Questo altro non è che una codifica, adeguata ad un calcolatore, della conoscenza dell'esperto che ci ha messo a disposizione il procedimento per distinguere, nelle suddette categorie, i funghi. Un metodo alternativo è invece quello di osservare tanti funghi, sia buoni che velenosi, e conoscendone la categoria, di imparare nel tempo a distinguerli. "Learning from examples" è il modello di software intelligente. In questo caso non vi è conoscenza trasferita da un esperto e codificata in un programma, bensì un software più evoluto (e quindi detto intelligente) che impara a risolvere problemi, valutando esempi di problemi già risolti. Questo modello, praticabile solo da qualche anno, successivamente all'avvento di calcolatori potenti, sta conquistando giorno dopo giorno fette di mercato.
Ma attenti agli abusi: se l'aggettivo *intelligente* non è affiancato dall'uso di questi modelli di software, ci troviamo di fronte ad un abuso. E ora, dopo questa interessante prolusione tecnica, con spunti di spicciola filosofia, torniamo alla domanda sottesa dal titolo: la motion detection è video analisi intelligente? Sapendo cosa si intende per "intelligente", proviamo a rispondere, ma preventivamente comprendiamo a che serve e come opera un algoritmo di **motion detection**.

A COSA SERVE?

Un tale algoritmo ha l'obiettivo di rilevare se all'interno della scena ci sono oggetti in movimento, come persone, auto o altro. In tal caso genera un allarme usato per attivare un'azione, che può consistere nel notificare un SMS di avviso su un telefonino o una e-mail magari corredata con alcuni fotogrammi selezionati tra quelli che hanno generato l'allarme; in tal modo il proprietario del sistema può verificare (anche da lontano) cosa sta accadendo. La maggior parte delle telecamere digitali sono corredate in fabbrica di un algoritmo di motion detection di cui si può configurare la sensibilità, ovvero determinare di quanto deve variare la scena per generare l'allarme.

COME FUNZIONA?

La maggior parte degli algoritmi disponibili sulle telecamere sono molto semplici e operano su un principio elementare: calcolano su tutta l'immagine la differenza tra il valore dei pixel omologhi tra frame successivi. In assenza di oggetti in movimento, tutti i pixel dell'immagine non cambiano valore (teoricamente!) e quindi la somma di tutte le variazioni è nulla. Quando una persona o un oggetto entra nella scena, i pixel ad esso associati nel frame precedente hanno il valore dello sfondo e in quello corrente il colore della persona; si genera quindi per tutti questi pixel una variazione la cui somma viene confrontata con una soglia di sensibilità. A titolo di esempio si veda la **Figura 1** (nella pagina successiva). È quindi importante evidenziare che l'algoritmo non *riconosce* le persone o gli oggetti e di questi deduce il movimento, come invece fanno gli algoritmi di video analisi intelligente: il moto è desunto dal fatto che ci sono state variazioni di valori di pixel in quantità tale da presumere che ci sia stato un cambiamento. Insomma si tratta di un algoritmo *cieco*!

CHE PROBLEMI CREA?

Il semplice principio di funzionamento determina diversi problemi. Anzitutto bisogna fissare la soglia sulla base della dimensione presunta del soggetto o dell'oggetto che si vuole rilevare, in maniera tale che in sua presenza scatti l'allarme. Per come funziona l'algoritmo questo non dipende solo dalla dimensione: se entra un soggetto vestito di chiaro su sfondo mediamente scuro, a parità di dimensione, esso crea una differenza complessiva molto più alta di un soggetto che veste di grigio. Potrebbe quindi accadere che l'algoritmo non genera un allarme (Falso Negativo) quando il soggetto è più piccolo di quello ipotizzato o quando il suo colore è poco diverso dallo sfondo. Il problema più

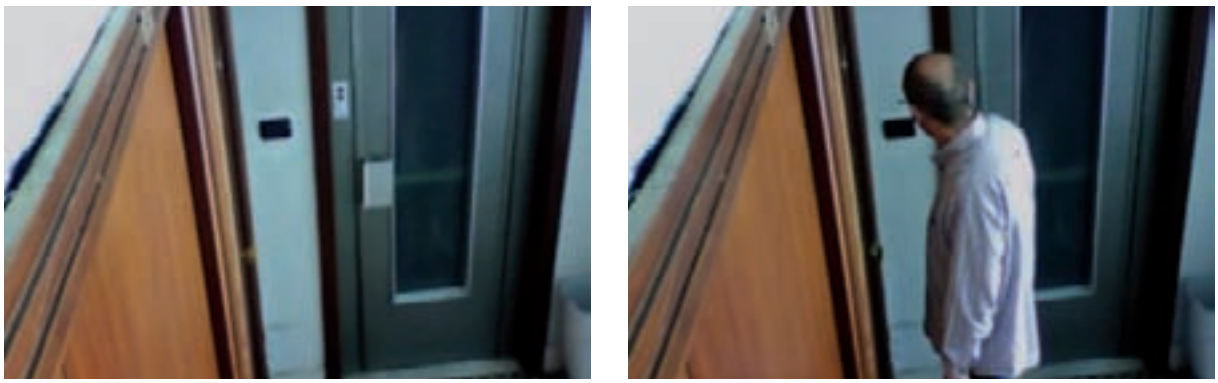


Figura 1: La telecamera (in modalità day) inquadra la porta su di un pianerottolo. L'ingresso di una persona determina correttamente l'allarme del motion detector. Si noti che la persona in questa inquadratura occupa circa 1/7 dell'area totale.

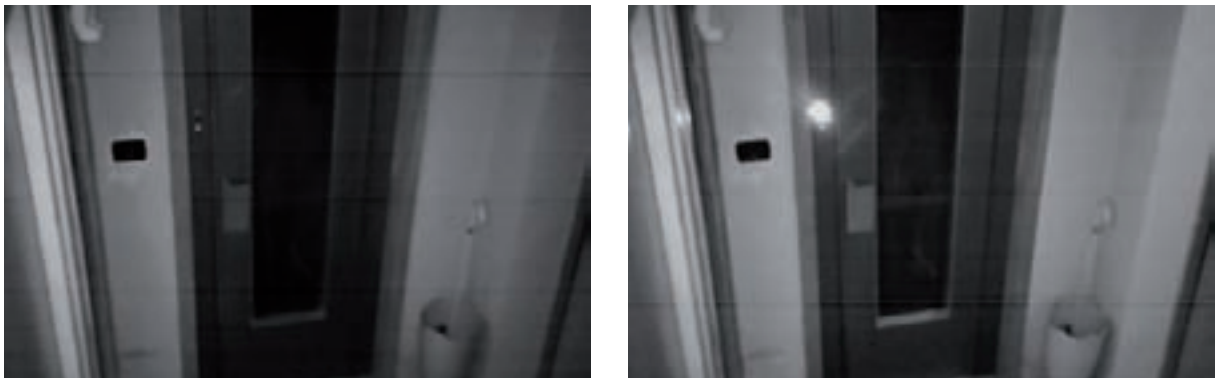


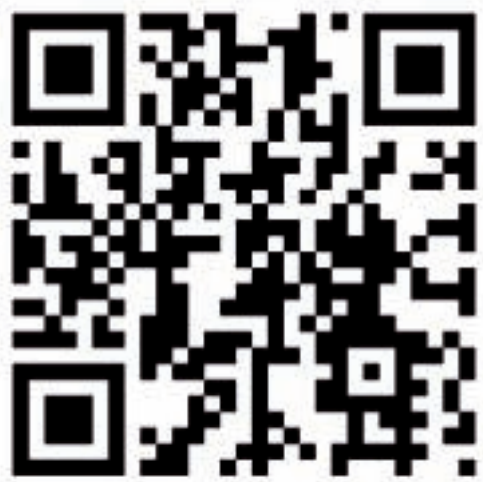
Figura 2: La telecamera in modalità night. Una persona, in un piano diverso da quello sorvegliato, accende le luci della scala e chiama l'ascensore. La differenza di luminosità complessiva della scena genera un falso allarme.

grave è quello relativo alla presenza di molti Falsi Positivi. Se si verifica un cambio di luminosità cambiano di conseguenza e contemporaneamente tutti i pixel, anche se non è presente alcun soggetto nella scena. Il fatto che tutti i pixel cambino valore, sebbene non di tantissimo, è tale che la differenza sia grande, cioè da superare la soglia di allarme. Un esempio è mostrato in **Figura 2.**

È INTELLIGENTE?

È evidente che un algoritmo di motion detection effettua un'analisi dell'immagine - e quindi può considerarsi sul piano teorico un algoritmo di video analisi - ma la semplicità delle elaborazioni effettuate lo colloca al di fuori della categoria dei sistemi di video analisi intelligente. La sua natura fa sì che l'impiego consigliato non sia quello relativo alla generazione di allarmi, in quanto se ne otterrebbe una scarsa affidabilità in relazione alla notifica di molti falsi positivi, ma piuttosto di comandare la registrazione: basandosi sull'evidenza che è inutile registrare se non ci sono variazioni nella scena, il motion detector avvia la registrazione quando rileva una variazione e la interrompe quando si ritorna in una soluzione di stabilità. In questo caso l'effetto della generazione erronea di una variazione (causata ad esempio da un cambio di luminosità) ha un effetto trascurabile, quello di aver avviato inutilmente una registrazione per pochi secondi. L'eliminazione di questi effetti negativi richiede quindi un algoritmo che sia capace effettivamente di riconoscere ciò che è presente nella scena, quali persone, oggetti o animali, e di analizzarne il movimento, annullando quindi ogni problematica legata a variazioni di luminosità; in tal modo si potranno addirittura discernerne situazioni complesse come una porta che si apre per il vento senza che vi siano persone presenti o simili, come richiede un'applicazione professionale di mercato.[1]

[1] Come il prodotto A.I. Intrusion al link **http://www.aitech-solutions.eu/ai-intrusion**



Fallo subito!

sec solution

La Redazione

Business intelligence, big data e videosorveglianza

Da diversi anni le realtà aziendali più evolute sono alla ricerca di strumenti che permettano un'analisi sempre più dettagliata dei dati raccolti da diverse fonti. Spesso si tratta di dati che in gran parte sono già a loro disposizione ma eterogenei e quindi complicati da raccogliere e interpretare. Diventa quindi sempre più importante disporre di uno strumento per la raccolta e l'analisi automatica di queste informazioni. Qualora il patrimonio di informazioni non fosse sufficiente con quanto attualmente raccolto dall'azienda, la richiesta si estende a strumenti innovativi per il recupero di ulteriori prospettive di analisi. Una delle risposte possibili è rappresentata da soluzioni di Business Intelligence che già da diversi anni rappresentano un trend crescente sia in termini di spending che in termini di soluzioni disponibili.

Dalla videoanalisi alla business imaging intelligence: l'analisi automatica delle immagini è un tema sempre più sentito dalla clientela, che parte dal retail per lambire ormai altri campi di azione. Ma come la mettiamo con l'accuratezza dell'analisi?

Risponde Franco Palleni,
Pro Imaging Segment Manager di Canon Italia

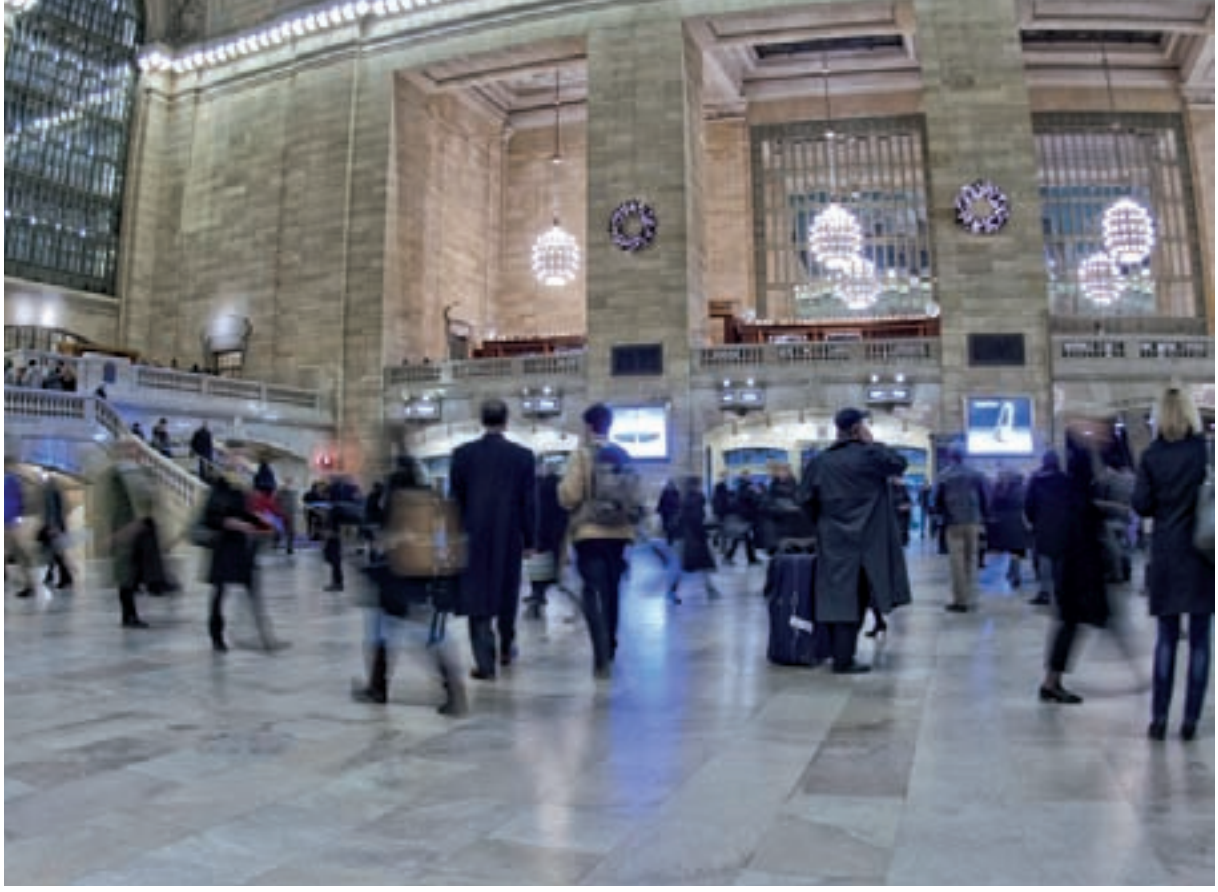
Il concetto di Business Imaging Intelligence per Canon nasce effettivamente da un'esigenza evidenziata dal retail ma che, di pari passo con il suo sviluppo, si è rivelata particolarmente efficace anche per altri ambienti: pensiamo solo ad aeroporti, stazioni, ma anche alle fiere. Del resto il monitoraggio dei flussi delle persone e di come esse si muovano in uno specifico ambiente è un tema ad ampio raggio e che interessa target molto diversi. Per quanto riguarda l'accuratezza della videoanalisi (che si è peraltro molto affinata negli anni), con la Business Imaging Intelligence si entra nel campo nel monitoraggio statistico dei flussi, quindi anche eventuali inaccuratezze dell'algoritmo sono mitigate dal fatto che ci si concentra su una visione globale del dato e non sul dato specifico, non essendo focalizzati unicamente sul tema sicurezza. E prima ancora l'accuratezza dell'immagine parte delle ottiche, che mitigano eventuali imprecisioni della videoanalisi. E Canon serve da sempre i professionisti dell'imaging con ottiche di altissima qualità.

www.canon.it

Tra gli strumenti maggiormente conosciuti si annoverano le soluzioni di BI (business intelligence) che analizzano dati provenienti da ERP (es. Oracle, SAP, etc) e dati provenienti dal Web (es. Google analitics, etc). Insieme a queste soluzioni, alcuni prodotti incorporano un'ulteriore e importante fonte di informazioni: quelle provenienti dall'Imaging, essenzialmente sfruttando strumenti di videoanalisi e applicando ai dati le metodologie consolidate per l'analisi di dati provenienti da fonti tradizionali. Possiamo ricondurre l'insieme di queste tre tipologie di soluzioni al paradigma di Big Data che, oltre ad essere un argomento molto discusso e dibattuto, rappresenta un'enorme potenzialità per gli strumenti di analisi più evoluti.

BUSINESS INTELLIGENCE E BIG DATA

La crescente maturità del concetto dei Big Data evidenzia alcune differenze con la Business Intelligence. Quella maggiormente diffusa tratta i dati e il loro utilizzo. In particolare si rileva che la business intelligence si avvale della cd. **statistica descrittiva**, utilizzando dati ad alto contenuto informativo per misurare e rilevare tendenze. In poche parole utilizza raccolte di dati limitati, modelli esemplificati e dati puliti. Big Data invece usa un sistema di **statistica inferenziale** con concetti di identificazione di sistemi non lineari, in modo tale da dedurre leggi partendo da un insieme di dati. Sul mercato si trovano soluzioni che, a differenza di quelle tradizionali di Business Intelligence, utilizzano anche la statistica inferenziale per la presentazione dei dati, incorporando quindi entrambi i concetti di statistica sopra riportati. Inutile sottolineare che la possibilità di accedere a dati importanti in tempo reale si è trasformato in un vantaggio e in un punto fondamentale di differenziazione per le attività e le operazioni decisionali.



DALLA VIDEOANALISI ALLA BUSINESS IMAGING INTELLIGENCE

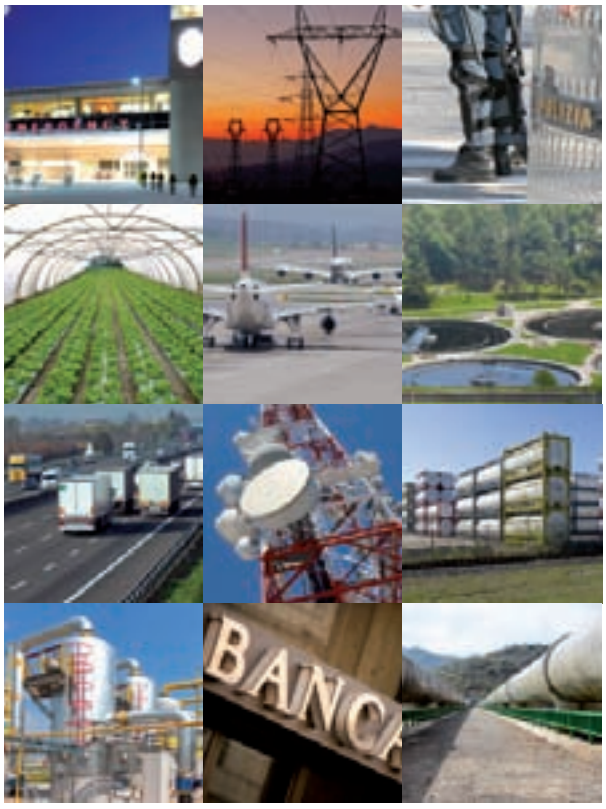
Le soluzioni che utilizzano l'Imaging per produrre nuove fonti dati per la Business Intelligence sfruttano processi di astrazioni successive passando dai dati grezzi a modelli di inferenza sulle aree di interesse. Nel dettaglio usano algoritmi ormai consolidati di videoanalisi quali l'**area counting**, il **gate flow**, l'**occupancy rate** e le **hot zone**, poi vengono creati modelli di comportamento che descrivono la fruizione di spazi pubblici, passando infine a modelli di *Visitatori, Ingressi* e *Zone Calde*.
Visitatori è il modello che descrive il numero di persone che visitano un area, e il tempo di permanenza. Questo modello di comportamento viene alimentato dai tre algoritmi *gateflow, area counting* e *occupancy rate* utilizzando una logica di "feed" che valuta dinamicamente quale degli algoritmi di base sia il più consono per l'analisi richiesta dal cliente.
Ingressi è il modello che descrive il numero di persone che entrano ed escono da una porta/accesso, settore e quale è la direzione preferenziale che queste prendono una volta entrate.
Il modello utilizza per il "feed" gli stessi algoritmi del modello *Visitatori*.
Zone calde è il modello che visivamente, attraverso gradazioni di colori su una mappa, riporta quali sono le aree in cui si concentrano le attività dei visitatori. Infine le **Aree** forniscono un rapido punto di partenza per esaminare le informazioni (ad es. a livello di store, di reparto, di area, di isola e così via). Altro fattore interessante di questi strumenti è che forniscono utili output analitici senza dover archiviare le immagini analizzate, rispettando quindi la **privacy** dei fruitori delle aree pubbliche.
In definitiva la BI si è molto evoluta grazie all'implementazione dell'Imaging e questi sistemi portano la pianificazione di strategie di marketing e merchandising su un nuovo livello: semplificandole e ampliandole con nuove fonti di informazioni.

La Redazione

Sicurezza e oltre, per andare *oltre* la sicurezza

Sicurezza & oltre: un talk show all'insegna di quell'_oltre_ contenuto già nel titolo e denso di attese e significati. Questo il fulcro del Congresso nazionale degli operatori di Sicurezza che si è tenuto l'8 Ottobre a Milano, segnando il ritorno di un appuntamento che a lungo ha accompagnato il settore sicurezza negli anni dispari.

Dal Congresso è subito emerso che quell'*oltre* la sicurezza incarna una forte valenza politica, associativa, istituzionale, tecnologica, ma soprattutto aggregativa a tutti i livelli - come aggregativa è stata la forza motrice dell'intero evento, pensato e voluto dalle principali Associazioni del comparto (AIPS, ANIE Sicurezza, ASSISTAL, ASSOTEL, ASSIV, ASSOSICUREZZA, AIIC) col supporto di Fiera Milano. Dal Congresso, incentrato sul tema della protezione delle infrastrutture critiche, è poi emerso che l'oltre non è uno scenario futuribile ma un futuro molto prossimo, che in certi casi è già un presente attivo. L'oltre è infatti pensare al nostro quotidiano come governato dalle infrastrutture critiche, perché quel tipo di infrastrutture – benché quasi mai codificate come tali - sono tutte intorno a noi: dalle utilities ai trasporti, dalle telecomunicazioni all'EXPO 2015.



L'oltre è pensare che la continuità operativa è un diritto di qualunque cittadino, e quindi anche una responsabilità di ciascuno di noi: dalla base della collettività all'industria, dall'amministratore pubblico fino al decisore politico. E in questo scenario, in tempi di spending review, è essenziale che il privato vada oltre e cominci ad organizzarsi in modo concreto a prescindere da un'iniziativa pubblica che stenta e sempre più stenterà a decollare.

Viviamo insomma in un contesto di social continuity dove tutti devono fare la loro parte: dalla definizione di una corretta catena di comando e controllo in emergenza, alla resilienza affrontata in chiave di prevenzione. Il tutto facendo sempre attenzione al triplice livello di integrazione - quindi di complessità – che presenta qualsiasi infrastruttura critica: il piano verticale (la catena dell'approvvigionamento, dove assai raramente ci si pone problemi di sicurezza), quello orizzontale (cioè territoriale, che passa da un vertice nazionale o globale ad

Un'immagine del talk show. Da sinistra: Emil Abirashid (Giornalista); Gianna Detoni (Presidente di Hi-Care); Manuel di Casoli (PMO-Field Operations Manager EXPO 2015); Damiano Toselli (Responsabile Security Corporate Telecom Italia); Luisa Franchina (Principal in Solving Efeso); Emiliano Cardoni (Senior Consultant in Hermes Bay).

un tessuto operativo di stampo locale) e quello trasversale del mondo cyber, che ormai attraversa diagonalmente qualunque attività, portando valore aggiunto ma anche nuovi rischi.

L'oltre è la somma di tutte queste criticità, ma anche la luce alla fine del tunnel: in questo scenario il cerino passa quindi al comparto sicurezza - pubblico e privato, tecnologico, dei servizi o dei media, appartenente all'impianto regolatorio o a quello strettamente operativo, italiano ma anche sovranazionale. Sta a tutti noi trovare un punto di sintesi che possa portare ad un livello più alto la consapevolezza collettiva dell'esistenza di una serie di rischi, spesso assai più vicini di quanto non si pensi, e della necessità di costruire assieme quel diritto, quasi sempre negato ma che ci appartiene, alla continuità operativa.

L'EXPO 2015 sarà una grande occasione per metterci alla prova come sistema paese, per dimostrare al mondo che siamo in grado di gestire con competenza e serietà il più grande evento di questa decade e che possono coesistere sotto lo stesso tetto padiglioni israeliani e palestinesi. E, perché no? - che anche il cipresso giapponese, finora mai espiantato in Occidente, non causerà una fitopandemia con seguente mattanza di olivi secolari, ma potrà coesistere allegramente con le migliaia di altre piante che fioriranno all'EXPO.

IP Security MAGAZINE
TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY
www.ipsecuritymagazine.it

ANNO 4 – Numero 14 – OTTOBRE 2014

Direttore responsabile
Andrea Sandrolini

Coordinamento editoriale
Ilaria Garaffoni
redazione@ethosmedia.it

Direzione Commerciale
Roberto Motta
motta@ethosmedia.it

Ufficio Traffico
Carolina Pattuelli
pattuelli@ethosmedia.it
tel. +39 051 0475136

Ufficio estero
international@ethosmedia.it

Pubblicità
Ethos Media Group srl
ethos@ethosmedia.it

Sede Legale
Via L. Teruzzi, 15 - 20861 Brugherio (MB)

Direzione, redazione, amministrazione
Ethos Media Group srl
Via Paolo Fabbri, 1/4 – 40138 Bologna (IT)
tel. +39 051 0475136
Fax +39 039 3305841
www.ethosmedia.it

Registrazione
Tribunale di Bologna al n° 8218
del 28/12/2011 - Dicembre 2011

Iscrizione al Roc
Ethos Media Group s.r.l.
è iscritta al ROC
(Registro Operatori di Comunicazione)
al n. 19315 del 2 marzo 2010

Periodicità - bimestrale

Privacy (banche dati)
Le finalità del trattamento dei dati dei destinatari del Periodico consiste nell'assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. Tali dati sono trattati nel rispetto del D.Lgs. 196/2003. Responsabile del trattamento dei dati raccolti in banche dati ad uso redazionale è il direttore responsabile a cui gli interessati potranno rivolgersi per esercitare i diritti previsti dall'art. 7 del D. Lgs. 196/2003

Grafica / impaginazione
zeronovecomunicazione.it

Ethos Media Group sr.l è associata ad ANES

WEBSITE

secsolution
security online magazine

security magazine online

www.secsolution.com è il portale d'informazione b2b di riferimento per i professionisti della security in Italia.
In pochi anni di operatività, **www.secsolution.com** si è consolidata come piattaforma autorevole di aggiornamento in materia di sicurezza fisica ed elettronica. Studiato per essere massimamente usabile, **www.secsolution.com** è un portale dalla navigazione intuitiva e che contiene un motore di ricerca interno selezionabile per tecnologia, brand e parole chiave. L'ampia gamma di sezioni tematiche, abbinata ad un vasto parco multimediale con audio, video, interviste e trailer di eventi, copre tutte le tematiche di interesse per gli operatori: da quelle strettamente tecnologiche a quelle normative, da quelle economico-fiscali alla formazione professionale, fino alle curiosità. L'update quotidiano seguibile anche su Twitter e Facebook, e la frequentatissima newsletter, inviata a cadenza settimanale ad un target altamente profilato, chiudono il cerchio dell'aggiornamento settoriale.

secsolution.com

il security magazine online
Per un aggiornamento
giornalistico quotidiano,
interattivo e ricco
di spunti e contenuti.

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

Ethos Media Group s.r.l.
Via Venini, 37
20127 Milano
Fax +39 039 3305841
ethos@ethosmedia.it
www.ethosmedia.it