White Paper

La sicurezza nell'era del Cloud

1 Introduzione

Nell'ambito dei sistemi informativi si sta prefigurando un cambiamento che influenzerà in modo significativo l'assetto delle infrastrutture aziendali. Si tratta del cloud computing, ovvero l'insieme di tecnologie che permettono l'utilizzo, in una logica on demand, di risorse hardware (storage, CPU) o software, distribuite in remoto sia all'interno che all'esterno del perimetro aziendale. Esso si traduce in tre possibili modelli di erogazione: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

E' convinzione comune che la spinta al cambiamento non sarà propiziata dall'innovazione tecnologica, quest'ultima ne costituirà soltanto il fattore abilitante. Saranno piuttosto motivazioni di ordine economico e di business che porteranno gli utenti a trovare percorsi diversi da quelli sinora attuati. Qual è il compito delle organizzazioni IT? Semplice, ma nello stesso tempo complesso: dovranno essere in grado di accompagnare questo cambiamento e disporre delle soluzioni che possano favorire una sostenibilità ottimale del nuovo paradigma.

*CA Technologies, protagonista di primo piano nel mercato della sicurezza e della tecnologia di **Identity and Access Management**, ritiene che il cloud costituisca la nuova frontiera tecnologica, ma nello stesso tempo è consapevole che il passaggio o migrazione di server aziendali verso il nuovo paradigma debba essere necessariamente accompagnato da soluzioni e strumenti in grado di assicurare lo stesso livello di protezione degli assett che è oggi possibile mettere in atto*

La migrazione dell'IT al cloud sarà un percorso inevitabile, affermano gli analisti. In quale modo verrà attuato è ancora del tutto imprevedibile. Public cloud, private cloud, o una combinazione di entrambe in una forma di tipo ibrido? Gli scenari possibili sono molteplici. L'ipotesi più accreditata è che non vi sarà una migrazione che interesserà l'intero spettro delle applicazioni oggi esistenti in area enterprise. Parte di queste continueranno a risiedere presso il cliente, parte migreranno sulla rete.

Le dinamiche che in questi ultimi anni hanno caratterizzato l'evoluzione dei sistemi informativi - ovvero una tendenza a una razionalizzazione e ottimizzazione degli impianti elaborativi con una forte spinta alla centralizzazione – rendono peraltro implicito un possibile passaggio a ecosistemi di tipo cloud. La massiva virtualizzazione operata a livello server all'interno dei comparti IT delle organizzazioni, ne costituisce un primo passo e, insieme, una premessa.

Una cosa è certa: affinché il cloud possa essere considerato una reale alternativa nei confronti degli ambienti tradizionali si dovrà essere capaci di dimostrare di poter garantire lo stesso grado di

sicurezza che attualmente un'azienda riesce a stabilire al proprio interno. L'adozione del cloud da parte delle imprese appare infatti frenata soprattutto dalla mancanza di sicurezza.

La diffidenza delle aziende nei confronti del nuovo paradigma infrastrutturale e di data center del cloud è alimentata da un luogo comune: quello della non affidabilità e incoerenza del cloud rispetto ai requisiti richiesti in ambito enterprise. Gli utenti si chiedono se il cloud è sicuro. Può esserlo? Secondo CA Technologies la risposta è sì.

Come proteggere un ambiente fisicamente disperso? Quali possibilità di controllo esistono su entità esterne, siano esse private o pubbliche? In definitiva la domanda che tutti si pongono è: "ci si può fidare del cloud?" La risposta da parte di CA Technologies è sì, ma a una serie di condizioni. Quali? Essenzialmente la capacità di trasferire in ambiente cloud tutte quelle soluzioni di sicurezza che sono già state applicate a livello centralizzato e che, in particolare, fanno riferimento al controllo e gestione delle identità, degli accessi e delle informazioni in ambienti complessi, fisici e virtualizzati.

Date queste premesse, va da sé che tutte quelle aziende che hanno in utilizzo e hanno acquisito esperienza in questo tipo di soluzioni possano essere considerate pronte a confrontarsi con il cloud. Ma quali e quante sono?

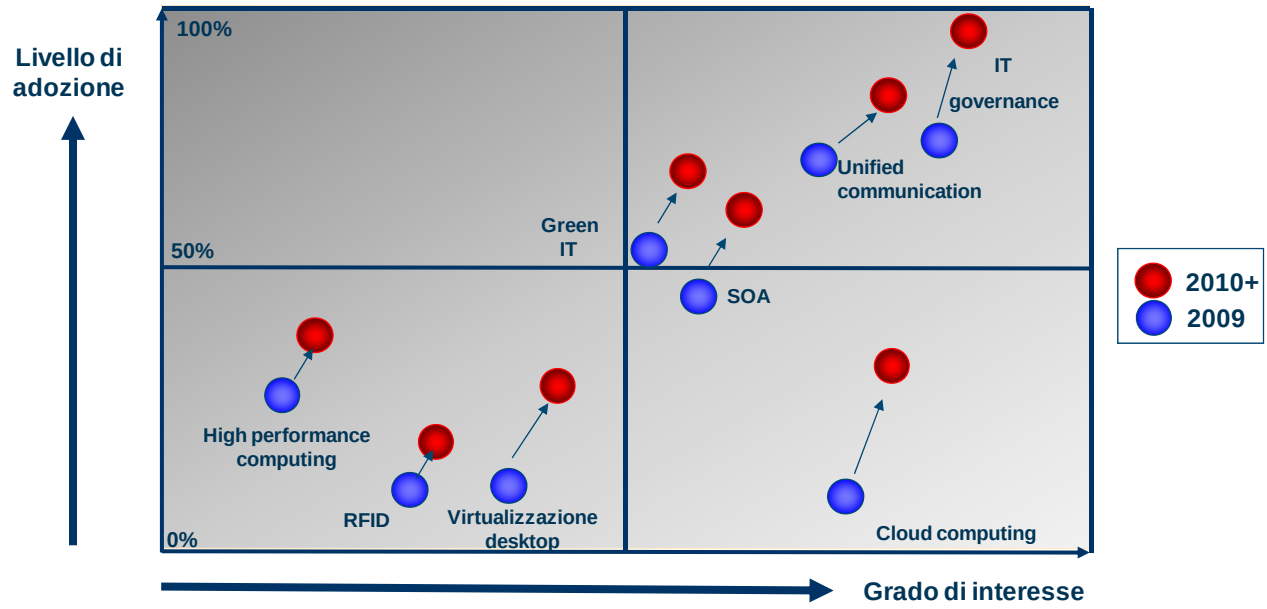
Per rispondere a questi interrogativi – ovvero comprendere quanto le aziende italiane sono predisposte, o potenzialmente predisposte, all'era del cloud – occorre conoscere l'attuale grado di sensibilità delle organizzazioni nei confronti di queste tematiche. La consapevolezza o meno di questo fenomeno è il fattore che può determinare l'adeguatezza tecnologica al deployment del nuovo ordine infrastrutturale: il cloud.

Al fine di comprendere lo stato della sicurezza delle aziende in Italia, e la predisposizione culturale e tecnologica al cloud, CA Technologies ha commissionato a NetConsulting un'indagine conoscitiva presso un campione rappresentativo delle grandi aziende che operano nel nostro Paese.

2 L'interesse del mercato nei confronti del cloud

Il grado di interesse manifestato dagli utenti verso il nuovo paradigma elaborativo del cloud è in evidente accelerazione e si inserisce all'interno di un percorso di innovazione dove trovano spazio priorità che tendono a soddisfare interventi improntati a un recupero di efficienza, produttività e ottimizzazione dei costi (Figura 1).

Figura 1 Interesse e adozione di tecnologie, architetture e metodologie innovative (2009-2010+)



Fonte: NetConsulting

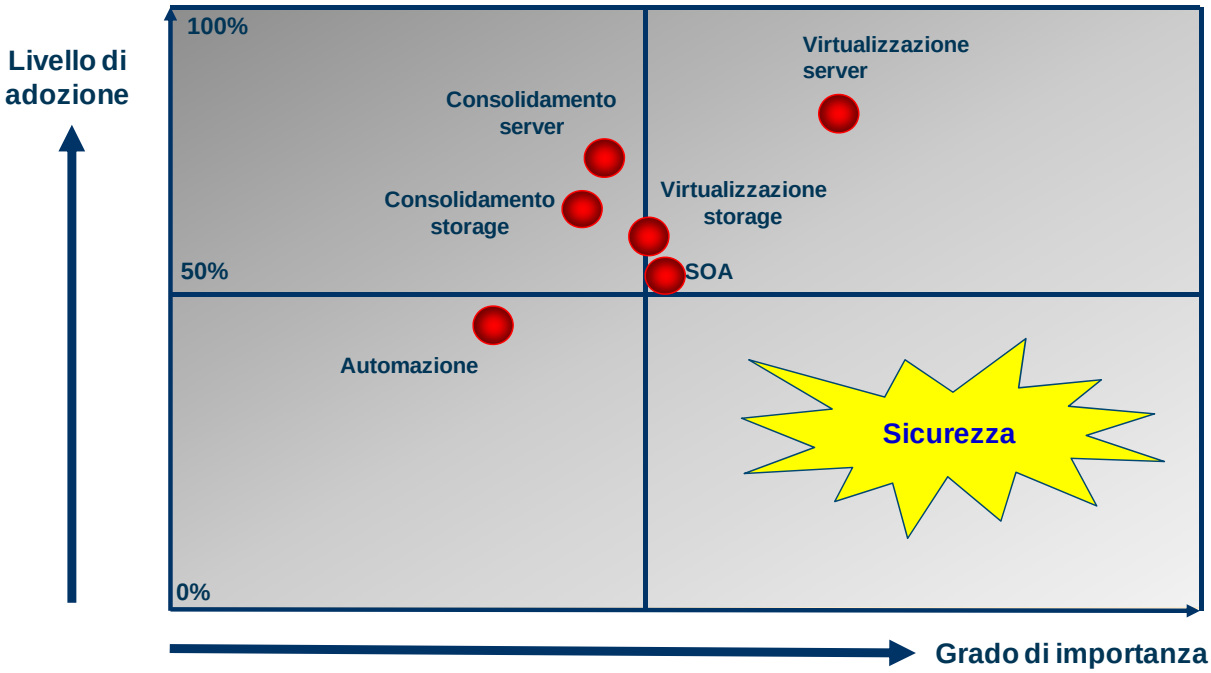
Obiettivo di CA Technologies è assicurare, così come accaduto in passato, la gestione dell'intero spettro delle architetture esistenti e in divenire – fisica, virtualizzata e cloud – garantendo la massima protezione degli investimenti sinora operati, così come una estensione degli stessi verso le nuove forme di computing prospettate dal cloud.

Tra le priorità assumono un ruolo di primo piano, da una parte, l'IT governance, ovvero un modello di gestione dell'IT che, attraverso l'adozione di strumenti e metodologie standard, implica la capacità di controllare, monitorare, pianificare e misurare risorse e fornitori IT per meglio indirizzare l'operato e le strategie dei Sistemi Informativi verso il raggiungimento di obiettivi di business. Dall'altra la comunicazione unificata, ovvero un'infrastruttura di rete convergente che abilita il lavoro collaborativo: un investimento per razionalizzare, ottimizzare e ridurre i costi della comunicazione così come per rendere più produttive le attività aziendali. E poi, ancora, la SOA, o architettura orientata ai servizi, che molte aziende hanno già intrapreso al fine di semplificare la gestione delle applicazioni e fornire integrazione logica tra diverse e composite componenti. Infine il green IT, inteso sia come volontà di raggiungere obiettivi di risparmio e contenimento dei costi in relazioni all'assorbimento di potenza energetica complessiva da parte dei data center, sia come strumento per l'attuazione di una politica di

responsabilità sociale in merito alla riduzione di emissioni gas in atmosfera, nel rispetto di norme internazionali che si fanno sempre più stringenti.

Tutte queste priorità di interesse corrispondono a una volontà di innovazione che coniuga elementi di forte centralizzazione e consolidamento delle risorse enterprise in funzione di obiettivi di business. Il cloud, pur presentando un livello di adozione ancora limitato, è sotto analisi da parte delle aziende e viene considerato funzionale a logiche di efficientamento delle infrastrutture. L'indagine di NetConsulting condotta per conto di CA Technologies rivela come questa tendenza sia presente anche in Italia ed evidenzia un atteggiamento di generale attenzione e di prospettiva (Figura 2).

Figura 2 Tecnologie propedeutiche al cloud: importanza a livello di adozione (2009)



Fonte: NetConsulting

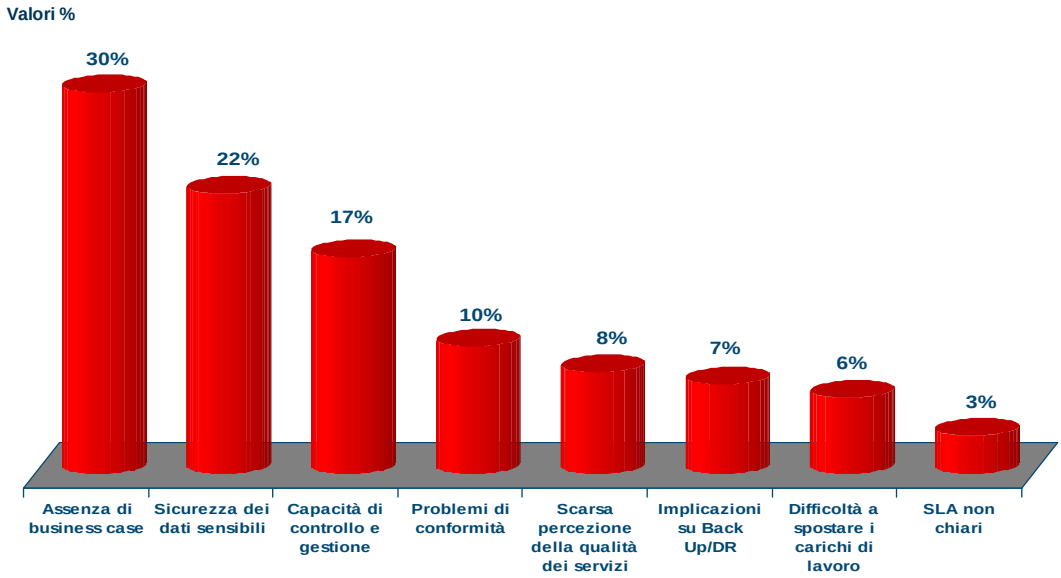
La missione di CA Technologies è traslare il valore dell'esperienza enterprise - conseguita con successo nei decenni passati sia in ambiente mainframe sia in ambiente distribuito - in una dimensione cloud, ovvero nella prospettiva elaborativa che condizionerà in misura sempre più forte l'evoluzione delle organizzazioni IT.

Esiste peraltro la consapevolezza che interventi di consolidamento e di virtualizzazione operati in questi anni, sia a livello server, sia a livello storage, costituiscano importanti elementi abilitanti il cloud. Ma affinché il quadro sia completo vi sono due aspetti che, pur non essendo fondamentali, sono sottovalutati dalle aziende: da una parte la capacità di controllare e rendere protetto l'ambiente virtualizzato, dall'altra la necessità di adottare strumenti di gestione che consentano di conseguire standardizzazione ed efficienza a livello operativo. Sicurezza e automazione, in una prospettiva cloud, devono essere considerate parte integrante delle tecnologie abilitanti e non possono essere disattese.

Per quanto il cloud, nella dimensione pubblica, sia oggi una realtà affermata e insostituibile - basti pensare ai servizi offerti dalle utility dell'ecosistema universale di internet, Google, Amazon, Yahoo!, Facebook - la sua adozione all'interno delle imprese appare frenata da tutta una serie di condizioni che inibiscono un passaggio rapido alle nuove forme di computing.

Secondo un'altra recente analisi dal titolo "Cloud Computing and the Perception of European Businnesses" condotta da CA a livello europeo (Figura 3), i motivi che attualmente rallentano l'adozione degli ambienti cloud sono diversi. Primo fra questi è la mancanza di business case che possano aiutare le aziende a comprendere le implicazioni della migrazione al cloud da un punto di vista più pragmatico. Certo, esiste un considerevole numero di aziende che hanno iniziato a utilizzare applicazioni SaaS, basti pensare ai clienti acquisiti finora da Salesforce.com, ma nel complesso si tratta piuttosto di parziali iniziative che non hanno per il momento modificato il cuore della macchina operativa.

Figura 3 Principali fattori di freno all'adozione del cloud in Italia



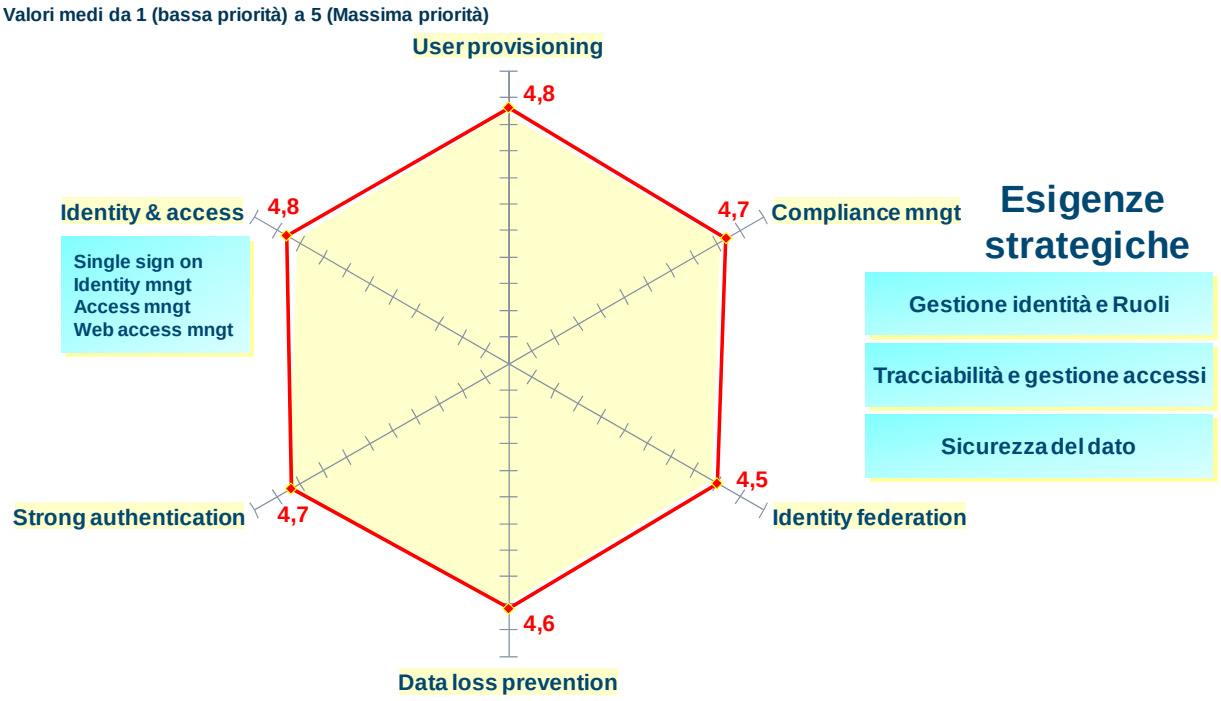
Fonte: Ca - Unleashing the Power of Virtualization, Cloud Computing and the Perceptions of European Business, 2010

CA è riconosciuta come società leader nel mercato dell'Identity and Access Management (IAM). Le soluzioni proposte in questo ambito sono state sviluppate come parte integrante di una strategia il cui obiettivo è conferire all'IT tutti gli strumenti per assicurare piena governabilità, gestione e protezione delle risorse in utilizzo, nonché piena operatività, efficienza e affidabilità delle attività di business di ogni singola e specifica realtà aziendale.

Al secondo posto, tra le maggiori preoccupazioni emerge il problema della sicurezza, giudicato come una criticità dal 22% delle aziende intervistate in Italia. Secondo quanto evidenziato dall'indagine vi sono, quindi, tutta una serie di fenomeni che iniziano a mettere in discussione gli asset IT tradizionali delle aziende e che, pur non avendo ancora modificato l'essenza della struttura, fanno sì che il cloud venga considerato come una possibile ipotesi futura. Perché questo accada, si dovranno innanzitutto risolvere le cause che determinano una generale incertezza e diffidenza. Quali? Il timore di esporsi a una condizione di vulnerabilità e perdita di controllo, l'incapacità di assicurare una gestione accurata e appropriata delle risorse extra-enterprise.

In questa partita, tesa a garantire valori essenziali di protezione che permettano di creare i presupposti per una implementazione *trusted* del cloud, le soluzioni di sicurezza prioritarie ruotano attorno a tutte quelle tecnologie che fanno riferimento all'Identity & Access Management (IAM). Le esigenze strategiche risiedono nella gestione delle identità, nella tracciabilità e gestione degli accessi e nella protezione delle informazioni. Si tratta, di fatto, delle stesse soluzioni che consentono di gestire in modo sicuro l'azienda, utilizzate in una forma ancora più estesa rispetto a come esse sono state finora adottate in ambito enterprise: user provisioning, identity and access management, strong authentication, data loss prevention, compliance management, identity federation…. Sono queste, sempre e comunque, le soluzioni che permetteranno di gestire in sicurezza un ambiente di tipo cloud (Figura 4).

Figura 4 Soluzioni di sicurezza essenziali per implementare il cloud computing

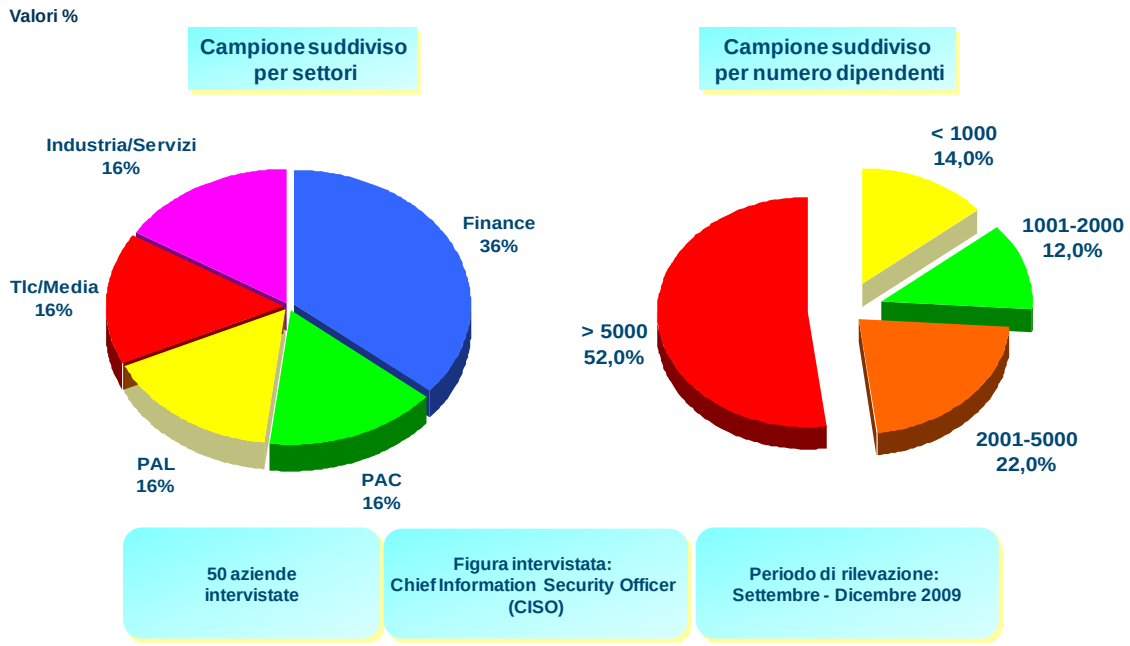


Fonte: NetConsulting

3 La sicurezza nelle aziende italiane

L'indagine che CA Technologies ha commissionato a NetConsulting è basata primariamente su interviste fatte ai responsabili della sicurezza nel periodo settembre-dicembre 2009. La dimensione delle 50 aziende oggetto del campione è prevalentemente quella delle grandi e grandissime organizzazioni: il 52% è infatti costituito da imprese/enti con un numero di dipendenti superiore a 5.000 mentre solo il 14% ha un numero di lavoratori inferiore a 1.000.

Figura 5 Suddivisione aziende per settore e numero dipendenti



Fonte: NetConsulting

Lo spettro della tipologia di settori in cui operano queste realtà è esemplificativo del profilo strutturale della grande azienda attiva nel territorio italiano: il 36% del campione fa riferimento al Finance (banche ed assicurazioni), il resto delle aziende intervistate è equamente distribuito negli altri settori, vale a dire Industria/Servizi, TLC/Media, PAL e PAC. Sono tutte realtà che contribuiscono in modo determinante alla spesa IT complessiva delle grandi aziende italiane, valutata da NetConsulting intorno a una cifra superiore ai 10 miliardi di euro ed equivalente a oltre il 50% della spesa globale delle imprese italiane.

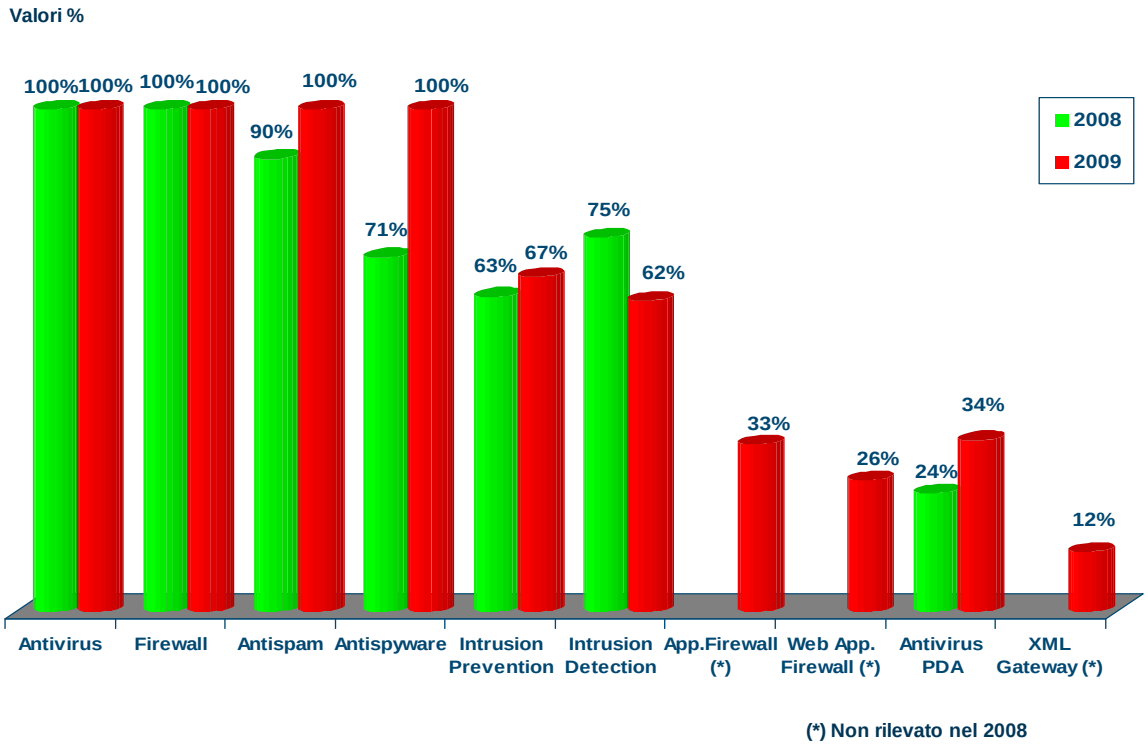
L'indagine di NetConsulting, pur analizzando anche lo stato di adozione degli strumenti di sicurezza perimetrale, ha volutamente rivolto l'attenzione all'adozione di soluzioni inerenti l'area della

gestione delle identità e del controllo degli accessi, in quanto considerata elemento e premessa essenziale per la protezione del cloud.

4 Threat Management

I dati raccolti confermano quanto evidenziato nella precedente indagine, svolta due anni fa, sullo stato della sicurezza: le tecnologie che fanno riferimento al threat management - gestione delle minacce o difesa del perimetro aziendale - hanno acquisito una diffusione capillare e sono diventate parte integrante e costitutiva dell'apparato di difesa e protezione di risorse a asset aziendali. Si tratta, quindi, di un mercato ormai maturo, su cui le aziende hanno conseguito una piena consapevolezza, e di soluzioni che rappresentano una base indispensabile per garantire che l'ambiente IT sia effettivamente al riparo da possibili minacce e attacchi provenienti dall'esterno. La domanda, pertanto, oggi è prevalentemente di sostituzione e aggiornamento, e al di là di alcune aree che presentano un potenziale inespresso, come ad esempio l'antivirus per PDA e smartphone, il mercato è da considerarsi saturo (Figura 6).

Figura 6 Threat management



Fonte: NetConsulting

Garantire la sicurezza di un ambiente cloud significa in prima istanza operare in una logica di Identity e Access Management ancora più sofistica di quella finora accettata all'interno di una infrastruttura IT dedicata. CA Technologies, attraverso un percorso di consolidamento delle soluzioni esistenti, nonché attraverso acquisizioni mirate, ha definito una roadmap di innovazione intesa a soddisfare esigenze sempre più puntuali, aderenti alle richieste che devono essere soddisfatte in ambienti di nuova generazione

5 Gestione delle identità

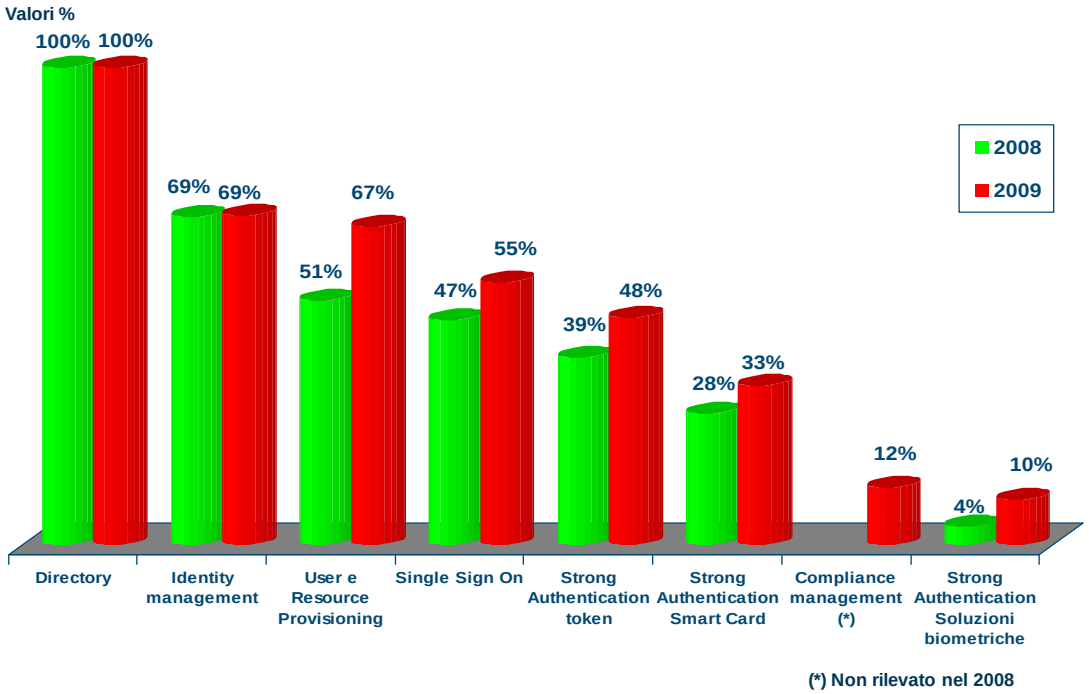
La gestione delle identità, che implica il riconoscimento dei singoli utenti e il controllo degli accessi in base al profilo loro assegnato, pienamente conseguibile attraverso l'utilizzo di molteplici tecnologie ad hoc, mostra un livello di adozione decisamente inferiore rispetto a quello degli strumenti di threat management. La percentuale di di utilizzo delle soluzioni di Identity and Access Management risulta tuttavia significativa e in notevole aumento rispetto alla rilevazione del 2008.

Al di là dell'esistenza di un fondamento primario di gestione degli utenti, comune a tutte le organizzazioni, rappresentato dal sistema di directory, viene confermato un livello di utilizzo esteso di soluzioni di identity management (adottate dal 69% delle aziende intervistate). Interessante è notare che, rispetto a un anno fa, l'adozione di soluzioni IAM diventa più articolata: tecnologie complementari, in grado di assicurare una più ampia automazione della gestione dei livelli di sicurezza tendono a diversificare le tecnologie abilitanti utilizzate. Da una parte il provisioning, vale a dire un sistema in grado di allocare automaticamente l'utilizzo di risorse in base al profilo o ruolo assegnato al singolo utente, dall'altra il Single Sign On (SSO), ovvero uno strumento che consente di semplificare l'accesso a una molteplicità di risorse attraverso un'unica identificazione.

In ulteriore aumento si dimostrano essere altre forme di accesso, ancora più sicure rispetto al semplice inserimento della password, come la strong authentication, in cui l'autenticazione dell'utente può avvenire tramite identificazione generata da token (molto utilizzati nell'accesso ai servizi di Internet Banking), da smart card o attraverso le meno diffuse soluzioni biometriche (rappresentate tipicamente dal riconoscimento dell'impronta digitale o dalla lettura dell'iride).

L'elemento che appare più debole, o ancora legato a una condizione di tipo embrionale, è la gestione della compliance in un'ottica IAM: chi, cosa, come un'utente può accedere a risorse e dati in ottemperanza a normative che le aziende sono tenute a rispettare in base a quanto prescritto a livello nazionale e internazionale (Figura 7).

Figura 7 Gestione delle identità



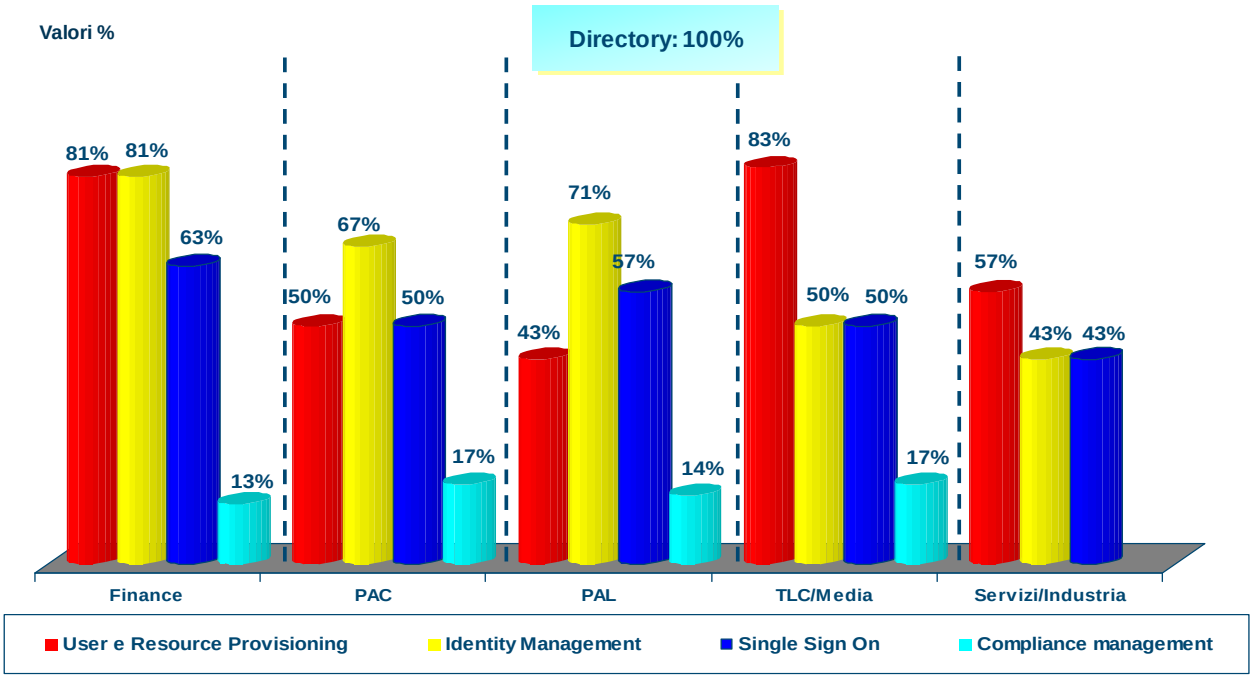
Fonte: NetConsulting

Il grado di adozione di soluzioni di gestione delle identità, declinato per singolo settore di appartenenza, si distingue per avere punte di alto utilizzo in merito a soluzioni primarie, come user e resource provisioning, superiore all'80% nelle Tlc e nel Finance. Quest'ultimo settore appare il più virtuoso nello sfruttare globalmente e intensivamente questo tipo di soluzioni.

Tranne le eccezioni menzionate, tutti i diversi comparti mostrano una grado di adozione mediamente superiore al 50% mentre il settore meno reattivo si rivela essere quello dell'Industria e dei Servizi, confermando peraltro un dato già emerso nelle survey precedenti. Di fatto il grado di adozione di tecnologia IAM ha un andamento in larga misura dipendente dal livello di criticità di business rispetto al contesto in cui operano le aziende (Figura 8).

Secondo CA Technologies, il cloud non compromette l'esperienza IAM acquisita internamente, piuttosto sollecita l'individuazione di un percorso di crescita che possa permettere di coniugare quanto finora implementato con le nuove sfide che attendono tutti coloro che dovranno convivere con realtà complesse e multiformi composte sia da sistemi appartenenti alle infrastrutture aziendali tradizionali, sia da sistemi di derivazione cloud.

Figura 8 Gestione delle identità (settori)



Fonte: NetConsulting

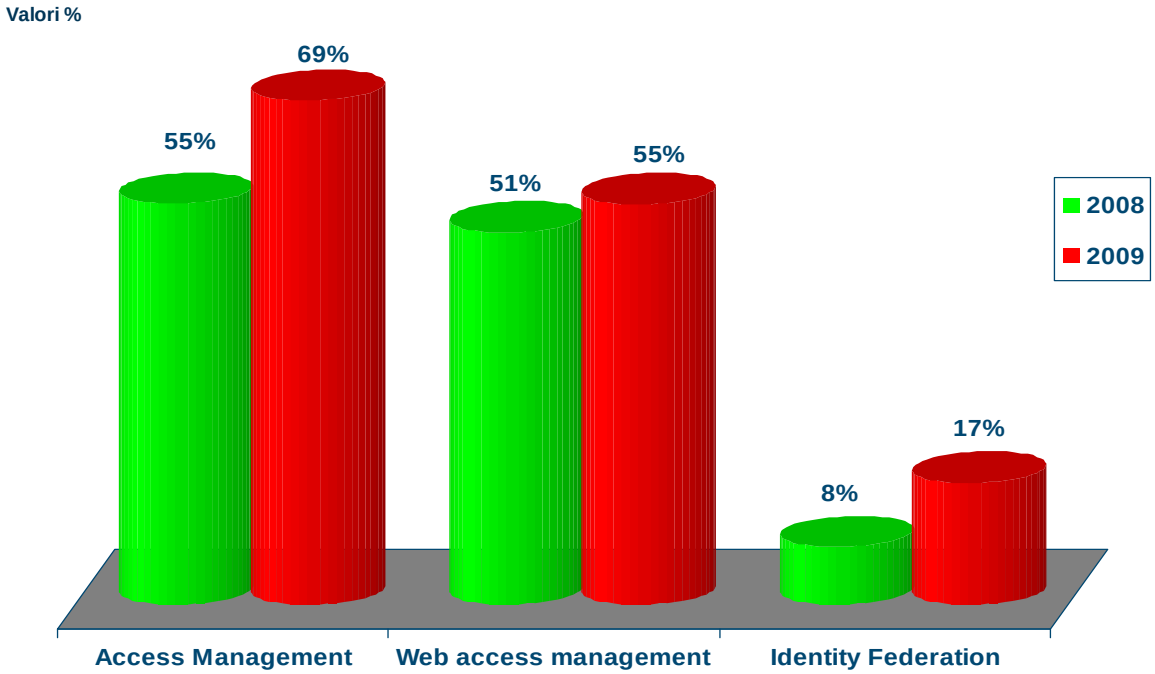
6 Gestione e controllo accessi

La progressiva affermazione di un più articolato utilizzo di servizi IAM si evince dal dato relativo all'adozione di strumenti di access management, in aumento generalizzato sia nella componente primaria, che privilegia l'accesso della popolazione interna al perimetro aziendale, sia nella componente deputata alla gestione degli accessi web. Le soluzioni, rispetto alla precedente indagine 2008, passano rispettivamente dal 55% al 69% e dal 51% al 55%.

Poco diffusa, con percentuali di adozione in assoluto scarsamente rilevanti, è la componente di *identity federation*. Quest'ultima è infatti appannaggio di organizzazioni al cui interno convivono più elementi societari o più enti, come tipicamente avviene nella Pubblica Amministrazione (33% di adozione). E' questo, probabilmente, il motivo della differenza sostanziale, in termini di adozione della *federation*, rispetto ai dati che contraddistinguono l'utilizzo di altre categorie di tecnologia di accesso. E' bene sottolineare come la scarsa dimestichezza con problematiche di *federation* è un fattore che rende le organizzazioni poco preparate a misurarsi in una prospettiva di tipo cloud

poiché, in un contesto di questo tipo, essa tende ad assumere una importanza centrale, indipendentemente dal settore di appartenenza (Figura 9)

Figura 9 Gestione e controllo accessi



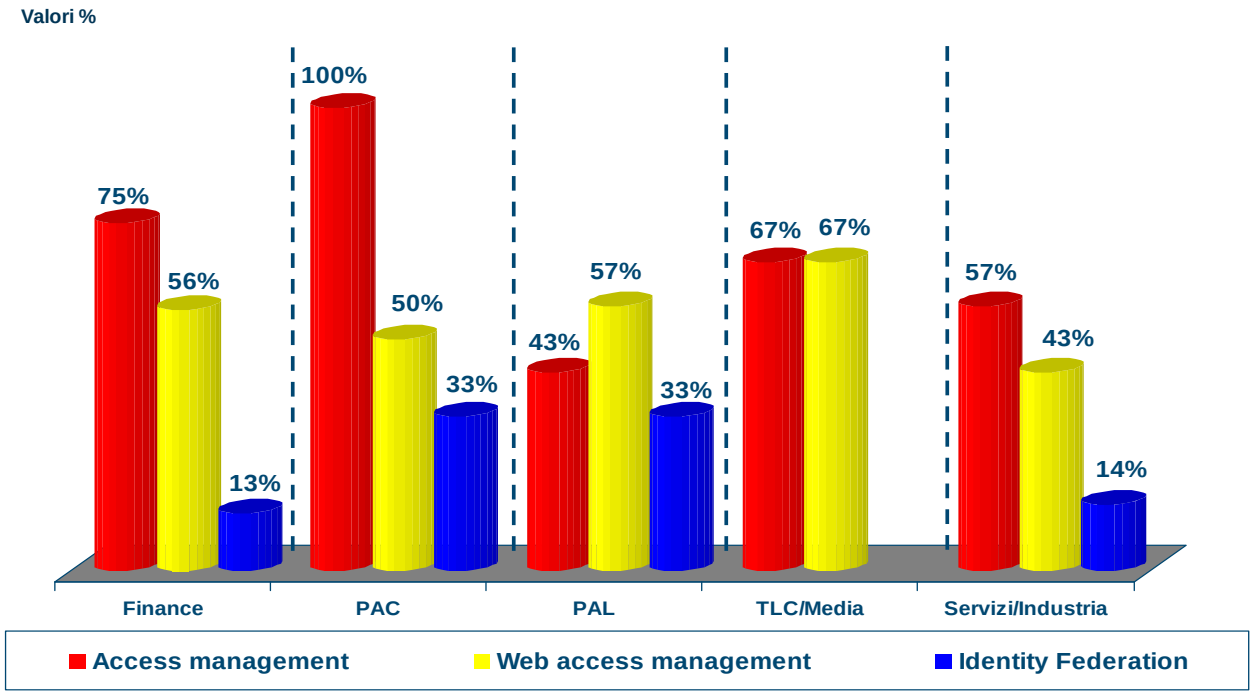
Fonte: NetConsulting

Soluzioni di accesso primario risultano determinanti in molte organizzazioni. Tipicamente si evidenziano utilizzi superiori al 50% un po' in tutti si settori. Si distingue in particolar modo la Pubblica Amministrazione Centrale. Il 100% delle aziende che appartengono a questo settore dichiara di avere in esercizio soluzioni di access management. Un dato che, verosimilmente, corrisponde alla necessità di allinearsi con quanto stabilito dal Garante della Privacy, il quale, tramite un provvedimento adottato a fine 2008, ha fissato le regole per l'adozione, da parte di enti e amministrazioni pubbliche, di misure tecniche e organizzative che riguardano nello specifico la figura degli amministratori di sistema a tutela della privacy dei dati personali.

In base alla normativa italiana, gli utenti privilegiati, come appunto gli amministratori di sistema, nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Ecco, quindi

una possibile spiegazione del massiccio utilizzo di soluzioni di gestione degli accessi nella PAC, il settore che, per ovvie ragioni, ha dovuto prima di altri allinearsi alle nuove disposizioni (Figura 10).

Figura 10 Gestione e controllo accessi (settori)



Fonte: NetConsulting

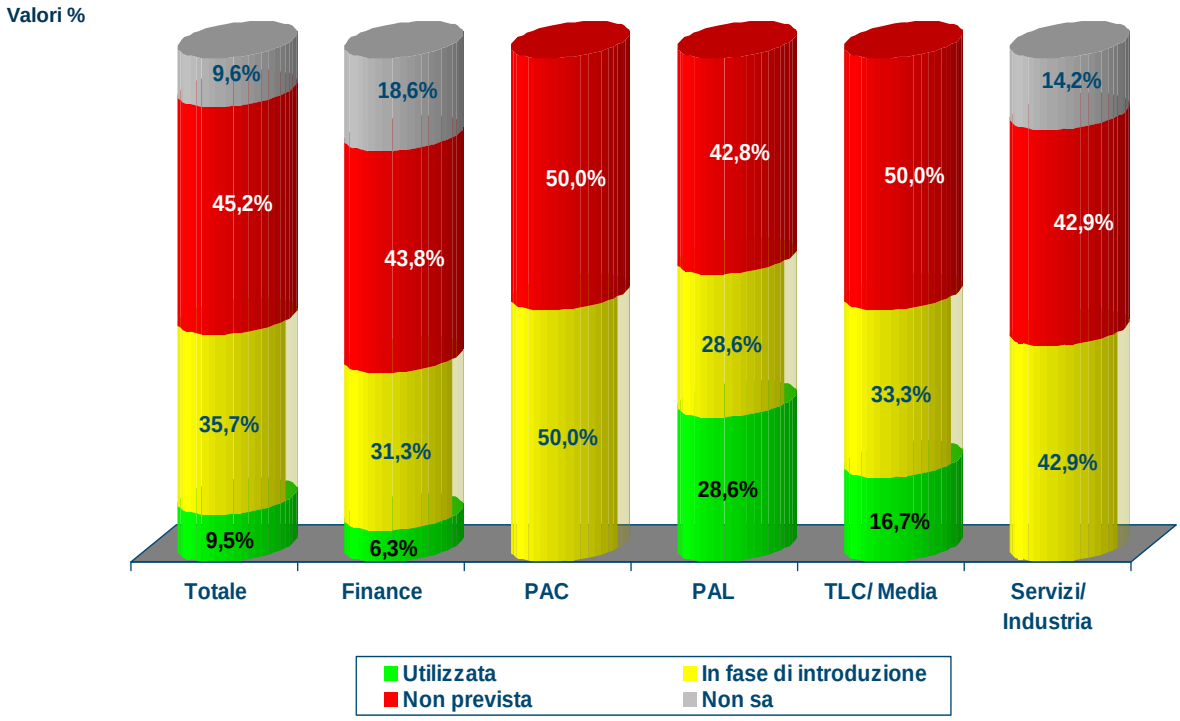
7 Protezioni dei dati

Una delle aree nelle quali si rileva ancora una scarsa sensibilità e un basso livello di adozione riguarda la tecnologia finalizzata alla protezione dei dati. Sono pochissime le aziende che percentualmente utilizzano soluzioni di *data loss prevention,* vale a dire tecnologie dedicate a gestire e controllare come e con quali limitazioni possono essere utilizzati i dati - sia da parte di utenti interni, sia da parte di utenti esterni – al fine di attenuare il rischio di attività illecite causate da un uso improprio degli stessi.

Complessivamente la media è inferiore al 10%, con punte del 28,6% nella PAL e del 16,7% nel settore TLC. E' comunque una risorsa che inizia a destare interesse, tanto è vero che una larga parte delle aziende oggetto del campione, il 35,7%, dichiara di prevederne l'introduzione.

Di fatto le soluzioni dedicate alla protezione dei dati e delle informazioni sono in una fase embrionale, la disponibilità di tecnologie dedicate a gestire e controllare come e con quali limitazioni possono essere utilizzati i dati, è stata finora limitata e, soprattutto, non associata in forma integrata a soluzioni IAM (Figura 11).

Figura 11 Protezioni dei dati – Data Loss Prevention



Fonte: NetConsulting

CA Technologies ritiene che i dipartimenti IT, e in particolare coloro addetti alla sicurezza, debbano avere un ruolo attivo nella gestione dei problemi di sicurezza inerenti la sicurezza di tutti i servizi o applicazioni che vengono acquisiti on demand da una cloud. Il rischio, in caso contrario, è diventare soggetti passivi di un modello imposto dall'esterno, che bypassa l'organizzazione IT rendendo più debole l'azienda nel suo complesso in quanto dipendente da regole esterne.

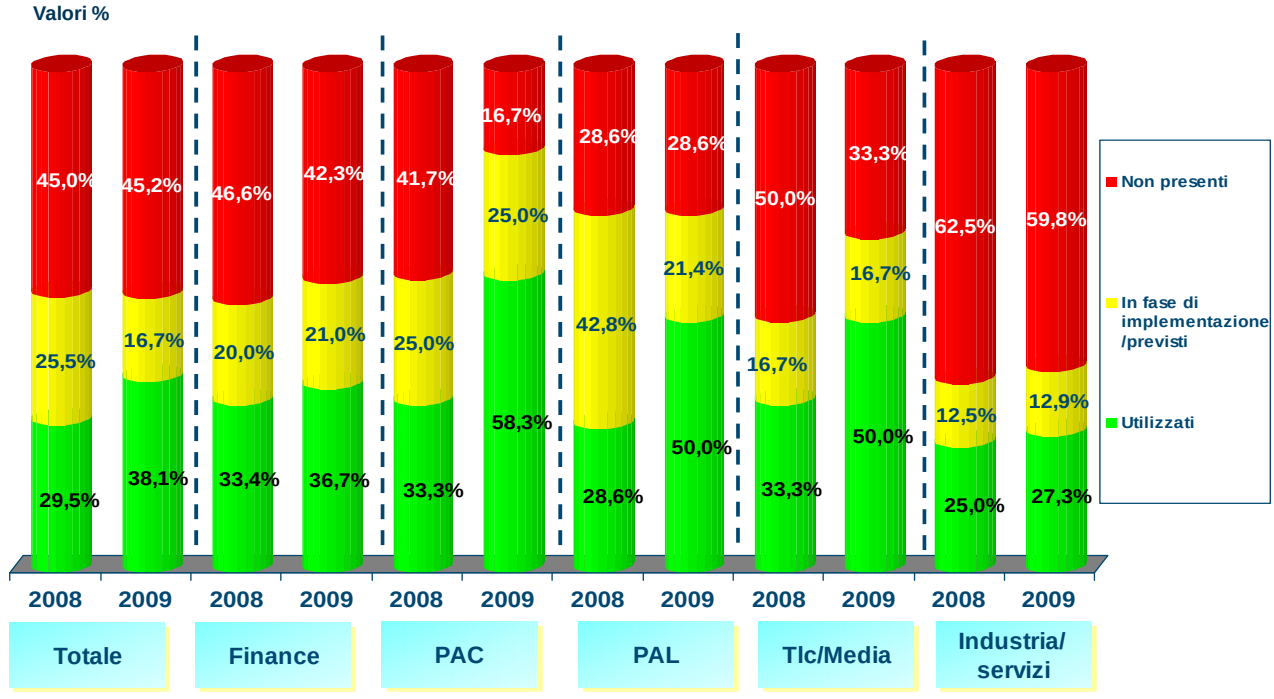
A questo proposito CA Technologies ha intrapreso una strategia di *Content Aware Identity and Access Management* che mira a definire una suite di gestione degli accessi e delle identità in grado di colmare il gap applicativo, inserendo la funzionalità di gestione del dato e delle informazioni all'interno del più ampio spettro di soluzioni o macro-componenti primarie di gestione delle identità e degli accessi.

8 Governance

L'efficienza ed efficacia nell'utilizzo di soluzioni di gestione e controllo dell'identità, degli accessi e delle informazioni può realizzarsi pienamente attraverso attività di monitoraggio basate su cruscotti integrati. Avere una visibilità immediata delle condizioni di sicurezza delle risorse aziendali può essere un vantaggio non secondario. Significa introdurre una prospettiva di Governance della sicurezza che aiuta a identificare con immediatezza eventi potenzialmente critici; significa, in definitiva, avere strumenti per attivare un controllo e una gestione più potente e semplificata.

L'indagine di NetConsulting rivela che, anche in quest'area, alla pari di quanto si evidenzia in altre componenti di sicurezza associate allo IAM, il tasso di adozione, così come l'interesse, è in sensibile aumento. Le aziende che hanno in esercizio applicazioni associate a questa tipologia di soluzioni di governance, rispetto al periodo precedente monitorato dall'indagine, sono passate dal 29,5% al 38,1%. Non solo, ma se si considera la porzione di organizzazioni che si dichiarano prossime a una loro implementazione, la percentuale di aziende diventa superiore al 50% (Figura 12).

Figura 12 Governance: cruscotti integrati per il monitoraggio di eventi legati alla sicurezza



Fonte: NetConsulting

Se ne desume che la sensibilità riguardo alla determinazione di un ambiente integrato ed efficiente coinvolge un sempre più vasto numero di aziende. Non esiste più soltanto l'esigenza di avere

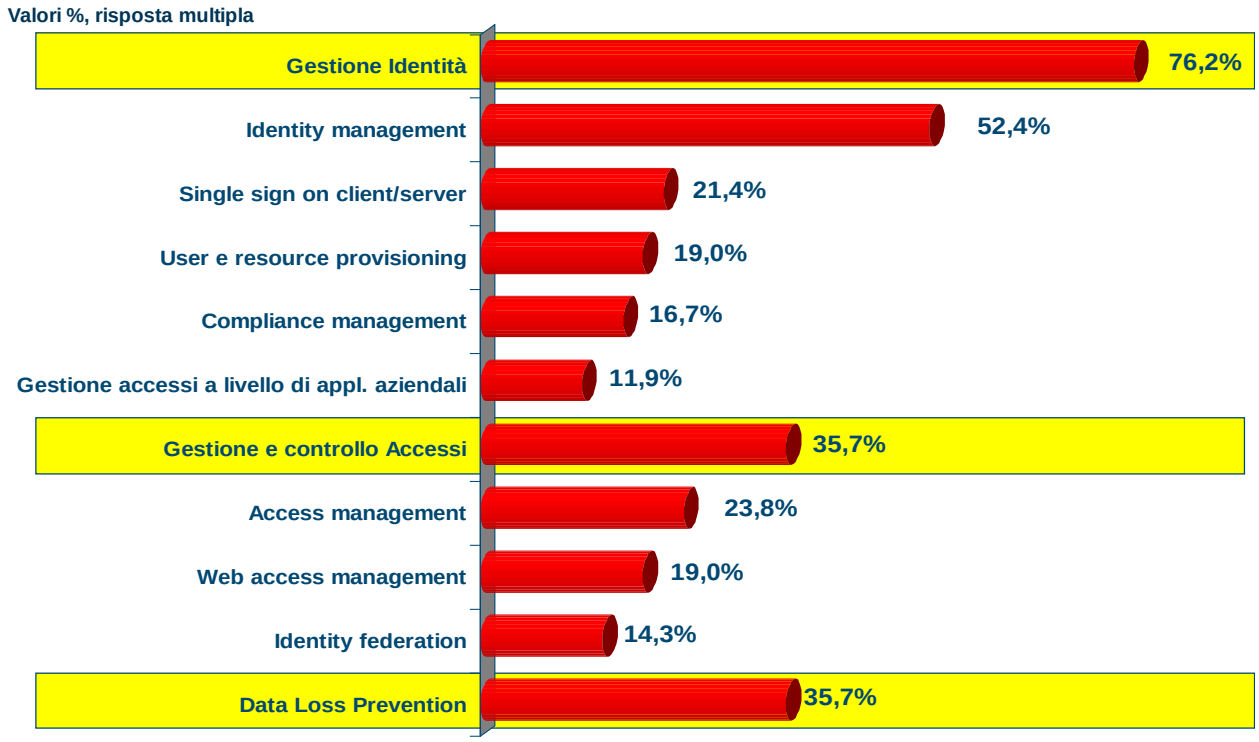
Le soluzioni proposte in ambito IAM da CA Technologies hanno rilevanza sia per i provider di cloud pubbliche sia per i provider di cloud private. Le attività di controllo che hanno più senso all'interno di questi ambienti sono innanzitutto quelle di federazione delle identità, di log management, di user management, di web access managment e di provisioning.
Per quanto riguarda la gestione degli utenti con accesso privilegiato, tipicamente amministratori di sistema, CA Access Control consente di mettere in sicurezza i sistemi operativi fisici e virtuali così come gestire il controllo dei cambiamenti delle password.

strumenti per attività specifiche che risiedono lungo la catena del valore dello stack IAM – indentità, accesso e informazioni – ma si avverte la necessità di disporre di soluzioni che consentano una visione olistica del tutto in funzione di una efficace governance della sicurezza. E' la Pubblica Amministrazione, sia centrale che locale, a essere in prima linea nell'adozione di queste soluzioni e che nel corso dell'anno ha impresso la più alta accelerazione nel loro utilizzo, mentre l'industria appare il settore meno reattivo ed esprime valori di quasi 10 punti percentuali inferiori alla media (27,3% contro 38,1%).

9 I progetti in corso e previsti in area sicurezza

Le aziende italiane anche nel 2009 hanno continuato a investire in sicurezza, confermando la priorità che questa tematica ha assunto negli ultimi anni. I progetti si concentrano principalmente nell'area della gestione delle identità, che continua a rappresentare quella di maggiore investimento. In particolare la maggior parte delle aziende si focalizza sull'attività primaria di identity management: è il 52,4% delle aziende a considerare attentamente attività progettuali in quest'area nel corso del 2010. Seguono poi la gestione degli accessi e le soluzioni per la protezione dei dati, equamente oggetto di attenzione da parte di un 35,7% delle imprese oggetto dell'indagine. Valori più bassi, ma sempre interessanti, vengono espressi in merito all'attivazione di progetti relativi a funzioni complementari all'interno di ciascuna macro-area. L'attenzione degli utenti si focalizza pertanto sulle funzioni primarie, ma tende ad assumere gradualmente un approccio più ricco e articolato, un fenomeno che si manifesta in tutti i settori monitorati dalla ricerca (Figura 13)

Figura 13 Principali aree di IT Security oggetto di progettualità nel 2010



Fonte: NetConsulting

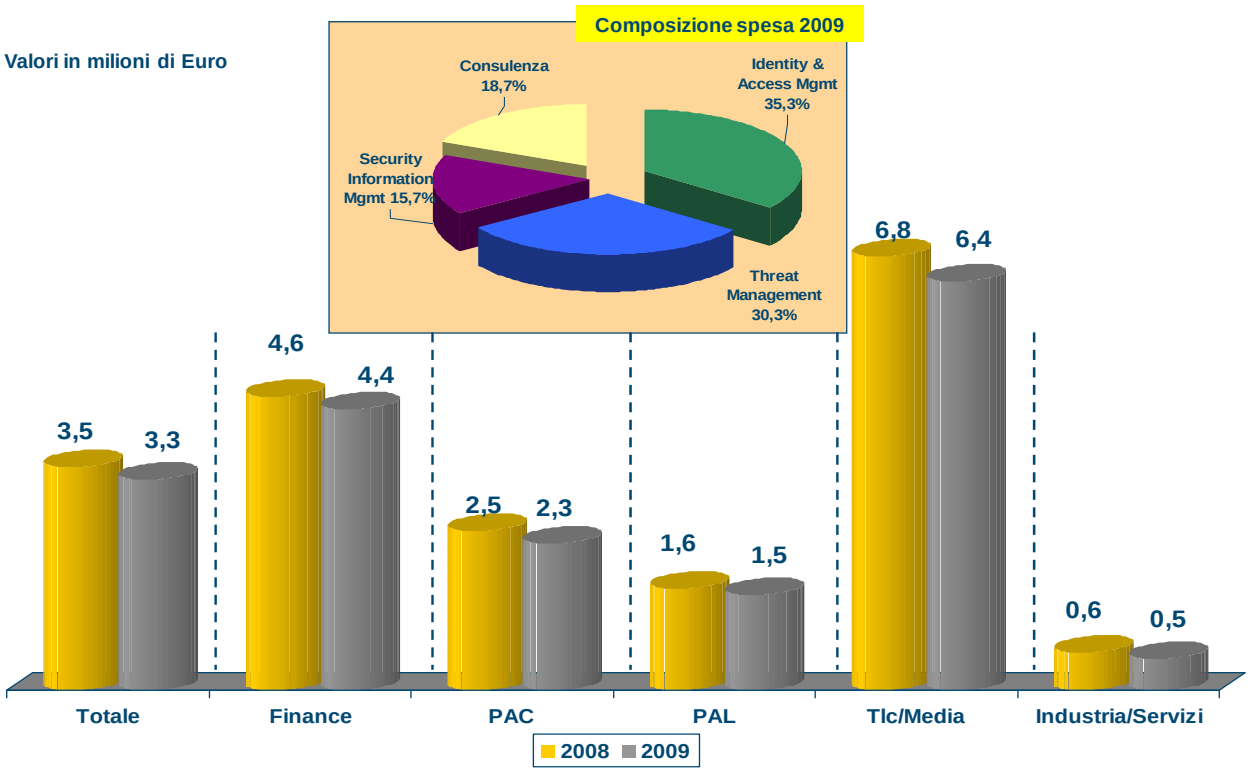
10 L'andamento della Spesa in IT security

Identità degli utenti e ruoli, autenticazione, controllo di accessi, single sign-on federato, attività di data loss prevention, sicurezza dei web services possono essere gestite con i prodotti IAM attualmente disponibili. CA Federation Manager può, per esempio, essere utilizzato per autenticare utenti Saleforce.com, Google Apps e di qualsiasi altro servizio cloud che supporti SAML. Funzionalità di provisioning possono essere esercitate nei confronti di utenti SalesForce.com e Google Apps.

La spesa complessiva per la sicurezza risulta essere in lieve flessione per quanto riguarda il valore assoluto, ma in crescita se analizzata dal punto di vista dell'incidenza sulla spesa IT complessiva. Considerate le difficili condizioni economiche e la costante attenzione al controllo dei costi e al contenimento dei budget IT, lo scenario fotografato da NetConsulting rivela quanto la sicurezza sia diventata ormai un elemento irrinunciabile per le imprese. Non esiste IT ed erogazione di servizi che non sottintenda una qualche forma di protezione del perimetro aziendale, delle identità, degli accessi e dei dati.

A conferma di questa attitudine sono i risultati relativi ai singoli segmenti di spesa. Nel 2009 il threat management ha assorbito il 30,3% del volume della spesa destinata alla sicurezza informatica, mentre il 35,3% è il valore percentuale della spesa nell'area dell'Identity & Access Management. Il profilo di spesa per la sicurezza tende quindi a modificarsi e a stabilire un rapporto che privilegia soluzioni che vanno al di là della difesa dei confini aziendali e che si concentrano attorno alla tematica di controllo di accessi e identità (Figura 14).

Figura 14 Spesa media per la sicurezza ICT (2008-2009)



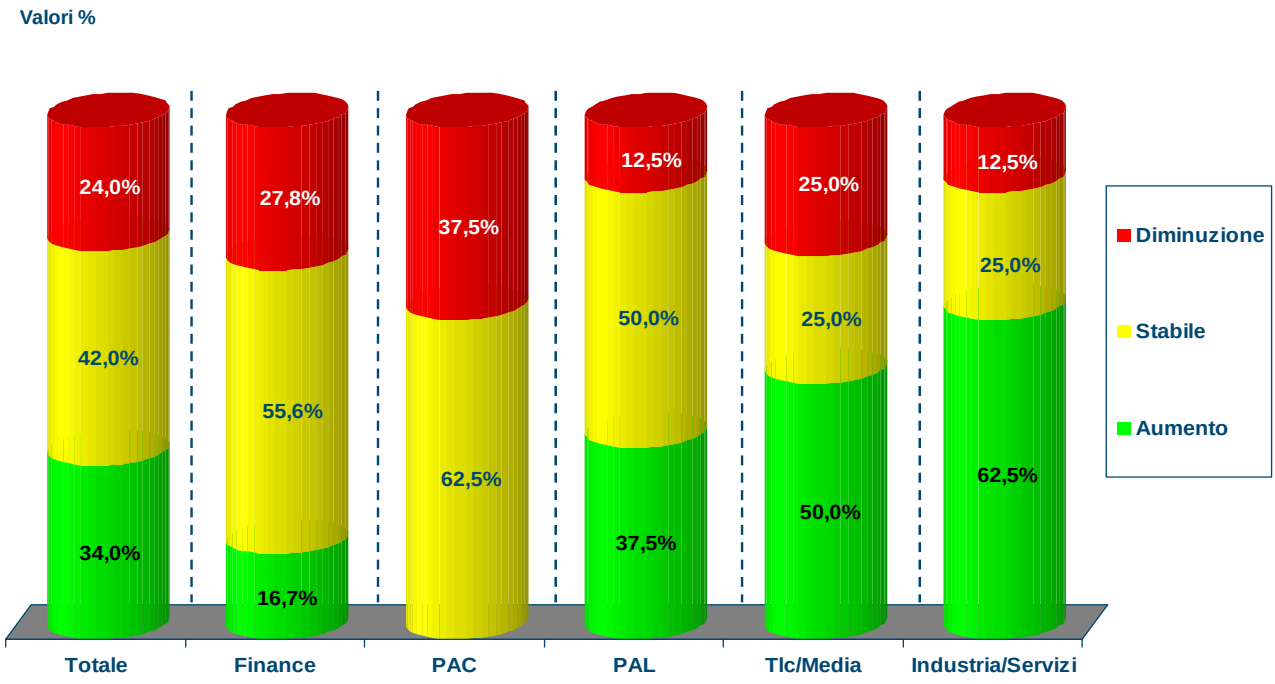
Fonte: NetConsulting

La spesa media pro-capite per singola azienda è risultata nel 2009 pari a 3,3 milioni di euro, in calo rispetto ai 3,5 rilevati per il 2008 dalle stesse aziende intervistate ed è il Telco a presentare il livello di spesa medio per azienda più elevato: 6,4 milioni di euro contro i 4,4 del Finance, i 2,3 della PAC, l'1.5 della PAL e lo 0,5 dell'industria/servizi

La priorità della sicurezza si rivela anche nella predisposizione agli investimenti: il 34% delle aziende afferma che la spesa dedicata alla sicurezza è in aumento; solo il 24% ritiene che sia in

diminuzione, in assoluta controtendenza con l'andamento della spesa IT nel suo complesso che nel 2009 ha registrato un calo di circa l'8% (Figura 15).

Figura 15 Spesa in sicurezza ICT (trend 2008-2009)



Fonte: NetConsulting

I fattori che costituiscono i driver per gli investimenti in sicurezza sono largamente determinati da esigenze di compliance così come dalla consapevolezza dei danni conseguenti eventuali vulnerabilità. Non emerge nulla di diverso da quanto evidenziato dalla precedente indagine, rispetto alla quale risulta sostanzialmente immutata la logica che favorisce gli investimenti nel loro complesso. Di contro, tra i fattori di freno, assume invece una più ampia incidenza la scarsità di risorse in termini di budget dedicato e la conseguente priorità di spesa basata su criteri ancor più selettivi a favore di interventi a più alta priorità.

La compliance, e l'obbligo di aderenza normativa, in particolare in riferimento alla protezione dei dati, così come stabilito dalla Legge sulla Privacy, interessa trasversalmente tute le aree di mercato, ma si estende sempre più a norma di carattere specifico per settore di attività, come per esempio il finance, in relazione alla gestione del rischio (Basilea 2, Solvency 2 e direttive Isvap).

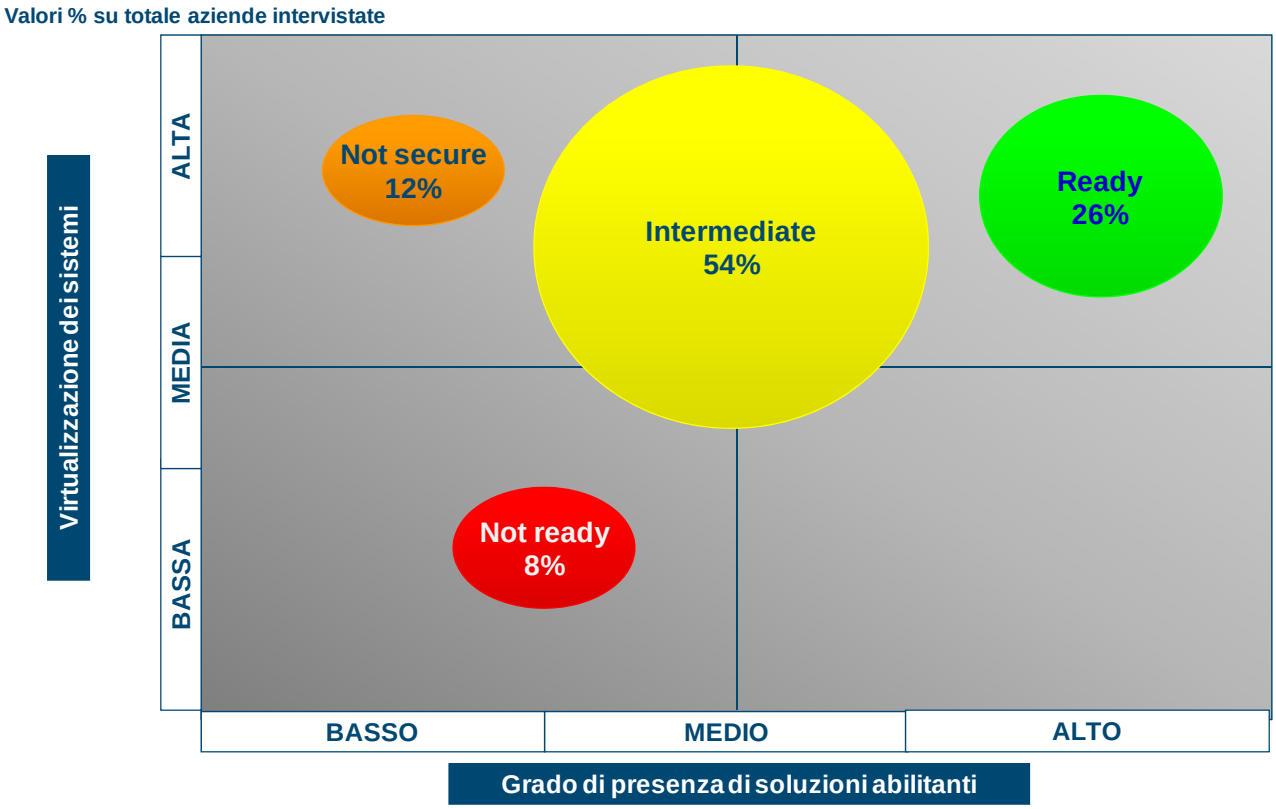
11 Livello di sicurezza e predisposizione al cloud

Quali e quante sono le aziende predisposte al cloud? Quante dispongono di infrastruttura virtualizzata e sistemi di sicurezza che possono costituire elementi abilitanti il nuovo paradigma architetturale? Per poter classificare le aziende in base al grado di maturità di predisposizione al cloud, occorre considerare due parametri:

- da un lato, quanto le aziende intervistate hanno già adottato soluzioni di sicurezza che, come precedentemente evidenziato, sono fondamentali per abilitare la realizzazione di un'architettura cloud. Si tratta di soluzioni per la gestione di identità (come identity management, user e re source provisioning, strong authentication, ecc.), per il controllo degli accessi (quali Identity Federation, Access Management) e per la protezione dei dati (come data loss prevention);
- dall'altro, il grado di presenza di sistemi virtualizzati, passo fondamentale verso l'adozione del cloud.

L'analisi di questi elementi nelle aziende intervistate fa emergere la presenza di 4 cluster principali, ognuno con precise caratteristiche (Figura 16).

Figura 16 Le aziende e la predisposizione al cloud



Fonte: NetConsulting

- L'8% del campione analizzato emerge come **not ready** in quanto presenta un livello medio basso di implementazione di soluzioni di sicurezza abilitanti, ma anche un ricorso limitato alla virtualizzazione dei sistemi; per queste aziende/enti l'adozione di soluzioni cloud sicure passa dall'evoluzione di entrambe le componenti analizzate;
- il 12% del campione si può classificare come **not secure** poiché presenta un alto grado di virtualizzazione cui si accompagna però un grado di adozione di soluzioni abilitanti la sicurezza in area cloud piuttosto basso;
- la parte più consistente del campione analizzato, 54%, definita **intermediate,** mostra una presenza media di soluzioni di sicurezza abilitanti abbinata ad un livello di utilizzo elevato medio-alto di sistemi di virtualizzazione;
- concludono la classificazione delle aziende i **ready** (26% delle aziende analizzate) presso le quali si rileva sia un alto grado di virtualizzazione dei sistemi sia una presenza pressoché assoluta di soluzioni necessarie per l'adozione del cloud in piena sicurezza ed efficienza: essendo già dotate dei requisiti necessari alla sua introduzione queste aziende/enti rappresentano la parte più evoluta del panel analizzato.

12 Conclusioni

L'indagine sulla sicurezza nell'era del cloud evidenzia come una buona percentuale di aziende abbia già in utilizzo soluzioni di sicurezza che costituiscono gli elementi abilitanti il passaggio al cloud. Un quarto delle aziende appare **ready,** già culturalmente e tecnologicamente predisposto a confrontarsi con il paradigma del cloud, poiché gestire in sicurezza un ambiente di questo tipo significa, in buona sostanza, estendere in una prospettiva esterna al perimetro aziendale, soluzioni, già sperimentate a livello enterprise, di controllo delle identità e degli accessi e di protezione dei dati, sia in ambiente fisico che virtualizzato. La percentuale più consistente delle aziende (54%) si trova invece in mezzo al guado, **intermediate**, una condizione in cui, pur in presenza di un ambiente fortemente virtualizzato, non corrisponde un utilizzo elevato di soluzioni IAM.

CA Technologies è in grado di interpretare un ruolo come partner tecnologico e di business a tutto tondo nelle diverse dimensioni di tipologia del cloud, quali infrastruttura, piattaforma, applicazione, sia nelle esigenze espresse in una dimensione pubblica, sia in quelle sollevate in una dimensione privata o in una qualsivoglia configurazione ibrida.

L'impegno di CA Technologies per il cloud è sintetizzato nella strategia Content Aware Identity and Access Management, che permette di avere un pieno controllo END-TO-END delle transazioni degli utenti a livello di identità, accesso, informazioni e compliance. Soluzioni e prodotti che consentono ai responsabili della sicurezza di avere una conoscenza ancora più approfondita rispetto a quanto finora possibile, mettendo i responsabili nella condizione di prendere le decisioni più opportune ed eventualmente correggere e modificare le policy aziendali per attuare una maggiore corrispondenza ai requisiti di sicurezza.

Obiettivo di CA Technologies è assicurare, così come accaduto in passato la gestione dell'intero spettro delle architetture esistenti e in divenire – fisica, virtualizzata e cloud – garantendo la massima protezione degli investimenti sinora operati, così come una estensione degli stessi verso le nuove forme di computing prospettate dal cloud.

CA Technologies, attraverso un percorso di consolidamento delle soluzioni esistenti, nonché attraverso acquisizioni mirate, ha definito una roadmap di innovazione intesa a soddisfare esigenze sempre più puntuali, aderenti alle richieste che devono essere soddisfatte in ambienti di nuova generazione.

A questo proposito è stata definita una strategia di Content Aware Identity and Access Management che affianca il controllo dell'informazione e della compliance ai livelli di gestione delle identità e degli accessi. La definizione e implementazione di questa strategia è un passaggio di grande importanza nell'evoluzione dell'ambiente IAM poiché implementa meccanismi di sicurezza a un livello di dettaglio mai conosciuto prima.