SOLUTION BRIEF CA IDENTITY SUITE

Identity management e governance per gli utenti di business

Colmare il divario tra IT e utenti di business

ca technologies

Executive summary

La sfida

Oggi i leader IT, i dirigenti della sicurezza o i business manager vivono in una realtà dinamica e in continua evoluzione. Gli ambienti IT sono sempre più distribuiti, complessi ed eterogenei. Tuttavia, decidere chi ha accesso a quali risorse e far rispettare in modo affidabile le relative policy è una sfida variegata, che dovrebbe coinvolgere tutti e tre gli ambiti interessati: IT, sicurezza e business.

Nel frattempo, l'IT deve fare i conti con budget e risorse ridotti. Hai quindi bisogno di un modo affidabile ma conveniente per affrontare queste sfide di identità critiche:

- Eseguire rapidamente l'onboarding di nuovi utenti per renderli produttivi il più velocemente possibile
- Assicurarsi che tutti gli utenti dispongano solo dei diritti di accesso appropriati in base ai rispettivi ruoli
- Automatizzare i processi chiave relativi all'identità, per migliorare l'efficienza e ridurre i costi
- Identificare e prevenire le potenziali violazioni delle policy (account orfani, diritti impropri...) prima che si verifichino
- Rispettare i requisiti di audit sapendo quali utenti hanno accesso a quali risorse

E, infine, uno dei più importanti fattori abilitanti nell'ambiente di oggi è il seguente:

- Fornire un'esperienza semplice e intuitiva che consenta agli utenti di business di accedere facilmente e comodamente ai servizi di identità di base.

L'opportunità

La sempre maggiore enfasi posta sul rafforzamento delle capacità degli utenti di business ha generato molte sfide per gli utenti della maggioranza delle soluzioni di gestione delle identità di oggi. Purtroppo, le poche soluzioni che offrono una user experience accettabile in genere non forniscono capacità di provisioning, gestione dei ruoli e governance sufficientemente ampie, né la scalabilità necessaria per supportare la gestione delle identità in tutta l'impresa estesa. Questo costringe a scegliere tra ampiezza delle funzionalità e facilità d'uso.

CA Identity Suite aiuta a colmare il divario tra le tecnologie IAM correnti e gli utenti di business in modo assolutamente originale. Si tratta di una suite integrata di funzionalità di Identity Management e Governance che combina funzionalità robusta e un'esperienza intuitiva, comoda e business-oriented. La suite può semplificare i processi di gestione delle identità, migliorare la soddisfazione degli utenti, supportare applicazioni on-premise e cloud e fornire scalabilità a livello consumer. E, soprattutto, può essere distribuita in modo facile e rapido.

Le sfide chiave per il successo dell'Identity Management e Governance

Questo documento evidenzia alcuni problemi chiave collegati alla gestione delle identità, fondamentali per l'open enterprise di oggi, illustra perché queste sfide possono alimentare o ostacolare il tuo business e fornisce una panoramica delle funzionalità offerte da CA Identity Suite che possono aiutare l'azienda ad affrontare con successo tali sfide.

Ognuna delle sfide che seguono può essere analizzata da un punto di vista sia di business che IT. In passato, la user experience per i servizi di identità era dominata da una prospettiva rivolta all'IT; ne derivavano interfacce difficoltose e soddisfazione ridotta. Ma l'ambiente di oggi richiede un collegamento tra IT e utenti di business, per espandere l'utilizzo dei servizi di identità e migliorare la user experience complessiva. Esploreremo il lato di business e tecnico di queste sfide.

Queste sfide richiedono una pianificazione estesa e dovrebbero essere parte di ogni piano di rollout:

- **Adozione da parte degli utenti**: migliorare e semplificare la user experience complessiva per aumentare l'adozione dei processi di identificazione
- **Richieste di accesso**: semplificare il processo di accesso alle applicazioni di cui gli utenti hanno bisogno
- **Gestione dei rischi collegati ai diritti**: prevenire le violazioni delle policy legate agli entitlement
- **Certificazioni di accesso**: migliorare la produttività dei manager
- **Accesso alle applicazioni utente**: fornire agli utenti un modo comodo per accedere alle applicazioni chiave
- **Analisi dell'identità in tempo reale**: garantire l'efficienza dei servizi di identità essenziali
- **Sfide di deployment**: migliorare il ROI e il time-to-value

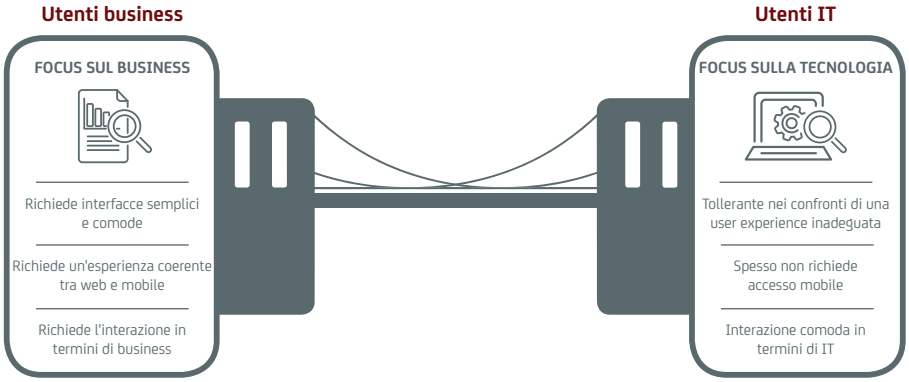
Le sfide: l'adozione da parte degli utenti

"I miei utenti sono frustrati dall'interfaccia scomoda che devono utilizzare per molte delle funzioni di identità. Questo limita gravemente la nostra capacità di implementare questi servizi per una popolazione di utenti più ampia all'interno della società".

Una delle sfide principali per arrivare al successo dei deployment di gestione delle identità è che la user experience per i servizi di identità di solito è altamente basata sull'IT. Questo, forse, poteva andare bene in passato. Tuttavia, ora che la gestione delle identità si estende oltre il dominio dell'utente IT puro, questo approccio non è più efficace. Terminologia e processi potenzialmente normalissimi per un utente IT esperto, possono essere fonte di confusione e frustrazione per la maggior parte degli utenti di business. Il risultato: adozione ridotta dei processi di identificazione, maggior carico per l'IT, mancato rispetto dei requisiti normativi e frustrazione degli utenti. Gli utenti devono poter disporre di applicazioni di business facili, veloci, senza necessità di formazione, sul device di loro scelta. Devono essere indirizzati verso i processi di identificazione di base, ma questo funzionerà solo se l'esperienza risulterà per loro semplice, intuitiva, e, soprattutto, orientata verso la prospettiva di business, piuttosto che IT.

La soluzione CA Identity Suite

CA Identity Suite aiuta a colmare il divario tra le tecnologie IAM correnti e gli utenti di business in modo assolutamente originale. Si tratta di una suite integrata di funzionalità di Identity Management e Governance che combina funzionalità robusta e un'esperienza intuitiva, comoda e business-oriented. Migliorando la produttività e la soddisfazione degli utenti di business, la user experience di CA Identity Suite è pensata per aumentare notevolmente la proposta di valore della soluzione IAM per le grandi aziende, liberando inoltre il reparto IT da un notevole carico amministrativo.



Alcuni dei numerosi vantaggi rilevanti in termini di user experience offerti dalla Suite includono:

- Un catalogo di diritti espressi nel linguaggio del business
- Dashboard e launcher per applicazioni web e mobile
- One Stop Shop: accesso centralizzato e facile a tutti i servizi di identità per gli utenti di business
- Esperienza tipo carrello per le richieste di accesso e il monitoraggio
- Esperienza tipo social network per il monitoraggio delle richieste di accesso
- Strumenti di consulenza proattivi
- Applicazione mobile che consente all'utente di gestire l'identità sempre e ovunque

CA Identity Suite, inoltre, facilita la generazione di dashboard individualizzate e personalizzate su misura per le particolari esigenze di ruoli specifici, come dirigenti, operatori della sicurezza e partner commerciali. Gli amministratori possono configurare un'interfaccia in base al ruolo dell'utente, nonché i servizia cui l'utente può avere accesso. Inoltre, l'interfaccia della suite può essere completamente personalizzata in base alle esigenze di branding dell'azienda, compresi logo, combinazione di colori, font, immagini di sfondo selezionate e altro ancora. Così, il portale rifletterà accuratamente l'identità del business.

"In un sondaggio condotto da un società di analisi esterna, il 97% dei clienti interpellati ha dichiarato che la user experience di Identity Suite è superiore a quella della concorrenza"

fonte: Sondaggio TechValidate

La sfida: le richieste di accesso

"Per i miei utenti, richiedere facilmente l'accesso alle applicazioni e ai sistemi di cui hanno bisogno per il loro lavoro risulta complesso. Il processo è macchinoso, e i nomi delle risorse sono spesso fonte di confusione per gli utenti di business".

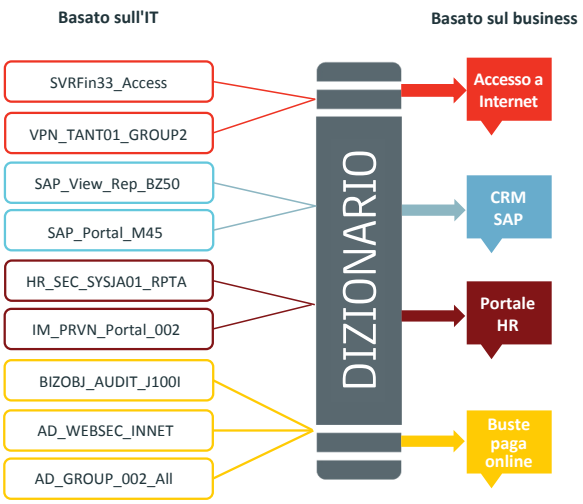
Gli utenti devono accedere alle applicazioni e ai dati di cui hanno bisogno, in modo rapido e semplice, pur mantenendo la compliance ai requisiti normativi. Tuttavia, i sistemi di richiesta di accesso tendono a essere basati su una serie di diritti pensati per gli amministratori, che ne comprendono il significato; rappresentano però un'imposizione per gli utenti, che hanno praticamente dovuto imparare un nuovo linguaggio per comprendere "come parla l'IT". Dato il sempre maggior numero di utenti di business impegnati nei processi di corporate identity, questa esperienza non intuitiva ostacola l'adozione, riduce la soddisfazione e spesso finisce per coinvolgere comunque il personale IT, costretto a intervenire per rispondere alle domande dell'utente di business in difficoltà.

È necessario un nuovo modo di interagire con gli utenti di business, e l'ambito delle richieste di accesso è un ottimo esempio dei vantaggi che questo nuovo approccio può fornire. Tuttavia, anche l'IT ha esigenze di cui tener conto in questo ambito, come l'automazione dei processi di base per le richieste di accesso e una verifica semplice delle richieste e delle approvazioni. Così, sono necessarie capacità che soddisfino le esigenze di automazione dell'IT, ma che siano anche facilmente utilizzabili dagli di utenti di business.

La soluzione CA Identity Suite

CA Identity Suite offre un'esperienza intuitiva e semplice, tipo "carrello della spesa", che semplifica notevolmente il processo di richiesta di accesso. Sul modello, noto a tutti, del processo utilizzato nei siti di vendita retail, gli utenti possono selezionare comodamente ruoli e diritti necessari per svolgere le proprie mansioni, visualizzare i privilegi di accesso correnti e verificare lo stato delle richieste precedenti.

Il catalogo dei diritti di business, assolutamente immediato, è il cuore del contributo di CA Identity Suite a un'esperienza semplice e business-oriented. Esso traduce nomi di risorse criptici, come "TSS_MNG_per_view" in denominazioni più intuitive, come "Libro paga online", semplificando agli utenti business l'individuazione delle risorse necessarie. È inoltre possibile raggruppare le applicazioni in categorie logiche per facilitare ulteriormente l'accesso, ad esempio creando un gruppo denominato "Accesso SRM", che comprende applicazioni SAP, applicazioni Oracle e capacità SalesForce che gli utenti di business tipicamente utilizzano, il tutto definito in termini a loro familiari. L'immagine seguente evidenzia l'associazione tra terminologia IT e business eseguita dal catalogo.



Identity Suite include strumenti di consulenza proattivi in grado di semplificare notevolmente il processo di richiesta di accesso. L'utente può visualizzare i ruoli suggeriti, e i diritti di accesso per utenti simili a lui. Questa consulenza proattiva aiuta l'utente a presentare la richiesta adatta all'accesso desiderato. Essa fornisce anche un punteggio di rischio, sulla base dell'accesso richiesto e del livello di rischio potenziale relativo. L'utente può quindi prendere una decisione maggiormente informata in relazione all'accesso da richiedere.

La sfida: Gestione del rischio collegato ai diritti

"A volte agli utenti vengono assegnati per errore diritti che violano la nostra policy di sicurezza. Voglio che quelle violazioni vengano impedite prima che si verifichino".

I diritti degli utenti impropri sono la root cause di una serie di recenti violazioni pubbliche. Questo è particolarmente vero per gli utenti con privilegi, che tendono ad avere diritti molto ampi. Tuttavia, il principio è lo stesso per tutti gli utenti: è necessario correggere i diritti non adeguati che violano la policy di sicurezza prima che vengano concessi ("controllo preventivo"), e rimuovere quelli eventualmente già concessi ("controllo reattivo"). A meno che siano in atto controlli efficaci in entrambi i casi, il rischio aumenterà e gli audit di compliance risulteranno più impegnativi.

Analogamente, a volte le policy cambiano e l'accesso concesso tempo fa oggi determina una violazione della nuova policy. Durante le certificazioni di accesso periodiche, tutto questo deve essere reso altamente visibile al responsabile, che potrà così anche de-certificare l'utente per quel diritto di accesso.

La soluzione CA Identity Suite

CA Identity Suite consente di formulare, applicare e convalidare insiemi di regole dei processi di business (BPR) per implementare la separazione dei doveri e altri vincoli logici che riguardano le relazioni tra utenti, ruoli e privilegi. Ad esempio, un BPR può modellare un vincolo per "soggetti con il permesso di accedere a X non possono avere il permesso di accedere a Y", o una relazione di dipendenza come "solo i soggetti con accesso A possono avere il permesso di eseguire B". In questo modo, le istanze che violano le policy di sicurezza definite possono essere evitate prima che si verifichino.

La suite può anche generare avvisi qualora vengano richiesti diritti contrastanti (i controlli preventivi di cui sopra). Essa assegnerà un punteggio di rischio basato sull'accesso richiesto e sulla relativa policy. Il punteggio di rischio si basa sull'utente, gli altri suoi diritti e su eventuali fattori contestuali che potrebbero essere rilevanti. Al richiedente è indicato questo livello di rischio quando la richiesta di approvazione viene presentata, per avvertirlo di una richiesta potenzialmente impropria. Allo stesso modo, il responsabile dell'approvazione vede questo punteggio di rischio durante il processo di approvazione, ottenendo visibilità completa in grado di impedire la concessione di un accesso ad alto rischio.

La suite offre anche controlli reattivi per porre rimedio a eventuali accessi impropri concessi in passato. Al momento della certificazione, la suite esegue verifiche tra policy e accesso e genera un avviso se l'utente dispone di diritti di accesso impropri che violano una o più policy. Il responsabile rileva le violazioni chiaramente indicate per ciascun utente, e può procedere alla loro immediata correzione. Entrambi i tipi di controlli possono ridurre significativamente il rischio che diritti impropri vengano concessi o non vengano individuati.

La sfida: Certificazione degli accessi

"Voglio rendere le certificazioni semplici e intuitive, in modo da migliorare la produttività dei miei manager, e semplificare le verifiche di compliance"

Abbiamo già visto quale sia l'importanza di una capacità automatizzata di tradurre le informazioni di accesso utente in un linguaggio e in un formato adeguati a ogni tipo di campagna di certificazione. Se i nomi di accesso sono intuitivi e comprensibili al business, se è possibile progettare un workflow flessibile per soddisfare le tue esigenze specifiche, e se il monitoraggio e lo stato di ogni campagna sono facilmente disponibili, aumenta la probabilità di successo del programma di certificazione.

La soluzione CA Identity Suite

Le capacità di certificazione di CA Identity Suite si basano sul catalogo dei diritti di business, che rende estremamente semplice ai responsabili comprendere i diritti di accesso di ciascun dipendente, nonché approvare, respingere o delegare con facilità i diritti di accesso di ogni utente. Inoltre, un punteggio di rischio è disponibile ai responsabili qualora un determinato diritto di accesso, o combinazione di diritti, risulti particolarmente rischioso. Fornendo visibilità su queste valutazioni di rischio, la certificazione non è più soltanto una questione "sì/no", ma può mettere in evidenza rischi che altrimenti non sarebbero visibili.

CA Identity Suite dispone della flessibilità per supportare molti tipi di campagne di certificazione diverse, tra cui:

- **Certificazione delle entità**: utilizzata per certificare i diritti di accesso associati a utenti, ruoli o entità di risorse selezionate da parte di responsabili, titolari di ruoli e responsabili delle risorse.
- **Ricertificazione**: consente di ripetere il processo di certificazione sulla base di una campagna precedente.
- **Differenziale**: avvia una campagna di certificazione basata esclusivamente sui diritti che hanno subito modifiche rispetto a una campagna precedente.
- **Auto-attestazione**: consente a ogni utente di certificare i propri privilegi, anziché far intervenire un responsabile o un titolare della risorsa. Questo tipo di campagna può soddisfare alcuni requisiti di legge per la certificazione della sicurezza dei dati.

Le campagne di certificazione possono essere noiose, richiedere tempo e, in ultima analisi, non risultare efficaci ai fini della riduzione del rischio. CA Identity Suite non solo migliora l'efficacia di questo processo dal punto di vista della sicurezza e della compliance, ma lo fa nel contesto di un'esperienza semplice ed estremamente intuitiva, che i manager apprezzeranno.

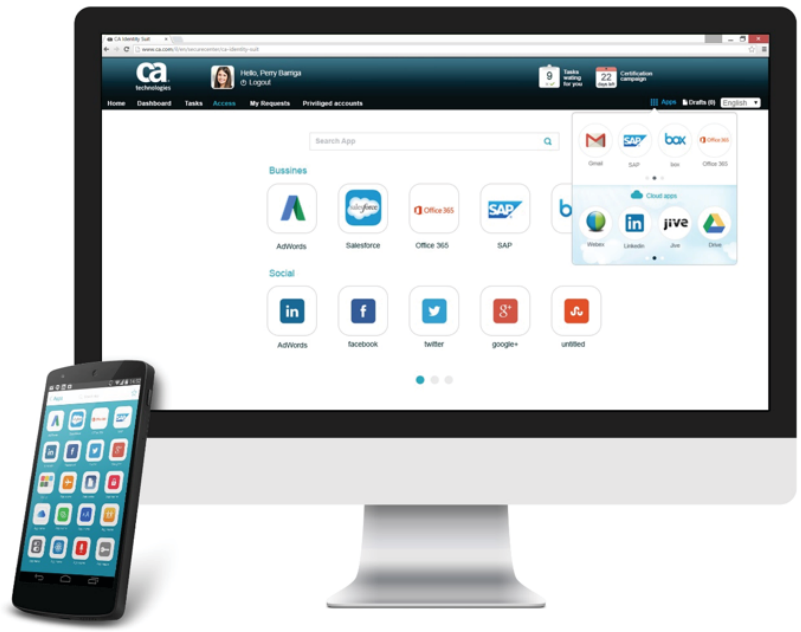
La sfida: Comodità dell'accesso alle app

"Vorrei che i miei utenti potessero accedere facilmente a tutte le loro applicazioni, nel cloud e on-premise, ma solo a quelle per cui dispongono dei diritti di accesso adeguati. Inoltre, ho bisogno che possano accedere facilmente a tutti i loro device"

Gli utenti diventano frustrati quando devono affrontare passaggi macchinosi per ottenere l'accesso a una delle tante applicazioni di cui hanno necessità. Accessi multipli e incapacità di avviare facilmente le applicazioni sono problemi comuni. E, con l'aumentare della mobility e degli utenti che si abituano alla comodità delle interfacce di questi device, le problematiche legate a frustrazione e produttività possono aumentare. Diventa necessario un metodo più comodo per ottenere un accesso rapido e facile alle applicazioni di ciascun utente, che fornisca single sign-on collettivo e includa solo le applicazioni cui ogni utente è autorizzato ad accedere.

La soluzione CA Identity Suite

CA Identity Suite include un launchpad per le applicazioni mobile e web che offre agli utenti una dashboard unificata per accedere facilmente e rapidamente a tutte le applicazioni web, cloud e mobile autorizzate. Il launchpad è accessibile da qualsiasi device e offre capacità di ricerca perfezionate. Una volta che gli utenti hanno effettuato l'accesso al portale di CA Identity, qualsiasi applicazione web è a portata di clic e tutte le applicazioni cui gli utenti accedono sul loro desktop sono sempre disponibili anche attraverso la versione mobile del portale. Questo launchpad mantiene la produttività dei dipendenti on-the-go con single sign-on completo alle applicazioni web mobile in un formato mobile-friendly.



La sfida: assicurare l'efficienza dei processi per soddisfare gli SLA

"Alcuni dei miei processi di identificazione non funzionano in modo ideale, e questo genera lamentele di altri dirigenti in relazione ai livelli di servizio che sto fornendo. Le informazioni sulla collocazione dei colli di bottiglia di cui dispongo, però, non sono sufficienti per risolverli".

I processi di identificazione sono spesso complessi e possono richiedere passaggi di workflow molteplici. Quando questi processi non funzionano in modo efficiente, come nel caso in cui un gruppo di utenti non porta a termine il proprio compito nel rispetto dei tempi, è possibile che l'intero sistema venga bloccato e che gli obiettivi dei livelli di servizio non vengano soddisfatti. Questo può determinare carenze a livello di auditing, o semplicemente una maggiore inefficienza, quando processi di base come le certificazioni di accesso non vengono completati secondo gli obiettivi di servizio concordati. Senza una visibilità adeguata sui dettagli del funzionamento di questi processi, la causa di questi problemi non può essere identificata, né tanto meno corretta rapidamente.

La soluzione CA Identity Suite

CA Identity Suite fornisce analisi di estensione in tempo reale, per comprendere in modo completo e ottimizzare il funzionamento dei processi di identificazione fondamentali. Questo può aiutare a identificare i colli di bottiglia e a garantire che gli SLA critici vengano soddisfatti. A titolo di esempio, il grafico sottostante fornisce una vista temporale degli SLA correnti per il mese appena trascorso, così come di valori chiave come SLA medi, massimi e minimi per un dato processo. Esso mostra inoltre il volume di ingresso delle nuove richieste in ogni giorno del mese passato, nonché una sintesi della gestione (completata, respinta) di tutte queste richieste. Questa funzionalità fornisce al manager una comprensione notevolmente maggiore, che consente di ottimizzare i processi, e di visualizzarne facilmente lo stato completo.

La sfida: difficoltà del deployment

"Il deployment della mia soluzione di gestione delle identità è lungo e complesso. In primo luogo, la sola installazione e configurazione del software richiede giorni interni; quindi ci vogliono anche alcune settimane per arrivare ad avere pochi casi di utilizzo di base, perché ho bisogno di codice personalizzato e di definire workflow, policy e interfaccia utente".

Il deployment di una soluzione di gestione delle identità solida può essere difficile e costoso. Installare e far funzionare poche funzionalità di base spesso richiede alcune settimane. Inoltre, requisiti quali connettori per applicazioni personalizzate possono richiedere molto tempo e risorse.

La soluzione CA Identity Suite

CA Identity Suite è in grado di ridurre *drasticamente* il tempo necessario per l'installazione e l'operatività, attraverso funzionalità come:

- **Appliance virtuale (vApp).** vApp elimina la fase di installazione tradizionale fornendo un'immagine di macchina virtuale preinstallata e preconfigurata, pronta per essere eseguita in configurazioni di produzione su piattaforme di virtualizzazione comuni. L'appliance virtuale include un sistema operativo in hardening, un server delle applicazioni e il software di CA Identity Suite. Essa include inoltre supporto integrato per procedure DevOps comuni come configurazioni ad alta disponibilità, aggiustamenti di capacità, aggregazioni di registri, patch di piattaforma e aggiornamenti software.

  Per distribuire i servizi di identità, è sufficiente trascinare il nome del servizio sul nome della macchina adeguata: l'installazione avverrà automaticamente. Se si trascina lo stesso servizio su più macchine, tutti i meccanismi di comunicazione per l'alta disponibilità (bilanciamento del carico, failover e così via) verranno impostati automaticamente. Non è richiesta alcuna configurazione manuale, lunga e soggetta a errori. Il risparmio di tempo è molto significativo.

  Il risultato di questo approccio è una drastica riduzione del time-to-value e del TCO, con la conseguente capacità di ottenere di più a parità di team e di budget. Questo metodo può consentire anche di risparmiare migliaia di dollari l'anno in costi di licenza software, dato che tutti i componenti base del sistema possono essere distribuiti liberamente senza necessità di licenze aggiuntive.
- **Deployment Xpress (Depx).** Depx rappresenta un miglioramento radicale nella modalità di distribuzione del software di gestione delle identità. Si compone di un insieme di scenari utente preconfigurati per i casi più comuni, tipicamente richiesti dalla maggioranza delle aziende, quali onboarding dell'utente, reimpostazione della password, certificazioni di accesso, onboarding di partner e simili. Ogni scenario è costituito da tutti gli elementi necessari per un deployment semplificato, come interfacce utente di modello, workflow e definizioni di policy. Il manager seleziona semplicemente gli scenari necessari, li mette nel carrello e quindi procede al checkout. A quel punto, tutti questi elementi chiave vengono caricati automaticamente in Identity Suite e distribuiti. È possibile personalizzare questi elementi (ad esempio, branding aziendale per l'interfaccia), ma non è richiesto codice personalizzato. Questi scenari accelerano il processo di deployment e possono ridurre notevolmente il time-to-value per il deployment dei servizi di identità tipici.
- **Altri strumenti Xpress.** Identity Suite include strumenti aggiuntivi che semplificano notevolmente il processo di gestione dell'ambiente di deployment e che includono:
  - Connector Xpress semplifica il processo di creazione dei connettori per le applicazioni proprietarie, facilitando inoltre la connessione a sistemi privi di connettori OOTB.
  - Config Xpress consente di spostare più rapidamente e facilmente i componenti tra gli ambienti di staging, per una gestione della configurazione semplificata e più tempo a disposizione per il testing funzionale.
  - Policy Xpress consente di configurare le policy sulle quali si basano i processi di business complessi e specifici dell'azienda. Un risultato che viene ottenuto in genere tramite codice personalizzato: questo strumento basato su procedure guidate consente di creare policy in-house nell'arco di poche ore, anziché richiedere settimane di programmazione.

Funzionalità principali

CA Identity Suite include le funzionalità principali seguenti:

- Portale delle identità self-service ("one stop shop"): centralizza i dati relativi ai diritti e fornisce un intuitivo "carrello" per le richieste di accesso.
- Riduzione dei tempi di deployment, da giorni a minuti!
- Catalogo dei diritti business-friendly: rende certificazione dei diritti e richieste di accesso più comprensibili agli utenti di business.
- Analisi proattiva: offre agli utenti di business consigli, prevenzione e avvisi in merito a potenziali violazioni delle policy.
- Provisioning degli utenti per una vasta gamma di app on-premise, servizi SaaS e sistemi non connessi.
- Self-service degli utenti: consente agli utenti di gestire le proprie informazioni per ridurre il carico di lavoro dell'IT.
- Deployment Xpress: i modelli di casi d'uso preconfigurati semplificano notevolmente il deployment iniziale e la gestione continua.
- Personalizzazione senza codice personalizzato: funzionalità avanzate quali Config Xpress, Policy Xpress e Connector Xpress consentono di personalizzare l'infrastruttura di gestione delle identità senza necessità di codice personalizzato.
- Ottimizzazione dei privilegi: verifica i diritti di sistema esistenti ed evidenzia i privilegi eccessivi o superflui.
- Modellazione dei ruoli tramite motore di analisi avanzato (in fase di brevetto): consente di classificare con efficienza volumi estremamente elevati di informazioni su utenti e privilegi, per individuare ruoli potenziali.

ca technologies

Entra in contatto con CA Technologies all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies lavora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visita il sito **ca.com/it**.

CS200-230014_1016