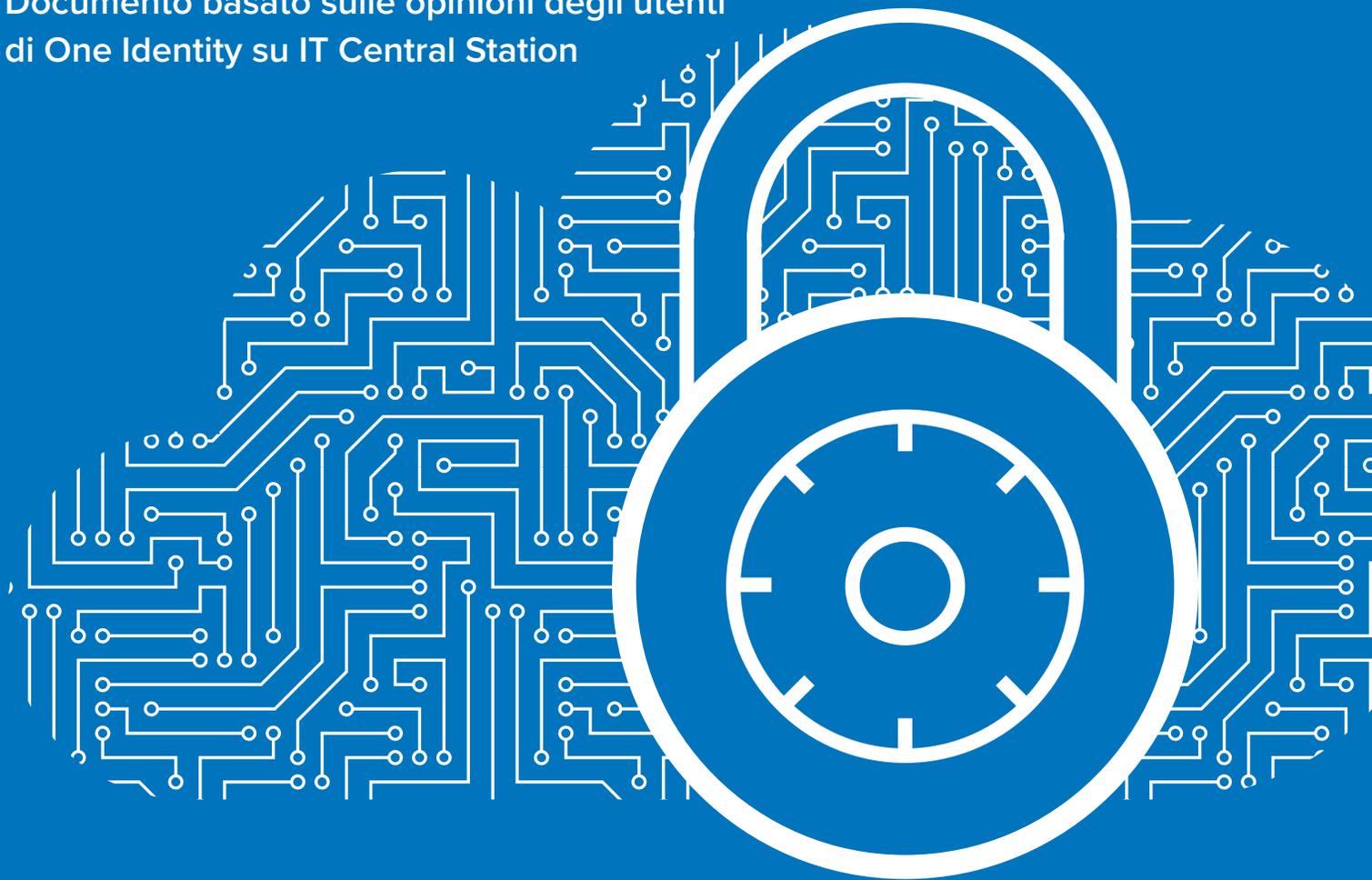


Rapporto PeerPaper™ 2021

10 buone prassi per la gestione e protezione di Microsoft Active Directory in un mondo IT in continua evoluzione

Documento basato sulle opinioni degli utenti di One Identity su IT Central Station



RIASSUNTO

Gran parte dei programmi di gestione dell'identità e dell'accesso (IAM) si basano su Microsoft Active Directory (AD) e Azure AD (AAD). Tuttavia, alla luce del passaggio al cloud, della modernizzazione ed espansione degli ambienti IAM in funzione della governance, i manager IT devono colmare le lacune di sicurezza ed efficienza di AD nativo e aumentare le funzionalità di AD, un prodotto spesso non all'altezza della situazione. Le aziende leader stanno definendo approcci pratici per proteggere e gestire l'AD ibrido alla luce dell'evoluzione della governance di identità e account attraverso l'adozione del cloud e altre tecnologie. Questo documento prende in esame le buone prassi emergenti basate sulle esperienze degli utenti reali con la soluzione One Identity Active Roles, come indicato nelle opinioni espresse in IT Central Station.

SOMMARIO

- Pagina 1. **Introduzione**
- Pagina 2. **L'IAM in un mondo IT e della sicurezza in continua evoluzione**
- Pagina 4. **Problemi di AD e degli altri sistemi legacy**
- Pagina 6. **Necessità di aumentare la sicurezza attraverso l'ottimizzazione dell'IAM**
- Pagina 9. **Ottimizzare il processo di gestione delle identità**
- Pagina 13. **Conclusioni**

INTRODUZIONE

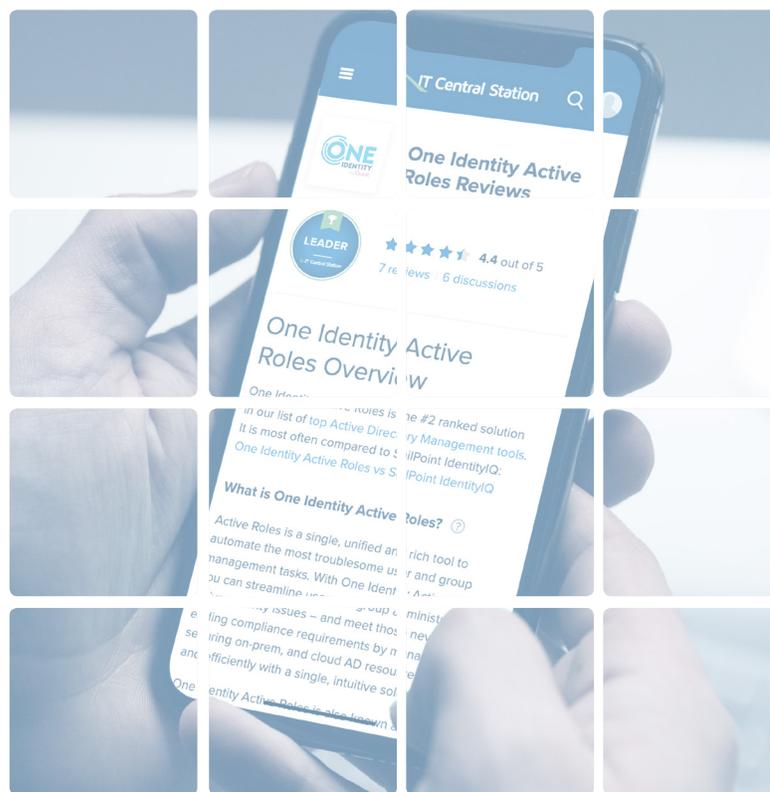
La sicurezza è uno dei principali problemi affrontati da CISO e dirigenti IT. Un framework per la gestione dell'identità e degli accessi (Identity and Access Management, IAM) sicuro e ben gestito è fondamentale per lo sviluppo di una strategia di sicurezza IT. I principali framework di sicurezza, come ad esempio quelli del NIST, considerano il controllo efficace delle identità e dei privilegi di accesso degli utenti come un fattore essenziale nell'ambito di una vasta gamma di contromisure. In questo campo, Microsoft Active Directory (AD) e Azure AD (AAD) restano un elemento centrale di gran parte dei programmi IAM. I responsabili della sicurezza devono risolvere diversi problemi legati

al sistema AD, soprattutto a causa dell'espansione dell'ambiente IT in funzione dell'ibrido e della maggiore complessità. Occorre espandere le funzionalità limitate e inefficienti degli strumenti nativi di AD. Sono state create soluzioni innovative per garantire un funzionamento ottimale di AD, mentre la governance dell'identità sta adottando il cloud e altre tecnologie.

Con l'esclusione dei casi indicati, tutte le aziende menzionate in questo documento dispongono di oltre 10.000 dipendenti.

L'IAM in un mondo IT e della sicurezza in continua evoluzione

Con il progressivo trasferimento nel cloud delle risorse digitali e la modernizzazione delle operazioni delle aziende, occorre affrontare nuove sfide legate all'IAM. I casi d'uso aziendali di One Identity Active Roles evidenziano l'adozione dell'IAM nel cloud da parte dei gestori delle identità. Ad esempio, un dirigente dei servizi di sicurezza IT di un'azienda aerospaziale/della difesa utilizza Active Roles per l'[Active Directory on-premise](#) della propria impresa. Nonostante ciò, i server di questa soluzione restano in hosting su Azure.



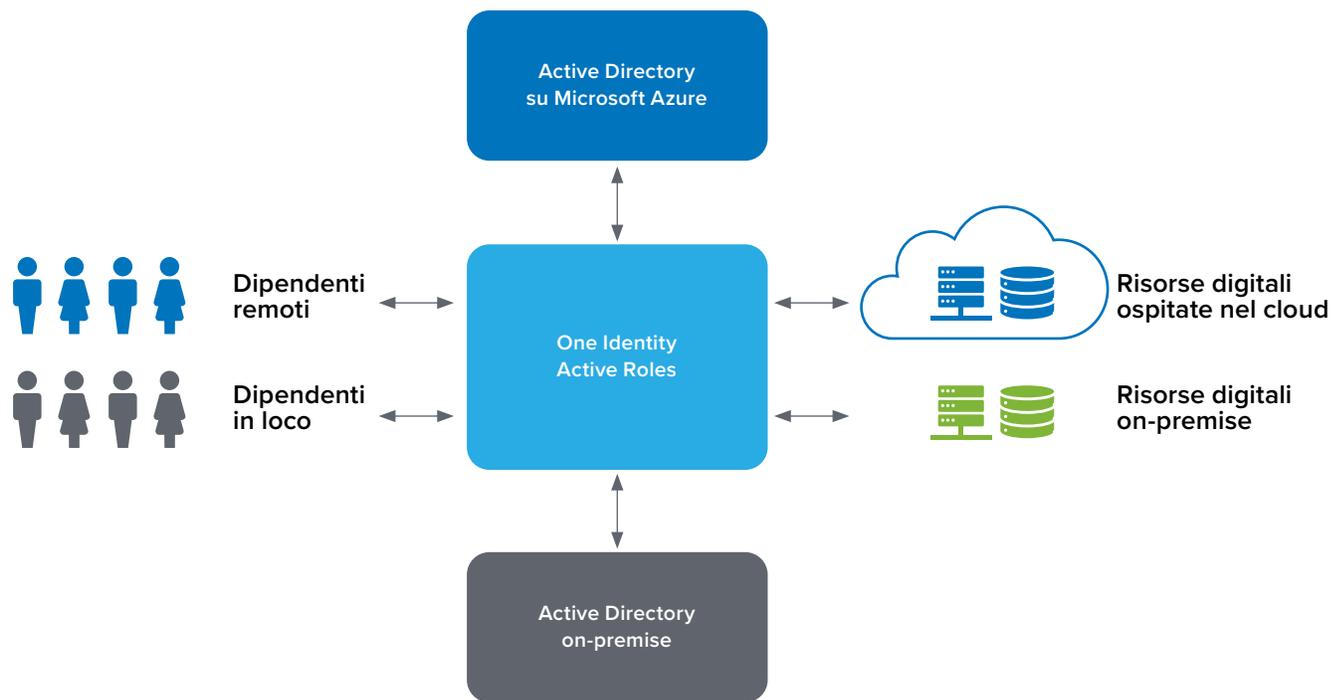


Figura 1. Il passaggio al cloud richiede un'IAM centralizzata per gestire l'accesso alle risorse digitali in hosting in qualsiasi luogo.

Un analista di business senior della George Washington University (GWU) utilizza Active Roles per la gestione di AD e la [creazione degli account](#). Questo analista ha dichiarato: "Esporteremo le proprietà native del gruppo di utenti di Azure AD per ottenere un maggiore

supporto. Eseguiamo il provisioning e il deprovisioning delle applicazioni e creiamo i rapporti richiesti". La figura 1 descrive una semplice architettura di riferimento per la distribuzione delle risorse digitali e istanze AD su hosting vicini e on-premise.

Un responsabile della sicurezza IT di un'azienda manifatturiera con oltre 5.000 dipendenti ha affermato quanto segue: "Inizialmente usavamo gli strumenti nativi di Microsoft. Siamo passati ad Active Roles poiché gli strumenti nativi erano dedicati alla gestione dei componenti principali e [non offrivano le funzionalità](#) di provisioning, deprovisioning, controllo degli accessi basato sui ruoli e cronologia delle modifiche da noi richieste. La soluzione precedente non offriva un approccio proxy per la gestione di Active Directory in modo centralizzato. Microsoft Active Directory è distribuito per natura, mentre Active Roles agisce in modo centralizzato".

"Prima di Active Roles, usavamo una [soluzione di scripting interna](#)", afferma un responsabile IT senior del Toronto District School Board. "Il cambiamento dipende dalla maggiore qualità del supporto e dalla necessità di eliminare i vecchi script di compilazione manuale, ormai non più supportati. In questo modo, disporremo un prodotto utilizzabile in chiave futura e dotato di un supporto adeguato. In confronto, gli strumenti nativi di Microsoft sono inadatti alle nostre esigenze: i connettori per la federazione degli utenti e la sincronizzazione con le altre soluzioni sono del tutto assenti".

Secondo un analista aziendale senior della GWU, Active Roles ha consentito al team di [eliminare Oracle Identity Manager](#) (OIM). "OIM è stato implementato circa nove anni fa, ma richiedeva un lungo periodo per il caricamento delle applicazioni e il passaggio a un provisioning basato sui ruoli. In sostanza, non siamo mai riusciti ad andare oltre la prima fase. Abbiamo usato tale sistema nel modo più avanzato possibile, creando un nuovo Active Roles per gestire gli altri aspetti. In caso di blocco di OIM, saremmo costretti a eseguire continui riavvii. Grazie ad Active Roles tutto questo appartiene al passato. Non eseguiamo un riavvio da un anno, ovvero dalla conclusione della migrazione".

“

Il cambiamento dipende dalla maggiore qualità del supporto e dalla necessità di eliminare i vecchi script di compilazione manuale, ormai non più supportati.

Necessità di aumentare la sicurezza attraverso l'ottimizzazione dell'IAM

Un'IAM migliore, più sicura, facile da gestire ed efficiente è un elemento essenziale per ottimizzare la sicurezza complessiva di un'organizzazione e ottenere un approccio efficace alla governance e amministrazione (AGA) di AD/AAD. Non è semplice mettere in atto questa visione. Esistono dieci buone prassi per l'IAM che offrono un approccio più efficace, sicuro ed efficiente. Una soluzione IAM deve impedire agli utenti di apportare modifiche non autorizzate. L'onere amministrativo può diventare elevato, quindi gli utenti cercano soluzioni basate sull'automazione e l'integrazione con altri sistemi. Anche la delega del controllo è un elemento fondamentale per ottenere un'IAM efficiente ed efficace. Le soluzioni IAM devono anche consentire l'adozione di un modello di controllo degli accessi con privilegi minimi, aprendo la strada alla "fiducia zero".



1. Ridurre le modifiche non autorizzate per contenere i rischi

Le modifiche non autorizzate ai controlli di identità e accesso sono una causa di grave rischio, poiché utenti sconosciuti potrebbero ottenere un accesso lasciando completamente all'oscuro gli amministratori. Active Roles offre funzioni integrative rispetto alla dotazione di AD, in modo da ridurre l'impatto di questo comportamento. Il responsabile della sicurezza IT di un'azienda manifatturiera spiega questo concetto: "La possibilità di eliminare i diritti di amministrazione principali [riduce la quantità di modifiche incontrollate](#), aumentando la disponibilità del servizio e contenendo l'entità dei risultati ottenuti negli audit. Active Roles [riduce i rischi](#) a cui è sottoposta la nostra organizzazione. Impedendo le modifiche alla sicurezza nativa di Active Directory e sfruttando un controllo accessi basato sui ruoli per la gestione di Active Directory attraverso tale applicazione, abbiamo ridotto i rischi in modo drastico".



La scelta di questa soluzione era legata alla necessità di una maggiore sicurezza".

Il responsabile tecnico della sicurezza di Liberty Global ha aggiunto: "Il ROI di Active Roles è legato alla [mitigazione dei rischi](#), ovvero alla possibilità di eliminare l'accesso non autorizzato e inquinare Active Directory. Ciò consentirebbe ad alcune persone di ottenere un accesso indebito a un sistema. Di conseguenza, potrebbero creare account multipli per un medesimo oggetto".

"Il prodotto consente di ottimizzare questo scenario, eliminando le modifiche caotiche apportate ad AD e [impossibili da individuare](#)", osserva un analista senior delle identità di un'azienda di beni di consumo. "Le persone devono lavorare senza eseguire azioni vietate.

In precedenza, le persone potevano aggiornare direttamente AD. Abbiamo ridotto il problema eseguendo ogni operazione tramite Active Roles. La scelta di questa soluzione era legata alla necessità di una maggiore sicurezza".

2. Integrare l'IAM nei sistemi di sicurezza

L'IAM è un'area dell'IT e della sicurezza che occorre integrare con altri sistemi aziendali. Secondo un responsabile della sicurezza di un'azienda manifatturiera, occorre usare Active Roles per fornire gli oggetti di Active Directory. Allo stesso tempo, questa azienda sta [usando tale prodotto per connettersi](#), attraverso Active Roles Synchronization Service, a un sistema di HR e per il provisioning e deprovisioning dei dipendenti. Il responsabile aggiunge: "In generale, usiamo il prodotto per fornire qualsiasi tipo di oggetto, gruppi di sicurezza e oggetti IT, in modo delegato. Active Roles Server consente di modificare la sicurezza di Active Directory in modo da delegare l'accesso per il provisioning a diversi team IT, senza modificare la sicurezza effettiva di Active Directory".



In generale, usiamo il prodotto per fornire qualsiasi tipo di oggetto, gruppi di sicurezza e oggetti IT, in modo delegato.

Un responsabile IT del settore aerospaziale utilizza l'interfaccia PowerShell di Active Roles per consentire ad altre parti del proprio ambiente e altre applicazioni, che potrebbero [interfacciarsi con tale prodotto](#), di apportare modifiche all'interno di Active Directory utilizzando i comandi di PowerShell. Il responsabile aggiunge: "Possiamo applicare lo stesso principio dei nostri diritti di sicurezza per imporre l'uso di Active Roles, riducendo il rischio dal punto di vista della protezione".

3. Delega per una maggiore sicurezza

I membri di IT Central Station hanno discusso delle proprie preferenze in termini di delega dell'accesso ai processi AD. Ad esempio, BeClever IT Solutions, una piccola azienda di servizi tecnologici, sta lavorando con un cliente alle prese con un problema legato a [permessi e deleghe](#). Molti utenti di questa azienda devono eseguire attività di amministrazione in AD. Si trattava di un problema legato agli errori potenziali causati da questi utenti. Active Roles consente di andare oltre gli amministratori di dominio e gestire gli utenti regolari. È possibile anche precompilare i valori di alcuni campi.

Secondo questo responsabile: "Si tratta di uno strumento eccellente, poiché disponiamo di diversi tecnici IT di base che non conoscono le funzioni avanzate di AD. La soluzione ha eliminato i noiosi compiti IT legati al provisioning". Il responsabile della sicurezza IT di un'azienda manifatturiera concorda: "Con l'accesso delegato ad Active Directory possiamo revocare numerosi [diritti di amministratore](#). Possiamo applicare un blocco più rigoroso e ottenere un ambiente più sicuro rispetto al prodotto precedente".

4. Adottare il modello a privilegi minimi e applicare la "zero trust"

Alcuni utenti di Active Roles di IT Central Station stanno utilizzando la soluzione per implementare un modello a privilegi minimi per la gestione degli accessi. Questo approccio sta ottenendo un crescente consenso a causa dell'eliminazione del tradizionale perimetro di sicurezza e la necessità, per le organizzazioni, di passare a un modello "zero trust". Come illustrato da un responsabile IT del settore aerospaziale: "Intendiamo usare il [modello a privilegi minimi](#) e ridurre al minimo i diritti nativi di Active Directory in modo da contenere i problemi successivi. Riducendo il numero delle persone dotate dei diritti nativi di Active Directory possiamo contenere i potenziali problemi da risolvere". La figura 2 indica una rappresentazione del modello a privilegi minimi usando un'immagine di "anelli" di privilegio crescente, con il privilegio minore posto nell'anello esterno.

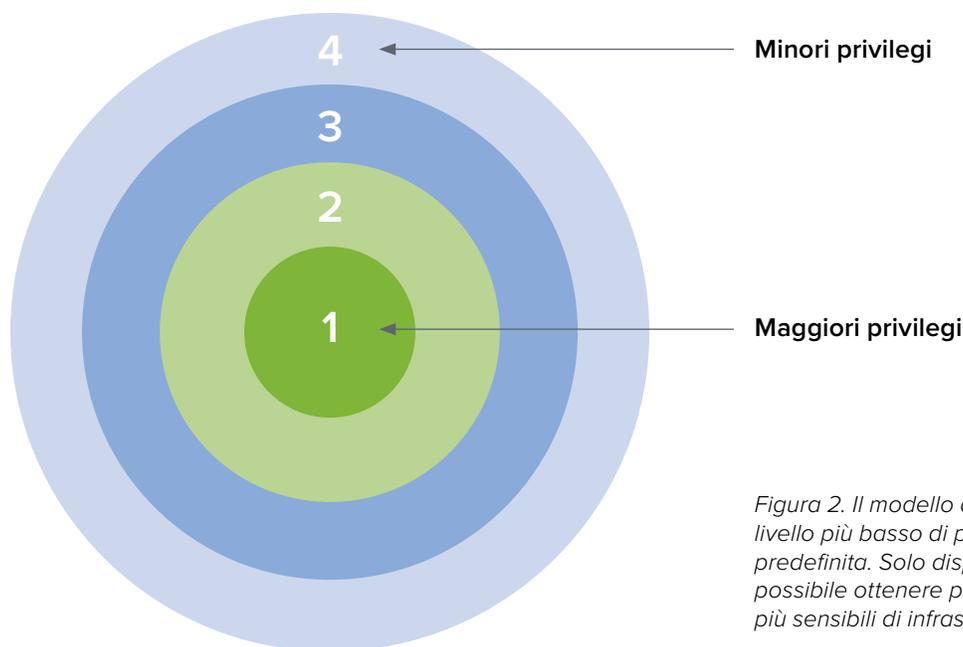


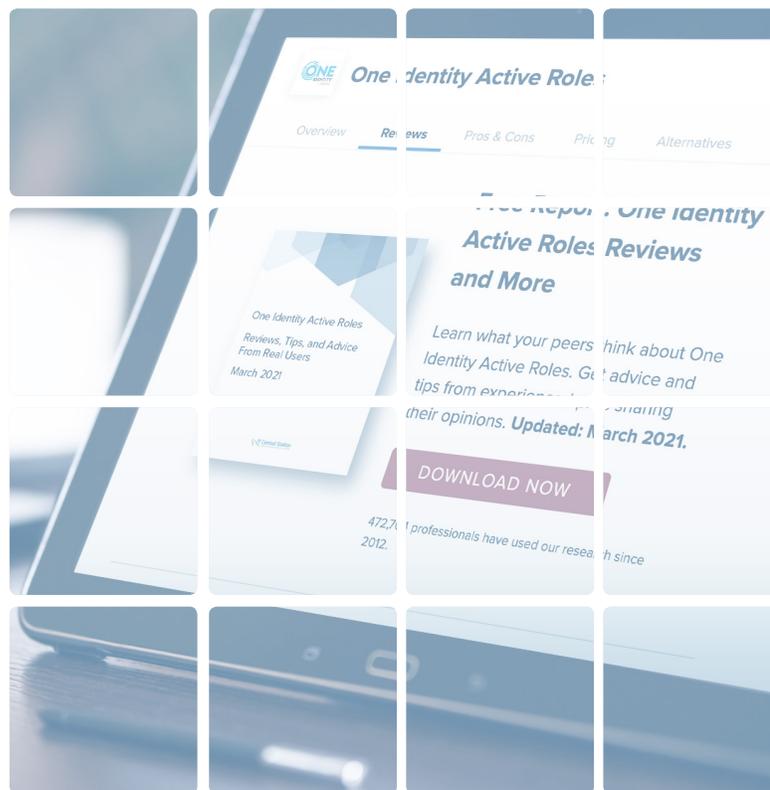
Figura 2. Il modello a privilegi minimi assegna agli utenti il livello più basso di privilegi di accesso per impostazione predefinita. Solo disponendo di un permesso specifico sarà possibile ottenere privilegi più elevati e accedere alle zone più sensibili di infrastrutture, dati e via dicendo.

Ottimizzare il processo di gestione delle identità

Alla luce dell'importanza di rafforzare la sicurezza attraverso l'ottimizzazione dell'IAM, in che modo è possibile migliorare il processo di gestione delle identità? I membri di IT Central Station hanno sottolineato l'importanza di un punto di controllo unificato, associato alla granularità del controllo. È importante anche risparmiare tempo e disporre di un processo di onboarding efficiente. Occorre anche automatizzare i flussi di lavoro di gestione delle identità, utilizzando politiche e modelli, sfruttando i gruppi dinamici per ottenere il massimo impatto.

5. Unificare la gestione mediante un singolo quadro di controllo

Gli utenti di Active Roles, come ad esempio un responsabile IT del settore aerospaziale, sono soddisfatti della possibilità di gestire diverse Active Directory [con una singola console](#) e disporre di un unico quadro di controllo on-premise. Secondo questa persona: "Disponiamo di un maggior numero di ambienti Active Directory, con la possibilità di gestirli e visualizzarli in un unico posto". Un analista senior di GUW concorda: "La flessibilità e l'espandibilità



di questa piattaforma offre efficienze nettamente superiori al previsto. Active Roles offre anche un [singolo quadro di controllo](#) per gestire AD e Azure AD. Possiamo gestire ogni aspetto da Active Roles, se necessario".

Un addetto della Marriott Phoenix ha commentato ulteriormente la questione del controllo. Secondo questa persona: "Active Roles offre un [controllo granulare](#) impossibile per AD. La disponibilità di uno strumento in grado di gestire tutte le modifiche apportate ad AD da un singolo quadro di controllo è molto positiva. Il prodotto consente anche al personale dell'help desk di agire rapidamente anche senza disporre di un elevato background tecnico".

6. Migliorare l'onboarding e la gestione del ciclo degli utenti

La gestione degli aspetti legati a identità e accesso del ciclo dei dipendenti è potenzialmente molto complesso e in grado di diventare un fattore di vulnerabilità. Ad esempio, gli ex dipendenti che conservano un accesso aziendale costituiscono una seria minaccia di sicurezza. Per ridurre questi rischi, una soluzione IAM deve offrire controlli efficienti del ciclo di vita degli utenti. Ad esempio, secondo il responsabile della sicurezza IT di un'azienda manifatturiera, la soluzione consente di [automatizzare il provisioning](#). Questa persona ha aggiunto: "Nel nostro sistema di HR stiamo automatizzando la creazione, cessazione e gestione continua di tutta la base di dipendenti. Disponiamo tra 5.000 e 6.000 dipendenti: tutti questi processi sono automatizzati. Il reparto IT non deve eseguire alcuna azione. Possiamo risparmiare centinaia di ore all'anno".

Questo utente ha aggiunto: "One Identity Active Roles migliora anche la precisione del [processo di onboarding](#). Il nostro processo di onboarding viene sottoposto a verifiche SOX (Sarbanes Oxley Act). Dieci anni fa, eravamo alle prese con centinaia di casi di mancata conformità. Oggi, abbiamo eliminato del tutto questi problemi". Il responsabile IT senior del consiglio scolastico di Toronto concorda: "Active Roles migliora la precisione del [nostro processo di onboarding](#). Riscontriamo una minore quantità di errori durante la sincronizzazione".

7. Automazione dei flussi di lavoro per la gestione delle identità

L'eccessiva dipendenza dai processi manuali per l'amministrazione dell'IAM è una scelta inefficiente e soggetta a errori. Gli amministratori preferiscono le soluzioni IAM in grado di automatizzare i processi di sicurezza. Secondo un

responsabile IT del settore aerospaziale: "Grazie all'[automazione di Active Roles](#) per l'onboarding, le politiche e i flussi di lavoro, i dati inseriti in Active Directory durante l'onboarding di qualsiasi tipo di oggetto sono precisi e in linea con i nostri standard, eliminando il materiale indesiderato. È un prodotto molto utile per snellire i processi.



Possiamo risparmiare centinaia di ore all'anno".

Senza disporre di uno strumento come Active Roles, il controllo delle modalità operative delle persone diventa uno degli aspetti più complessi per la gestione di Active Directory. Il modo in cui è possibile installare o impostare un nuovo utente può essere diverso da quello utilizzato da un'altra persona. Ad esempio, è possibile assegnare a una persona una serie di criteri da rispettare usando un prodotto diverso da Active Roles. Questo operatore dovrà interpretare e rispettare questi dettami. Active Roles consente di applicare queste politiche in modo da rendere i dati inseriti in Active Directory più puliti e coerenti. La coerenza dei dati ottimizza l'automazione e consente di impostare persone e oggetti in modo corretto".

Altri commenti sull'automazione:

- "Il prodotto migliora anche l'[automazione](#). Usavamo già tale paradigma, che adesso abbiamo ottimizzato. Abbiamo acquisito una maggiore quantità di dati da Trillium e SAP e popolato l'Active Directory con una mentalità aperta. Active Roles ha consentito ai due membri del nostro staff di risparmiare 0,2 FTE". Responsabile IT senior del Toronto District School Board
- "Il prodotto ha consentito di eliminare le attività che stavano rallentando il nostro dipartimento IT, soprattutto in relazione ad alcune [automazioni dei flussi di lavoro](#).

Attraverso Active Roles Synchronization Service, possiamo elaborare i dati provenienti dalle HR e aggiornare automaticamente questi attributi e campi dati in Active Directory senza agire in modo manuale o eseguire importazioni di massa". Responsabile della sicurezza IT di un'azienda manifatturiera con più di 5.000 dipendenti

- "Abbiamo introdotto il [provisioning automatizzato basato sui ruoli](#) grazie ad Active Roles. Inoltre, grazie all'uso dei flussi di lavoro e delle attività programmate, abbiamo automatizzato e gestito in modo centralizzato diversi processi, in modo da aggirare le limitazioni degli altri prodotti. Ad esempio, abbiamo sincronizzato i gruppi più estesi, ovvero quelli con oltre 50.000 membri, usando Azure AD". Analista aziendale senior della George Washington University

8. Risparmiare tempo e aumentare l'efficienza

Una soluzione IAM ottimale consente al personale IT e di sicurezza di risparmiare tempo. Si tratta dello scenario evidenziato dall'analista aziendale senior della GWU, che ha usato Active Roles per consentire al proprio team di lavorare [in modo più intenso ed efficiente](#). Il responsabile tecnico della sicurezza di Liberty Global ha riscontrato un'esperienza simile. Questa soluzione ha [eliminato numerosi compiti IT tediosi](#), soprattutto in caso di fuoriuscita delle persone dall'azienda.

Secondo questo utente: "Esistono 10 o 15 azioni basate su script che vengono eseguite da Active Roles in modo sempre uguale e puntuale. In precedenza, gli amministratori avrebbero dovuto eseguire numerose operazioni, ad esempio nascondere la casella di posta, disabilitare l'utente, rimuovere i gruppi e via dicendo. Inoltre, la cronologia degli audit del prodotto è molto utile. Essa registra i cambiamenti apportati a

un utente, l'autore degli stessi e il momento in cui vengono applicati, ottenendo numerosi vantaggi. Avendo esternalizzato numerose attività, dobbiamo gestire un pubblico in continuo cambiamento. Questi strumenti consentono di lavorare in modo strutturato, consentendo a tutti di eseguire la medesima operazione allo stesso tempo".



La soluzione ha consentito ai clienti di risparmiare tempo automatizzando attività che avrebbero richiesto da 30 a 45 minuti".

Alcuni utenti hanno quantificato il risparmio di tempo ottenuto. Il CTO della BeClever IT Solutions aggiunge: "La soluzione [ha consentito ai clienti di risparmiare tempo](#) automatizzando attività che avrebbero richiesto da 30 a 45 minuti". Secondo un responsabile IT del settore aerospaziale, nella propria organizzazione di 55.000 persone: "Si verifica l'avvicendamento del personale ogni giorno". In questo ambiente: "Active Roles [ha consentito di eliminare fino a 500 richieste](#) alla settimana. La soluzione ha eliminato le attività amministrative che stavano rallentando il reparto IT. Adesso, gli operatori IT non devono più aggiornare il gruppo quando una persona entra in azienda o fuoriesce dalla stessa". Un analista senior della GWU ha aggiunto: "Active Roles consente di [risparmiare almeno due settimane](#) al mese. Il prodotto ha ridotto il nostro carico di lavoro del 50%".

9. Utilizzo di politiche e modelli in grado di ottimizzare il controllo basato sui ruoli

Le politiche e i modelli basati sui ruoli consentono di migliorare il controllo degli accessi, risparmiare tempo e aumentare la precisione della

governance e amministrazione di AD. Come affermato dal responsabile del personale della Marriott Phoenix: "I [modelli integrati](#) di Active Roles consentono di creare gruppi di sicurezza senza la necessità di costruirli autonomamente. In questo modo, è possibile semplificare il processo e renderlo più semplice da rivedere, in modo da apportare modifiche più facilmente". Secondo il responsabile tecnico della sicurezza di Liberty Global: "Active Roles [consente di usare i criteri](#). Il pacchetto include numerosi criteri di esempio. Sono disponibili modelli di accesso e numerosi esempi. Inoltre, il pacchetto dispone di flussi di lavoro molto potenti".

10 Utilizzare i gruppi dinamici per ridurre i rischi e automatizzare gli aggiornamenti

"La caratteristica di Active Roles che preferisco sono i [gruppi dinamici](#), che è possibile aggiornare e creare al volo. Si tratta di un enorme vantaggio", ha spiegato un responsabile IT del settore aerospaziale. Il responsabile ha aggiunto: "Riceviamo regolarmente richieste dall'azienda per la creazione di un gruppo contenente tutti i membri di un dipartimento, un elenco di

distribuzione per le e-mail, un gruppo per proteggere un file server ecc. Con Active Roles, possiamo creare questo tipo di gruppo e collocare in esso qualsiasi account utente dotato di un dipartimento corrispondente a un dato valore".

“

Non dobbiamo attendere che una persona controlli ogni singolo gruppo per verificare se un dato individuo sia presente in esso.

Secondo un analista senior della GWU, l'utilizzo dei gruppi dinamici riduce i rischi e migliora la sicurezza attraverso l'eliminazione degli account orfani, che costituiscono una grave vulnerabilità. Secondo questa analista: "Usando un gruppo dinamico, se una persona non appartiene più al feed inviato dal sistema HR, verrà immediatamente [rimossa](#). Non dobbiamo attendere che una persona controlli ogni singolo gruppo per verificare se un dato individuo sia presente in esso. È possibile sfruttare le buone prassi interne e soddisfare il requisito di un accesso minimo".

CONCLUSIONI

L'IAM sta diventando un'attività sempre più impegnativa alla luce della maggiore complessità degli ambienti IT e della migrazione degli stessi verso il cloud, anche parzialmente. Microsoft Active Directory è un prodotto efficace per le funzioni IAM di base, ma la gestione dell'identità e il controllo degli accessi richiedono soluzioni basate su AD più sofisticate e automatizzate. Come illustrato dagli utenti di One Identity Active Roles nelle recensioni su IT Central Station, una soluzione ideale deve aumentare l'efficienza dell'IAM e consentire di risparmiare tempo. È possibile ridurre le modifiche non autorizzate e ottenere una maggiore sicurezza attraverso funzionalità come delega, gruppi dinamici, politiche e modelli. La presenza di un punto di controllo unificato offre ulteriori guadagni di efficienza. In definitiva, le soluzioni come Active Roles, in grado di operare nel cloud, on-premise e in modalità ibrida, costituiscono la base per apportare continui miglioramenti all'IAM e alla sicurezza di un'organizzazione, alla luce dell'evoluzione continua dell'IT e della sicurezza.

INFORMAZIONI SU IT CENTRAL STATION

Recensioni degli utenti, discussioni aperte e altre risorse per i professionisti della tecnologia aziendale.

Internet ha cambiato il modo in cui vengono prese le decisioni di acquisto. Adesso utilizziamo le valutazioni e i siti di recensioni per conoscere l'opinione degli altri utenti prima di acquistare prodotti di elettronica, prenotare un hotel, recarsi da un medico o scegliere un ristorante. Nel mondo della tecnologia aziendale, gran parte delle informazioni online e ricevute via posta elettronica proviene dai fornitori. Occorre un'informazione obiettiva fornita da altri utenti. IT Central Station offre ai professionisti della tecnologia una community utile per condividere informazioni sulle soluzioni aziendali.

IT Central Station offre informazioni preziose, obiettive e rilevanti espresse dagli utenti. Convalidiamo i recensori sottoponendoli a un triplo processo di autenticazione e proteggiamo la tua privacy creando un ambiente in cui è possibile eseguire pubblicazioni anonime ed esprimere liberamente le proprie opinioni. Di conseguenza, la community è una risorsa preziosa che offre accesso alle informazioni richieste e la connessione con le persone informate in modo puntuale.

www.itcentralstation.com

IT Central Station non approva né suggerisce alcun prodotto o servizio. Le opinioni dei recensori indicati in questo documento, nei siti Web e nei materiali di IT Central Station non rispecchiano le opinioni di IT Central Station.

INFORMAZIONI SU ONE IDENTITY

One Identity, un'azienda di Quest Software, consente alle organizzazioni di implementare una strategia di sicurezza incentrata sulle identità in locale, nel cloud o in un ambiente ibrido. Grazie alla nostra linea esclusiva, ampia e integrata di prodotti per la gestione delle identità, tra cui amministrazione degli account, governance, gestione delle identità e degli accessi privilegiati, le organizzazioni possono lavorare in tutta sicurezza, collocando le identità al centro del proprio programma e impartendo un accesso adeguato a tutti i tipi di utenti, sistemi e dati. Per ulteriori informazioni, visita la pagina Onelidentity.com