SOLUTION BRIEF

Come proteggere le credenziali con privilegi nei data center tradizionali e virtuali, cloud pubblici e privati e ambienti ibridi?

ca technologies

Gestire e proteggere le credenziali con privilegi è essenziale per ridurre i rischi e soddisfare i requisiti di compliance. Le aziende devono valutare soluzioni per la gestione delle password con privilegi in termini di controlli dettagliati, ambito di copertura e grado di allineamento al cloud. CA Privileged Access Manager offre perfomance eccellenti in tutte e tre le dimensioni, fornendo una soluzione di nuova generazione per la gestione delle credenziali con privilegi che consente di ridurre i rischi IT, migliora l'efficienza operativa e protegge gli investimenti aziendali, supportando le infrastrutture tradizionali così come quelle virtualizzate e cloud ibride.

Executive summary

La sfida

L'adozione della virtualizzazione e del cloud computing sta accrescendo l'importanza e la complessità di un problema noto: gestire e proteggere in modo efficace le password degli account con privilegi. La gestione delle password con privilegi nell'infrastruttura tradizionale (dispositivi di rete, server, mainframe e così via) è un problema di sicurezza e compliance che si trascina ormai da tempo. La situazione è ulteriormente complicata dal gran numero di credenziali con privilegi hard-coded nelle applicazioni. Esempi di credenziali di questo tipo sono le coppie di chiavi SSH e le chiavi codificate in PEM necessarie per accedere alle risorse Amazon Web Services (AWS).

L'opportunità

Una protezione efficace delle credenziali con privilegi in tutta l'azienda consente di ridurre il rischio che vengano sfruttate per attacchi dall'esterno o abusi interni. Le aziende che adottano approcci al privileged access management che integrino le 12 capacità essenziali illustrate in questo documento hanno la possibilità di ridurre i rischi di fallimento dell'auditing, violazioni della compliance, perdita di dati di valore elevato e costose interruzioni dei servizi, tutti problemi riconducibili alla mancata protezione degli account con privilegi.

Vantaggi

CA Privileged Access Manager offre un set completo di controlli per la protezione e la gestione di tutti i tipi di credenziali per ogni tipo di risorse, ovunque siano situate, pensato per gli ambienti cloud ibridi di oggi. Consente alle aziende di ridurre notevolmente i rischi, i costi di proprietà e i workload operativi, con risultati maggiori rispetto a quanto sarebbe possibile con soluzioni alternative con minori controlli dettagliati, estensione della copertura e allineamento con il cloud computing.

Sezione 1.

Nozioni fondamentali sulla gestione delle password con privilegi

Le password degli utenti con privilegi (di qui in avanti, password con privilegi) si distinguono dalle normali password utente per il fatto che rappresentano il varco di accesso alle risorse più sensibili dell'azienda, vale a dire gli account amministrativi (ad esempio admin, root, SYS, sa) e le funzionalità associate utilizzati per configurare e controllare l'infrastruttura IT aziendale. Dati i rischi connessi, è abbastanza ovvio che gestire e proteggere correttamente le credenziali di questo tipo è importante, un punto, tra l'altro, sottolineato dai numerosi gruppi di requisiti associati codificati negli standard e nelle norme di sicurezza più diffusi, come ad esempio la NIST Special Publication 800- 53 e il PCI-DSS (Payment Card Industry Data Security Standard).

Requisiti normativi a parte, la gestione delle password con privilegi non solo rappresenta una best practice dal punto di vista della gestione dei rischi, ma è essenziale per correggere il gran numero di comportamenti non sicuri troppo spesso adottati nelle aziende di oggi. La presenza di password deboli, obsolete o troppo esposte (ad esempio annotate su un post-it o in foglio di calcolo), l'uso di un numero eccessivo di password, la condivisione delle password, l'incapacità di attribuire in modo chiaro le azioni compiute con gli account condivisi, il mancato utilizzo della strong authentication e l'assenza di funzioni per la revoca centralizzata sono solo alcuni esempi dei problemi quotidiani.

Secondo il Verizon Data Breach Investigations 2015, il 95% delle violazioni può essere ricondotto al furto di credenziali, il 10% all'uso improprio delle credenziali da parte di soggetti interni di fiducia.[1]

Il vero problema, tuttavia, è che una qualsiasi di queste condizioni aumenta la probabilità di successo di attacchi di spear phishing, attacchi mirati e, in ultima analisi, furto dei dati, per non parlare delle violazioni della compliance. Lo conferma il Verizon Data Breach Investigations Report 2015, secondo cui il 95% delle violazioni può essere ricondotto al furto di credenziali e il 10% all'uso improprio delle credenziali da parte di soggetti interni di fiducia.[1] Risultati come questi rendono evidente il motivo per cui le aziende di oggi hanno bisogno di una soluzione di classe enterprise come CA Privileged Access Manager per la gestione delle credenziali con privilegi, la protezione e il controllo degli accessi.

L'impatto del cloud ibrido

I problemi tradizionali appena descritti rappresentano solo la punta dell'iceberg. Date i notevoli vantaggi in termini di costi, adattabilità e reattività offerti dalle configurazioni cloud ibride, in cui i servizi e le applicazioni IT utilizzano sia l'infrastruttura tradizionale che quella virtualizzata, attingendo a data center aziendali e in cloud, l'adozione diffusa di questo modello è inevitabile. Oltre ai vantaggi, tuttavia, i cloud ibridi introducono anche nuove sfide associate alla gestione delle password con privilegi, tra cui:

- Maggiori volumi, in quanto le esigenze operative e la semplicità di deployment delle macchine virtuali determinano un aumento delle entità che fanno richiesta di accesso con privilegi (e di conseguenza di password con privilegi)
- Ambito più esteso, in quanto la potenza della virtualizzazione e delle console di gestione cloud aggiungono al mix un nuovo tipo di account/risorsa con privilegi
- Maggiore dinamismo, visto che è possibile aggiungere nuovi server e sistemi on demand e addirittura in blocco (ad esempio 10, 20 o più per volta)
- Possibile creazione di isole di identità, visto che ogni servizio cloud dispone di un archivio di identità e di un'infrastruttura a sé stante[2]

Al di là delle sfide poste dal cloud ibrido, al momento di valutare le possibili soluzioni i responsabili della sicurezza IT devono considerare altri due aspetti del problema della gestione delle password con privilegi. Prima di tutto, devono tenere conto dello scenario machine-to-machine o Application-to-Application (A2A), in cui le password utilizzate da un sistema o un'applicazione per accedere a un altro sistema o applicazione sono hard-coded nell'applicazione stessa o disponibili in un file di configurazione in formato testo. Il secondo elemento da considerare è il problema, spesso sottovalutato, che la maggior parte delle aziende può disporre anche di migliaia di chiavi, ad esempio per le implementazioni SSH. Anche se non si tratta di password tradizionali di tipo frase, fungono comunque da credenziali di autenticazione per account con privilegi e per questo motivo vanno anch'esse gestite e protette per ridurre i rischi associati.

La conclusione è che, nell'era del cloud ibrido, la gestione delle password con privilegi è più importante e complessa che mai.

Sezione 2.

La soluzione di privileged access management di CA Technologies

CA Privileged Access Manager offre una soluzione completa per il privileged access management. Oltre alla capacità di controllare gli accessi, monitorando e registrando le attività degli utenti con privilegi negli ambienti cloud ibridi, CA Privileged Access Manager integra funzionalità chiave per la gestione delle password con privilegi, essenziali per una soluzione di nuova generazione. È importante che i team di sicurezza IT riconoscano che la gestione e la protezione delle password, oltre ad avere un valore intrinseco, rappresentano anche il mezzo per un fine superiore. In particolare, rappresentano il primo passo (o un passo complementare) nel processo più ampio e altrettanto importante di controllare e gestire in modo efficace l'accesso alle risorse ad alto rischio. Se la distinzione sembra sottile è in gran parte perché, all'atto pratico, le implementazioni funzionali di meccanismi di autenticazione (cioè password) e controllo degli accessi sono spesso complementari, quindi la nostra mente tende ad accomunarle

In ogni caso, gli obiettivi di progettazione per le funzionalità di gestione della password con privilegi incluse in CA Privileged Access Manager sono uguali a quelli applicati nel resto della soluzione. Nello specifico, il nostro obiettivo è stato quello di sviluppare una soluzione che non solo fornisca un set completo di controlli e funzionalità per una gamma completa di obiettivi e use case, ma che sia allo stesso tempo coerente con le opzioni di delivery, le prassi e le architetture dell'era cloud.

Controlli completi

Quando si tratta di valutare una soluzione di gestione delle password con privilegi, consigliamo di verificare innanzitutto se la soluzione integra o meno un set completo di controlli che aiuti il team di sicurezza a superare i rischi posti dagli approcci tradizionali alla creazione, alla gestione e all'utilizzo di credenziali amministrative sensibili. Le specifiche aree da esaminare includono rilevamento, vaulting, applicazione delle policy, recupero e capacità di supportare l'evoluzione in un'implementazione di privileged access management completo di tutte le funzionalità.

Sezione 3.

Le 12 capacità essenziali per il privileged access management

N. 1 Rilevamento automatico/semplificato

In mancanza di uno strumento che consenta di automatizzare o semplificare il rilevamento, il processo di implementazione della gestione delle password con privilegi può essere oneroso, per non parlare dei problemi provocati da errori o omissioni che possono lasciare l'ambiente di computing aziendale vulnerabile ai sofisticati attacchi di oggi. Per questo motivo, CA Privileged Access Manager include un'ampia serie di metodi per il rilevamento di device, sistemi, applicazioni, servizi e account, che include l'uso delle associazioni di porta, delle informazioni di directory, delle console di gestione e delle API più diffuse. Ad esempio, CA Privileged Access Manager utilizza le API disponibili per le soluzioni di virtualizzazione e cloud management supportate per avvisare gli amministratori della creazione di nuove macchine virtuali. In più, la soluzione semplifica l'importazione in blocco di elenchi di sistema dai file di testo, oltre che l'inserimento di voci ad hoc attraverso la console di gestione. Infine, è importante notare la scelta in fase di progettazione di evitare tecniche di rilevamento più invasive (e potenzialmente più rischiose) che richiedano l'utilizzo di agenti basati sulla destinazione che usino hook o shim per lo stack TCP locale.

N. 2 Storage/vaulting sicuro

Un vault crittografato fornisce un punto di controllo centralizzato ed è essenziale per eliminare i metodi di storage non sicuri (come i fogli di calcolo), che rendono troppo facile condividere e compromettere le credenziali. Il vault di CA Privileged Access Manager è un archivio credenziali sicuro, una soluzione conforme agli standard FIPS 140-2 livello 1 che utilizza la crittografia AES a 256 bit per memorizzare tutti i tipi di credenziali, non solo le password. Ecco alcune altre caratteristiche interessanti della soluzione:

- Possibilità di utilizzare i moduli di protezione hardware integrati (HSM), ad esempio quelli forniti da SafeNet e Thales, per gestire un'implementazione FIPS 140-2 livello 2 o livello 3. Questo è particolarmente importanti per i client e gli use case di alto profilo avversi al rischio, come quelli associati ai sistemi bancari e finanziari, in cui è opportuno conservare le chiavi utilizzate per crittografare le credenziali separatamente dalle credenziali crittografate. La soluzione supporta più opzioni di deployment, tra cui appliance hardware con schede PCI onboard, appliance virtuali CA Privileged Access Manager che eseguono chiamate a moduli HSM collegati alla rete e appliance CA Privileged Access Manager di entrambi i tipi che eseguono chiamate a un prodotto AWS "HSM-as-a-service".
- Routine di crittografia white-box di efficacia comprovata, che proteggono le chiavi di crittografia durante l'utilizzo (in memoria) all'interno di un sistema. Questo approccio è progettato per impedire agli hacker di intercettare/ricomporre le chiavi monitorando le API di crittografia standard e la memoria e di avere la meglio su alternative di livello inferiore basate sulla suddivisione in blocchi (chunking) delle chiavi o sul semplice offuscamento. L'integrazione di questa tecnologia è particolarmente importante per gli use case A2A, in cui il sistema che esegue l'accesso deve anche eseguire il vaulting delle credenziali ed esiste un maggior rischio di compromissione (per la posizione relativamente esposta).

N. 3 Applicazione automatica delle policy

CA Privileged Access Manager automatizza la creazione, l'uso e la modifica delle password, eliminando così la tendenza a riutilizzare password deboli (ma semplici da ricordare). CA Privileged Access Manager consente di impostare policy flessibili per imporre l'uso di password complesse, implementare i requisiti di modifica, quali la rotazione delle password a intervalli di tempo specificati (ad esempio giornalmente o settimanalmente) e regolamentarne l'utilizzo (ad esempio concedere l'accesso solo all'interno di finestre temporali specificate oppure richiedere l'autorizzazione doppia/multipla per l'accesso alle password). Poiché queste policy possono essere applicate in modo gerarchico e a gruppi di risorse di destinazione, non solo è possibile adattarle ai requisiti e alle capacità necessarie per risorse di destinazione diverse, ma anche la loro applicazione diventa in effetti dinamica, visto che qualsiasi risorsa aggiunta a un gruppo ne eredita automaticamente le policy. In background, anche CA Privileged Access Manager interagisce direttamente con le risorse di destinazione, per fare in modo che tutte le credenziali restino sincronizzate (vale a dire, che quando vengono modificate in un punto, lo siano anche nell'altro).

N. 4 Recupero, presentazione e utilizzo sicuri

Inserire le credenziali con privilegi in un vault protetto non ha senso se non è possibile anche recuperarle e utilizzarle in modo sicuro. La prima fase di questo processo è l'autenticazione precisa di chi, o di cosa, nel caso di applicazioni e script, stia cercando di accedere a una credenziale o di utilizzarla. A questo proposito, CA Privileged Access Manager sfrutta appieno l'infrastruttura di gestione delle identità esistente, grazie all'integrazione con Active Directory, directory compatibili LDAP e sistemi di autenticazione come RADIUS. La soluzione include inoltre il supporto per:

- Token a due fattori (ad esempio tramite CA Advanced Authentication o analoghi forniti da RSA e SafeNet)
- Certificati X.509/PKI
- Schede PIV (Personal Identity Verification) e CAC (Common Access Card) necessarie per la compliance con i mandati HSPD-12 e OMB M-11-11 per il settore federale,
- SAML
- Tecniche multifattore composite (ad esempio combinazione di password e token RSA)

Nella modalità operativa preferita, CA Privileged Access Manager presenta quindi le credenziali richieste al sistema di destinazione per conto dell'entità che esegue l'accesso (utente o applicazione). Questo approccio offre ulteriori vantaggi in termini di sicurezza. Prima di tutto, rispetto alle semplici soluzioni di check-in/check-out, le credenziali non vengono mai mostrate né distribuite all'entità che esegue l'accesso. Questo ne riduce notevolmente il rischio di esposizione. Inoltre, poiché l'autenticazione nel sistema di destinazione è completamente automatica e gli utenti non hanno bisogno di gestire/ricordare le password, è possibile implementare policy che impongano un livello di complessità delle password molto superiore. Poiché tutti gli accessi ai sistemi di destinazione avvengono tramite CA Privileged Access Manager, la soluzione consente la piena attribuzione delle attività eseguite dagli utenti con privilegi, anche per gli account admin condivisi.

Per completezza, è importante sottolineare che anche per tutte le comunicazioni di rete tra i soggetti che eseguono l'accesso, CA Privileged Access Manager e le destinazioni, viene utilizzata la crittografia SSL. In più, CA Privileged Access Manager supporta una modalità di funzionamento alternativa, in cui le entità che eseguono l'accesso possono recuperare autonomamente le credenziali e inviarle ai sistemi di destinazione.

N. 5 Transizione semplice e completa al privileged access management

CA Privileged Access Manager offre alle aziende inizialmente interessate solo alla gestione delle password tutto il necessario per passare a un'implementazione del privileged access management completa, se e quando si renderanno

conto della necessità di farlo. Ecco alcune delle funzionalità più importanti che il reparto di sicurezza IT avrà a disposizione quando sarà pronto ad approfittarne:

- Controllo granulare basato sui ruoli degli accessi e dei workflow associati (ad esempio per la richiesta e la concessione di autorizzazioni aggiuntive)
- Avvio automatico di sessioni/connessioni con le risorse di destinazione (con supporto di RDP, SSH, web e svariate altre modalità e opzioni di accesso)
- Monitoraggio in tempo reale delle sessioni utente con privilegi, oltre che imposizione basata su policy delle azioni consentite e negate (ovvero i comandi che uno specifico utente può utilizzare)
- Logging, inclusa l'integrazione SIEM basata sui log di sistema
- Registrazione completa delle sessioni, con controlli di riproduzione simili a quelli di un videoregistratore che consentono di passare direttamente agli eventi di interesse
- Prevenzione degli attacchi leapfrog, per impedire che gli utenti possano aggirare le autorizzazioni concesse sfruttando le destinazioni accessibili per ottenere accesso ad altre destinazioni non autorizzate

Inoltre, l'implementazione di queste funzionalità aggiuntive non potrebbe essere più semplice. CA Privileged Access Manager fornisce tutte le funzionalità di gestione delle password con privilegi e controllo degli accessi in un'unica soluzione strettamente integrata. Inoltre, offre gestione unificata delle policy nell'intera soluzione, un approccio che semplifica ulteriormente l'implementazione e l'amministrazione.

Copertura completa

La seconda importante area da valutare nella scelta di una soluzione per la gestione delle password con privilegi è l'ambito di copertura. In altre parole, rispetto al set completo di controlli illustrati nella sezione precedente, quali sono i tipi di entità che eseguono l'accesso, le credenziali e i sistemi di destinazione effettivamente supportati dalla soluzione?

N. 6 Copertura completa per le destinazioni tradizionali

CA Privileged Access Manager include un'ampia gamma di connettori a sistemi di destinazione, che offrono integrazione out-of-the-box per qualunque tipo di infrastruttura IT, device di rete, sistema e applicazione, tra cui:

- Account di dominio, di servizio e di amministratore locale di Windows®
- Principali distribuzioni Linux® e UNIX®
- AS/400
- Device di rete Cisco e Juniper
- Sistemi basati su Telnet/SSH
- SAP
- Remedy
- Database ODBC/JDBC
- Server di sistema e di applicazione

Facilmente estendibile, CA Privileged Access Manager è inoltre dotato di funzionalità di personalizzazione flessibili, che consentono alle aziende di estendere rapidamente il supporto a sistemi proprietari e sviluppati internamente.

N. 7 Supporto per virtualizzazione e console di gestione cloud

Le funzionalità out-of-the-box di CA Privileged Access Manager per la gestione e la protezione delle credenziali non sono limitate alle destinazioni tradizionali. Includono infatti la copertura per le più diffuse soluzioni cloud e di virtualizzazione, tra cui VMware vSphere, VMware NSX, Amazon Web Services e Microsoft® Online Services. In più, le funzionalità applicabili a queste soluzioni non sono limitate alle singole istanze di macchine virtuali, applicazioni o servizi associati. La copertura comprende anche le console di gestione corrispondenti, che, visto il potere che conferiscono, vanno anch'esse riconosciute e trattate come risorse con privilegi.

N. 8 Supporto dell'autenticazione machine-to-machine

Come accennato in precedenza, le credenziali con privilegi non vengono utilizzate solo da esseri umani. In molte aziende, anche numerose applicazioni e sistemi sono abilitati ad accedere a risorse sensibili, come altre applicazioni o database. A questo scopo, in genere le credenziali associate vengono incorporate nel codice dell'applicazione che esegue l'accesso oppure rese disponibili in fase di esecuzione tramite un file di configurazione. Nessuna delle due opzioni è particolarmente sicura o gestibile. CA Privileged Access Manager offre copertura per gli use case A2A, consentendo agli sviluppatori di integrare un client leggero di CA Privileged Access Manager nelle applicazioni. Questo approccio fornisce alle "applicazioni con privilegi" tutto ciò che occorre per registrarsi in CA Privileged Access Manager, recuperare dinamicamente le password necessarie e proteggerle mentre sono in memoria nel sistema locale. Inoltre, numerosi meccanismi consentono di autenticare le applicazioni con privilegi e verificarne l'integrità prima che CA Privileged Access Manager rilasci le credenziali richieste.

Utilizzando CA Privileged Access Manager per gli scenari A2A, le aziende possono eliminare più efficacemente le credenziali A2A esposte/insicure archiviandole in una posizione centrale protetta, automatizzare la gestione delle credenziali A2A e l'applicazione delle policy, nonché semplificare le attività di auditing e compliance correlate.

N. 9 Supporto per la gestione delle chiavi

Oltre a supportare le operazioni di crittografia, molti tipi di chiavi fungono anche da token per la conferma dell'identità. Anche se queste chiavi non sono password nel senso tradizionale del termine, operano comunque come password e sono soggette a minacce, rischi e problematiche analoghe, come copia, condivisione, esposizione involontaria e backdoor non controllate. Poiché in genere queste chiavi vengono utilizzate in modo trasparente o sono incorporate nelle soluzioni per proteggere gli utenti dalla loro relativa complessità, sono facilmente soggette anche a restare isolate (orfane) e/o a proliferare nel tempo. Per questo motivo, è opportuno applicare a queste credenziali alternative molti degli stessi controlli usati per gestire e proteggere le password. Di fatto, le best practice consigliate per contrastare le minacce correlate includono:

- Spostamento delle chiavi autorizzate in posizioni protette
- Rotazione regolare di tutte le chiavi (per garantire la cancellazione dell'accesso in caso di divulgazione delle chiavi)
- Applicazione di restrizioni sull'origine per le chiavi autorizzate[3]
- Applicazione di restrizioni sui comandi per le chiavi autorizzate

A questo scopo, CA Privileged Access Manager è dotato di controlli e altre funzionalità dedicate alle credenziali alternative di questo tipo, incluse le chiavi SSH e codificate in PEM usate per accedere alle risorse e alle console di gestione AWS. In altre parole, con CA Privileged Access Manager queste credenziali possono essere: (1) inserite in vault, (2) ruotate e controllate mediante policy configurate e (3) recuperate e utilizzate in modo da ridurre al minimo le probabilità di furto o esposizione.

Delivery nell'era cloud

Nell'era del cloud ibrido, un altro importante fattore discriminante per il successo di una soluzione di gestione delle password con privilegi è l'idoneità, in termini non solo fisici, ma anche di allineamento con le esigenze e le funzionalità delle reti cloud.

N. 10 Opzioni di delivery on-premise, come macchina virtuale e basate su cloud

CA Privileged Access Manager supporta tre comode opzioni di deployment, che aiutano le aziende a restare al passo con le complesse architetture cloud ibride:

- Appliance fisica con hardening, disponibile in più modelli per il montaggio a rack tradizionale nel data center aziendale
- Istanza AMI (Amazon Machine Instance), preconfigurata per il deployment con l'infrastruttura Amazon EC2
- Appliance virtuale compatibile con OVF, pronta all'uso e preconfigurata per il deployment in ambienti VMware

Indipendentemente dalle opzioni di deployment scelte, le aziende otterranno una soluzione che consente di gestire l'intera infrastruttura cloud ibrida.

N. 11 Approccio e architettura allineati al cloud

CA Privileged Access Manager è progettato per integrare numerose funzionalità specifiche per gli ambienti cloud ibridi. Ecco tre esempi:

- Rilevamento e protezione automatici - Negli ambienti cloud ibridi, gli operatori possono creare (o ritirare) qualsiasi numero di sistemi con un solo comando. CA Privileged Access Manager tiene conto di questo aspetto, sfruttando le API applicabili per rilevare automaticamente le risorse virtualizzate e cloud e quindi eseguire il provisioning (o deprovisioning) delle credenziali e delle policy di gestione degli accessi appropriate.
- Capacità di evitare la creazione di "isole di identità" (come nella federazione delle identità) - Uno dei metodi utilizzati da CA Privileged Access Manager per eliminare le isole di informazioni sulle identità consiste nel supporto completo dell'infrastruttura di identità aziendale esistente. Un altro metodo, specifico per le implementazioni di AWS, consiste nel supporto degli utenti temporanei, un approccio che evita alle aziende di dover conservare informazioni di identità separate nel sottosistema di Identity and Access Management AWS.
- Abilitazione dell'automazione - Una API completa consente l'automazione e l'accesso programmatico a tutte le funzionalità di CA Privileged Access Manager (ad esempio da sistemi di gestione e di orchestrazione esterni)

N. 12 Scalabilità e affidabilità native per il cloud

La gestione delle credenziali con privilegi è un elemento critico dell'infrastruttura IT aziendale. Questo è particolarmente vero quando l'applicazione viene estesa per il supporto degli use case A2A, il cui funzionamento è completamente automatico. A questo scopo, CA Privileged Access Manager include funzionalità native per il clustering e la distribuzione del carico, in grado di soddisfare le esigenze di scalabilità e disponibilità elevata degli ambienti più grandi e impegnativi. Rispetto alle alternative comuni, con CA Privileged Access Manager non vi è alcuna necessità di investire in utilità di bilanciamento del carico esterne separate, non esistono i ritardi delle performance tipici degli approcci attivo-passivo e non c'è bisogno di acquistare la licenza di ulteriori funzioni "facoltative". Se necessario e operativamente accettabile dal punto di vista della latenza, è persino possibile configurare i cluster di CA Privileged Access Manager per abilitare la ridondanza tra data center geograficamente distribuiti e ambienti cloud.

CA Privileged Access Manager è una soluzione di nuova generazione per la gestione delle credenziali con privilegi, progettata per ridurre i rischi di sicurezza e migliorare l'efficienza operativa nell'intera infrastruttura aziendale ibrida.

Sezione 4.

Conclusioni: vincere la sfida della gestione delle credenziali con privilegi nell'era del cloud

Gestire e proteggere le credenziali con privilegi è essenziale per ridurre i rischi e per la compliance con i requisiti normativi correlati. È anche un problema che sta crescendo in complessità e rilievo, poiché gli ambienti cloud ibridi introducono console di gestione caratterizzate da un potere senza precedenti, con la capacità di aggiungere e rimuovere letteralmente centinaia di sistemi di destinazione con pochi clic.

Le aziende che intendono affrontare questa area fondamentale della strategia di sicurezza delle informazioni devono valutare le soluzioni candidate in termini di profondità dei controlli, ambito di copertura e livello di allineamento al cloud. Come illustrato in questo documento, CA Privileged Access Manager offre performance eccellenti in tutte e tre le dimensioni, fornendo alle aziende di oggi esattamente ciò di cui hanno bisogno: una soluzione di nuova generazione per la gestione delle credenziali con privilegi progettata per favorire la riduzione dei rischi IT, migliorare l'efficienza operativa e proteggere gli investimenti aziendali, supportando le infrastrutture tradizionali così come quelle virtualizzate e cloud ibride.

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 sfruttare le opportunità offerte dall'economia delle applicazioni. 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, visitare il sito ca.com/it.

1 2015 Verizon Data Breach Investigations Report

2 *"Nuove piattaforme, nuovi requisiti. Gestione delle identità con privilegi per il cloud ibrido", white paper CA Technologies, marzo* 2013

3 *"Managing SSH Keys for Automated Access - Current Recommended Practice"*, documento draft di IETF, aprile 2013

CS200-169152_1215