WHITE PAPER | FEBBRAIO 2015

Progettare un'architettura CA Single Sign-On per una sicurezza avanzata

Utilizzare le impostazioni esistenti per un'architettura più sicura

ca technologies

Sommario

Riepilogo

Sfida

La soluzione CA Single Sign-On (CA SSO) è ampiamente diffusa in tutto il mondo per proteggere e offrire accesso single sign-on per tutta una serie di applicazioni con diverse esigenze di sicurezza. CA SSO utilizza diversi metodi per gestire le sessioni utente, il più diffuso dei quali consiste nell'uso dei cookie. In molti casi gli amministratori configurano CA SSO per l'invio di questi cookie a moltissimi server web, anche a quelli che non hanno l'esigenza di accedere al cookie di sessione. Configurando un'applicazione per l'invio di un cookie a una moltitudine di server, si viene a generare una vulnerabilità nell'architettura che consente a un hacker di sottrarre i cookie e riprodurli per assumere l'identità di un utente autenticato.

L'opportunità

CA SSO contribuisce a ridurre al minimo il rischio di attacchi basati sulla riproduzione delle sessioni, grazie all'approccio "Enhanced session assurance with DeviceDNA™" in attesa di brevetto. CA SSO offre diverse impostazioni con lo scopo di incrementare la sicurezza delle sessioni, tra cui l'uso dei cookie "solo host", ovvero cookie di sessione progettati espressamente solo per essere ritrasmessi all'host che li ha creati. Questo approccio può essere applicato offrendo la tecnologia SSO a un livello più ampio e inter-applicazione per gli utenti finali e consentendo agli agenti di comunicare da un dominio a un altro sfruttando un provider di cookie centrale. Il provider di cookie può fornire un riferimento monouso a una sessione archiviata in un archivio di sessioni centralizzato per passare la sessione da un'applicazione alla successiva.

I vantaggi

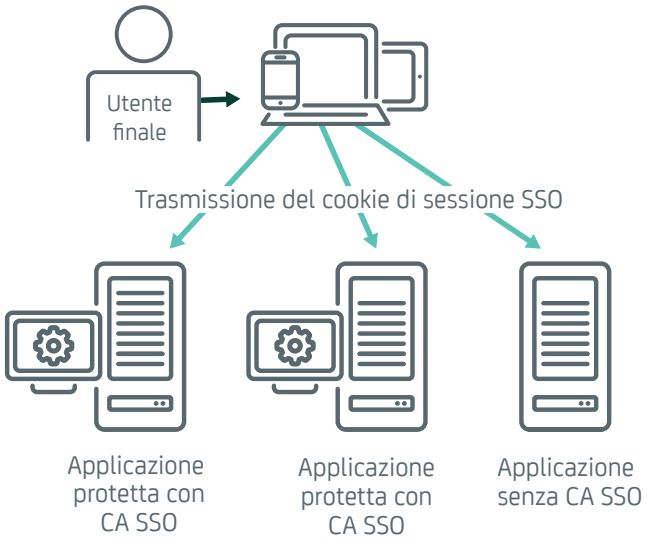
Grazie a CA SSO, gli amministratori possono configurare il comportamento dell'architettura per tutte le applicazioni o per un sottoinsieme di applicazioni. L'uso di un'architettura "solo host" può aumentare la sicurezza rendendo molto più difficile l'acquisizione di un cookie di sessione da parte di un hacker e limitando anche l'esposizione di una sessione sottratta a una determinata applicazione, fino al momento in cui i timeout per inattività o la funzionalità di session assurance non sono in grado di rilevare e interrompere la sessione rubata.

Sezione 1:

L'importanza di proteggere le sessioni CA SSO

L'hijacking delle sessioni, noto anche come hijacking di cookie, non è una minaccia nuova. È diventata un rischio quasi permanente per la sicurezza dall'avvento di HTTP 1.1 come standard e non si limita ai token di sessione di CA SSO. Secondo la OWASP Foundation, il furto di sessioni fa parte dell'attacco A2 "Broken Authentication and Session Management" nei 10 rischi più importanti per la sicurezza delle applicazioni web. Se una sessione viene sottratta, può essere riprodotta e le applicazioni web mostreranno le informazioni all'autore dell'attacco nel contesto dell'identità sottratta. Inoltre, tutti i log registreranno le richieste dell'hacker come provenienti da un utente autenticato valido, per cui l'attacco diventa estremamente difficile da rilevare.

Nella maggior parte dei deployment, la sessione CA SSO è configurata in modo da essere condivisa da tutte le applicazioni web che condividono lo stesso dominio (DNS) cookie, ad esempio qualsiasi server web in ca.com. Se da una parte è il metodo più semplice per assicurare che il cookie raggiunga tutte le applicazioni CA SSO previste, è anche il più vulnerabile perché il browser web fornirà la sessione CA SSO alle applicazioni che ne hanno bisogno ma anche a quelle che non ne hanno bisogno e tutte le applicazioni condividono un token di sessione comune.

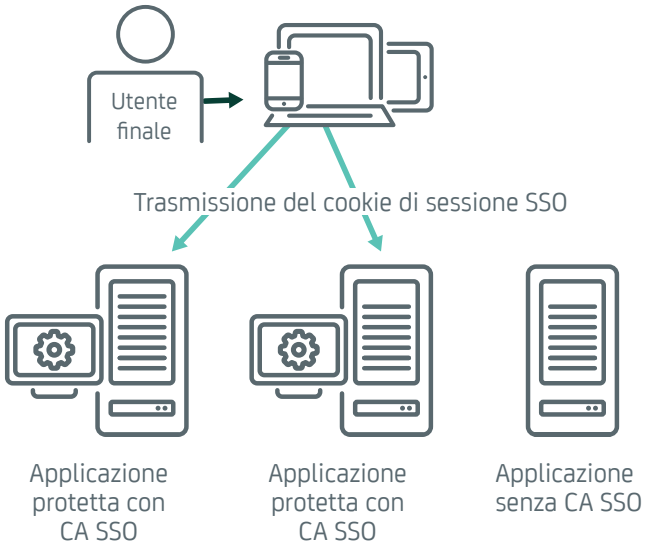


Sezione 2:

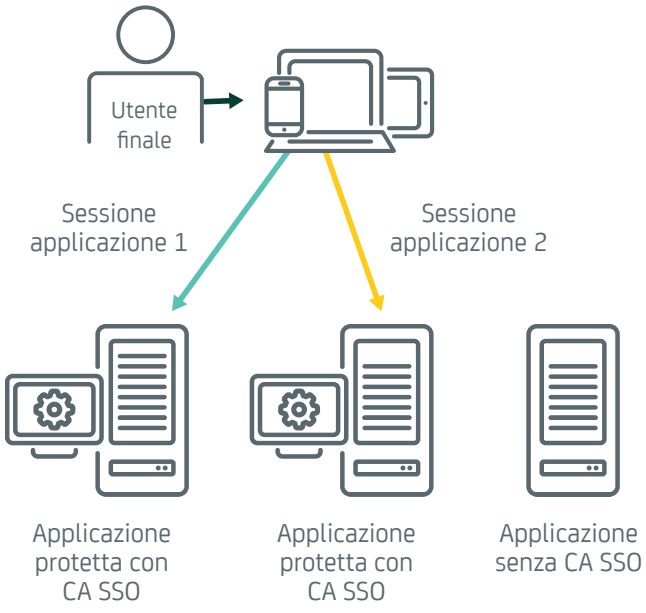
Principali impostazioni per modificare il comportamento di CA SSO

Sono disponibili diverse impostazioni che consentono di incrementare il livello di sicurezza e impedire il passaggio accidentale di una sessione alle applicazioni che non la richiedono. Queste impostazioni modificheranno il comportamento tipico di CA SSO per adattarlo a scenari con un grado di sicurezza più elevato.

La prima modifica di comportamento è l'invio del cookie di CA SSO solo alle applicazioni che lo richiedono. Questo impedisce che il cookie venga passato a siti che non hanno motivo di visualizzare la sessione. Questa variazione viene effettuata impostando l'ambito di distribuzione del cookie su specifici host anziché su tutti i server in un dominio comune.



CA SSO può essere configurato anche per l'uso di specifiche sessioni per specifiche applicazioni, riducendo ulteriormente il rischio che una sessione sottratta venga utilizzata per più applicazioni.



Principali impostazioni per controllare la sicurezza delle sessioni CA SSO

Le seguenti impostazioni sono incluse in CA SSO da molti anni e rappresentano modifiche di configurazione al comportamento degli agenti e dei gateway. Sono tutte disponibili in Agent Configuration Object (ACO).

CookieDomain

L'impostazione CookieDomain consente di definire il valore del dominio cookie utilizzato per creare i cookie mediante l'intestazione della risposta HTTP set-cookie. Il valore predefinito di questa impostazione è una stringa vuota, che indica all'agente che il dominio cookie deve essere ricavato dall'intestazione HTTP_HOST di una richiesta in base all'impostazione CookieDomainScope descritta di seguito. Il valore "NONE" indica che non deve essere impostato alcun valore del dominio cookie. In questo modo viene definito un cookie "solo server". In alternativa, è possibile impostare un valore specifico per il dominio cookie, ad esempio ".app.ca.com". L'impostazione di un valore specifico per il dominio cookie richiede cautela poiché il dominio specificato per un cookie deve corrispondere a una parte del dominio della richiesta su cui viene rilasciato. Di conseguenza, il valore del dominio cookie non può essere arbitrario. Se un determinato agente web gestirà le richieste in arrivo su più host HTTP, NON deve essere utilizzato un valore specifico per il dominio cookie, che in effetti raramente risulta necessario.

CookieDomainScope

L'impostazione CookieDomainScope controlla l'ambito di una sessione definendo il modo in cui un valore di dominio cookie verrà ricavato dall'intestazione HTTP_HOST di una richiesta. Il valore predefinito è 0. Questo valore indica l'ambito globale, che definisce il dominio cookie nel dominio di primo livello, ad esempio "ca.com". Il valore "1" non è consentito in quanto ".com", ".net" e così via non sono domini cookie consentiti. "2" corrisponde a "0". I valori superiori a 2 indicano un ambito più definito, dove il dominio di HTTP_HOST lo consente. Ad esempio, il valore "0" o "2" determinerebbe l'impostazione del dominio cookie ".ca.com" per HTTP_HOST "myserver.security.ca.com". Il valore "1" non è consentito (viene ignorato a favore del valore predefinito "0") e il valore "3" comporterebbe l'impostazione di un dominio cookie ".security.ca.com". Il valore "4" definirebbe il valore di "myserver.security.ca.com". In questo caso, tuttavia, è più appropriato impostare CookieDomain su "NONE" come descritto in precedenza. CookieDomainScope viene ignorato quando CookieDomain è impostato su NONE, che indica che devono essere utilizzati i cookie "solo server". Nel caso dei cookie solo server, l'ambito è SEMPRE il valore completo di HTTP_HOST meno un valore di porta specificato.

CookieProvider

Utilizzando i cookie solo host, e volendo comunque avere SSO tra le applicazioni, è necessaria la presenza di un sito provider di identità centralizzato che possa fornire le informazioni di sessione alle altre applicazioni. CookieProvider di CA SSO è appunto un server centralizzato progettato per passare le informazioni di sessione ad altre applicazioni web remote. Tutti i gateway o gli agenti CA SSO possono agire da provider di cookie. Gli agenti che utilizzano questo CookieProvider usano l'URL di CookieProvider specificato nell'impostazione ACO.

EnableCookieProvider

EnableCookieProvider indica a un gateway o agente SSO che può svolgere la funzione di provider di cookie. È consigliabile disattivare questa impostazione su tutti gli ACO agente tranne il provider di cookie previsto. Questo consente di impedire che un hacker acquisisca privilegi aggiuntivi se ha sottratto una sessione CA SSO per un'applicazione e tenta di utilizzarla per accedere ad altre applicazioni.

StoreSessionInServer

Tradizionalmente, i provider di cookie CA SSO inseriscono la sessione nei dati della stringa della query HTTP nell'ambito di un reindirizzamento alla destinazione finale. L'inserimento di questi dati nella stringa di query può consentire agli hacker di ottenere l'accesso alla sessione. Anziché utilizzare questo approccio, è possibile indicare al provider di cookie CA SSO di archiviare la sessione in un archivio di sessioni centralizzato e quindi passare un riferimento monouso alla sessione archiviata nella stringa di query. L'applicazione che richiede la sessione otterrà quindi la sessione dal server di policy con cui è in comunicazione, anziché leggerla direttamente dalla stringa di query. Questo approccio è analogo al profilo artifact SAML.

LimitCookieProvider

Quando si usa un provider di cookie centralizzato, questo può essere utilizzato per creare nuovi cookie di sessione CA SSO per gli agenti remoti oppure consentire a un agente remoto di creare una nuova sessione presso il provider di cookie se l'utente accede direttamente al sito remoto. Questa impostazione può imporre che tutte le autenticazioni vengano effettuate all'interno del dominio del provider di cookie centrale e rifiuterà le sessioni che vengono create in applicazioni remote. L'uso di questa impostazione dipenderà dalle policy di sicurezza e aziendali. Se è possibile usare una posizione centrale per tutte le pagine di accesso, questa impostazione è consigliata.

TrackSessionDomain

Per fare in modo che una sessione CA SSO venga utilizzata solo per il sito a cui è destinata, è possibile utilizzare l'impostazione ACO TrackSessionDomain. Questa impostazione indica all'agente web di crittografare e archiviare il dominio previsto di una sessione all'interno del cookie di sessione stesso. Durante le richieste successive, l'agente web confronta il dominio previsto all'interno del cookie di sessione con il dominio della risorsa richiesta e rifiuta il cookie di sessione se i due domini non corrispondono.

TrackCPSessionDomain

Un provider di cookie CA SSO si occupa della gestione della trasformazione di una sessione CA SSO da un dominio a un altro. Per consentire il corretto funzionamento di questa trasformazione quando viene utilizzato TrackSessionDomain, è necessario indicare al provider di cookie di rinominare il dominio all'interno della sessione in modo che possa essere utilizzato in altre posizioni. L'impostazione TrackCPSessionDomain indica al provider di cookie di convalidare il dominio del cookie di cui dispone prima di trasformarlo per un'altra applicazione. Questo evita che il provider di cookie possa essere utilizzato per trasformare i cookie in modo arbitrario da un dominio a un altro, ad esempio inviando al provider di cookie un cookie ".app1.ca.com" rubato da trasformare in ".app2.ca.com".

ValidTargetDomain

Il parametro ValidTargetDomain identifica i domini e gli host validi per i sistemi remoti durante l'elaborazione. Prima che l'utente venga reindirizzato, l'agente confronta i valori nell'URL di reindirizzamento con i domini che risultano in questo parametro. In assenza di questo parametro, l'agente reindirizza l'utente verso destinazioni in qualsiasi dominio. Questa impostazione consente di evitare gli attacchi cross-site mediante reindirizzamenti alle pagine di accesso, provider di cookie e URL di session assurance.

Sezione 3:

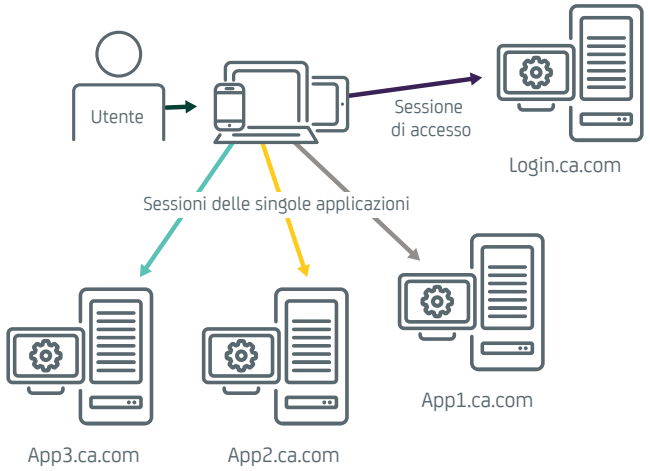
Progettare un'architettura per la massima sicurezza

L'uso di queste impostazioni può contribuire a realizzare un'architettura che prevede che ogni applicazione abbia una sessione separata utilizzabile solo per tale applicazione, richiedendo l'autenticazione di tutti gli utenti in una posizione centrale e mantenendo comunque la funzionalità SSO.

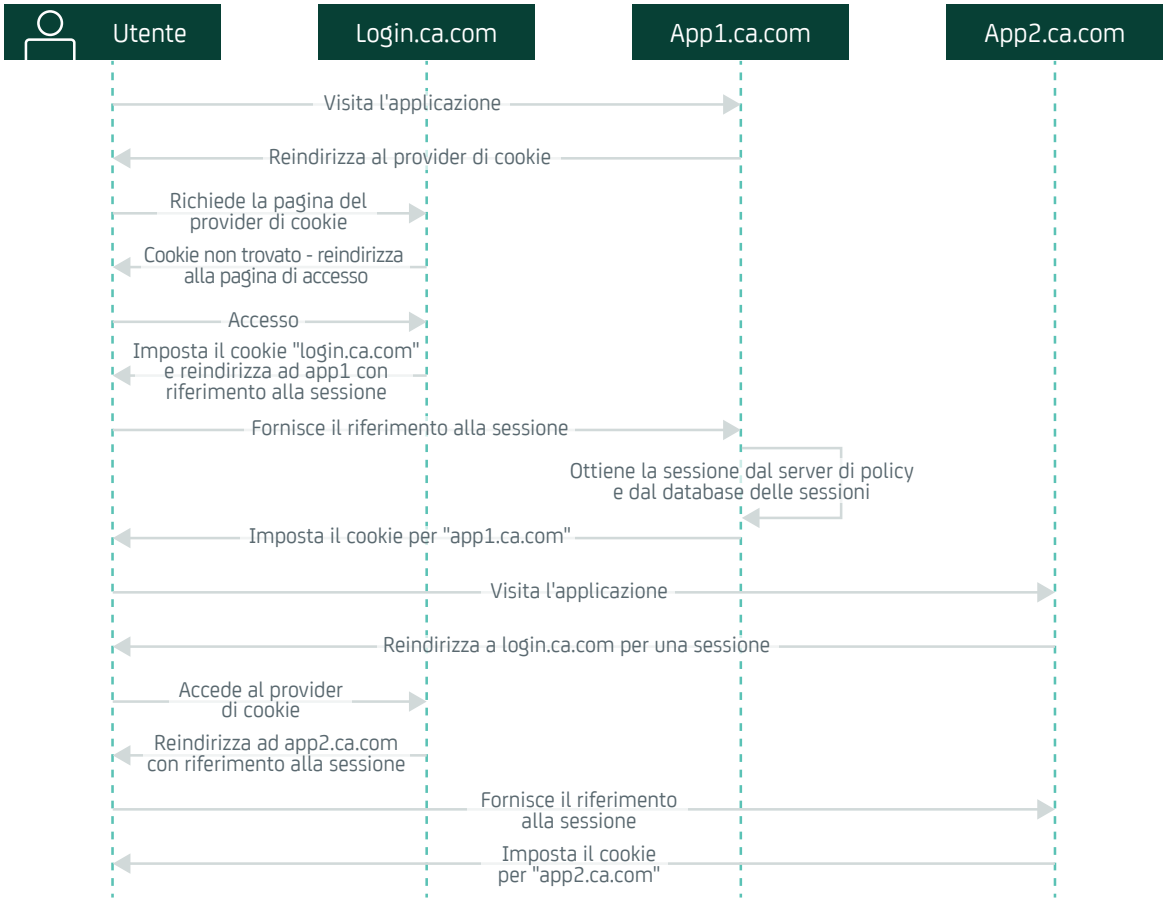
In questo esempio è presente un sito centrale, login.ca.com, che svolge la funzione di provider di cookie e ospita le pagine di accesso e più applicazioni.

	Impostazione predefinita	Login.ca.com	App1.ca.com	App2.ca.com	App3.ca.com
CookieDomain	"" (stringa vuota)	NONE	NONE	NONE	NONE
CookieDomainScope	0 (uso dell'ambito del dominio di primo livello)	Predefinito	Predefinito	Predefinito	Predefinito
CookieProvider		Predefinito	https://login.ca.com/siteminderagent/SmMakeCookie.ccc		
EnableCookieProvider	Sì	Sì	No	No	No
StoreSessionInServer	No	Sì	Sì	Sì	Sì
LimitCookieProvider	No	Sì	No	No	No
TrackSessionDomain	No	Sì	Sì	Sì	Sì
TrackCPSessionDomain	No	Sì	Predefinito	Predefinito	Predefinito
ValidTargetDomain	Tutti i domini ("")	App1.ca.com App2.ca.com App3.ca.com	Predefinito	Predefinito	Predefinito

Le impostazioni riportate sopra determinano un'architettura analoga alla seguente:



Di seguito è riportata una vista di alto livello:

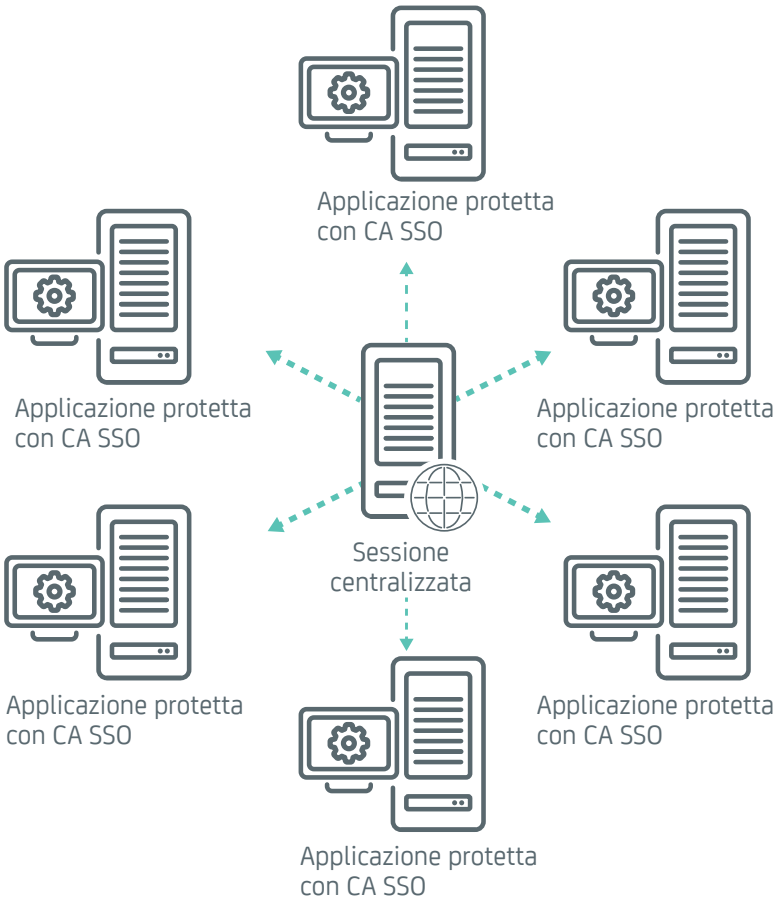


Questa architettura, unitamente ad altri controlli per le sessioni CA SSO, tra cui i cookie solo SSL e solo HTTP, Enhanced Session Assurance with DeviceDNA per il fingerprinting dei device e policy adeguate per il timeout di inattività/sessione, possono blindare un ambiente CA SSO per aumentare la sicurezza delle sessioni, mantenendo comunque la funzionalità SSO per gli utenti finali.

Sezione 4:

Conclusioni

Dato che le aziende impiegano sistemi di autenticazione avanzati multi-fattore basati sul rischio, la sicurezza dei token di sessione forniti dopo l'autenticazione assume un valore sempre più rilevante, poiché rappresentano la vulnerabilità logica più immediata nell'infrastruttura. CA SSO può gestire le sessioni e l'accesso single sign-on in un'ampia gamma di siti mediante i cookie "solo host" e può utilizzare il fingerprinting dei device per verificare che la sessione provenga dall'host per cui è stata rilasciata. L'impiego di un'architettura che utilizza cookie solo host rende molto più difficile il furto dei cookie di sessione grazie all'implementazione di una topologia a stella centralizzata al posto di un'unica sessione per l'interno domino.



Questa architettura limita anche la portata di un'eventuale esposizione in caso di compromissione di una sessione. Dato che ogni applicazione dispone di un cookie di sessione separato, in caso di furto di una sessione, il cookie di sessione rubato può essere utilizzato solo per l'applicazione a cui è destinato e non per accedere ad altre applicazioni fino a quando la funzionalità di session assurance, i timeout o altri controlli non abbiano invalidato la sessione rubata.

Sezione 5:

Riferimenti

Top 10 di OSAWP: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Sezione 6:

L'autore

Aaron Berman attualmente ricopre il ruolo di Senior Advisor per l'organizzazione sul campo di CA Technologies, con responsabilità che includono la strategia di prodotto e di vendita, la comunicazione e la collaborazione come estensione della gestione di prodotto. Vanta oltre 15 anni di esperienza nella risoluzione dei problemi, progettazione, implementazione e definizione della strategia per le soluzioni di gestione degli accessi web, inclusa la progettazione dei test di carico con 100 milioni di utenti su CA Single Sign-On (in precedenza CA SiteMinder) e CA Identity Manager (in precedenza CA IdentityMinder) e l'organizzazione di diversi eventi Federation Interop. Prima di entrare in CA Technologies e di collaborare con Netegrity, Aaron ha gestito i servizi di supporto e pre-vendita per le soluzioni di gestione degli accessi web presso Raptor Systems/Axent Technology. Aaron in precedenza è stato VP, Principal Architect per l'organizzazione dei servizi di CA Technologies. Aaron ha conseguito una laurea in informatica alla Syracuse University.

Per ulteriori informazioni, visitare il sito **ca.com/it/secure-sso**

ca technologies

È possibile entrare in contatto con CA Technologies collegandosi al sito 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 Lhttps://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CS200-112938_0215