Sicurezza Smartsheet

Un approfondimento su funzionalità, prassi e protezioni di sicurezza Smartsheet

Executive Summary

Smartsheet comprende bene che le piattaforme Software as a Service (SaaS) di livello enterprise devono fornire vari strati di difesa e tutta una serie di protezioni e controlli IT per tenere al sicuro i dati sensibili di un'azienda. È altresì importante che tali soluzioni siano flessibili e integrabili con i sistemi e i processi di sicurezza dei dati esistenti.

Questo whitepaper vuole mostrare le funzionalità, le protezioni e le prassi di sicurezza e governance di Smartsheet. Ci concentreremo soprattutto sulle funzionalità controllate dal cliente che Smartsheet consiglia di implementare per poter mantenere un ambiente di lavoro sicuro, conforme e ben gestito. Nota: questo whitepaper non include funzionalità di sicurezza che attualmente non sono ancora disponibili a livello generale.

Panoramica

Per proteggere al meglio la tua organizzazione, ti consigliamo di implementare controlli in tre aree principali: gestione di identità e accessi, governance dei dati e configurazione globale degli account. Oltre a questi argomenti, il documento include informazioni generali sulle prassi di sicurezza, privacy e conformità di Smartsheet.

- **La gestione di identità e accessi** si concentra sul controllo delle modalità di accesso degli utenti a Smartsheet, garantendo che ogni ruolo e identità degli utenti nella piattaforma si allineino a struttura e politiche dell'organizzazione. Inoltre, discuteremo di come garantire la sicurezza quando si collabora con utenti esterni, in base alle tue preferenze.

- **La governance dei dati** deve essere applicata a livello utente e nell'intera organizzazione. Per gli utenti, un approccio con privilegi minimi è l'opzione predefinita in Smartsheet, e sono disponibili controlli aggiuntivi per limitare e controllare ulteriormente la visibilità, in modo che gli utenti vedano solo ciò di cui hanno bisogno, quando ne hanno bisogno. A livello di organizzazione, parleremo sia di meccanismi semplici come la condivisione sicura e i report utente, sia di funzionalità avanzate opzionali disponibili come i criteri di uscita dei dati.

- **La configurazione globale degli account** ti permette di personalizzare l'aspetto del tuo ambiente Smartsheet in modo da allinearlo al brand dell'organizzazione. Anche qualcosa di semplice come un indizio visivo che conferma che gli utenti si trovano in un ambiente protetto dell'organizzazione può aiutare a garantire la sicurezza. Assicura la coerenza fissando branding e personalizzazione in modo che ogni asset creato sia allineato al brand.

- **I criteri di sicurezza, privacy e conformità** si riferiscono alle azioni e protezioni mantenute da Smartsheet al di fuori della nostra piattaforma per aiutare a garantire un'elevata protezione dei dati dei clienti. Smartsheet ha implementato strategie approfondite di difesa leader nel settore tramite una combinazione di persone, processi e tecnologie per proteggere riservatezza, integrità e disponibilità di ambienti e asset Smartsheet.

Sommario

Gestione delle identità

Gestire l'identità di un utente in Smartsheet e, pertanto, il suo accesso al sistema è importante tanto quanto gestire i dati nella piattaforma.

Nelle fasi iniziali dell'implementazione di Smartsheet, deciderai quale metodo di autenticazione utilizzare. Smartsheet offre varie opzioni: e-mail e password, e Single Sign-On (SSO) da Google, Microsoft, provider SAML 2.0 e Apple.

Puoi selezionare uno o più metodi per la tua organizzazione, ma ti consigliamo di applicare un singolo metodo di autenticazione SSO per tutti gli utenti, mantenendo disabilitati gli altri metodi. Ti consigliamo anche di aggiungere un altro strato di sicurezza implementando l'autenticazione a più fattori (MFA) quando configuri l'SSO.

Smartsheet dispone di un set robusto di API REST. L'API Smartsheet usa OAuth 2.0 per l'autenticazione e l'autorizzazione. È richiesta un'intestazione HTTP con un token di accesso per autenticare ogni richiesta. Per una maggiore sicurezza, usa OAuth 2.0 per tutte le integrazioni che crei come best practice.

Gestione degli accessi

Gestire gli utenti e il loro accesso è una funzione amministrativa fondamentale che può influire sia sulla sicurezza che sull'adozione di Smartsheet da parte della tua organizzazione. Le organizzazioni devono infatti trovare il giusto equilibrio tra la collaborazione e la gestione dei rischi legati a dati e team sempre più distribuiti. Per supportare questo approccio, Smartsheet offre tre modelli di governance distinti in linea con le modalità primarie con cui i nostri clienti desiderano gestire l'applicazione.

Modelli di governance Smartsheet

Il primo approccio è il nostro modello decentralizzato (federato), dove sono unità di business individuali a controllare direttamente i propri acquisti e piani. In questo modello, l'IT non è tipicamente coinvolto nell'amministrazione e fatturazione dei piani, e governance e gestione degli utenti sono affidate ai singoli reparti. Questo modello si applica generalmente alle prime fasi delle aziende nel percorso Smartsheet.

Il nostro secondo approccio è il modello centralizzato (consolidato) dove i piani Smartsheet sono stati tutti consolidati in un singolo abbonamento gestito dall'IT. In questo modo si ha un controllo diretto su spesa, gestione degli utenti e controlli di sicurezza. Questo modello è ideale per i team IT che vogliono mantenere una supervisione efficace su ogni aspetto della propria esperienza Smartsheet.

Infine, il nostro modello condiviso (ibrido) vuole fornire un approccio ambivalente, dove l'IT controlla le impostazioni dell'organizzazione tramite Manager Piano Aziendale, mentre licenze e gestione degli utenti sono gestite direttamente dagli amministratori di sistema della linea di business. Anche la fatturazione è suddivisa in base ai piani, cosa che supporta la divisione in reparti o un modello in cui le spese di Smartsheet sono incorporate nei budget di reparto anziché fatturate centralmente all'IT.

Per garantire standard di sicurezza elevati, Smartsheet consiglia di utilizzare i nostri modelli condivisi o centralizzati, che forniscono un controllo IT più diretto sui piani.

Amministrazione utenti

Man mano che vari team nella tua azienda adottano singolarmente Smartsheet per le proprie esigenze, potrebbero essere creati vari piani separati. Fusioni e acquisizioni possono contribuire a creare un ambiente con diversi piani Smartsheet.

Per gestire gli utenti in questi piani tramite il modello decentralizzato, ti consigliamo di abilitare l'Individuazione account per ciascuno di essi. Quando nuovi utenti utilizzano Smartsheet, loro o altre persone nel dominio della tua organizzazione possono vedere un elenco dei piani Smartsheet associati alla tua azienda, disponendo così di metodi centralizzati per richiedere di unirsi a tali piani esistenti anziché iniziarne uno nuovo. Tali richieste vengono automaticamente instradate agli amministratori di sistema (tramite il Centro dell'Amministratore Smartsheet) per la revisione e l'approvazione.

Se hai più piani separati e vuoi gestire gli utenti con il modello centralizzato, potresti dover completare un consolidamento dell'account. Nota: i clienti con funzionalità Advance come Dynamic View, Connettori e Control Center dovranno collaborare con l'assistenza Smartsheet per alcuni aspetti del consolidamento.

Se stai usando il modello condiviso e Manager Piano Aziendale, una best practice consiste nell'organizzare i piani in base a reparti/team/centri di costo. In questo modo potrai definire una politica per assegnare automaticamente gli utenti ai piani pertinenti in base alla loro affiliazione a una di queste entità.

Gestione degli utenti

Smartsheet comprende che aggiungere un utente alla volta non sia più applicabile con decine, centinaia o persino migliaia di utenti. Pertanto, ti consigliamo per iniziare di sfruttare la funzionalità di importazione utenti in blocco nel Centro dell'Amministratore per aggiungere facilmente fino a 1000 utenti alla volta alla tua organizzazione Smartsheet. In modo simile, puoi anche usare gli aggiornamenti in blocco per modificare i ruoli in massa per gli utenti esistenti.

Fusioni o acquisizioni spesso portano a rebranding, con gli utenti che ottengono nuovi indirizzi e-mail. Unione utenti può aiutarti ad aggiornare in blocco gli indirizzi e-mail primari degli utenti e a eliminare eventuali account duplicati.

Un piano Smartsheet consolidato può usare due funzionalità aggiuntive per semplificare e automatizzare ulteriormente la gestione degli utenti.

- Il provisioning automatico degli utenti (UAP) automatizza il processo di aggiunta di utenti a un account aziendale. Conduci automaticamente gli utenti nel tuo account quando accedono a Smartsheet con il loro indirizzo e-mail aziendale. Inoltre, puoi scegliere se concedere licenze agli utenti o far sì che vengano aggiunti automaticamente all'account come collaboratori senza licenza (gratuiti).

    - Se hai scelto il nostro modello consolidato, ti consigliamo di abilitare il provisioning automatico dell'utente in modo che i dipendenti vengano aggiunti automaticamente all'account centrale controllato dall'IT.

    - Se usi il nostro modello condiviso (e se la tua organizzazione ha informazioni di reparto/centro dei costi documentate per il tuo elenco utenti), ti consigliamo di attivare il provisioning automatico dell'utente, di modo che sia possibile importare le informazioni per associare automaticamente gli utenti al piano corretto quando richiedono una licenza. Può anche essere utilizzato per automatizzare il movimento degli utenti senza licenza tra i piani.

- Integrazione di directory ti permette di sincronizzare direttamente i tuoi utenti Microsoft Azure Active Directory (AD) in Smartsheet. Integra Smartsheet nella tua automazione esistente in Azure AD per automatizzare pienamente l'onboarding e l'offboarding degli utenti, riducendo al minimo il rischio che gli utenti rimangano o tornino nei propri account Smartsheet. Come vantaggio aggiuntivo, gli attributi AD a livello di utente come reparto/centro di costi/divisione sono inclusi in un Chargeback Report Smartsheet, disponibile nel Centro dell'Amministratore e utilizzabile per facilitare i riaddebiti interni. Una best practice consigliata consiste nel sincronizzare tutti gli utenti nella Directory nell'account Smartsheet della tua organizzazione. In questo modo, tali utenti non potranno creare account Smartsheet aggiuntivi di "shadow IT" quando accedono per la prima volta. Come secondo strato difensivo, puoi mantenere abilitato il provisioning automatico dell'utente per tutti gli utenti che potrebbero non essere già sincronizzati tramite la Directory.

Quando una persona lascia la tua organizzazione, è importante rimuoverne l'accesso a Smartsheet. Forniamo due modi per farlo. L'eliminazione di un utente rimuove l'utente stesso e i relativi asset dal tuo account Smartsheet, ma ciò può causare la rimozione di elementi ancora in uso, interrompendo potenzialmente il funzionamento di soluzioni che fanno affidamento su tali dati. Smartsheet consiglia invece la disattivazione degli utenti. In questo modo, il loro accesso a Smartsheet sarà sempre completamente bloccato, ma manterranno l'accessibilità ai loro contenuti, così da evitare problematiche relative alla stabilità della soluzione o al trasferimento di proprietà

Ruoli e tipi di utenti in Smartsheet

A prescindere dal metodo di provisioning dell'utente, dovrai determinare i ruoli Smartsheet per le persone nella tua organizzazione.

Nota: l'assegnazione di un ruolo non dà alla persona l'accesso agli asset Smartsheet nella tua organizzazione. Gli asset devono essere condivisi direttamente con tali persone. Pertanto, saranno sia il ruolo che le autorizzazioni di accesso agli asset a determinare ciò che gli stakeholder possono vedere e fare in Smartsheet. Smartsheet supporta i seguenti ruoli primari:

- Utente con licenza: usa funzionalità con licenza, come la creazione di fogli.

- Amministratore di gruppo: crea e gestisce gruppi Smartsheet.*

  *I ruoli Amministratore di gruppo devono anche essere Utenti con licenza

- Amministratore di sistema: gestisce utenti, impostazioni dell'account e controlli di sicurezza.

Ti consigliamo fortemente di assegnare almeno due Amministratori di sistema attivi all'account Smartsheet dell'organizzazione, in modo che non ci siano interruzioni in caso uno dei due non sia disponibile in un dato momento.

Gli Amministratori di gruppo possono creare gruppi Smartsheet, consentendo agli utenti di condividere contenuti con il gruppo anziché doverli condividere singolarmente con ciascun membro. Gli Amministratori di gruppo possono gestire solamente i gruppi di cui sono proprietari. In base alle necessità, per limitare la collaborazione esterna, limita le appartenenze ai gruppi ai soli stakeholder nella tua organizzazione.

Se non assegni uno dei ruoli precedenti a un utente, il suo accesso sarà limitato solo agli asset Smartsheet (fogli, report, dashboard o WorkApp) condivisi con lui. Per creare asset Smartsheet, gli stakeholder devono essere utenti con licenza e possono richiederne una direttamente tramite l'app Smartsheet. Gli Amministratori di sistema possono tracciare e rispondere alle richieste singolarmente o in blocco tramite la sezione Gestione delle richieste di licenza del Centro dell'Amministratore. Se disponi già di un processo per gestire le richieste di licenza, prendi in considerazione l'uso di una Schermata di aggiornamento personalizzata per indirizzare gli utenti a inviare le proprie richieste di licenza tramite tali processi interni.

Collaboratori esterni

Qualsiasi stakeholder al di fuori del tuo dominio con cui hai condiviso gli asset Smartsheet è considerato un collaboratore esterno. Smartsheet permette alla tua organizzazione di collaborare liberamente con parti esterne affidabili, senza costi associati per loro. Per garantire la sicurezza nelle collaborazioni esterne, ti consigliamo di sfruttare tre controlli amministrativi centrali:

Condivisione sicura ti permette di specificare domini o indirizzi e-mail affidabili e autorizzati per la collaborazione esterna.

Report di accesso ai fogli forniscono un elenco di collaboratori esterni che hanno accesso ai contenuti Smartsheet della tua organizzazione.

Revoca dell'accesso agli elementi, centralmente tramite il Centro dell'Amministratore, di modo che i collaboratori esterni siano rimossi dai contenuti a cui non hanno più bisogno di accedere.

Governance dei dati

Una governance dei dati efficace è indispensabile per le aziende di oggi che vogliono garantire che le informazioni che posseggono siano create, usate, condivise e protette in conformità alle normative applicabili, alla politica aziendale e alle best practice del settore.

Questi controlli sono necessari non solo per scopi normativi ma anche per garantire efficienza, riservatezza e continuità del business.

A livello dell'utente, l'organizzazione deve fornire strumenti efficaci per limitare la visibilità, mostrando solo le informazioni pertinenti ai rispettivi stakeholder.

A livello dell'organizzazione, l'azienda deve disporre di strumenti applicabili per creazione e applicazione efficaci della politica.

Governance dei dati a livello utente

La maggior parte degli utenti conosce i livelli di autorizzazione in Smartsheet (visualizzatore, editor, amministratore e proprietario). Dynamic View e WorkApps forniscono controlli aggiuntivi e più granulari, oltre alla flessibilità, permettendo di disporre di funzionalità di governance dei dati efficaci a livello utente. Limitare l'accesso ai soli contenuti più pertinenti permette di garantire l'efficienza dei processi (poiché gli utenti devono concentrarsi necessariamente sugli elementi che richiedono attenzione), ma anche la sicurezza, estendendo l'approccio di Smartsheet dei privilegi minimi di default su una scala più granulare.

Dynamic View

Non tutti i processi aziendali necessitano di una trasparenza completa. Molti di questi, come gestione degli ordini, collaborazione tra vendor, progetti che includono team interni ed esterni, richiedono un controllo rigoroso su cosa viene condiviso con chi.

Dynamic View permette una collaborazione senza compromettere la riservatezza. Tramite Dynamic View, i proprietari dei fogli possono condividere in modo selettivo righe e campi pertinenti con collaboratori

specifici, senza condividere i fogli sottostanti. Sono così possibili vari casi d'uso in cui utenti business specifici possono condividere in modo selettivo elementi con i vendor, i team interni ed esterni misti o tra un'organizzazione e l'altra, portando alla collaborazione solo in determinati campi. Tutti hanno accesso alle informazioni di cui hanno bisogno e solo a queste.

WorkApps

WorkApps ti permette di snellire il tuo lavoro e semplificare la collaborazione con app semplici da navigare create direttamente a partire dai tuoi fogli, moduli, dashboard, report e molto altro. Puoi personalizzare l'esperienza dell'app per i membri del tuo team in base al ruolo di ciascuno, e lavorare in gruppo partendo dalle stesse serie di dati sottostanti. Le app scalano utilizzando la stessa stessa sicurezza di classe enterprise e multilivello della piattaforma Smartsheet.

WorkApps elimina la necessità di condividere gli asset sottostanti che costituiscono la WorkApp. Puoi creare una WorkApp con una visualizzazione filtrata di fogli e report selezionati, ma nessuno di questi fogli e report deve essere per forza condiviso con l'utente finale. Quest'ultimo, infatti, vedrà solo la visualizzazione "WorkApp" di questi asset.

Controlli dei criteri di governance dei dati a livello organizzazione

Smartsheet permette agli amministratori di garantire che le funzionalità della piattaforma vengano usate rispettando i criteri di governance dell'organizzazione. Questi controlli permettono agli amministratori di implementare linee guida di governance efficaci per garantire che i dati vengano gestiti correttamente e solo da coloro che devono interagire con essi.

Gli amministratori possono scegliere come gli utenti interagiranno con determinate funzionalità. I proprietari dei fogli devono poter pubblicare i propri fogli e creare nuove automazioni? Disponi di un sistema di archiviazione specifico da cui è necessario allegare i file? I collaboratori esterni devono poter scaricare i contenuti condivisi con loro? Questi sono esempi di domande che gli amministratori dovrebbero porsi per valutare con efficacia i controlli da implementare nell'organizzazione.

Questi controlli dei criteri si estendono anche alla condivisione sicura. Se vuoi limitare la condivisione di dati e asset a domini o indirizzi e-mail specifici, questo è lo strumento da usare. Come detto in precedenza, la condivisone sicura determina anche se la tua organizzazione può condividere elementi Smartsheet con altre organizzazioni, come vendor e partner.

Controllo widget Contenuto Web

Le dashboard supportano la possibilità di integrare contenuti interattivi (video, diagrammi, documenti e altro). Gli amministratori hanno la possibilità di abilitare o disabilitare questa funzionalità e di definire un elenco approvato di domini supportati per il widget Contenuto Web. Come best practice, ti consigliamo di limitarlo ai domini interni dell'azienda.

Autorizzazioni di automazione

Controlla chi può ricevere automazione dai fogli. Le opzioni sono organizzate da Con restrizioni (abilita azioni solo per gli utenti in condivisione sul foglio) a Senza restrizioni (dove l'automazione è applicabile a qualsiasi indirizzo e-mail e integrazione di terzi, come Slack). Ti consigliamo di rivedere questo controllo per assicurarti che la sua configurazione corrisponda al livello di collaborazione interna ed esterna desiderato dalla tua organizzazione.

Controlli sugli allegati

Determina se i membri del piano possono caricare file dai propri computer, allegando un collegamento (URL) a un sito, o da servizi di archiviazione cloud terzi come Google Drive, OneDrive, Box, Dropbox, Evernote o Egnyte. Per prevenire l'inserimento di dati da origini non approvate, abilita solo i provider di allegati approvati per l'uso in base ai criteri interni della tua organizzazione.

Controlli di pubblicazione

La pubblicazione di un foglio, di un report o di una dashboard genera un URL univoco a cui chiunque può accedere senza accedere a Smartsheet, e il codice iframe che puoi incorporare nel codice sorgente di un sito web per visualizzare il foglio o il report.

Puoi impedire la pubblicazione di fogli, report, dashboard e iCal: il pulsante Pubblica non verrà più visualizzato sull'asset Smartsheet. Puoi anche restringere l'accesso agli elementi pubblicati ai soli utenti all'interno dell'organizzazione Smartsheet. Abbiamo riscontrato che i clienti attenti alla sicurezza in genere tendono a consentire la pubblicazione, ma limitano l'accesso agli elementi pubblicati ai soli utenti all'interno del loro account.

Condivisione sicura

Usa questa funzionalità per limitare la condivisione in base al dominio o a indirizzi e-mail specifici, ad esempio per garantire che i fogli siano condivisi solo con persone con un indirizzo e-mail aziendale. Smartsheet consiglia fortemente di implementare la condivisione sicura per controllare la collaborazione esterna. Inoltre, per semplificare aggiornamenti e manutenzione del tuo elenco di condivisione sicura, ti consigliamo di raccogliere le richieste di aggiornamento tramite un modulo web Smartsheet.

Controlli degli invii dei moduli offline

Quando usi l'app per dispositivi mobili, Smartsheet abilita automaticamente l'invio dei moduli offline, per supportare i casi d'uso in cui gli utenti potrebbero non avere una connessione stabile (ad esempio nei cantieri edilizi). Questo controllo permette agli amministratori di disattivare o riattivare gli invii dei moduli offline, per controllare se un utente possa avviare l'app per dispositivi mobili senza una connessione, per inviare i moduli.

Controlli di integrazioni per la comunicazione

Smartsheet supporta Google Chat, Microsoft Teams, Slack e Cisco Webex come servizi di comunicazione. Gli amministratori dell'account possono abilitare uno o più servizi, a tua discrezione.

Registrazione e reporting

Puoi scaricare report che coprono vari aspetti dell'utilizzo di Smartsheet nella tua organizzazione per una visibilità costante su utilizzo, utenti, contenuti, fatturazione e accesso di Smartsheet:

Report di accesso al foglio

Genera un file Excel che elenca i nomi di tutti i fogli, i report e le dashboard di proprietà degli utenti con licenza sull'account, il nome del workspace in cui sono salvati gli elementi (se applicabile), i collaboratori con cui è stato condiviso ciascun foglio e il timestamp dell'ultima modifica. Ti consigliamo di rivedere periodicamente questo report per controllare l'elenco dei collaboratori esterni che hanno accesso agli asset di proprietà di persone nella tua organizzazione.

Report degli elementi pubblicati

Genera un file Excel contenente l'elenco degli elementi che sono stati pubblicati. Ideale per la sicurezza dei dati o per tracciare chi ha pubblicato determinati elementi. Usa questo report per prendere decisioni informate sulla configurazione del controllo su Pubblica, in base alle necessità.

Report elenco utenti

Genera un file Excel che elenca tutti i membri (invitati e attivi) sull'account, un timestamp di quando sono stati aggiunti all'account, i loro livelli di accesso (Amministratore di sistema, Amministratore di gruppo e così via), il numero dei fogli da loro posseduti e il timestamp dell'ultimo accesso a Smartsheet.

Report della cronologia di login

Gli Amministratori di sistema su account multiutente possono utilizzare il Centro dell'Amministratore per ricevere via e-mail un file Excel con un elenco cronologico degli accessi recenti.

Chargeback Report

Disponibile nel Centro dell'Amministratore. I clienti che usano l'integrazione di directory possono usarlo per facilitare i chargeback interni. Vengono aggiunte colonne per divisione, reparto e centro di costi al report esistente creato quando i clienti scaricano il proprio elenco utenti, fornendo i dati necessari per eseguire il reporting di chargeback interno.

Per un tracciamento ancor più granulare delle azioni degli utenti a livello di foglio, dashboard e cella, puoi usare il log delle attività, la cronologia cella e le colonne di sistema.

- **Log delle attività:** fornisce un audit trail delle modifiche apportate a un asset, indica chi le ha apportate e quando sono state apportate. Ciò include modifiche come l'eliminazione delle righe (con i dati eliminati), chi ha visualizzato l'elemento e le modifiche alle autorizzazioni di condivisione.

- **Cronologia cella:** visualizza un log delle modifiche apportate a livello di cella, chi ha apportato quali modifiche e quando le modifiche sono state apportate. Gli utenti possono copiare e incollare con facilità la cronologia cella per ripristinare le informazioni precedenti che potrebbero essere state eliminate o modificate per errore.

- **Colonne di sistema:** mostrano l'ora dell'ultima modifica di ciascuna riga e il collaboratore che ha apportato tale modifica.

Controlli avanzati di governance dei dati

Smartsheet offre svariate funzionalità avanzate per il controllo della governance di dati per i clienti con necessità di sicurezza dei dati molto rigorose. Queste funzionalità sono incluse in Smartsheet Advance Platinum e Smartsheet Safeguard.

Chiavi di crittografia gestite dal cliente

Smartsheet utilizza la crittografia per salvaguardare i dati dei clienti e aiutarli a mantenere il controllo su di essi. Le chiavi di crittografia gestite dal cliente (CMEK) sono pensate per le organizzazioni con dati sensibili o normati che richiedono una gestione tramite una propria chiave di crittografia. Tali chiavi permettono alle organizzazioni enterprise di usare le applicazioni SaaS cloud e mantenere al contempo un controllo sui dati paragonabile a quello di un'installazione on-premise, aggiungendo un livello di crittografia gestito dal cliente all'archiviazione dei dati Smartsheet per supportare criteri di sicurezza e governance avanzati.

Nota: per usare le chiavi di crittografia gestite dal cliente (CMEK), i clienti devono avere accesso ad Amazon Web Services Key Management Service (AWS KMS), perché le chiavi dei clienti sono configurate e gestite direttamente in AWS.

Smartsheet usa le CMEK per crittografare i dati della tua organizzazione in modo che rimangano sempre sotto il tuo controllo. In particolare, Smartsheet non archivia o controlla tali chiavi di crittografia e deve richiederle e recuperarle da AWS Key Management Service (KMS) del cliente ogni volta che necessita di accedere ai dati del tuo foglio.

Poiché è la tua organizzazione a controllare le CMEK archiviate in AWS Key Management System, puoi revocare l'accesso Smartsheet a tali chiavi e, quindi, l'accesso ai dati in ogni momento. Distruggendo le chiavi master in AWS Key Management System, la tua organizzazione può di fatto eliminare i tuoi dati dai sistemi Smartsheet. Un malintenzionato con una copia del database, del codice sorgente e delle chiavi di crittografia cloud di Smartsheet non potrebbe comunque leggere i dati crittografati con le chiavi di crittografia gestite dal cliente.

Criteri di uscita dei dati

La condivisione dei dati comporta sempre alcuni rischi, ma quando si tratta di contenuti particolarmente riservati è fondamentale garantire che i dati aziendali rimangano solo nel tuo account e sotto il tuo controllo.

Gli Amministratori di sistema possono usare i criteri di uscita dei dati per proteggere le informazioni riservate tramite controlli granulari su come questi dati possono essere esportati all'interno e all'esterno dell'organizzazione.

I criteri di uscita dei dati possono essere implementati per impedire ai collaboratori interni ed esterni di intraprendere le seguenti azioni su fogli, report e dashboard:

- Salva come nuovo
- Salva come modello
- Invia come allegato
- Pubblica
- Stampa
- Esporta

Gli utenti che tentano un'azione vietata riceveranno una notifica di comportamento proibito a causa del criterio di uscita dei dati implementato dall'organizzazione.

Questi limiti sono pensati per impedire ai collaboratori di salvare o condividere informazioni riservate per scopi illeciti.

Reporting degli eventi

Per garantire la sicurezza delle informazioni, molte aziende richiedono approfondimenti costanti su come vengono utilizzate le loro applicazioni aziendali come Smartsheet. È buona cosa mantenere la visibilità su quanto segue:

- Chi crea fogli
- Chi crea workspace
- Chi elimina oggetti
- Chi ha condiviso un foglio e con chi

Il Reporting degli eventi fornisce visibilità granulare su comportamento e attività degli utenti nell'account Smartsheet della tua organizzazione. Questa funzionalità ti permette di monitorare la perdita di dati e identificare i modelli anomali di utilizzo, in modo da poter applicare criteri di sicurezza e conformità organizzative in modo più rigoroso.

Il Reporting degli eventi fornisce un feed di dati JSON degli eventi di utilizzo di Smartsheet ("Eventi") con un piano (org) a cui si fa accesso tramite l'API di Reporting degli eventi. Il servizio crea report su oltre 120 eventi in Smartsheet e archivia fino a sei mesi di dati, a partire dalla data di abilitazione del feed.

Per trarre vantaggi da tale feed, i dati di Reporting degli eventi sono tipicamente integrati in altri sistemi di sicurezza che forniscono monitoraggio, notifica, creazione e applicazione di criteri e prevenzione della perdita dei dati. Queste app sono vendute da terze parti, solitamente sistemi broker di sicurezza dell'accesso cloud (Cloud Access Security Broker, CASB), di gestione di informazioni ed eventi di sicurezza (Security Information and Event Management, SIEM) o una combinazione di CASB e SIEM. A volte, le aziende sviluppano i propri sistemi di monitoraggio e risposta anziché affidarsi a quelli forniti da terze parti.

Casi d'uso chiave del Reporting degli eventi:

- Prevenzione della perdita di dati
- Gestione di dati personali identificabili (PII)
- Governance dei dati
- Ottenimento di insight sulla collaborazione

Controlli sulla conservazione dei dati

Più contenuti sono presenti nelle applicazioni SaaS della tua organizzazione, più rischi correrà il tuo business.

I controlli sulla conservazione dei dati di Smartsheet forniscono alle organizzazioni la possibilità di creare una politica che indichi i contenuti da eliminare in base ai criteri da applicare.

Questi criteri possono essere basati sulla data di creazione di un foglio o sull'ora dell'ultima modifica, garantendo così che solo i contenuti attivi o recenti siano conservati nell'istanza di Smartsheet e limitando il profilo del rischio.

Configurazione account globale

La sicurezza degli account non si limita a funzionalità tecniche come crittografia dei dati, classificazione o opzioni di autenticazione. La sicurezza può anche significare semplicemente l'apposizione del logo dell'organizzazione su ogni elemento che le appartiene.

I controlli di configurazione account globale ti permettono di implementare branding visuale (e altre restrizioni) per far sapere agli utenti che stanno accedendo alle informazioni corrette.

Gli Amministratori di sistema possono aggiungere loghi globalmente per portare l'implementazione Smartsheet in linea con i requisiti di branding dell'organizzazione. Sfrutta il blocco del branding per assicurarti che ogni nuovo asset abbia lo stesso brand.

I controlli della personalizzazione e le configurazioni degli account Smartsheet ti permettono anche di configurare schermate di benvenuto personalizzate. Puoi creare schermate guida personalizzate con descrizioni su come iniziare, schermate di richiesta licenza per aiutare gli utenti a contattarti o schermate di benvenuto personalizzate e brandizzate che vengono visualizzate all'accesso di un utente. Le schermate possono includere un requisito di approvazione dei termini di servizio da parte dell'utente prima che possa accedere ad altri dati.

La combinazione di un'identità visiva coerente con informazioni personalizzate aiuta gli utenti a sapere che stanno accedendo agli strumenti e ai dati giusti, per una maggiore sicurezza

Prassi di sicurezza, privacy e conformità di Smartsheet

Tramite un approccio olistico, i programmi di sicurezza informatica, privacy e protezione dei dati di Smartsheet hanno inizio dai criteri di sicurezza dei dati strategici definiti e supportati dall'Information Security Steering Committee (ISSC) e dal team di leadership esecutiva di Smartsheet. Questi criteri sono pensati per allinearsi alle prassi di gestione dei rischi strategiche di un'organizzazione, per gestire e monitorare in modo proattivo i rischi di sicurezza, per promuovere tale sicurezza tramite una maturità dei processi e un'architettura di sistema efficiente e per permettere agli utenti di effettuare decisioni oculate sui rischi di sicurezza grazie a formazione e consapevolezza.

Sicurezza dei dati

Creiamo la sicurezza nella nostra piattaforma per garantire che la tua risorsa più preziosa, i tuoi dati, sia protetta. Smartsheet collabora con terze parti per condurre audit delle nostre prassi di sicurezza, incluse valutazione e attestazione SOC2 Type II e valutazioni di sicurezza tecniche di terze parti con aziende specializzate in penetration test. Inoltre, il programma di gestione delle vulnerabilità di Smartsheet automatizza identificazione e correzione delle vulnerabilità di rete e sistema negli ambienti aziendali e di produzione di Smartsheet. Smartsheet utilizza la crittografia per salvaguardare i tuoi dati e aiutarti a mantenere il controllo su di essi. Ecco ciò su cui puoi fare affidamento con Smartsheet: tutti i dati vengono archiviati in modo robusto con codici cifrati approvati dal National Institute of Standards and Technology (NIST), tecnologia Transport Layer Security (TLS), crittografia a riposo AES a 256 bit e il servizio Amazon S3 per archiviare e servire i file caricati.

Privacy

In Smartsheet, diamo valore alla tua privacy e rispettiamo il tuo diritto di sapere come le informazioni che ti riguardano vengono raccolte e utilizzate. La nostra informativa sulla privacy descrive come Smartsheet raccoglie, utilizza e divulga le informazioni personali ed altre informazioni che raccogliamo attraverso i nostri siti web, le nostre applicazioni mobili e la piattaforma di esecuzione del lavoro Smartsheet.

- Riconosciamo i diritti di privacy dei nostri clienti potenziali, clienti effettivi e partner e rispettiamo le normative globali sulla privacy, incluso il Regolamento generale sulla protezione dei dati (GDPR) dell'UE.

- Offriamo un Data Processing Agreement (DPA) per i clienti che richiedono termini specifici per il trattamento dei contenuti che includono dati personali. Se è stata determinata la necessità di un DPA con Smartsheet, è possibile inviare un modulo per l'accettazione dei termini del DPA alla pagina smartsheet.com/legal/DPA

Gestione operativa

Abbiamo implementato politiche e procedure progettate per garantire che i tuoi dati siano sicuri e che ne vengano effettuati backup su più ubicazioni fisiche. I nostri team valutano continuamente le nuove minacce alla sicurezza e implementano contromisure aggiornate progettate per impedire l'accesso non autorizzato o tempi di inattività non programmati del Servizio di abbonamento. L'accesso a tutti i sistemi di produzione e i dati Smartsheet è limitato ai membri autorizzati del team Technical Operations di Smartsheet, in base ai principi dei privilegi minimi e della necessità effettiva. Smartsheet pubblica le informazioni sullo stato dei sistemi nel sito dello stato di Smartsheet. Smartsheet avvisa solitamente i clienti in caso di incidenti di sistema rilevanti via e-mail e/o messaggio di testo se si sono iscritti agli aggiornamenti automatici sul sito dello stato di Smartsheet.

Sicurezza, continuità e ridondanza dei data center

Collaboriamo con partner di hosting riconosciuti nel settore per permettervi di fornire servizi alla vostra organizzazione in maniera riservata su una piattaforma affidabile. Disponiamo di ridondanza dei dati su più siti, con hosting in strutture AWS. Le nostre strutture sono valutate e certificate SOC 1, SOC 2, ISO 27001 e FISMA. Il nostro monitoraggio include protocolli di scansione biometrica, sorveglianza continua e una gestione 24/7 dell'ambiente di produzione. Smartsheet dispone di processi interni e piani per gestire al meglio eventi di continuità aziendale e scenari di ripristino di emergenza. Questi piani vengono rivisti e testati ogni anno e sono distribuiti al personale pertinente nell'organizzazione. I nostri data center sono geograficamente isolati l'uno dall'altro (circa 970 chilometri) per impedire che, in caso di disastri naturali su larga scala, vengano interessati allo stesso tempo.

Audit e certificazioni

I seguenti audit e certificazioni di sicurezza e privacy sono applicabili ai servizi applicativi core di Smartsheet.

- **SOC 2/SOC 3:** Smartsheet si sottopone a esami e test annuali come parte del processo di audit SOC. I report di audit risultanti attestano l'efficacia operativa e di progettazione dei controlli interni nella nostra azienda, incluse sicurezza, disponibilità e riservatezza.

- **Certificazione Privacy Shield UE-USA e Svizzera-USA:** i dati dei clienti inviati ai Servizi coperti rientrano nell'ambito di una certificazione annuale del Privacy Shield Framework UE-USA e del Privacy Shield Framework Svizzera-USA come delineato del Dipartimento del Commercio degli Stati Uniti. La certificazione corrente è disponibile alla pagina privacyshield.gov/list cercando “Smartsheet”.

- **FedRAMP (moderato):** Smartsheet è stata selezionata per il programma FedRAMP Connect dalla Joint Authorization Board (JAB), che ha dato priorità a Smartsheet Gov per la certificazione in base alla richiesta degli enti governativi federali. Smartsheet Gov è un ambiente Smartsheet separato con stato FedRAMP autorizzato, il che facilita l'utilizzo di Smartsheet da parte del Governo degli Stati Uniti per gestire il proprio lavoro e per rispettare i requisiti di sicurezza e conformità.

- **Sarbanes-Oxley Act 2002:** Smartsheet è un'azienda quotata in borsa e deve garantire la conformità al Sarbanes-Oxley (SOX). La conformità SOX aiuta a creare un team interno coeso e migliora la comunicazione tra i team coinvolti negli audit.

Come indicato nella nostra pagina web di informazioni legali, Smartsheet usa un'infrastruttura fornita da Amazon Web Services, Inc. ("AWS") per ospitare i dati dei clienti. Le informazioni sugli audit e sulle certificazioni di sicurezza e privacy ricevute da AWS, inclusi i report SOC e la certificazione ISO 27001, sono disponibili sul sito web di AWS Security e sul sito web di AWS Compliance. Per un elenco completo di white paper e data sheet aggiuntivi sulle certificazioni, visita la pagina Compliance dello Smartsheet Trust Center.

Conclusione e risorse aggiuntive

Il lavoro di oggi (e domani) necessita di una piattaforma di gestione del lavoro moderna, sicura e facile da usare. Grazie a focus e investimenti costanti, abbiamo creato Smartsheet da zero con requisiti e funzionalità rigorosi per la riservatezza dei dati. Oltre a ciò che è disponibile oggi, abbiamo una serie di funzionalità di sicurezza aggiuntive che stiamo attualmente sviluppando. Per ulteriori informazioni sulle funzionalità, i programmi e le protezioni di sicurezza di Smartsheet, visita smartsheet.com/trust e le risorse aggiuntive di seguito:

Guida online per Amministratori di sistema Smartsheet
Funzioni di Smartsheet per Piano
Integrazioni di Smartsheet
Documentazione sulle API Smartsheet

sales@smartsheet.com
+44 (20) 39001410
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet