Segurança do Smartsheet

Uma visão aprofundada dos recursos, práticas e proteções de segurança do Smartsheet

Resumo executivo

Na Smartsheet, entendemos que as plataformas empresariais de software como serviço (SaaS) devem oferecer várias camadas de defesa e uma infinidade de proteções e controles de TI para manter os dados confidenciais da empresa seguros. Também é importante que essas soluções sejam flexíveis e se integrem aos sistemas e processos de segurança de dados em vigor.

Este white paper tem o objetivo de apresentar os recursos, as proteções e as práticas de segurança e governança do Smartsheet. Primeiramente, vamos nos concentrar nos recursos controlados pelo cliente que a Smartsheet recomenda implementar para manter um ambiente de trabalho seguro, em conformidade e bem governado. Observação: este white paper não inclui recursos de segurança que ainda não estão disponíveis ao público geral.

Visão geral

Para proteger melhor a sua empresa, recomendamos a implementação de controles em três áreas principais de concentração: gerenciamento de identidade e acesso, governança de dados e configuração de contas globais. Além desses tópicos, este documento inclui informações gerais sobre as práticas de segurança, privacidade e conformidade da Smartsheet.

- **O gerenciamento de identidade e acesso** concentra-se no controle de como seus usuários têm acesso ao Smartsheet, garantindo que a função e a identidade de cada usuário na plataforma estejam alinhadas à sua estrutura e políticas organizacionais. Além disso, discutiremos como garantir a segurança ao colaborar com usuários externos, com base nas suas preferências de segurança.

- **A governança de dados** deve ser aplicada tanto para os usuários como para toda a empresa. Para os usuários, uma abordagem de privilégio mínimo é o padrão na Smartsheet, com controles adicionais disponíveis para restringir e controlar ainda mais a visibilidade. Assim, os usuários serão expostos apenas ao que precisarem, quando precisarem. No nível organizacional, abordaremos mecanismos simples, como compartilhamento seguro e relatórios de usuários, além de recursos avançados opcionais disponíveis, como políticas de saída de dados.

- **A configuração global de contas** permite personalizar a estética do ambiente do Smartsheet para que corresponda à marca da sua empresa. Até mesmo algo tão simples como um sinal visual confirmando que os usuários estão dentro do ambiente protegido da empresa pode ajudar a garantir a sua segurança. Garanta a consistência fixando a marca e a personalização para que todos os ativos criados estejam alinhados com sua marca.

- **As práticas de segurança, privacidade e conformidade** se referem às ações e proteções que a Smartsheet mantém fora de nossa plataforma para ajudar a garantir que os dados dos clientes permaneçam altamente seguros. A Smartsheet implementou estratégias avançadas de defesa líderes do setor por meio de uma combinação de pessoas, processos e tecnologias para proteger a confidencialidade, a integridade e a disponibilidade dos ambientes e ativos da empresa.

Sumário

Gerenciamento de identidades

Gerenciar a identidade de um usuário no Smartsheet e, portanto, o acesso ao sistema é tão importante quanto gerenciar os dados na plataforma.

No início da implementação do Smartsheet, você decidirá qual método de autenticação quer usar. O Smartsheet oferece diferentes opções: e-mail e senha e métodos de login único (SSO) do Google, Microsoft, provedores SAML 2.0 e Apple.

É possível selecionar um ou mais métodos para a sua empresa, embora seja recomendável aplicar um só método de autenticação SSO para todos os usuários, com outras formas desativadas. Também recomendamos adicionar outra camada de segurança implementando a autenticação multifator (MFA) ao configurar o SSO.

O Smartsheet tem um conjunto robusto de APIs REST. A API do Smartsheet usa o OAuth 2.0 para autenticação e autorização. Um cabeçalho HTTP com um token de acesso é necessário para autenticar cada solicitação. Para aumentar a segurança, use o OAuth 2.0 em todas as integrações que você criar como parte das melhores práticas.

Gerenciamento de acesso

Gerenciar usuários e o acesso deles é uma função administrativa essencial que pode afetar tanto a segurança como a implementação do Smartsheet por parte da sua empresa. As empresas precisam encontrar um equilíbrio delicado, incentivando a colaboração e gerenciando os riscos envolvidos à medida que os dados e as equipes se tornam cada vez mais distribuídos. Para ajudar com isso, a Smartsheet oferece três modelos de governança distintos, conforme as principais maneiras pelas quais nossos clientes procuraram gerenciar o aplicativo.

Modelos de governança do Smartsheet

A primeira abordagem é o nosso modelo descentralizado (centralizado), em que as unidades de negócios individuais controlam diretamente as próprias compras e planos. Nesse modelo, o departamento de TI, normalmente, não está envolvido na administração, e a cobrança, a governança e o gerenciamento de usuários do plano são deixados a critério do departamento. Esse modelo, geralmente, vale para empresas no início da jornada com o Smartsheet.

Nossa segunda abordagem é o modelo centralizado (consolidado), em que todos os planos do Smartsheet foram consolidados em uma só assinatura, administrada pelo departamento de TI. Isso proporciona controle direto sobre gastos, gerenciamento de usuários e controles de segurança. Esse modelo é mais adequado para equipes de TI que querem manter uma supervisão rigorosa de todos os aspectos da experiência com o Smartsheet.

Por fim, nosso modelo compartilhado (híbrido) tem o objetivo de oferecer uma abordagem intermediária, em que o departamento de TI controla as configurações de toda a empresa usando o Gerenciador do plano Empresa, já o gerenciamento de licenças e usuários é controlado diretamente pelos administradores de sistemas da linha de negócios. A cobrança também é separada por plano, facilitando a cobrança por departamento ou um modelo em que os gastos com o Smartsheet são integrados aos orçamentos departamentais em vez de serem faturados centralmente para o departamento de TI.

Para garantir altos padrões de segurança, a Smartsheet recomenda nossos modelos compartilhados ou centralizados, que oferecem controle de TI mais direto sobre seus planos.

Administração de usuário

À medida que várias equipes da sua empresa implementarem o Smartsheet de maneira independente para as próprias necessidades, poderão ser criados vários planos separados. As fusões e aquisições podem contribuir para um ambiente com vários planos do Smartsheet.

Para gerenciar usuários nesses planos usando o modelo descentralizado, recomendamos ativar a Descoberta de conta para cada um desses planos. À medida que novos usuários são expostos ao Smartsheet, isso permite que eles ou qualquer pessoa do domínio da sua empresa vejam uma lista dos planos do Smartsheet associados a ela, proporcionando um meio centralizado de solicitar a adesão a um desses planos atuais em vez de iniciar um novo. Essas solicitações são automaticamente encaminhadas aos administradores do sistema (por meio do Centro de administração do Smartsheet) para revisão e aprovação.

Se você tiver vários planos separados e quiser gerenciar usuários com o modelo centralizado, talvez seja necessário concluir uma consolidação de conta. Observação: os clientes com recursos Advance, como Dynamic View, Connectors e Control Center, precisarão entrar em contato com o suporte do Smartsheet para receber mais assistência com algumas questões da consolidação.

Se estiver usando o modelo compartilhado e o Gerenciador do plano Empresa, uma das melhores práticas é organizar os planos por departamento/equipe/centro de custo. Isso permite que você estabeleça uma política para atribuir automaticamente os usuários aos planos relevantes com base na afiliação a uma dessas entidades.

Gerenciamento de usuários

A Smartsheet entende que a adição de um usuário por vez pode não ser dimensionada à medida que a implementação aumenta para dezenas, centenas ou até milhares de usuários. Por isso, ao começar, recomendamos aproveitar o recurso de importação de usuários em massa em nosso Centro de administração, que adiciona facilmente até 1.000 usuários de uma vez à sua empresa com o Smartsheet. Da mesma forma, você também pode usar a atualização em massa para editar funções em massa para usuários atuais.

As fusões ou aquisições, geralmente, resultam em mudança de marca, com os usuários recebendo novos endereços de e-mail. A Mesclagem de usuários pode ajudar você a atualizar em massa os endereços de e-mail principais dos usuários e a limpar as contas duplicadas.

Um plano consolidado do Smartsheet pode usar dois recursos adicionais para simplificar e automatizar ainda mais o gerenciamento de usuários:

- O Provisionamento automático (UAP) automatiza o processo de inclusão de usuários em uma conta empresarial. Quando os usuários se inscreverem ou entrarem no Smartsheet com o endereço de e-mail da empresa, eles serão automaticamente adicionados à sua conta. Além disso, você pode escolher se os usuários devem receber licenças em vez de entrar automaticamente na conta como colaboradores não licenciados (gratuitos).

    - Se você implementou nosso modelo consolidado, recomendamos ativar o provisionamento automático para que os funcionários entrem automaticamente na conta central controlada pelo departamento de TI.

    - Se estiver usando nosso modelo compartilhado (e se a sua empresa tiver documentado informações de departamento/centro de custo para a sua lista de usuários), recomendamos ativar o provisionamento automático, pois essas informações podem ser importadas para associar automaticamente os usuários ao plano certo quando eles solicitarem uma licença. Ele também pode ser usado para automatizar a movimentação de usuários não licenciados entre planos.

- As Integrações de diretório permitem sincronizar diretamente seus usuários do Microsoft Azure Active Directory (AD) com o Smartsheet. Conecte o Smartsheet à sua automação atual no Azure AD para automatizar totalmente a integração e o desligamento de usuários, minimizando o risco de permanecerem ou revisitarem as próprias contas do Smartsheet. Como benefício adicional, os atributos do AD em nível de usuário, como departamento/centro de custo/divisão, são incluídos em um relatório de estorno do Smartsheet, que está disponível no Centro de administração e pode ser usado para facilitar o estorno interno. Uma das melhores práticas é sincronizar todos os usuários do Directory com a conta do Smartsheet da sua empresa. Isso evita que esses usuários criem contas adicionais de "TI invisível" no Smartsheet ao fazer login pela primeira vez. Como uma segunda camada de defesa, você também pode deixar o provisionamento automático ativado para alcançar todos os usuários que talvez ainda não estejam sincronizados por meio do Directory.

Quando uma pessoa deixa sua empresa, é importante remover seu acesso ao Smartsheet. Oferecemos duas maneiras de fazer isso. A exclusão de um usuário remove esse usuário e os ativos que ele tem da sua conta do Smartsheet, mas isso pode fazer com que os itens que ainda estão em uso sejam removidos, talvez prejudicando as soluções que dependam desses dados. Em vez disso, a Smartsheet recomenda Desativar usuários. Isso ainda impede totalmente que eles acessem o Smartsheet, mas preserva a acessibilidade ao conteúdo, eliminando quaisquer considerações necessárias sobre a estabilidade da solução ou transferências de propriedade

Funções e tipos de usuários no Smartsheet

Independentemente do método de provisionamento de usuários, será necessário determinar as funções do Smartsheet para as pessoas da sua empresa.

Uma atribuição de função não dá à pessoa acesso aos ativos do Smartsheet em sua empresa. Os ativos também devem ser compartilhados diretamente com essas pessoas. Dessa forma, as permissões de acesso a funções e ativos determinarão o que as partes interessadas podem ver e fazer no Smartsheet. O Smartsheet oferece suporte para estas funções principais:

- Usuário licenciado: usa recursos licenciados, como a criação de planilhas.

- Administrador de grupo: cria e gerencia grupos do Smartsheet.*

  * As funções de administrador de grupo também devem ser de usuários licenciados

- Administrador de sistema: gerencia usuários, configurações de conta e controles de segurança.

É altamente recomendável designar pelo menos dois administradores de sistema ativos para a conta do Smartsheet de sua empresa. Assim, não haverá interrupções se um administrador de sistema não estiver disponível em um determinado momento.

Os administradores de grupo podem criar grupos do Smartsheet, permitindo que os usuários compartilhem conteúdo com o grupo, em vez de exigir que o façam com cada membro. Os administradores de grupo só podem gerenciar os grupos dos quais são proprietários. Conforme necessário, para limitar a colaboração externa, restrinja a participação no grupo apenas aos participantes de sua empresa.

Se você não atribuir nenhuma das funções acima a um usuário, o acesso dele será limitado apenas aos ativos do Smartsheet (planilhas, relatórios, painéis ou WorkApps) compartilhados com ele. Para criar ativos do Smartsheet, as partes interessadas devem ser usuários licenciados e podem solicitar uma licença diretamente pelo aplicativo Smartsheet. Os administradores de sistema podem acompanhar e responder às solicitações individualmente ou em massa por meio da seção Gerenciamento de solicitações

de licença do centro de administração. Se você já tiver um processo estabelecido para gerenciar solicitações de licença, recomendamos aproveitar as vantagens de uma Tela de atualização personalizada para direcionar os usuários a enviar suas solicitações de licença por meio desses processos internos.

Colaboradores externos

Qualquer parte interessada fora de seu domínio que seja compartilhada com seus ativos do Smartsheet é considerada um colaborador externo. O Smartsheet permite que sua empresa colabore livremente com qualquer parte externa confiável, sem nenhum custo associado para esses colaboradores externos. Para garantir a segurança ao fazer parcerias externas, recomendamos o uso de três controles administrativos centrais:

O Compartilhamento seguro permite especificar domínios ou endereços de e-mail confiáveis e autorizados para colaboração externa.

Os Relatórios de acesso a planilhas mostram uma lista de colaboradores externos que têm acesso ao conteúdo do Smartsheet de sua empresa.

Revogar o acesso a itens, de maneira centralizada por meio do centro de administração, para que os colaboradores externos sejam removidos do conteúdo que não precisam mais acessar.

Governança de dados

A governança de dados eficaz é indispensável para as empresas de hoje garantirem que as informações delas sejam criadas, usadas, compartilhadas e protegidas conforme as normas, políticas da empresa e melhores práticas do setor vigentes.

Esses controles são necessários não apenas para fins regulatórios, mas também para garantir a eficiência, a confidencialidade e a continuidade dos negócios:

Para os usuários, a empresa precisa oferecer ferramentas eficazes para restringir a visibilidade, mostrando apenas informações relevantes às partes interessadas.

Para a empresa, ela precisa estar equipada com ferramentas aplicáveis para criar e aplicar políticas eficazes.

Governança de dados para usuários

A maioria dos usuários está familiarizada com os níveis de permissão no Smartsheet (visualizador, editor, administrador e proprietário). O Dynamic View e os WorkApps oferecem controles e flexibilidade adicionais e mais específicos, ajudando a proporcionar recursos eficazes de governança de dados para os usuários. Limitar o acesso apenas ao conteúdo mais relevante ajuda a garantir a eficiência do processo (já que os usuários devem necessariamente se concentrar nos itens que precisam de atenção), mas também garante a segurança, ampliando a abordagem do Smartsheet de privilégio mínimo por padrão para uma escala mais granular.

Dynamic View

Nem todos os processos de negócios garantem total transparência. Muitos processos (gerenciamento de pedidos, colaboração com fornecedores, projetos que envolvem equipes internas e externas mistas) exigem um controle rígido sobre o que é compartilhado com quem.

O Dynamic View permite a colaboração sem comprometer a confidencialidade. Usando o Dynamic View, os proprietários de planilhas podem compartilhar seletivamente linhas e campos relevantes com colaboradores específicos, sem compartilhar as planilhas subjacentes. Isso permite vários casos de uso em que usuários comerciais específicos podem compartilhar seletivamente elementos com fornecedores, equipes internas e externas mistas ou entre empresas, convidando à colaboração apenas em determinados campos. Todos têm acesso somente às informações de que precisam.

WorkApps

Os WorkApps permitem que você agilize seu trabalho e simplifique a colaboração usando aplicativos fáceis de navegar criados diretamente a partir de suas planilhas, formulários, painéis, relatórios e muito mais. Você pode personalizar a experiência no aplicativo para os membros da sua equipe, com base na função de cada pessoa, e trabalhar em conjunto a partir dos mesmos conjuntos de dados subjacentes. Os aplicativos são dimensionados usando a mesma segurança multinível para empresas que a da plataforma Smartsheet.

Os WorkApps eliminam a necessidade de compartilhar os ativos subjacentes que constituem o WorkApps. É possível criar um WorkApp com uma visualização filtrada de planilhas e relatórios selecionados, mas nenhuma dessas planilhas ou relatórios precisa ser compartilhada com o usuário final. Ele só vê a exibição "WorkApps" desses ativos.

Controles da política de governança de dados para a empresa

O Smartsheet permite que os administradores garantam que os recursos da plataforma sejam usados conforme as políticas de governança da empresa. Esses controles permitem que os administradores implementem boas proteções de governança de dados para garantir que os dados sejam tratados corretamente e somente por aqueles que precisam interagir com esses dados.

Os administradores podem escolher como querem que os usuários interajam com recursos específicos. Os proprietários de planilhas devem poder publicar suas planilhas e criar novas automações? Você tem um sistema de armazenamento específico do qual os arquivos devem ser anexados? Os colaboradores externos devem poder baixar o conteúdo compartilhado com eles? Esses são exemplos de perguntas que os administradores devem fazer para si a fim de avaliar efetivamente os controles apropriados a serem implementados em toda a empresa.

Esses controles de política também se estendem ao compartilhamento seguro. Se você quiser limitar o compartilhamento de dados e ativos a domínios ou endereços de e-mail específicos, essa é a ferramenta que deve ser usada. Conforme mencionado anteriormente, o compartilhamento seguro também determina se sua empresa pode compartilhar itens do Smartsheet com outras empresas, como fornecedores e parceiros.

Controle de widget de conteúdo web

Os painéis oferecem a possibilidade de integrar conteúdo interativo (vídeos, gráficos, documentos e muito mais). Os administradores podem ativar ou desativar esse recurso e definir uma lista aprovada de domínios compatíveis com o widget de conteúdo web. Como parte das nossas melhores práticas, recomendamos limitar isso aos domínios internos da empresa.

Permissões de automação

Controle quem pode receber automação de planilhas. As opções são organizadas de Restrito (ativa apenas ações para usuários compartilhados com a planilha) a Irrestrito (em que a automação é aplicável a qualquer endereço de e-mail e integração de terceiros, como o Slack). Recomendamos que você revise esse controle para garantir que a configuração corresponda ao nível desejado de colaboração interna e externa da sua empresa.

Controles de anexo

Determine se os membros do plano podem carregar arquivos dos próprios computadores, anexando um link (URL) a um site ou de serviços de armazenamento em nuvem de terceiros, incluindo Google Drive, OneDrive, Box, Dropbox, Evernote ou Egnyte. Para evitar a entrada de dados de fontes não aprovadas, habilite somente os provedores de anexos aprovados para uso com base nas políticas internas de sua empresa.

Controles de publicação

A publicação de uma planilha, relatório ou painel gera um URL exclusivo que qualquer pessoa pode acessar sem fazer login no Smartsheet e um código iframe que pode ser integrado ao código-fonte de um site para exibir a planilha ou o relatório.

Você pode proibir a publicação de planilhas, relatórios, painéis e iCal: o botão Publicar não aparece mais no ativo do Smartsheet. Você também pode restringir o acesso aos itens publicados apenas às pessoas da sua empresa no Smartsheet. Observamos que os clientes com conhecimentos de segurança, geralmente, permitem a publicação, mas limitam o acesso aos itens publicados às pessoas na conta daqueles.

Compartilhamento seguro

Use essa capacidade para restringir o compartilhamento por domínio ou por endereços de e-mail específicos (por exemplo, garantir que as planilhas sejam compartilhadas apenas com as pessoas que possuem um endereço de e-mail corporativo). A Smartsheet recomenda muito a implementação do compartilhamento seguro para controlar a colaboração externa. Além disso, para simplificar as atualizações e a manutenção da sua lista de compartilhamento seguro, recomendamos que você colete todas as solicitações de atualização usando um formulário da Web do Smartsheet.

Controles de envios de formulários off-line

Ao usar o aplicativo móvel, o Smartsheet permite automaticamente o envio de formulários off-line para dar suporte a casos de uso em que os usuários podem não ter uma conexão estável (por exemplo, em um canteiro de obras). Esse controle oferece aos administradores a capacidade de desativar (ou ativar novamente) os envios de formulários off-line para controlar se um usuário pode iniciar o aplicativo móvel sem uma conexão para enviar formulários.

Controles de integração de comunicação

O Smartsheet é compatível com o Google Chat, o Microsoft Teams, o Slack e o Cisco Webex como serviços de comunicação. Os administradores da conta podem ativar um ou vários serviços, a seu critério.

Registros e relatórios

Você pode baixar relatórios que abrangem diferentes aspectos do uso do Smartsheet em toda a sua empresa para ter visibilidade contínua do uso, dos usuários, do conteúdo, da cobrança e do acesso ao Smartsheet:

Relatório de acesso a planilha

Gera um arquivo do Excel que lista os nomes de todas as planilhas, relatórios e painéis pertencentes a usuários licenciados na conta, o nome da área de trabalho em que esses itens são salvos (se for o caso), os colaboradores compartilhados em cada planilha e o registro de data e hora da última modificação. Recomendamos revisar esse relatório periodicamente para auditar a lista de colaboradores externos que têm acesso a ativos pertencentes a pessoas de sua empresa.

Relatório de itens publicados

Gera um arquivo Excel listando todos os itens que foram publicados. Ótimo para segurança de dados ou para controlar quem publicou itens específicos. Use esse relatório para informar a configuração do controle de publicação, conforme necessário.

Relatório da lista de usuários

Gera um arquivo Excel listando todos os membros (convidados e ativos) da conta, um registro de data e hora de quando foram adicionados à conta, seus níveis de acesso (administrador de sistema, administrador de grupo, etc.), o número de planilhas que possuem e o registro de data e hora do último login no Smartsheet.

Relatório de histórico de login

Os administradores do sistema em contas de vários usuários podem usar o centro de administração para receber um arquivo do Excel com uma lista do histórico de login recente por e-mail.

Relatório de estorno

Disponível no centro de administração, os clientes que usam a integração de diretório podem usar os relatórios de estorno para facilitar o estorno interno. Isso adiciona colunas para divisão, departamento e centro de custo ao relatório existente criado quando os clientes baixam a lista de usuários, proporcionando os dados necessários para realizar relatórios internos de estorno.

Para um acompanhamento mais granular das ações do usuário no nível da planilha, do painel e da célula, você pode usar o registro de atividade, o histórico da célula e as colunas do sistema.

- **Registro de atividade:** apresenta uma trilha de auditoria das alterações feitas em um ativo, quem as fez e quando foram feitas. Isso inclui edições como a exclusão de linhas (com os dados que foram excluídos), quem visualizou o item e alterações na permissão de compartilhamento.

- **Histórico da célula:** exibe um registro das alterações feitas no nível da célula, detalhando quem fez as alterações, quais foram elas e quando foram feitas. Os usuários podem usar facilmente o recurso copiar e colar do histórico da célula para restaurar informações anteriores que possam ter sido excluídas ou alteradas indevidamente.

- **Colunas do sistema:** exibe a hora em que cada linha foi editada pela última vez e o colaborador que fez a alteração.

Controles avançados de governança de dados

O Smartsheet oferece vários recursos avançados que proporcionam controle de governança de dados para clientes com necessidades de segurança de dados especialmente rigorosas. Esses recursos estão inclusos no Smartsheet Advance Platinum e no Smartsheet Safeguard.

Chaves de criptografia gerenciadas pelo cliente

O Smartsheet usa criptografia para proteger os dados dos clientes e ajudá-los a manter o controle sobre eles. As chaves de criptografia gerenciadas pelo cliente (CMEK) foram criadas para empresas que possuem dados confidenciais ou regulamentados que exigem o gerenciamento da própria chave de criptografia. As chaves de criptografia gerenciadas pelo cliente permitem que as organizações empresariais usem aplicativos SaaS em nuvem e mantenham um controle de dados comparável ao de uma instalação local, adicionando uma camada de criptografia gerenciada pelo cliente ao armazenamento de dados do Smartsheet para dar suporte a políticas avançadas de segurança e governança de dados.

Observação: para usar as chaves de criptografia gerenciadas pelo cliente, os clientes devem ter acesso ao Sistema de gerenciamento de chaves da Amazon Web Services (AWS KMS), pois as chaves do cliente são configuradas e gerenciadas diretamente na AWS.

O Smartsheet usa as chaves de criptografia gerenciadas pelo cliente para criptografar os dados da sua empresa de modo que elas permaneçam sob seu controle o tempo todo. Em específico, o Smartsheet não armazena nem controla essas chaves de criptografia e deve solicitar e recuperar as chaves do Serviço de gerenciamento de chaves (KMS) da AWS de nosso cliente sempre que precisar acessar os dados de sua planilha.

Uma vez que sua empresa controla as chaves de criptografia gerenciadas pelo cliente armazenadas no Sistema de gerenciamento de chaves da AWS, você pode revogar o acesso do Smartsheet à chave de criptografia gerenciada pelo cliente e, assim, o acesso aos seus dados a qualquer momento. Ao destruir as chaves-mestras no Sistema de gerenciamento de chaves da AWS, sua empresa pode excluir efetivamente seus dados dos sistemas do Smartsheet. Uma parte mal-intencionada com uma cópia do banco de dados do Smartsheet, do código-fonte e das chaves de criptografia da nuvem ainda não conseguiria ler nenhum dos dados criptografados com chaves de criptografia gerenciadas pelo cliente.

Políticas de saída de dados

O compartilhamento de dados sempre envolve algum nível de risco, mas, ao usar um conteúdo especificamente confidencial, é fundamental garantir que os dados da empresa permaneçam apenas na sua conta e sob seu controle.

Os administradores de sistema podem usar políticas de saída de dados para proteger informações confidenciais por meio de controle granular sobre como os dados podem ser exportados dentro e fora da empresa.

As políticas de saída de dados podem ser implementadas para impedir que colaboradores internos e externos realizem as seguintes ações em planilhas, relatórios e painéis:

- Salvar como novo
- Salvar como modelo
- Enviar como anexo
- Publicar
- Imprimir
- Exportar

Os usuários que tentarem uma ação restrita receberão uma notificação de que o comportamento é proibido devido à política de saída de dados que a sua empresa implementou.

Esses limites são feitos para evitar que os colaboradores salvem ou compartilhem informações confidenciais para fins maliciosos.

Relatório de eventos

Para garantir a segurança das informações, muitas empresas precisam de uma visão contínua de como seus aplicativos de negócios, como o Smartsheet, estão sendo usados. É prudente manter a visibilidade a:

- Quem está criando planilhas
- Quem está criando áreas de trabalho
- Quem está excluindo objetos
- Quem compartilhou uma planilha com quem

O relatório de eventos oferece visibilidade detalhada ao comportamento e à atividade do usuário na conta do Smartsheet da sua empresa. Esse recurso permite monitorar a perda de dados e identificar padrões anômalos de uso para que você possa aplicar com mais rigor as políticas organizacionais de segurança e conformidade.

O relatório de eventos oferece um feed de dados JSON de eventos de uso do Smartsheet ("Eventos") em um plano (organização), acessado por meio da API de relatório de eventos. O serviço informa sobre mais de 120 eventos no Smartsheet e armazena até seis meses de dados, a partir da data em que o feed é ativado.

Para se beneficiar desse feed, os dados do relatório de eventos, geralmente, são integrados a outros sistemas de segurança que proporcionam monitoramento, notificação, criação e aplicação de políticas e prevenção contra perda de dados (DLP). Esses aplicativos são vendidos por terceiros; geralmente sistemas de Agente de segurança de acesso à nuvem (CASB), sistemas de Gerenciamento de eventos e informações de segurança (SIEMs) ou uma combinação de CASB e SIEM trabalhando juntos. Às vezes, as empresas desenvolvem os próprios sistemas de monitoramento e resposta em vez de confiar naqueles fornecidos por terceiros.

Principais casos de uso do relatório de eventos:

- Prevenção de perda de dados
- Tratamento de dados de informações de identificação pessoal (PII)
- Governança de dados
- Veja insights sobre colaboração

Controles de retenção de dados

Quanto mais conteúdo sua empresa tiver em qualquer aplicativo SaaS, maior será o risco assumido por ela.

Os controles de retenção de dados do Smartsheet oferecem às empresas a capacidade de criar uma política que determina quando o conteúdo deve ser excluído, com base nos critérios que elas decidirem aplicar.

Essas políticas podem ser baseadas na data em que uma planilha foi criada ou na última vez em que foi modificada, garantindo que apenas o conteúdo ativo ou recente seja mantido em sua instância do Smartsheet e limitando seu perfil de risco.

Configuração global de contas

A segurança da conta não se limita a recursos técnicos, como criptografia de dados, classificação ou opções de autenticação. A segurança pode ser algo tão simples quanto incluir o logotipo de sua empresa em todos os itens que pertencem a ela.

Os controles globais de configuração de conta permitem implementar a marca visual (e outras restrições) para que os usuários saibam que estão acessando as informações corretas.

Os administradores de sistema podem adicionar logotipos globalmente para alinhar a implementação do Smartsheet com os requisitos de marca da empresa. Use o bloqueio de marca para garantir que cada novo ativo tenha a mesma marca.

Os controles de personalização e as configurações de conta do Smartsheet também permitem que você defina telas de boas-vindas personalizadas. É possível criar telas de ajuda personalizadas com descrições sobre como começar, telas de solicitação de licença para ajudar os usuários a entrar em contato com você ou telas de boas-vindas personalizadas e com a sua marca que aparecem quando um usuário faz login. As telas podem incluir uma exigência de que o usuário aprove os termos de serviço antes de acessar mais informações.

A combinação de uma identidade visual consistente com informações personalizadas ajuda os usuários a saber que estão acessando as ferramentas e informações corretas e aumenta a sua segurança

Práticas de segurança, privacidade e conformidade da Smartsheet

Utilizando uma abordagem holística, os programas de segurança cibernética, privacidade e proteção de dados do Smartsheet começam com políticas estratégicas de segurança da informação definidas e apoiadas pelo Comitê de Direção de Segurança da Informação (ISSC) do Smartsheet e pela equipe de liderança executiva. Essas políticas foram criadas para se alinharem às práticas estratégicas de gerenciamento de riscos da empresa, gerenciar e monitorar proativamente os riscos de segurança, promover a segurança por meio da maturidade dos processos e da arquitetura eficaz do sistema e permitir que os usuários tomem decisões prudentes sobre os riscos de segurança por meio de treinamento e conscientização.

Segurança de dados

Incluímos segurança à nossa plataforma para garantir que seu ativo mais valioso (seus dados) esteja protegido. A Smartsheet contrata terceiros para realizar auditorias de nossas práticas de segurança, incluindo uma avaliação e atestado SOC2 Tipo II e avaliações de segurança técnica de terceiros com empresas de teste de invasão. Além disso, o programa de gerenciamento de vulnerabilidades da Smartsheet automatiza a identificação e a correção das vulnerabilidades da rede e do sistema nos ambientes corporativos e de produção do Smartsheet. O Smartsheet usa criptografia para proteger seus dados e ajudar você a manter o controle sobre eles. Eis o que você pode esperar do Smartsheet: todos os dados são armazenados de maneira durável com números aprovados pelo Instituto Nacional de Padrões e Tecnologia (NIST), tecnologia de segurança de camada de transporte (TLS), criptografia AES de 256 bits em repouso e o serviço S3 da Amazon para armazenar e disponibilizar arquivos carregados.

Privacidade

Na Smartsheet, valorizamos sua privacidade e respeitamos seu direito de saber como as informações sobre você são coletadas e usadas. Nosso aviso de privacidade descreve como o Smartsheet coleta, usa e divulga informações pessoais e de outra natureza, coletadas por meio de nossos sites, aplicativos móveis e da plataforma de execução de tarefas do Smartsheet.

- Reconhecemos os direitos de privacidade de nossos clientes potenciais, clientes e parceiros, bem como aderimos a normas globais de privacidade, como o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia.

- Oferecemos um contrato de processamento de dados para nossos clientes que exigem termos específicos para o processamento de conteúdo que inclui informações pessoais. Se determinar que precisa de um DPA com a Smartsheet, você poderá enviar um formulário concordando com os termos do DPA em smartsheet.com/legal/DPA

Gerenciamento operacional

Implementamos políticas e procedimentos projetados para garantir que seus dados sejam mantidos protegidos e com backups em vários locais físicos. Nossas equipes estão constantemente avaliando novas ameaças de segurança e implementando contramedidas atualizadas, projetadas para impedir acessos não autorizados ou tempos de inatividade não planejados do serviço de assinatura. O acesso a todos os sistemas e dados de produção do Smartsheet é limitado a membros autorizados da equipe de operações técnicas da Smartsheet, com base nos princípios de privilégio mínimo e necessidade de conhecimento. A Smartsheet publica informações sobre o status do sistema no site de status do Smartsheet. A Smartsheet, normalmente, notifica os clientes sobre incidentes graves no sistema por e-mail e/ou mensagem de texto caso tenham se inscrito para receber atualizações automáticas no site de status do Smartsheet.

Segurança, continuidade e redundância do data center

Colaboramos com parceiros de hospedagem reconhecidos no setor para garantir que você possa prestar serviços à sua empresa com segurança, em uma plataforma na qual possa confiar. Temos redundância de dados em vários locais, hospedagem em instalações da AWS, e nossas instalações são examinadas e certificadas pelos relatórios e normas SOC 1, SOC 2, ISO 27001 e FISMA. Nosso monitoramento inclui protocolos de escaneamento biométrico, vigilância contínua e gerenciamento do ambiente de produção 24 horas por dia, 7 dias por semana. A Smartsheet mantém processos e planos internos para processar eventos de continuidade de negócios e situações de recuperação de desastres. Esses planos são revisados e testados anualmente, bem como distribuídos aos funcionários qualificados em toda a empresa. Nossos data centers estão geograficamente isolados (aproximadamente 965 km) uns dos outros para evitar que sejam afetados simultaneamente caso haja um desastre natural em grande escala.

Auditorias e certificações

As seguintes auditorias e certificações relacionadas à segurança e à privacidade são válidas aos principais serviços de aplicativos Smartsheet.

- **SOC 2/SOC 3:** o Smartsheet é submetido a exames e testes anuais como parte do processo de auditoria SOC. Os relatórios de auditoria externa resultantes atestam o projeto e a eficácia operacional dos controles internos em nossos negócios, incluindo segurança, disponibilidade e confidencialidade.

- **Certificação de Proteção de Privacidade da UE-EUA e da Suíça-EUA:** os dados de clientes enviados aos serviços cobertos estão dentro do escopo de uma certificação anual da Estrutura de Proteção de Privacidade da UE-EUA e da Estrutura de Proteção de Privacidade da Suíça-EUA, conforme administrado pelo Departamento de Comércio dos EUA. A certificação atual está disponível em privacyshield.gov/list, pesquisando "Smartsheet".

- **FedRAMP (moderado):** o Smartsheet foi selecionado para o programa FedRAMP Connect pelo Conselho de Autorização Conjunta (JAB), que priorizou o Smartsheet Gov para certificação com base na demanda dos órgãos do governo federal. O Smartsheet Gov é um ambiente separado do Smartsheet com status de autorização FedRAMP, facilitando o uso do Smartsheet pelo governo dos EUA para gerenciar seu trabalho e, ao mesmo tempo, ajudando-o a atender aos requisitos de segurança e conformidade.

- **Lei Sarbanes-Oxley de 2002:** a Smartsheet é uma empresa pública e precisa estar em conformidade com a lei Sarbanes-Oxley (SOX). A conformidade com a SOX ajuda a formar uma equipe interna coesa e melhora a comunicação entre as equipes envolvidas nas auditorias.

Conforme observado em nossa página jurídica, o Smartsheet usa a infraestrutura fornecida pela Amazon Web Services, Inc. ("AWS") para hospedar os dados dos clientes. As informações sobre as auditorias e certificações relacionadas à segurança e à privacidade recebidas pela AWS, incluindo a certificação ISO 27001 e os relatórios SOC, estão disponíveis nos sites de Segurança e de Conformidade da AWS. Para ver uma lista completa de nossas certificações e outros white papers e folhas de dados, acesse a página de Conformidade no Smartsheet Trust Center.

Conclusão e recursos adicionais

O trabalho de hoje (e de amanhã) precisa de uma plataforma moderna de gerenciamento de trabalho que seja segura e fácil de usar. Por meio de foco e investimento contínuos, criamos o Smartsheet desde o início com requisitos e recursos rigorosos de confidencialidade de dados. Além do que está disponível hoje, temos vários outros recursos de segurança sendo desenvolvidos no momento. Para saber mais sobre os recursos, programas e proteções de segurança do Smartsheet, acesse smartsheet.com/trust e os recursos adicionais abaixo:

Ajuda on-line para administradores de sistema do Smartsheet
Recursos do Smartsheet por plano
Integrações ao Smartsheet
Documentação da API do Smartsheet

sales@smartsheet.com
(844) 324-2360
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet