Smartsheet-Sicherheit

Ein detaillierter Überblick über die Sicherheitsfunktionen, -verfahren und -maßnahmen von Smartsheet

Zusammenfassung

Wir von Smartsheet sind uns darüber im Klaren, dass Software-as-a-Service-Plattformen (SaaS-Plattformen) der Enterprise-Klasse mehrere Schutzebenen und eine Vielzahl von IT-Schutzmaßnahmen und -Steuerelementen anbieten müssen, um sensible Unternehmensdaten zu schützen. Außerdem müssen diese Lösungen flexibel sein und sich in bestehende Datensicherheitssysteme und -prozesse integrieren lassen.

In diesem Whitepaper sollen die Sicherheits- und Governance-Funktionen, -Schutzmaßnahmen und -Praktiken von Smartsheet vorgestellt werden. In erster Linie konzentrieren wir uns auf vom Kunden gesteuerte Funktionen, deren Implementierung Smartsheet empfiehlt, um eine sichere, konforme und gut verwaltete Arbeitsumgebung aufrechtzuerhalten. Hinweis: Dieses Whitepaper umfasst nur allgemein verfügbare Funktionen. Einige Funktionen müssen möglicherweise zusätzlich erworben werden oder sind nicht in allen Planstufen enthalten.

Überblick

Um Ihre Organisation bestmöglich zu schützen, empfehlen wir die Implementierung von Steuerelementen in drei Fokusbereichen: Identitäts- und Zugriffsmanagement, Daten-Governance und globale Kontokonfiguration. Zusätzlich zu diesen Themen umfasst dieses Dokument allgemeine Informationen in Bezug auf die Sicherheits-, Datenschutz- und Compliance-Praktiken von Smartsheet.

- **Identitäts- und Zugriffsmanagement** konzentriert sich darauf, den Zugriff Ihrer Benutzer*innen auf Smartsheet zu steuern und sicherzustellen, dass die Rolle und Identität der einzelnen Benutzer*innen auf der Plattform Ihrer Organisationsstruktur und Ihren Richtlinien entsprechen. Außerdem geht es darum, wie Sie die Sicherheit bei der Zusammenarbeit mit externen Benutzer*innen basierend auf Ihren Sicherheitseinstellungen gewährleisten.

- **Daten-Governance** muss sowohl auf Benutzerebene als auch über die Organisation hinweg umgesetzt werden. Für Benutzer*innen gilt in Smartsheet standardmäßig das Prinzip der geringsten Privilegien. Zusätzliche Steuerelemente sind verfügbar, um die Sichtbarkeit weiter einzuschränken und zu kontrollieren, sodass Benutzer*innen nur tatsächlich erforderliche Informationen zum tatsächlich erforderlichen Zeitpunkt zu sehen bekommen. Auf Organisationsebene decken wir sowohl einfache Mechanismen wie die sichere Freigabe und Benutzerberichte als auch optionale erweiterte Funktionen wie Datenegressrichtlinien ab.

- Die **globale Kontokonfiguration** ermöglicht Ihnen, die Ästhetik der Smartsheet-Umgebung an die Marke Ihrer Organisation anzupassen. Auch einfache Dinge wie etwa ein visueller Hinweis, dass sich Benutzer*innen in der geschützten Umgebung der Organisation befinden, tragen bereits dazu bei, die Sicherheit zu gewährleisten. Stellen Sie die Konsistenz sicher, indem Sie Branding und Anpassungen festschreiben, sodass jedes einzelne Asset Ihrer Marke entspricht.

- **Sicherheits-, Datenschutz- und Compliance-Praktiken** beziehen sich auf die Aktionen und Schutzmaßnahmen, die Smartsheet außerhalb der Plattform ergreift, um das hohe Maß an Schutz für Kundendaten sicherzustellen. Smartsheet verfolgt branchenführende Defense-in-Depth-Strategien (mehrschichtige Sicherheitsstrategien) und setzt auf eine Kombination aus Mitarbeitenden, Prozessen und Technologie, um unsere Plattform und Kundendaten zu schützen.

Inhaltsverzeichnis

Seite 5

Identitätsmanagement

Authentifizierungsmethoden

Multi-Faktor-Authentifizierung (MFA)

Sitzungsmanagement

Management des Benutzerlebenszyklus

API-Sicherheit und Token-Management

Zugriffsmanagement

Governance-Modelle

Benutzeradministration

Lizenzierungs-/Abonnementmodelle

Benutzerverwaltung

Rollen und Benutzertypen in Smartsheet

Gäste

Seite 8

Daten-Governance

Daten-Governance auf Benutzerebene

Steuerelemente für Daten-Governance-Richtlinien auf Organisationsebene

Protokollierung und Berichterstellung

Erweiterte Steuerung der Daten-Governance

Globale Kontokonfiguration

Seite 14

Sicherheits-, Datenschutz- und Compliance-Praktiken von Smartsheet

Infrastruktur und Architektur

Datensicherheit

Datenschutz

KI-Sicherheit und Datenschutz

Betriebsmanagement

Sicherheit, Kontinuität und Redundanz im Rechenzentrum

Smartsheet-Regionen

Audits und Zertifizierungen

Seite 15

Fazit und zusätzliche Ressourcen

Identitätsmanagement

Die Verwaltung der Identität von Benutzer*innen in Smartsheet – und damit ihres Zugriffs auf das System – ist genauso wichtig wie die Verwaltung der Daten innerhalb der Plattform. Smartsheet bietet eine Reihe von mehrschichtigen Funktionen für das Identitätsmanagement, die auf die Bedürfnisse von Unternehmen jeder Größe zugeschnitten sind – von der Durchsetzung der Authentifizierung und dem automatisierten Lebenszyklusmanagement bis hin zur API-Sicherheit und kontinuierlichen Überwachung.

Authentifizierungsmethoden

Zu Beginn entscheiden Sie, welche Authentifizierungsmethode Sie für Smartsheet verwenden möchten. Sie haben mehrere Optionen: E-Mail und Kennwort sowie Einmalanmeldung (Single Sign-on, SSO) über Google, Microsoft, Apple und SAML 2.0-Anbieter.

Die SAML 2.0-Unterstützung von Smartsheet ist mit den größten Identityprovidern (IdPs) auf Enterprise-Niveau kompatibel, darunter Okta, Microsoft Entra ID und PingIdentity. Diese umfassende Kompatibilität ermöglicht Unternehmen, ihre bestehenden IdP-Investitionen zu nutzen und einheitliche Authentifizierungsrichtlinien für alle SaaS-Anwendungen durchzusetzen.

Wir empfehlen, eine einzige SSO-Authentifizierungsmethode für alle Benutzer*innen durchzusetzen und alle anderen Anmeldemethoden zu deaktivieren. Dadurch werden schwächere, auf Anmeldeinformationen basierende Angriffsflächen beseitigt und die Authentifizierungs-Governance innerhalb Ihres Identityproviders zentralisiert.

Für Organisationen mit mehreren Domänen oder föderierten IT-Umgebungen unterstützt Smartsheet die SSO-Durchsetzung auf Domänenebene. Systemadmins können festlegen, dass sich Benutzer*innen einer bestimmten E-Mail-Domäne, z. B. „@regionaloffice.com“ oder „@subsidiary.org“, über einen definierten Identityprovider authentifizieren müssen. Dies ermöglicht maßgeschneiderte Identitätsrichtlinien für alle Geschäftsbereiche und stärkt die Governance und Risikominderung.

Multi-Faktor-Authentifizierung (MFA)

Wir empfehlen die Implementierung der Multi-Faktor-Authentifizierung (MFA) als zusätzliche Sicherheitsebene neben SSO. Die MFA-Durchsetzung wird am besten auf Identityprovider-Ebene verwaltet, sodass Ihr Sicherheitsteam die MFA-Richtlinien für alle verbundenen Anwendungen zentral steuern kann.

Für Benutzer*innen ohne SSO unterstützt Smartsheet MFA per Authentifizierungs-App als zusätzliche Sicherheitsebene für die Anmeldung. Die Authentifizierungs-App wird entweder mit E-Mail und Kennwort oder einem E-Mail-basierten Einmalcode (One-Time Passcode, TOTP) als primäre Anmeldemethode gekoppelt. Systemadmins für Enterprise-Pläne können MFA per Authentifizierungs-App auf Plan- oder Domänenebene festlegen. Für einzelne Benutzer*innen können in Grenzfällen Ausnahmen eingerichtet werden.

Hinweis: MFA per Authentifizierungs-App gilt für den Anmeldeprozess der Smartsheet-Hauptanwendung. Premium-Apps und Add-on-Funktionen verwenden die vorhandenen Smartsheet-Authentifizierungsmethoden, die für Ihre Organisation konfiguriert wurden.

Sitzungsmanagement

Admins für Enterprise-Pläne können Zeitlimits für Sitzungsinaktivität konfigurieren, sodass Benutzer*innen nach einem definierten Zeitraum der Inaktivität – von 15 Minuten bis zu 30 Stunden – automatisch aus ihrer Web- oder Desktop-Sitzung abgemeldet werden. Eine geeignete Richtlinie für diese Zeitlimits verringert das Risiko eines unbefugten Zugriffs durch unbeaufsichtigte Sitzungen und sollte Teil Ihrer grundlegenden Sicherheitskonfiguration sein.

Management des Benutzerlebenszyklus

Die zeitnahe Bereitstellung bzw. Aufhebung der Bereitstellung von Benutzerkonten gehört zu den wichtigsten Kontrollen in jedem SaaS-Sicherheitsprogramm. Smartsheet unterstützt die **SCIM-Integration (System for Cross-Domain Identity Management)** über Verzeichnisintegrationen mit Microsoft Entra ID und Okta. Das ermöglicht die automatisierte Bereitstellung und Aufhebung der Bereitstellung von Benutzerkonten direkt über Ihren Identityprovider.

Wenn SCIM aktiviert ist, wird das Smartsheet-Konto von Mitarbeitenden automatisch erstellt oder deaktiviert, wenn sie bei Ihrem IdP angelegt oder entfernt werden. Dadurch wird das Risiko beseitigt, dass verwaiste Konten weiterhin Zugriff haben. Dies reduziert auch den Verwaltungsaufwand und sorgt dafür, dass der Zugriff immer mit Ihrem maßgeblichen Verzeichnis übereinstimmt.

Smartsheet unterstützt auch die **Just-in-Time-Bereitstellung (JIT)** über SAML, die bei der ersten erfolgreichen SSO-Anmeldung von Benutzer*innen automatisch ein Benutzerkonto erstellt, ohne dass ein*e Admin vorab eine Bereitstellung durchführen muss. Dies ist besonders nützlich für große Organisationen oder Unternehmen mit hohem Onboarding-Volumen.

Empfohlene Vorgehensweisen:

- Aktivieren Sie SCIM über die Verzeichnisintegration mit Ihrem IdP als primären Mechanismus für das Management des Benutzerlebenszyklus.
- Verwenden Sie die JIT-Bereitstellung als Ergänzung für Umgebungen mit hohem Onboarding-Volumen.
- Richten Sie regelmäßige Zugriffsüberprüfungen ein, um veraltete oder verwaiste Konten zu identifizieren und zu entfernen.

API-Sicherheit und Token-Management

Smartsheet bietet eine Reihe robuster REST-APIs. Die Smartsheet-API verwendet **OAuth 2.0** für die Authentifizierung und Autorisierung und erfordert bei jeder Anforderung einen HTTP-Header mit einem gültigen Zugriffstoken. Verwenden Sie als Best Practice OAuth 2.0 für alle von Ihnen erstellten Integrationen, um einen sicheren, klar abgegrenzten API-Zugriff zu gewährleisten.

Neben OAuth 2.0 unterstützt Smartsheet persönliche API-Zugriffstoken für einzelne Benutzer*innen. Diese Token sind mit erheblichen Privilegien verbunden und erfordern eine sorgfältige Verwaltung. Systemadmins können einen Ablaufzeitraum für Token auf Planebene konfigurieren, um sicherzustellen, dass persönliche API-Token nicht auf unbestimmte Zeit gültig bleiben. Dadurch wird das Risiko durch kompromittierte, vergessene oder verwaiste Token reduziert, die an ehemalige Mitarbeitende oder eingestellte Integrationen gebunden sind. Der Ablaufzeitraum sollte mit Ihren allgemeinen Richtlinien für den Lebenszyklus von Anmeldeinformationen abgestimmt werden, wobei Sicherheitsanforderungen und die betrieblichen Auswirkungen einer regelmäßigen Token-Rotation sorgfältig abzuwägen sind.

Über das Ablaufdatum hinaus sollten Unternehmen außerdem Folgendes beachten:

- **Überprüfen Sie persönliche API-Token regelmäßig,** um ungenutzte, zu weit gefasste oder nicht mehr benötigte Token zu identifizieren.
- **Rotieren Sie Token regelmäßig** bzw. umgehend, wenn ein Verdacht auf Kompromittierung besteht.
- **Wenden Sie das Prinzip der geringsten Rechte an,** wenn Sie OAuth-basierte Integrationen von Drittanbietern konfigurieren – fordern Sie nur die Berechtigungen an, die für die Integration erforderlich sind.
- **Überprüfen Sie regelmäßig OAuth-verbundene Anwendungen von Drittanbietern,** um sicherzustellen, dass nur genehmigte Integrationen Zugriff auf die Daten Ihrer Organisation behalten.

Zugriffsmanagement

Die Verwaltung von Benutzer*innen und ihres Zugriffs ist eine grundlegende administrative Funktion, die sich sowohl auf die Sicherheit als auch auf die Einführung von Smartsheet in Ihrer Organisation auswirkt. Organisationen müssen das richtige Gleichgewicht finden und sowohl die Zusammenarbeit fördern als auch die Risiken verwalten, die mit der immer stärkeren Verteilung von Daten und Teams einhergehen. Dafür bietet Smartsheet drei unterschiedliche Governance-Modelle, die sich an den primären Möglichkeiten unserer Kunden orientieren, die Anwendung zu verwalten.

Smartsheet-Governance-Modelle

Der erste Ansatz ist unser dezentralisiertes (föderiertes) Modell, bei dem einzelne Geschäftsbereiche direkt ihren eigenen Einkauf und ihre Pläne kontrollieren. Bei diesem Modell ist die IT-Abteilung in der Regel nicht an der Verwaltung beteiligt und die Planabrechnung, Governance und Benutzerverwaltung erfolgen nach Ermessen der jeweiligen Abteilung. Dieses Modell richtet sich in der Regel an Unternehmen, die gerade erst mit der Verwendung von Smartsheet begonnen haben.

Der zweite Ansatz ist das zentralisierte (konsolidierte) Modell, bei dem alle Smartsheet-Pläne in ein einzelnes, von der IT geregeltes Abonnement konsolidiert wurden. Dies bietet direkte Kontrolle über Ausgaben, Benutzerverwaltung und Sicherheitssteuerung. Dieses Modell ist am besten für IT-Teams geeignet, die einen präzisen Überblick über sämtliche Aspekte der Smartsheet-Erfahrung wünschen.

Zu guter Letzt soll unser Hybrid-Modell einen Mittelweg bieten, bei dem die IT-Abteilung organisationsweite Einstellungen mit Enterprise Plan Manager kontrolliert, während die Lizenz- und Benutzerverwaltung direkt von Systemadmins der einzelnen Geschäftsbereiche geregelt wird. Die

Abrechnung erfolgt ebenfalls nach Plan getrennt und unterstützt die Abrechnung auf Abteilungsebene oder ein Modell, bei dem Ausgaben von Smartsheet in das Budget der einzelnen Abteilungen aufgenommen werden, anstatt zentral von der IT-Abteilung abgerechnet zu werden.

Um hohe Sicherheitsstandards zu gewährleisten, empfiehlt Smartsheet unsere Hybrid- oder zentralisierten Modelle, die Ihnen mehr direkte IT-Kontrolle über Ihre Pläne ermöglichen.

Benutzerverwaltung

Wenn verschiedene Teams in Ihrem Unternehmen Smartsheet unabhängig voneinander für eigene Anforderungen verwenden, können Sie mehrere separate Pläne erstellen. Auch Fusionen und Übernahmen führen möglicherweise zu einer Umgebung mit mehreren Smartsheet-Plänen.

Um Benutzer*innen in diesen Plänen mit dem dezentralisierten Modell zu verwalten, empfehlen wir die Aktivierung der Kontoermittlung für jeden dieser Pläne. Wenn neue Benutzer*innen mit Smartsheet in Berührung kommen, ist es ihnen oder jeder anderen Person der Domäne Ihrer Organisation möglich, eine Liste der Smartsheet-Pläne anzuzeigen, die Ihrem Unternehmen zugewiesen sind. Dies ist eine zentralisierte Möglichkeit, den Beitritt zu einem dieser bestehenden Pläne anzufordern, anstatt einen neuen zu erstellen. Diese Anforderungen werden zur Überprüfung und Genehmigung automatisch an Ihre Systemadmins weitergeleitet (über Smartsheet Admin Center).

Wenn Sie mehrere separate Pläne haben und Benutzer*innen mit dem zentralisierten Modell verwalten möchten, müssen Sie möglicherweise eine Kontenzusammenführung durchführen. Hinweis: Kunden mit Advance-Funktionen wie Dynamic View, Connectors und Control Center müssen mit dem Smartsheet-Support zusammenarbeiten, um bei einigen Aspekten der Zusammenführung weitere Unterstützung zu erhalten.

Wenn Sie das Hybrid-Modell und Enterprise Plan Manager verwenden, empfiehlt es sich, Pläne nach Abteilungen/Teams/Kostenstellen zu organisieren, sodass Sie eine Richtlinie definieren können, mit der Benutzer*innen je nach Zugehörigkeit zu einer dieser Entitäten automatisch den relevanten Plänen zugewiesen werden.

Lizenzierungs-/Abonnementmodelle

Die meisten Smartsheet-Kunden sind zu unserem aktuellen Preismodell übergegangen, das transparente, vorhersehbare Preise, eine schnellere Wertschöpfung und eine einfachere Verwaltung bietet. Einige Kunden bleiben jedoch bei unserem alten Mitarbeitermodell – die Unterschiede zwischen diesen beiden Modellen sind möglicherweise nicht sofort ersichtlich.

Altes Mitarbeitermodell

Unser altes Mitarbeitermodell basierte darauf, Ersteller*innen Zugriff auf das Produkt zu gewähren und gleichzeitig den Rollen „Bearbeiter“ und „Kommentierer“ eine kostenlose Zusammenarbeit zu ermöglichen. Dies führte zu einem erheblichen Wachstum durch virale Verbreitung, aber auch dazu, dass weniger Benutzer*innen die Vorteile der Plattform voll ausschöpfen konnten. Nur Benutzer*innen, die Sheets, Berichte, Dashboards oder Arbeitsbereiche erstellen mussten, waren zur Zahlung verpflichtet. Im Rahmen dieses Modells standen Systemadmins vor der Herausforderung, die Smartsheet-Benutzertypen zu verstehen, ihre Benutzer*innen effektiv zu verwalten, Lizenzen angemessen zuzuweisen und der Unternehmensführung den Wert der Plattform zu demonstrieren.

Benutzermodell

Auch wenn das Erstellen von Elementen eine wichtige Rolle spielt, ist Smartsheet eine Plattform für kollaboratives Arbeitsmanagement – Zusammenarbeit steht bei uns im Mittelpunkt. Die Stärke und der Mehrwert der Smartsheet-Plattform kommen besonders darin zum Ausdruck, dass sie Teams ermöglicht, Prozesse, Programme und Projekte zu erstellen und gemeinsam an wichtigen Geschäftsinitiativen zu arbeiten. Das Benutzermodell bewältigt die Herausforderungen unseres alten Modells. Es passt sich an neue Geschäftsbedürfnisse an und hilft Ihnen, Ihre Ziele zu erreichen, während Ihr Unternehmen wächst. Dafür sorgen folgende Neuerungen:

- neue Benutzertypen
- vorläufige Nutzung
- Abstimmungszeiträume und Ausgleichszahlungen

Weitere Informationen zu unserem Benutzermodell finden Sie in der Kurzdarstellung.

Benutzerverwaltung

Smartsheet ist sich bewusst, dass das einzelne Hinzufügen von Benutzer*innen nicht mehr praktikabel ist, wenn die Nutzung auf Dutzende, Hunderte oder sogar Tausende Benutzer*innen anwächst. Daher empfehlen wir, zu Beginn die Funktion für den Massenimport von Benutzer*innen in Admin Center zu verwenden, mit der Sie Ihrer Smartsheet-Organisation bis zu 1.000 Benutzer*innen auf einmal hinzufügen können. Ebenso können Sie Massenaktualisierungen verwenden, um Rollen und Benutzertypen in großem Umfang zu bearbeiten.

Fusionen und Übernahmen gehen oft mit einem Rebranding einher, bei dem Benutzer*innen eine neue E-Mail-Adresse erhalten. Über die Benutzerzusammenführung können Sie die primäre E-Mail-Adresse von mehreren Benutzer*innen auf einmal aktualisieren und doppelte Konten löschen.

Ein konsolidierter Smartsheet-Plan bietet drei zusätzliche Funktionen, um die Benutzerverwaltung weiter zu optimieren und automatisieren.

- Das automatisierte Benutzer-Provisioning (UAP) automatisiert das Hinzufügen von Benutzer*innen zu einem Enterprise-Konto. Wenn sich Benutzer*innen mit ihrer Firmen-E-Mail-Adresse bei Smartsheet registrieren oder anmelden, werden Sie automatisch Ihrem Konto hinzugefügt. Zusätzlich können Sie festlegen, ob Benutzer*innen Lizenzen erhalten oder dem Konto automatisch als vorläufige Mitglieder beitreten.
- Wenn Sie unser konsolidiertes Modell verwenden, empfehlen wir die Aktivierung des automatisierten Benutzer-Provisionings, damit Mitarbeitende automatisch dem zentralen, von der IT-Abteilung kontrollierten Konto beitreten.
- Wenn Sie das Hybrid-Modell verwenden (und wenn Ihr Unternehmen über dokumentierte Abteilungs-/Kostenstelleninformationen für Ihre Benutzerliste verfügt), empfehlen wir die Aktivierung des automatischen Benutzer-Provisionings, da diese Informationen importiert werden können, um Benutzern automatisch den richtigen Plan zuzuweisen, wenn sie eine Lizenz anfordern. Es kann auch verwendet werden, um Bewegungen unlizenzierter Benutzer*innen zwischen verschiedenen Plänen zu automatisieren.
- Verzeichnisintegrationen ermöglichen Ihnen die direkte Synchronisierung Ihrer Microsoft Entra ID- oder Okta-Verzeichnisbenutzer*innen mit Smartsheet. Binden Sie Smartsheet in Ihre bestehende Automatisierung in Entra ID oder Okta ein, um das Onboarding und Offboarding von

Benutzer*innen vollständig zu automatisieren und das Risiko zu minimieren, dass Benutzer*innen in ihren Smartsheet-Konten verweilen oder diese erneut aufrufen. Ein weiterer Vorteil sind die in einem Chargeback-Bericht von Smartsheet enthaltenen Attribute auf Benutzerebene wie Abteilung/Kostenstelle/Geschäftseinheit. Der Bericht ist in Admin Center verfügbar und kann zur Optimierung des internen Chargebacks verwendet werden. Empfohlene Best Practice ist die Synchronisierung aller Benutzer*innen im Verzeichnis mit dem Smartsheet-Konto Ihrer Organisation. Dadurch wird verhindert, dass diese Benutzer*innen bei der ersten Anmeldung unbemerkt zusätzliche Smartsheet-Konten erstellen. Als zweite Sicherheitsebene können Sie auch das automatisierte Benutzer-Provisioning aktiviert lassen, um alle Benutzer*innen abzufangen, die noch nicht über das Verzeichnis synchronisiert werden.

Wenn eine Person Ihre Organisation verlässt, muss ihr Zugriff auf Smartsheet entfernt werden. Durch das Entfernen von Benutzer*innen aus Ihrem Plan wird ihr Zugriff auf Smartsheet widerrufen und sie werden aus freigegebenen Assets im Rahmen Ihres Plans entfernt. Beachten Sie, dass die Assets ausscheidender Benutzer*innen im System verbleiben, aber möglicherweise keine*n Inhaber*in haben – Systemadmins sollten die Inhaberschaft dieser Assets vor oder nach dem Entfernen überprüfen und übertragen, um fehlerhafte Automatisierungen oder unzugängliche Inhalte zu vermeiden.

Rollen und Benutzertypen in Smartsheet

Unabhängig von Ihrer Benutzer-Provisioning-Methode müssen Sie Smartsheet-Rollen für die Personen in Ihrer Organisation festlegen.

Hinweis: Eine Rollenzuweisung sorgt nicht dafür, dass die Person Zugriff auf die Smartsheet-Assets in Ihrer Organisation erhält. Die Assets müssen zusätzlich direkt für diese Personen freigegeben werden. Somit bestimmen sowohl die Rolle als auch die Berechtigungen für den Zugriff auf Assets darüber, was Stakeholder in Smartsheet sehen und tun können. Smartsheet unterstützt die folgenden primären Rollen:

- Authentifizierte Benutzer: können je nach Lizenztyp und Berechtigungen auf den Smartsheet-Service zugreifen und diesen nutzen.
    - Mitglieder: Benutzer*innen mit uneingeschränktem Zugriff, die Assets erstellen und verwalten sowie Dateien bearbeiten oder hochladen können.
    - Vorläufige Mitglieder: Benutzer*innen mit uneingeschränktem Zugriff für einen begrenzten Zeitraum.
    - Betrachter: Benutzer*innen mit einem kostenlosen Platz, die Informationen ansehen können.
    - Gäste: Externe Benutzer*innen, die Informationen bearbeiten, kommentieren oder ansehen können.
- Gruppenadmins: erstellen und verwalten Smartsheet-Gruppen (müssen auch lizenzierte Benutzer*innen sein)*.
- Systemadmins: verwalten Benutzer*innen, Kontoeinstellungen und die Sicherheitssteuerung.

Wir empfehlen dringend, mindestens zwei aktive Systemadmins für das Smartsheet-Konto Ihrer Organisation zuzuweisen, damit Sie immer Zugriff und administrative Kontrolle haben – einschließlich der

Möglichkeit, ein Administratorkonto im Falle einer Kompromittierung oder anderer Sicherheitsvorfälle zu verwalten oder wiederherzustellen.

Gruppenadmins können Smartsheet-Gruppen erstellen, die es Benutzer*innen ermöglichen, Inhalte für die gesamte Gruppe anstatt für einzelne Mitglieder freizugeben. Gruppenadministratoren können nur Gruppen verwalten, die sie besitzen. Falls zur Einschränkung der Zusammenarbeit mit externen Mitarbeitern erforderlich, lässt sich die Gruppenmitgliedschaft auf Stakeholder in Ihrer Organisation beschränken.

Wenn Sie einem Benutzer keine der oben aufgeführten Rollen zuweisen, wird sein Zugriff auf die Smartsheet-Assets (Sheets, Berichte, Dashboards oder WorkApps) eingeschränkt, die für ihn freigegeben wurden. Stakeholder*innen müssen lizenzierte Benutzer*innen sein, um Smartsheet-Assets zu erstellen. Sie können direkt über die Smartsheet-App eine Lizenz anfordern. Systemadmins können Anforderungen einzeln oder massenweise im Abschnitt Lizenzanforderungsmanagement in Admin Center nachverfolgen und bearbeiten. Wenn Sie bereits einen Vorgang für die Verwaltung von Lizenzanforderungen etabliert haben, profitieren Sie möglicherweise von einem benutzerdefinierten Upgrade-Bildschirm, der Benutzer*innen zum Einreichen ihrer Lizenzanforderung auf diese internen Prozesse verweist.

Gäste

Benutzer*innen außerhalb Ihrer Domäne, für die Smartsheet-Assets freigegeben wurden, gelten als Gäste. Smartsheet ermöglicht Ihrer Organisation, mit vertrauenswürdigen externen Parteien zusammenzuarbeiten, ohne dass für diese Gäste Kosten anfallen. Um die Sicherheit bei der Zusammenarbeit mit externen Mitarbeitenden sicherzustellen, empfehlen wir den Einsatz von drei zentralen Admin-Steuerelementen:

Die sichere Freigabe ermöglicht Ihnen die Angabe bestimmter Domänen oder E-Mail-Adressen, die vertrauenswürdig und für die Zusammenarbeit mit externen Mitarbeitenden autorisiert sind.

Sheetzugriffsberichte enthalten eine Liste der Gäste, die Zugriff auf die Smartsheet-Inhalte Ihrer Organisation haben.

Über das Admin Center kann der Zugriff auf Elemente zentral widerrufen werden, sodass Gäste von Inhalten entfernt werden, die sie nicht mehr benötigen.

Authentifizierungssteuerung für Gäste

Um vertrauliche Inhalte bei der Zusammenarbeit mit externen Benutzer*innen weiter zu schützen, bietet Smartsheet eine erweiterte Authentifizierung für Gäste, die dafür sorgt, dass nur autorisierte Benutzer*innen Zugriff auf Ihre Inhalte erhalten.

Die Einmalanmeldung für externe Mitarbeitende (EC-SSO) ermöglicht Systemadmins, **die Verwendung der vom Unternehmen festgelegten Identityprovider durchzusetzen**. So wird sichergestellt, dass nur über SSO verifizierte Benutzer*innen auf freigegebene Inhalte zugreifen können. Darüber hinaus gibt die Multi-Faktor-Authentifizierung für externe Mitarbeitende (EC-MFA) Admins die Möglichkeit, **die MFA-Durchsetzung für externe Benutzer*innen als Zugriffsbedingung festzulegen**. Wenn diese Option aktiviert ist, überprüft Smartsheet beim Anmelden der externen Benutzer*innen über deren Identityprovider, ob die Multi-Faktor-Authentifizierung (MFA) verwendet wurde. Wird diese Anforderung nicht erfüllt, wird der Zugriff blockiert.

Diese Funktionen bieten IT- und Sicherheitsteams auf Enterprise-Ebene die Flexibilität und das Vertrauen, die Zusammenarbeit sicher zu skalieren, insbesondere in stark regulierten oder risikosensiblen Umgebungen.

Daten-Governance

Effektive Daten-Governance ist für moderne Unternehmen unerlässlich, um sicherzustellen, dass Informationen im Besitz der Organisation in Übereinstimmung mit geltenden Vorschriften, Unternehmensrichtlinien und branchenbasierten Best Practices erstellt, verwendet, freigegeben und geschützt werden.

Diese Steuerelemente sind nicht nur aus regulatorischen Gründen erforderlich, sondern gewährleisten außerdem die Effizienz, Vertraulichkeit des Geschäfts und Geschäftskontinuität:

- Auf Benutzerebene muss die Organisation effektive Tools bereitstellen, um die Sichtbarkeit einzuschränken, damit nur relevante Stakeholder relevante Informationen zu sehen bekommen.
- Auf Organisationsebene muss das Unternehmen mit geeigneten Tools für eine effektive Erstellung und Durchsetzung von Richtlinien ausgestattet sein.

Daten-Governance auf Benutzerebene

Die meisten Benutzer*innen sind mit den Berechtigungsstufen in Smartsheet (Betrachter, Kommentierer, Bearbeiter, Admin und Inhaber) vertraut. Dynamic View und WorkApps bieten zusätzliche, detailliertere Einstellungen und eine höhere Flexibilität, um effektive Daten-Governance-Funktionen auf Benutzerebene zur Verfügung zu stellen. Die Einschränkung des Zugriffs auf die relevantesten Inhalte fördert die Prozesseffizienz (da sich Benutzer*innen auf die Elemente konzentrieren müssen, die ihre Aufmerksamkeit erfordern), gewährleistet aber außerdem die Sicherheit, indem das von Smartsheet verfolgte Prinzip der geringsten Privilegien standardmäßig auf einer detaillierteren Ebene angewendet wird.

Dynamic View

Nicht alle Geschäftsprozesse erfordern vollständige Transparenz. Bei vielen Prozessen – Auftragsmanagement, Zusammenarbeit mit Anbietern, Projekte, an denen sowohl interne als auch externe Teams beteiligt sind – muss engmaschig kontrolliert werden, welche Inhalte für wen freigegeben werden.

Dynamic View ermöglicht die Zusammenarbeit ohne Kompromisse bei der Vertraulichkeit. Mit Dynamic View können Sheetinhaber*innen relevante Zeilen und Felder selektiv für bestimmte Mitarbeitende freigeben, ohne die zugrunde liegenden Sheets freizugeben. Dies ermöglicht verschiedene Anwendungsfälle, bei denen bestimmte Unternehmensbenutzer Elemente selektiv für Anbieter, gemischte interne und externe Teams oder organisationsübergreifend freigeben und zur Zusammenarbeit nur in bestimmten Bereichen einladen können. Alle haben Zugriff auf die erforderlichen Informationen – und zwar ausschließlich darauf.

WorkApps

WorkApps ermöglichen Ihnen, Ihre Arbeit zu optimieren und die Zusammenarbeit unter Verwendung benutzerfreundlicher Apps zu vereinfachen, die direkt aus Sheets, Formularen, Dashboards, Berichten

und mehr erstellt werden. Sie können das jeweilige App-Erlebnis für Ihre Teammitglieder individuell an deren jeweilige Rolle anpassen und dabei gemeinsam mit denselben zugrunde liegenden Datensätzen arbeiten. Apps werden mit derselben mehrstufigen Sicherheit der Enterprise-Klasse wie die Smartsheet-Plattform skaliert.

WorkApps beseitigen die Notwendigkeit, die in der WorkApp enthaltenen Assets freizugeben. Sie können eine WorkApp mit einer gefilterten Ansicht ausgewählter Sheets und Berichte erstellen, ohne dass diese Sheets oder Berichte für die Endbenutzer freigegeben werden müssen. Den Benutzer*innen wird nur die „WorkApp“-Ansicht dieser Assets angezeigt.

Einstellungen für Daten-Governance-Richtlinien auf Organisationsebene

Smartsheet ermöglicht Admins, sicherzustellen, dass die Funktionen der Plattform in Übereinstimmung mit den Governance-Richtlinien der Organisation verwendet werden. Mithilfe dieser Steuerelemente implementieren Administratoren gute Leitlinien für die Daten-Governance, um sicherzustellen, dass Daten korrekt und nur von Personen verarbeitet werden, die mit diesen Daten umgehen müssen.

Administratoren legen selbst fest, wie Benutzer mit bestimmten Funktionen interagieren sollen. Sollen Sheetinhaber in der Lage sein, ihre Sheets zu veröffentlichen und neue Automatisierungen zu erstellen? Haben Sie ein bestimmtes Speichersystem, von dem aus Dateien angehängt werden müssen? Sollen externe Mitarbeiter in der Lage sein, für sie freigegebene Inhalte herunterladen? Dies sind einige Beispiele für Fragen, die sich Admins stellen sollten, um die geeigneten Einstellungen für die organisationsweite Implementierung effektiv zu evaluieren.

Diese Richtlinien gelten auch für die sichere Freigabe. Wenn Sie die Freigabe von Daten und Assets auf bestimmte Domänen oder E-Mail-Adressen einschränken möchten, ist dies das richtige Tool. Wie bereits erwähnt wird anhand der sicheren Freigabe auch festgelegt, ob Ihre Organisation Smartsheet-Elemente für andere Organisationen wie Anbieter und Partner freigeben kann.

Sicherheit bei Drittanbieterintegrationen

Smartsheet bietet ein mehrschichtiges OAuth 2.0-Sicherheitsmodell, bei dem Zugriffstoken durch die zugrunde liegenden Freigabeberechtigungen der autorisierenden Benutzer*innen begrenzt sind, sodass Integrationen niemals die Zugriffsrechte der Person überschreiten können, die sie autorisiert hat. Enterprise-Admins können über Admin Center planweite Richtlinien für den Ablauf von Token durchsetzen, wodurch alle OAuth-Token nach einer konfigurierbaren Dauer automatisch widerrufen werden. Admins können das Offboarding von Benutzer*innen auch über die Okta- oder Entra ID-Verzeichnissynchronisierung (über SCIM) automatisieren, sodass zugehörige Token neutralisiert werden, wenn Mitarbeitende das Unternehmen verlassen. Für kontinuierliche Transparenz erfassen die Ereignisberichte von Smartsheet über 100 Arten von administrativen und Benutzeraktivitäten in einem sechsmonatigen Audit-Protokoll und lassen sich direkt in Skyhigh Security CASB und Microsoft Defender for Cloud Apps integrieren, um Anomalien zu erkennen und auslöserbasierte Alarme zu erstellen.

MAM-Einstellungen von Microsoft Intune

Da Unternehmen zunehmend auf mobilen Zugriff angewiesen sind, um die Produktivität ihrer Mitarbeitenden aufrechtzuerhalten, bietet Smartsheet ab April 2026 Mobile Application Management (MAM)-Einstellungen über Microsoft Intune. Damit können IT-Admins Sicherheitsrichtlinien der Enterprise-Klasse durchsetzen, ohne Geräte vollständig registrieren zu müssen.

Organisationen mit den Plänen Pro, Business, Enterprise und Advance Work Management können detaillierte Richtlinien konfigurieren, z. B. Anforderungen für die Authentifizierung mit PIN und biometrischen Daten, Datenverschlüsselung, Einschränkungen für das Kopieren/Einfügen und für Screenshots, Blockierung der Tastatur von Drittanbietern, Druckschutz, Durchsetzung einer Betriebssystem-Mindestversion, Jailbreak- und Root-Erkennung sowie die automatisierte Datenlöschung nach einem definierten Offline-Zeitraum. Dieser Ansatz auf Anwendungsebene ermöglicht Unternehmen, Daten in der Smartsheet-Mobil-App zu schützen und gleichzeitig die Privatsphäre der Mitarbeitenden auf privaten Geräten zu schützen – und so Sicherheitskonformität mit einer positiven Benutzererfahrung in Einklang zu bringen.

Steuerung des Widgets für Webinhalte

Dashboards unterstützen das Einbetten interaktiver Inhalte (Videos, Diagramme, Dokumente und mehr). Administratoren haben die Möglichkeit, diese Funktion zu aktivieren oder deaktivieren und eine genehmigte Liste unterstützter Domänen für das Widget für Webinhalte zu definieren. Als Best Practice empfehlen wir, dies auf interne Unternehmensdomänen zu beschränken.

Automatisierungsberechtigungen

Steuern Sie, wer Automatisierungen von Sheets erhalten kann. Die Optionen sind organisiert von „Eingeschränkt“ (aktiviert Aktionen nur für Benutzer, für die das Sheet freigegeben ist) bis hin zu „Uneingeschränkt“ (Automatisierung gilt für sämtliche E-Mail-Adressen und Drittanbieterintegrationen, wie z. B. Slack). Wir empfehlen die Überprüfung dieser Steuerung, um sicherzustellen, dass die Konfiguration mit dem von Ihrer Organisation gewünschten Maß an interner und externer Zusammenarbeit übereinstimmt.

Anlagensteuerung

Legen Sie fest, ob Planmitglieder Dateien von ihrem eigenen Computer oder von Cloud-Speicherservices von Drittanbietern wie Google Drive, OneDrive, Box, Dropbox, Evernote oder Egnyte durch das Anhängen eines Links (URL) hochladen können. Um die Aufnahme von Daten aus nicht genehmigten Quellen zu verhindern, aktivieren Sie nur die Anbieter von Anlagen, die gemäß den internen Richtlinien Ihres Unternehmens genehmigt wurden.

Veröffentlichungssteuerung

Durch das Veröffentlichen eines Sheets, Berichts oder Dashboards werden eine eindeutige URL, auf die jeder zugreifen kann, ohne sich bei Smartsheet anzumelden, sowie ein iFrame-Code erzeugt, den Sie in den Quellcode einer Website einbetten können, um das Sheet oder den Bericht dort anzuzeigen.

Sie können die Veröffentlichung von Sheets, Berichten, Dashboards und iCal untersagen – in diesem Fall wird die Schaltfläche „Veröffentlichen“ nicht mehr auf dem Smartsheet-Asset angezeigt. Sie können außerdem den Zugriff auf veröffentlichte Elemente auf Personen in Ihrer Smartsheet-Organisation beschränken. Wir haben festgestellt, dass sicherheitsbewusste Kunden in der Regel die Veröffentlichung zulassen, aber den Zugriff auf veröffentlichte Elemente auf Personen in ihrem Konto beschränken.

Sichere Freigabe

Mit dieser Funktion können Sie die Freigabe nach Domäne oder nach spezifischer E-Mail-Adresse einschränken (z. B. um sicherzustellen, dass Sheets nur für Personen freigegeben werden, die eine E-Mail-Adresse des Unternehmens haben). Die Durchsetzung der sicheren Freigabe geht über direkte Freigabeaktionen hinaus – eingebettete Inhalte in Dashboards werden auch nur Betrachter*innen

angezeigt, die gemäß den Einstellungen für die sichere Freigabe Ihrer Organisation autorisiert sind. **Smartsheet empfiehlt ausdrücklich, die sichere Freigabe zu implementieren, um die Zusammenarbeit mit externen Mitarbeitenden zu steuern**. Um die Aktualisierung und Pflege Ihrer Liste für die sichere Freigabe zu vereinfachen, empfehlen wir Ihnen außerdem, die Liste mithilfe von Anforderungen zu verwalten, die über ein Smartsheet-Webformular erfasst werden.

Steuerung von Offline-Formulareinreichungen

Bei Verwendung der Mobil-App aktiviert Smartsheet automatisch die Offline-Einreichung von Formularen, um Anwendungsfälle zu unterstützen, in denen Benutzer*innen möglicherweise keine konsistente Verbindung haben (z. B. auf einer Baustelle). Dieses Steuerelement ermöglicht Admins, die Offline-Einreichung von Formularen zu deaktivieren (oder wieder zu aktivieren), um zu kontrollieren, ob Benutzer*innen die Mobil-App ohne Verbindung starten können, um Formulare zu übermitteln.

Steuerung der Kommunikationsintegration

Von Smartsheet unterstützte Kommunikationsservices sind Google Chat, Microsoft Teams, Slack und Cisco Webex. Kontoadmins können nach eigenem Ermessen einen Service oder mehrere Services aktivieren.

Protokollierung und Berichterstellung

Sie können Berichte herunterladen, die verschiedene Aspekte der Smartsheet-Nutzung über Ihre Organisation hinweg abdecken, um kontinuierliche Einblicke in die Nutzung, Benutzer*innen, Inhalte, Abrechnung und den Zugriff im Zusammenhang mit Smartsheet zu erhalten:

Sheetzugriffsbericht

Generiert eine CSV-Datei mit den Namen aller Sheets, Berichte und Dashboards, die zum Plan im Konto gehören, dem Namen des Arbeitsbereichs, in dem diese Elemente gespeichert sind (falls zutreffend), den Mitarbeitenden, für die die Sheets freigegeben wurden, und dem Zeitstempel der letzten Änderung. Wir empfehlen die regelmäßige Überprüfung dieses Berichts, um die Liste der externen Mitarbeitenden zu prüfen, die Zugriff auf Assets im Eigentum der Personen in Ihrer Organisation haben.

Bericht über veröffentlichte Elemente

Generiert eine Excel-Datei mit allen veröffentlichten Elementen. Gut geeignet für die Datensicherheit oder um nachzuverfolgen, wer bestimmte Elemente veröffentlicht hat. Anhand dieses Berichts können Sie die Konfiguration der Veröffentlichungssteuerung nach Bedarf festlegen.

Benutzerlistenbericht

Generiert eine CSV-Datei mit allen Mitgliedern (eingeladen und aktiv) im Plan, einem Zeitstempel, aus dem hervorgeht, wann sie zum Plan hinzugefügt wurden, ihren Zugriffsstufen (Systemadmin, Gruppenadmin usw.), der Anzahl der Sheets, deren Inhaber*innen sie sind, und dem Zeitstempel der letzten Anmeldung bei Smartsheet.

Bericht zum Anmeldeverlauf

Systemadmins in Mehrbenutzerkonten können sich über Admin Center einen Bericht mit einer Liste des aktuellen Anmeldeverlaufs per E-Mail senden lassen.

Chargeback-Bericht

Der Chargeback-Bericht ist im Admin Center verfügbar und kann von Kunden, die die Verzeichnisintegration verwenden, zur Optimierung des internen Chargebacks genutzt werden. Hierdurch werden dem vorhandenen Bericht Spalten für Geschäftseinheit, Abteilung und Kostenstelle hinzugefügt, wenn Kunden ihre Benutzerliste herunterladen, und die für die interne Chargeback-Berichterstattung erforderlichen Daten bereitgestellt.

Weitere Protokollierungs-/Überwachungsmechanismen

- **Aktivitätsprotokoll:** Bietet ein Protokoll der Änderungen, die an einem Asset vorgenommen wurden, sowie der Person, die sie vorgenommen hat, und den Zeitpunkt der Änderungen. Dies beinhaltet Bearbeitungen wie das Löschen von Zeilen (einschließlich der gelöschten Daten), die Person, die das Element angezeigt hat, und die Angabe, ob Änderungen an Freigabeberechtigungen vorgenommen wurden.

- **Zellenverlauf:** Zeigt ein Protokoll der Änderungen auf Zellebene sowie die Person, die sie vorgenommen hat, ihre Rolle und den Zeitpunkt der Änderungen an. Benutzer*innen können einfach Daten aus dem Zellenverlauf kopieren und einfügen, um frühere Informationen wiederherzustellen, die unter Umständen fälschlicherweise gelöscht oder geändert wurden.

- **Systemspalten:** Zeigen den Zeitpunkt der letzten Bearbeitung jeder Zeile sowie die Person an, die die Änderung vorgenommen hat.

- **Sicherheitsbewertung:** Hilft Systemadmins, ihre Smartsheet-Sicherheitslage zu bewerten und zu stärken. Dazu wird eine datengesteuerte Bewertung bereitgestellt, die auf den implementierten Sicherheitsfunktionen basiert. Die Bewertung richtet sich nach Best Practices der Branche und enthält eine kategorisierte Aufschlüsselung der Richtlinien und eine intuitive Messzahl, um die Sicherheitslage und Verbesserungen im Laufe der Zeit nachzuverfolgen. Die Funktion kann über Admin Center aufgerufen werden.

- **Ereignisberichte:** Eine erweiterte Funktion, die Einblicke in über 100 Arten von Sicherheits- und Benutzeraktivitätsereignissen bietet, um ein umfassendes Protokoll zu erstellen. Weitere Informationen zu Ereignisberichten finden Sie weiter unten.

Erweiterte Steuerung der Daten-Governance

Smartsheet bietet einige erweiterte Funktionen, die Kunden mit besonders strengen Datenschutzanforderungen die Daten-Governance-Steuerung ermöglichen. Diese Funktionen sind in Smartsheet Advance Platinum und Smartsheet Safeguard enthalten.

Datenegressrichtlinien

Die Datenfreigabe birgt immer ein gewisses Maß an Risiko in sich, doch beim Umgang mit besonders vertraulichen Daten muss unbedingt sichergestellt werden, dass Unternehmensdaten in Ihrem Konto und unter Ihrer Kontrolle bleiben.

Systemadministratoren können Datenegressrichtlinien zum Schutz vertraulicher Daten verwenden, indem sie detailliert steuern, wie Daten sowohl innerhalb als auch außerhalb Ihrer Organisation exportiert werden können.

Datenegressrichtlinien können implementiert werden, um zu verhindern, dass interne und externe Mitarbeiter die folgenden Aktionen in Sheets, Berichten und Dashboards durchführen:

- Als neu speichern
- Als Vorlage speichern
- Als Anlage senden
- Veröffentlichen
- Drucken
- Exportieren

Benutzer, die versuchen, eine eingeschränkte Aktion auszuführen, erhalten eine Benachrichtigung, dass dieses Verhalten aufgrund der von Ihrer Organisation implementierten Datenegressrichtlinie untersagt ist.

Diese Einschränkungen sollen Mitarbeitende daran hindern, vertrauliche Informationen zu böswilligen Zwecken zu speichern oder freizugeben.

Ereignisberichte

Um die Informationssicherheit zu gewährleisten, benötigen viele Unternehmen kontinuierliche Einblicke in die Art und Weise, auf die ihre Geschäftsanwendungen wie Smartsheet verwendet werden. Die Transparenz folgender Aspekte sollte sichergestellt werden:

- Wer Sheets erstellt
- Wer Arbeitsbereiche erstellt
- Wer Objekte löscht
- Wer für wen ein Sheet freigegeben hat

Ereignisberichte bieten detaillierte Einblicke in das Benutzerverhalten und Aktivitäten innerhalb des Smartsheet-Kontos Ihrer Organisation. Mit dieser Funktion können Sie Datenverluste überwachen und ungewöhnliche Nutzungsmuster identifizieren, um die Sicherheits- und Compliance-Richtlinien Ihrer Organisation besser durchzusetzen.

Ereignisberichte bieten einen JSON-Datenfeed von Smartsheet-Nutzungsereignissen („Ereignissen“) in einem Plan (Organisation) und werden über die Ereignisberichte-API abgerufen. Bei dem Service werden zu mehr als 120 Ereignissen in Smartsheet Berichte erstellt und ab dem Datum, an dem der Feed aktiviert wird, bis zu sechs Monate lang Daten gespeichert.

Um von diesem Feed zu profitieren, werden Ereignisberichte in der Regel in andere Sicherheitssysteme integriert, die Überwachung, Benachrichtigungen, Richtlinienerstellung und -durchsetzung und Schutz vor Datenverlusten (DLP) bieten. Diese App werden von Drittanbietern verkauft – in der Regel Cloud Access Security Broker Systems (CASB-Systeme), Security Information and Event Management Systems (SIEM-Systeme) oder eine Kombination aus CASB- und SIEM-Systemen. Ab und zu entwickeln Unternehmen ihre eigenen Überwachungs- und Reaktionssysteme, anstatt auf die Systeme von Drittanbietern zurückzugreifen.

Wichtige Anwendungsfälle für Ereignisberichte:

- Schutz vor Datenverlusten
- Umgang mit personenbezogenen Daten
- Daten-Governance
- Einblicke in die Zusammenarbeit gewinnen

Datenspeicherungssteuerung

Je mehr Inhalte Ihre Organisation in einer SaaS-Anwendung aufbewahrt, desto größer ist das Risiko, dem Ihr Unternehmen ausgesetzt ist.

Die Datenspeicherungssteuerung von Smartsheet gibt Organisationen die Möglichkeit, eine Richtlinie zu erstellen, die basierend auf durchzusetzenden Kriterien vorschreibt, wann Inhalte gelöscht werden sollen.

Diese Richtlinien können auf dem Datum basieren, an dem ein Sheet erstellt oder das letzte Mal geändert wurde, um sicherzustellen, dass nur aktive oder aktuelle Inhalte in Ihrer Smartsheet-Instanz verbleiben und Ihr Risikoprofil eingeschränkt wird.

Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK)

Smartsheet verwendet Verschlüsselung, um die Daten von Kunden zu schützen und ihnen zu helfen, die Kontrolle darüber zu behalten. In der Regel befinden sich die Daten von Kundenunternehmen in einer mandantenfähigen Architektur, die mit Standardschlüsseln verschlüsselt ist, die über AWS KMS verwaltet und regelmäßig geändert werden.

Vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) sind für Organisationen mit sensiblen oder regulierten Daten bestimmt, für die sie ihren eigenen Verschlüsselungsschlüssel verwalten müssen. CMEK ermöglichen es Enterprise-Organisationen, Cloud-SaaS-Anwendungen zu verwenden und zugleich eine Datensteuerung aufrechtzuerhalten, die mit der einer lokalen Installation vergleichbar ist. So wird dem Datenspeicher in Smartsheet eine vom Kunden verwaltete Verschlüsselungsebene hinzugefügt, um erweiterte Datensicherheits- und Governance-Richtlinien zu fördern.

Bei CMEK-Kunden befinden sich die Daten in physisch isolierten Single-Tenant-Aurora-Clustern, die mit einem KMS-Schlüssel verschlüsselt sind, der im eigenen AWS-Konto des Kunden gehostet wird – Smartsheet hat keinen Zugriff auf die Root-Schlüssel. Um CMEK zu verwenden, brauchen Kunden Zugriff auf Amazon Web Services Key Management Service (AWS KMS), da Kundenschlüssel direkt in AWS eingerichtet und verwaltet werden.

Smartsheet verwendet CMEK, um die Daten Ihrer Organisation so zu verschlüsseln, dass sie jederzeit unter Ihrer Kontrolle bleiben. Genauer gesagt speichert oder kontrolliert Smartsheet diese Verschlüsselungsschlüssel nicht und muss diese Schlüssel von der AWS KMS-Instanz des Kunden anfordern und abrufen, wenn auf Ihre Sheetdaten zugegriffen werden muss.

Da Ihre Organisation die Kontrolle über den in AWS KMS gespeicherten CMEK hat, können Sie Smartsheet jederzeit den Zugriff auf den CMEK und damit den Zugriff auf Ihre Daten entziehen. Durch das Löschen der Hauptschlüssel in AWS KMS kann Ihre Organisation die Daten effektiv sperren. Eine böswillige Partei könnte mit CMEK verschlüsselte Daten auch mit einer Kopie der Datenbank, des Quellcodes und der Cloud-Verschlüsselungsschlüssel von Smartsheet nicht lesen. CMEK kann als eigenständiges Angebot erworben werden, sofern Kunden die entsprechenden Kaufkriterien erfüllen.

Globale Kontokonfiguration

Die Kontosicherheit ist nicht auf technische Funktionen wie die Datenverschlüsselung, die Klassifizierung oder Authentifizierungsoptionen beschränkt. Sicherheit kann auch einen so einfachen Vorgang wie die Anbringung des Logos Ihrer Organisation auf sämtlichen zugehörigen Elementen beinhalten.

Die Einstellungen der globalen Kontokonfiguration ermöglichen Ihnen, ein visuelles Branding (und weitere Einschränkungen) zu implementieren, damit Ihre Benutzer*innen wissen, dass Sie auf die richtigen Informationen zugreifen.

Systemadmins können Logos global hinzufügen, um Ihre Smartsheet-Bereitstellung an organisationsweiten Branding-Anforderungen auszurichten. Mit der Branding-Sperre stellen Sie sicher, dass jedes neue Asset mit dem gleichen Branding versehen wird.

Steuerelemente für die Anpassung und Kontokonfigurationen von Smartsheet ermöglichen es Ihnen außerdem, benutzerdefinierte Willkommensbildschirme festzulegen. Sie können Folgendes erstellen: benutzerdefinierte Hilfebildschirme mit Beschreibungen der ersten Schritte, Lizenzanforderungsbildschirme, über die Benutzer*innen Sie kontaktieren können, oder benutzerdefinierte und mit Branding versehene Willkommensbildschirme, die angezeigt werden, wenn sich Benutzer*innen anmelden. Die Bildschirme können eine Anforderung enthalten, dass Benutzer*innen die Nutzungsbedingungen annehmen müssen, bevor sie weitere Informationen abrufen können.

Wenn Sie eine konsistente visuelle Identität mit benutzerdefinierten Informationen kombinieren, wissen Benutzer*innen, dass sie auf die richtigen Tools und Informationen zugreifen, was die Sicherheit optimiert.

Sicherheits-, Datenschutz- und Compliance-Praktiken von Smartsheet

Die Cybersicherheits-, Datenschutz- und Datensicherheitsprogramme bei Smartsheet basieren auf einem ganzheitlichen Ansatz und beginnen mit strategischen Informationssicherheitsrichtlinien, die von der Unternehmensführung definiert und unterstützt werden. Diese Richtlinien wurden so konzipiert, dass sie mit den strategischen Risikomanagementpraktiken des Unternehmens übereinstimmen, Sicherheitsrisiken proaktiv verwalten und überwachen, die Sicherheit durch Prozessreife und eine effektive Systemarchitektur fördern und die Benutzer*innen mittels Schulungen und Sensibilisierung in die Lage versetzen, umsichtige Entscheidungen über Sicherheitsrisiken zu treffen.

Modell der geteilten Verantwortung

Effektive Sicherheit erfordert die Koordination aller Ebenen des Technologie-Stacks. Smartsheet nutzt ein dreistufiges Modell, bei dem AWS die zugrunde liegende Cloud-Infrastruktur sichert, Smartsheet die Plattform und die Anwendungsebene sichert und Kunden die Verantwortung für ihre eigene Kontoverwaltung, ihre Daten und ihre Authentifizierungspraktiken tragen.

Infrastruktur und Architektur

Die Plattform von Smartsheet basiert vollständig auf Amazon Web Services (AWS) und Google Cloud Platform (GCP) und wurde mit strikten Umgebungsabgrenzungen konzipiert, um die Integrität und Vertraulichkeit von Kundendaten in jeder Phase des Softwarelebenszyklus zu schützen.

Umgebungssegmentierung: Jede Umgebung – einschließlich Entwicklungs-, Staging- und Produktionsregionen in den USA, der EU, Australien und GovCloud – wird in einem eigenen AWS-Konto und einer eigenen Organisationseinheit oder einem GCP-Projekt betrieben. Dadurch wird sichergestellt, dass Arbeitslasten außerhalb der Produktion vollständig von Systemen getrennt sind, die Kundendaten verarbeiten. Für die regionsübergreifende Netzwerkkonnektivität verwendet Smartsheet AWS CloudWAN, das logische Routing-Segmente erzwingt – dedizierte Netzwerkbahnen, die den jeweils isolierten Umgebungen zugewiesen sind. Der Datenverkehr zwischen Umgebungen muss die Inspektionsinfrastruktur der AWS Network Firewall durchlaufen, die regelbasierte Kontrollen anwendet und den gesamten Datenverkehr zwischen den Umgebungen protokolliert. In jeder Region werden redundante Inspektionsknoten bereitgestellt, um sicherzustellen, dass dieser Schutz kontinuierlich verfügbar bleibt.

Mandantenisolation: Jedem Smartsheet-Kunden wird eine eindeutige Mandantenkennung zugewiesen, die bei allen Vorgängen zur Datenspeicherung, -abfrage und -bereitstellung konsistent verwendet wird. Dadurch wird sichergestellt, dass kein Prozess auf Daten anderer Kunden zugreifen kann. Auf Infrastrukturebene unterliegen in Containern gespeicherte Arbeitslasten Netzwerk- und Sicherheitsrichtlinien, die die laterale Kommunikation zwischen Mandantenkontexten einschränken. Das Modell für dedizierte Konten pro Umgebung stellt sicher, dass die Umgebung isoliert wird und Entwicklungs- oder Testaktivitäten niemals Live-Kundendaten beeinträchtigen.

Sicherer Entwicklungslebenszyklus (SDLC): Sicherheit ist in jede Phase der Produktentwicklung integriert. Bevor Code geschrieben wird, überprüfen Sicherheitsentwickler*innen die Architektur und das Design, um Fehler zu möglichst geringen Kosten zu identifizieren. Darauf folgt eine strukturierte Bedrohungsmodellierung, bei der mithilfe von Datenflussdiagrammen potenzielle Angriffsvektoren identifiziert und sämtliche Erkenntnisse zur Nachverfolgung dokumentiert werden. Ergänzend dazu erfolgt eine gezielte Code-Überprüfung, um sicherzustellen, dass die vorgesehenen Gegenmaßnahmen korrekt implementiert sind. Kontinuierliche statische Anwendungssicherheitstests (Continuous Static Application Security Testing, SAST) und dynamische Anwendungssicherheitstests (Dynamic Application Security Testing, DAST) sind in die CI/CD-Pipelines integriert und scannen automatisch jede Codeänderung, bevor sie die Produktionsumgebung erreichen kann.

Penetrationstests: Smartsheet führt Penetrationstests als Standardbestandteil der Sicherheitsüberprüfung durch. Sie werden auf der Grundlage der Risikoklassifizierung angewendet. Die Tests werden vom internen Sicherheitsteam von Smartsheet oder von qualifizierten externen Dritten durchgeführt. Sie folgen in der Regel einer Gray-Box-Methode, die Tester*innen Zugriff auf den Quellcode sowie eine Staging-Umgebung bietet, um Schwachstellen aufzudecken, die bei rein externen Tests möglicherweise übersehen werden. Kontinuierliche automatisierte Schwachstellenscans ergänzen diese punktuellen Bewertungen in der gesamten Infrastruktur, einschließlich Compute-Instanzen, Containern, Funktionen und Compute-Images.

Nachverfolgung und Behebung von Schwachstellen: Schwachstellen, die durch Scans oder Tests identifiziert werden, werden durchgängig mit SLA-basierten Behebungszielen nachverfolgt, die in der Smartsheet-Richtlinie für das Schwachstellenmanagement definiert sind.

Cloud Security Posture Management (CSPM): Smartsheet nutzt Wiz CSPM für sein Cloud-Security-Management-Tool zur Erkennung, Nachverfolgung und Behebung von Sicherheitsproblemen in der Cloud.

Wiz CSPM ist die primäre Lösung für das Cloud-Sicherheitsmanagement, die umfassende Einblicke in die Multi-Cloud-Umgebung gewährleistet. Durch die Bereitstellung einer einheitlichen „diagrammbasierten“ Ansicht der Infrastruktur ermöglicht Wiz Smartsheet, komplexe Angriffspfade zu identifizieren und Risiken auf der Grundlage der tatsächlichen Gefährdung statt anhand von isolierten Schwachstellen zu priorisieren.

Wichtige Sicherheitsvorteile:

- **Kontinuierliche Compliance-Überwachung:** Wiz ordnet die Cloud-Konfigurationen von Smartsheet automatisch den branchenüblichen Frameworks (wie SOC 2, ISO 27001 und FedRAMP) zu, um die kontinuierliche Einhaltung unserer regulatorischen Verpflichtungen sicherzustellen.

- **Erkennung und Behebung in Echtzeit:** Die Plattform bietet kontinuierliche Scans von Cloud-Ressourcen und warnt Sicherheitsteams in Echtzeit vor Fehlkonfigurationen, Identitätsrollen mit übermäßigen Berechtigungen oder offengelegten Geheimnissen.
- **Geringere Angriffsfläche:** Durch die Korrelation von Softwareschwachstellen mit der Erreichbarkeit des Netzwerks kann Smartsheet große Risiken schnell beheben und sicherstellen, dass die Infrastruktur gegen externe Bedrohungen gesichert bleibt.

Datensicherheit

Wir haben die Sicherheit direkt in unsere Plattform integriert, um sicherzustellen, dass Ihr wichtigster Vermögenswert – Ihre Daten – geschützt wird. Smartsheet beauftragt Dritte mit der Durchführung von Audits unserer Sicherheitspraktiken, einschließlich einer Bewertung und Bescheinigung nach SOC 2 Typ II (oder einem gleichwertigen Prüfungsstandard) sowie technischen Sicherheitsbewertungen mit Penetrationstests. Darüber hinaus automatisiert das Schwachstellenmanagement-Programm von Smartsheet die Identifizierung und Behebung von Netzwerk- und Systemschwachstellen in Smartsheet-Unternehmens- und Produktionsumgebungen. Smartsheet verwendet eine Verschlüsselung, um Ihre Daten zu schützen und Ihnen zu helfen, die Kontrolle über sie zu behalten.

Kundendaten werden in der Infrastruktur von Amazon Web Services gehostet. Im Ruhezustand gespeicherte Daten werden mit dem branchenüblichen AES-256-Verschlüsselungsalgorithmus verschlüsselt, der über Amazon RDS-Verschlüsselung bereitgestellt wird. Übertragene Daten werden durch die TLS 1.2-Technologie geschützt. Verschlüsselungsschlüssel werden über AWS KMS mit einem zweistufigen Modell verwaltet: Ein Schlüsselverschlüsselungsschlüssel (Key Encryption Key, KEK) schützt Datenverschlüsselungsschlüssel (Data Encryption Keys, DEKs), mit denen Kundendaten verschlüsselt werden. Bei Standardplänen verwaltet Smartsheet den KEK in Ihrem Namen mit automatischer Rotation. Für Organisationen, die eine direkte Kontrolle benötigen, sind vom Kunden verwaltete Verschlüsselungsschlüssel (CMEK) als eigenständiges Add-on verfügbar – siehe Abschnitt „CMEK“ weiter oben.

Datenschutz

Datenschutz ist für Smartsheet von zentraler Bedeutung. Je nach Art der Daten erfüllen wir zwei unterschiedliche Rollen. Wir sind ein Datenverantwortlicher für personenbezogene Daten, die wir direkt erfassen – wie Konto-, Nutzungs- und Abrechnungsinformationen – und ein Auftragsverarbeiter für Kundeninhalte, d. h. die Daten, die Kunden auf die Plattform hochladen oder übermitteln. Als Auftragsverarbeiter verarbeiten wir diese Daten nur gemäß den Anweisungen der Kunden, die die Kontrolle behalten.

Datenschutz ist eines unserer Grundprinzipien und prägt die Art und Weise, wie wir Funktionen entwickeln und Entscheidungen treffen – nicht etwas, das wir nachträglich ergänzen. Daher verwenden wir Kundeninhalte nicht für unsere eigenen Zwecke – auch nicht für Marketing oder das Trainieren von Foundation-Modellen Dritter.

Smartsheet verfolgt einen globalen Datenschutzansatz, der die Anforderungen wichtiger Vorschriften wie der DSGVO, der DSGVO des Vereinigten Königreichs und des CCPA erfüllen oder übertreffen soll. Im Folgenden finden Sie eine Liste von Zertifizierungen. Hier ist eine kurze Zusammenfassung unserer wichtigsten Verpflichtungen:

- **Datenverarbeitungsvereinbarung (DPA)** – unsere DPA (Data Processing Agreement) ist automatisch Teil der Smartsheet-Benutzervereinbarung für alle Kunden und enthält die Standardvertragsklauseln der EU und des Vereinigten Königreichs. Kunden, die ein separat unterschriebenes Exemplar wünschen, können dies über die Smartsheet-DPA-Seite anfordern – die Bedingungen bleiben unverändert.
- **Datenresidenz** – Kunden können auswählen, wo ihre Kundeninhalte gehostet werden. Weitere Informationen finden Sie im Abschnitt „Smartsheet-Regionen“.
- **Datenschutz „by design“ und „by default“** – wir integrieren die Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in unsere Anwendungsfunktionen. Die Gewährleistung des Datenschutzes ist eine Kernfunktion, keine Nebensache.
- **Unterauftragsverarbeiter** – wir veröffentlichen eine Liste der von Smartsheet eingesetzten Unterauftragsverarbeiter und prüfen und wenden vertragliche Sicherheitsvorkehrungen für Dritte an, die Kundeninhalte verarbeiten. Weitere Informationen finden Sie im Abschnitt „Risikomanagement für Lieferanten und Lieferketten“.
    - **Folgenabschätzungen für Übertragungen** – um unsere Kunden bei der Einhaltung von Datenschutzbestimmungen zu unterstützen, haben wir Folgenabschätzungen für Übertragungen durchgeführt, die im Smartsheet-Sicherheitspaket verfügbar sind. Wenden Sie sich an Ihre*n Vertriebsmitarbeiter*in oder reichen Sie dieses Formular ein, um eine Kopie zu erhalten.

KI-Sicherheit und Datenschutz

Die KI-Funktionen von Smartsheet basieren auf denselben Sicherheits- und Datenschutzprinzipien, die für den Rest unserer Plattform gelten.

Ihre Daten werden zu keinem Zeitpunkt mit den Daten anderer Kunden vermischt. Sie werden niemals verwendet, um die Foundation-Modelle Dritter zu trainieren. Sie haben stets die Kontrolle über Ihre Daten. Jede KI-Aktion oder -Empfehlung lässt sich erklären, überprüfen und bis zu ihrer Quelle zurückverfolgen.

Eingegebene Prompts und generierte Ausgaben werden nur für Support- und Missbrauchsüberwachungszwecke gespeichert und nach 180 Tagen automatisch gelöscht.

Organisationen mit spezifischen Richtlinienanforderungen, die eine vollständige Deaktivierung von KI-Funktionen erfordern, können diese Option über den Smartsheet-Support anfordern. Die Deaktivierung von KI-Funktionen wirkt sich negativ auf die Fähigkeit von Kunden aus, den Smartsheet-Service vollständig zu nutzen.

Einen vollständigen Überblick darüber, wie Ihre Daten von Smartsheet-KI-Tools verarbeitet werden, finden Sie in unserem Whitepaper zur KI-Sicherheit oder auf der Webseite zu verantwortungsvoller KI.

Betriebsmanagement

Wir haben Richtlinien und Methoden implementiert, um sicherzustellen, dass Ihre Daten geschützt und an mehreren physischen Standorten gesichert sind. Unsere Teams untersuchen kontinuierlich neue Sicherheitsbedrohungen und implementieren aktualisierte Gegenmaßnahmen, um nicht autorisierten Zugriff auf den Abonnementdienst zu verhindern oder nicht geplante Ausfälle zu vermeiden. Der Zugriff auf alle Smartsheet-Produktionssysteme und -Daten ist auf der Grundlage des Prinzips der geringsten Privilegien und des tatsächlichen Informationsbedarfs auf autorisierte Mitglieder des Smartsheet-Teams für den technischen Betrieb beschränkt.

Die Cloud-Infrastruktur von Smartsheet ist redundant und zuverlässig – mit einer garantierten Verfügbarkeit (SLA) von 99,9 % oder besser. Echtzeitinformationen zur Serviceverfügbarkeit und -leistung werden auf der Smartsheet-Statusseite veröffentlicht. Kunden, die sich für automatische Updates angemeldet haben, werden per E-Mail und/oder SMS über wichtige Vorfälle benachrichtigt.

Reaktion auf Vorfälle und Benachrichtigung bei Datenschutzverletzungen

Smartsheet verfügt über dokumentierte Pläne zur Reaktion auf Vorfälle, die jährlich überprüft und getestet werden. Im Falle eines Sicherheitsvorfalls umfasst unser Reaktionsprozess die Vorbereitung, Erkennung und Analyse, Eindämmung, Beseitigung und Wiederherstellung sowie Aktivitäten nach dem Vorfall. Sofern gesetzlich oder vertraglich vorgeschrieben, benachrichtigt Smartsheet die von unseren Kunden bereitgestellten Kontakte innerhalb der gesetzlich vorgeschriebenen Fristen. Kunden sollten alle Sicherheitsbedenken über den Smartsheet-Support melden. Ausführliche Informationen zu unseren Verfügbarkeitsverpflichtungen finden Sie in unserem Service-Level-Agreement.

Offenlegung von Schwachstellen und Bug-Bounty-Programm

Smartsheet betreibt ein aktives Bug-Bounty-Programm, das unabhängige Sicherheitsforschende einlädt, Schwachstellen in unserer Plattform zu identifizieren und verantwortungsbewusst offenzulegen. Dieses Programm stellt eine bewusste Erweiterung unserer Sicherheitslage dar. Es bietet eine zusätzliche Überprüfungsebene neben unseren internen Tests und ermöglicht uns, Probleme zu erkennen und zu lösen, bevor sie ausgenutzt werden können. Für verantwortungsvolle Meldungen werden finanzielle Prämien vergeben, die sich am Schweregrad der identifizierten Schwachstelle orientieren.

Programmumfang: Das Bug-Bounty-Programm umfasst die Hauptplattform und die Enterprise-Funktionen von Smartsheet, darunter die primäre Smartsheet-Anwendung, die Enterprise-Zugriffssteuerung, Dynamic View, Ereignisberichte und Plattformintegrationen wie Salesforce- und Jira-Connectors. Brandfolder und Outfit sind ebenfalls im Umfang enthalten. Das Programm wird über die interne Bug-Bounty-Plattform von Smartsheet verwaltet. Forschende erhalten eigene Testkonten, um ihre Arbeit sicher durchzuführen. Nicht im Umfang enthaltene Aktivitäten sind u. a. Tests mit Konten, die Forschenden nicht gehören, automatisierte Scans und Denial-of-Service-Tests, Phishing-Tests und alle Tests, die sich auf Live-Kundendaten auswirken könnten.

Klassifizierung des Schweregrads: Alle gemeldeten Schwachstellen werden anhand eines vierstufigen Schweregradmodells bewertet und klassifiziert:

- **Kritisch (S1):** Probleme, die die Übernahme des Servers oder Kontos, den unbefugten Zugriff auf oder die Änderung von Kundendaten oder einen Denial-of-Service ermöglichen – ohne dass

hierfür Anmeldedaten oder Benutzerzugriff erforderlich sind. Beispiele hierfür sind SQL-Injection, offengelegte Geheimnisse oder fehlende Zugriffssteuerungen für unsichere Objekt-IDs.
- **Hoch (S2):** Die gleichen Auswirkungsklassen wie „Kritisch“, aber zum Ausnutzen der Schwachstellen sind ein authentifizierter Zugriff oder vorhandene Anmeldeinformationen erforderlich. Beispiele dafür sind Cross-Site-Scripting-Schwachstellen, die Session-Hijacking ermöglichen, oder die Möglichkeit, Inhalte durch die Umgehung von Standardkontrollen dauerhaft zu löschen.
- **Mittel (S3):** Probleme, die nur begrenzte Auswirkungen auf andere Benutzer*innen innerhalb derselben Organisation oder auf freigegebene Assets haben. Beispiele hierfür sind die Ausweitung von Berechtigungen innerhalb eines freigegebenen Sheets oder die Verwendung unsicherer kryptografischer Primitives.
- **Gering (S4):** Alle anderen Sicherheitsprobleme, die die oben genannten Kriterien nicht erfüllen.

SLAs für die Behebung: Sobald eine Schwachstelle bestätigt und bewertet wurde, verpflichtet sich Smartsheet zu den folgenden Zeitplänen für die Behebung:

- **Kritisch:** Behebung oder Minderung so schnell wie möglich, spätestens jedoch innerhalb von **15 Tagen**.
- **Hoch:** Behebung oder Minderung innerhalb von **30 Tagen**.
- **Mittel:** Behebung oder Minderung innerhalb von **90 Tagen**.
- **Gering:** Behebung oder Minderung innerhalb von **180 Tagen**.

Diese SLAs gelten ab dem Datum der Erkennung oder externen Offenlegung. Bei Problemen mit dem Schweregrad „Kritisch“ wird von allen erforderlichen Teammitgliedern erwartet, dass sie die Behebung priorisieren und auf die Bearbeitung anderer Aufgaben verzichten, bis das Problem gelöst ist.

Verantwortungsbewusste Offenlegung: Smartsheet verpflichtet sich, während des gesamten Offenlegungsprozesses mit Sicherheitsforschenden zusammenzuarbeiten. Forschende werden gebeten, die Ergebnisse privat zu melden, keine Tests mit Kundenkonten durchzuführen und alle Handlungen zu vermeiden, die die Serviceverfügbarkeit beeinträchtigen könnten. Im Gegenzug verpflichtet sich Smartsheet zu einer zeitnahen Bestätigung, transparenter Kommunikation und einer angemessenen Anerkennung und Vergütung für gültige Ergebnisse. Organisationen, die ein potenzielles Sicherheitsproblem außerhalb des Bug-Bounty-Programms melden möchten, können Smartsheet unter bugbounty@smartsheet.com direkt kontaktieren. Smartsheet behält sich das Recht vor, Bug-Bounty-Programme jederzeit zu beenden oder auszusetzen.

Risikomanagement für Lieferanten und Lieferketten

Smartsheet führt bei allen Unterauftragsverarbeitern eine Due-Diligence-Prüfung durch, bevor sie hinzugezogen werden, wobei alle Anbieter, die auf Kundeninhalte zugreifen, diese verarbeiten oder speichern, einer genaueren Prüfung unterzogen werden. Diese Überprüfungen umfassen die Untersuchung relevanter Sicherheitsdokumentation wie SOC 1- und/oder SOC 2-Typ-II-Berichte, Ergebnisse von Penetrations- und Schwachstellentests, PCI-DSS-Audits und Sicherheitsbewertungen durch Dritte. Unterauftragsverarbeiter werden jedes Jahr neu bewertet, um zu bestätigen, dass ihre Sicherheitskontrollen weiterhin den Standards von Smartsheet entsprechen.

Jeder Unterauftragsverarbeiter ist verpflichtet, Verträge zu unterzeichnen, die die Sicherheits- und Datenschutzerwartungen von Smartsheet widerspiegeln. Diese Vereinbarungen umfassen Datenverarbeitungsanforderungen, Sicherheitsstandards, Meldepflichten für Vorfälle und Regeln, die

diese Erwartungen auf alle zusätzlichen Anbieter übertragen, die der Unterauftragsverarbeiter gegebenenfalls einsetzt.

Damit Kunden besser nachvollziehen können, wer an der Verarbeitung ihrer Daten beteiligt ist, veröffentlicht Smartsheet eine öffentlich zugängliche Liste der Unterauftragsverarbeiter. Weitere Informationen zur Verwendung von Unterauftragsverarbeitern finden Sie im Smartsheet-Sicherheitspaket. Wenden Sie sich an Ihre*n Vertriebsmitarbeiter*in oder reichen Sie dieses Formular ein, um eine Kopie zu erhalten.

Sicherheit, Kontinuität und Redundanz im Rechenzentrum

Wir arbeiten mit branchenweit anerkannten Hostingpartnern zusammen, um sicherzustellen, dass Sie Dienste für Ihre Organisation zuverlässig auf einer vertrauenswürdigen Plattform bereitstellen können. Wir verfügen über eine standortübergreifende Datenredundanz und hosten unsere Services in AWS-Rechenzentren. Unsere Rechenzentrumsumgebungen sind nach SOC 1, SOC 2, ISO 27001 und FedRAMP/DISA IL5 geprüft und zertifiziert. Wir gewährleisten eine kontinuierliche Überwachung und die Verwaltung der Produktionsumgebung rund um die Uhr. Smartsheet hält interne Prozesse und Pläne aufrecht, um mit Ereignissen in Bezug auf die Geschäftskontinuität und Szenarien im Zusammenhang mit der Notfallwiederherstellung umzugehen. Diese Pläne werden jährlich überprüft und getestet und in der gesamten Organisation an entsprechendes Personal weitergegeben. Durch unser AWS-Hosting nutzen wir mehrere Rechenzentren mit unabhängiger Stromversorgung, HLK und Brandunterdrückungssystemen, um zu verhindern, dass im Falle einer Naturkatastrophe mehrere Rechenzentren gleichzeitig betroffen sind.

Smartsheet-Regionen

Mit Smartsheet-Regionen haben Sie die Kontrolle darüber, wo Ihre Daten gehostet werden, und können so die regionalen Datenschutz- und Governance-Anforderungen Ihrer Organisation einfacher erfüllen. Drei regionale Instanzen sind verfügbar: USA (US), Europäische Union (EU) und Australien (AU).

Die EU-Instanz wird in einem AWS-Rechenzentrum in Frankfurt am Main gehostet. Die AU-Instanz wird in einem AWS-Rechenzentrum in Sydney, Australien, gehostet. Daten, die in einer regionalen Instanz erstellt wurden, verbleiben in dieser Region – Inhalte können nicht über regionale Grenzen hinweg übertragen oder aufgerufen werden.

Weitere Informationen zu den Optionen für Smartsheet-Regionen finden Sie im Smartsheet Trust Center und auf unserer Seite zur Datenresidenz.

Audits und Zertifizierungen

ISO- und SOC 2-Compliance

Smartsheet validiert seine Sicherheitslage anhand einer Kombination aus Trust Services-Kriterien und der ISO/IEC-Standardfamilie (oder im Wesentlichen gleichwertigen Standards). Diese Zertifizierungen bieten eine unabhängige Bestätigung unseres Engagements für betriebliche Exzellenz.

- **SOC 2 Typ II:** Smartsheet wird jährlich von einem externen Wirtschaftsprüfungsunternehmen geprüft. Dabei werden das Design und die betriebliche Wirksamkeit unserer Kontrollen getestet.
    - **Umfang:** Dieser Bericht umfasst die gesamte Smartsheet-Anwendungsumgebung, einschließlich der Hauptplattform und der Infrastruktur in unseren gehosteten Rechenzentren.
    - **Trust Services-Kriterien:** Sicherheit, Verfügbarkeit und Vertraulichkeit.

- **ISO/IEC 27001, 27017 und 27018 (Sicherheit und Cloud):** Diese Zertifizierungen validieren unser Informationssicherheitsmanagementsystem (ISMS). 27001 ist unser grundlegendes Sicherheits-Framework, aber wir halten uns auch an 27017 für bestimmte Sicherheitssteuerungen für Cloud-Dienste und an 27018 zum Schutz personenbezogener Daten in öffentlichen Clouds.

- **ISO/IEC 27701 (Datenschutz):** Als Erweiterung unseres Sicherheits-Frameworks konzentriert sich dieser Standard auf unser Privacy Information Management System (PIMS), um sicherzustellen, dass wir als Datenverantwortlicher und Auftragsverarbeiter globale Datenschutzanforderungen wie die DSGVO, die DSGVO des Vereinigten Königreich und den CCPA erfüllen.

- **ISO/IEC 22301 (Kontinuität):** Diese Zertifizierung stellt sicher, dass wir über ein robustes System für das Geschäftskontinuitätsmanagement verfügen, um bei unvorhergesehenen Ereignissen ausfallsicher und verfügbar zu bleiben.

- **ISO/IEC 42001 (KI-Management – *In Arbeit*):** Wir streben derzeit diese Zertifizierung an, um ein formelles Managementsystem für künstliche Intelligenz zu etablieren und sicherzustellen, dass unsere KI-gesteuerten Funktionen ethisch und sicher entwickelt und bereitgestellt werden.

- **Datenschutzrahmen EU-USA (DPF):** Smartsheet und seine verbundenen Unternehmen nehmen am Datenschutzrahmen EU-USA (EU-US DPF), an der Erweiterung des Datenschutzrahmens EU-USA für das Vereinigte Königreich und dem Datenschutzrahmen Schweiz-USA (Swiss-US DPF) gemäß den Vorgaben des US-Handelsministeriums (insgesamt der „Datenschutzrahmen“) teil. Wir verpflichten uns zur Einhaltung der Grundsätze des Datenschutzrahmens in Bezug auf personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum („EWR“), dem Vereinigten Königreich und der Schweiz in die USA übermittelt werden. Weitere Informationen zum Datenschutzrahmen und unsere Zertifizierung finden Sie auf der Website des DPF-Programms. Die Verpflichtungen von Smartsheet gemäß den Grundsätzen des Datenschutzrahmens unterliegen den Ermittlungs- und Vollstreckungsbefugnissen der US-amerikanischen Kartellbehörde (United States Federal Trade Commission, FTC).

- **HITRUST Readiness**: Smartsheet hat den Status „HITRUST Readiness“ erreicht, was unsere Ausrichtung auf das HITRUST CSF-Framework und unser Engagement für robuste Sicherheits- und Datenschutzkontrollen widerspiegelt. Diese Auszeichnung unterstreicht unsere Fähigkeit, Kunden mit strengen Compliance-Anforderungen zu unterstützen, unter anderem im Gesundheitswesen, im Finanzwesen und in anderen stark regulierten Sektoren.

- **FedRAMP (Moderate):** Smartsheet wurde für das FedRAMP Connect-Programm durch das Joint Authorization Board (JAB) ausgewählt, das Smartsheet Gov basierend auf der Nachfrage von Regierungsbehörden priorisierte. Smartsheet Gov ist eine separate Smartsheet-Umgebung mit FedRAMP-Autorisierung und wurde mit Stufe 4 (IL4) des US-Verteidigungsministeriums bewertet. Dadurch wird es für die US-Regierung und zivile Behörden einfacher, Smartsheet für die Verwaltung ihrer Arbeit zu verwenden und ihre Sicherheits- und Compliance-Anforderungen zu erfüllen.

- **Sarbanes-Oxley Act von 2002:** Als ehemals börsennotiertes Unternehmen war Smartsheet zuvor zur Einhaltung des Sarbanes-Oxley Act (SOX) verpflichtet. Auch wenn wir dieser regulatorischen Anforderung nicht mehr unterliegen, hat sich Smartsheet entschieden, SOX-konforme interne Kontrollen beizubehalten, um eine starke Finanz-Governance und kontinuierliche Prüfungsbereitschaft zu gewährleisten. Diese Kontinuität spiegelt unser Engagement für betriebliche Exzellenz und organisatorische Integrität wider.

Wie auf unserer Webseite mit rechtlichen Informationen aufgeführt, verwendet Smartsheet von Amazon Web Services, Inc. („AWS“) bereitgestellte Infrastruktur, um Kundendaten zu hosten. Informationen zu sicherheits- und datenschutzbezogenen Audits und Zertifizierungen, die AWS erhalten hat, darunter die Zertifizierung nach ISO 27001 und SOC-Berichte, sind auf der Sicherheits-Website und der Compliance-Website von AWS verfügbar.

Eine vollständige Liste unserer Zertifizierungen und weitere Informationen finden Sie auf der Compliance-Seite im Smartsheet Trust Center. **Um direkten Zugriff auf wichtige Sicherheitsdokumente wie unseren CAIQ- und SOC 2-Bericht zu erhalten, wenden Sie sich bitte an die*den zuständige*n Mitarbeiter*in oder CSM für Ihr Konto, um ein „Sicherheitspaket“ anzufordern.**

Fazit und zusätzliche Ressourcen

Für die Arbeit von heute (und morgen) braucht es eine moderne Plattform für das Arbeitsmanagement, die benutzerfreundlich und sicher ist. Durch kontinuierlichen Fokus und laufende Investitionen haben wir Smartsheet von Grund auf mit strengen Anforderungen und Funktionen zur Vertraulichkeit von Daten aufgebaut. Neben den bereits verfügbaren Funktionen befinden sich einige zusätzliche Sicherheitsfunktionen derzeit in Entwicklung.

Den Systemstatus in Echtzeit finden Sie auf der Smartsheet-Statusseite. Sicherheitsdokumentation, Zertifizierungen und Compliance-Ressourcen finden Sie in unserem Trust Center.