Kiteworks | servicenow

LÖSUNGSÜBERSICHT

FÜR VERANTWORTLICHE DER SERVICENOW AI PLATFORM, IT-SERVICE-MANAGEMENT- UND SICHERHEITSTEAMS

KONTROLLIERTER DATENAUSTAUSCH IN DER SERVICENOW AI PLATFORM

Dateien auf Datensätzen folgen den Datenrichtlinien Ihres Unternehmens, der Nachweis liegt im Datensatz

Die Herausforderung

Teams steuern IT-Service, Betrieb und Änderungen auf der ServiceNow AI Platform, und jedes Ticket wird zur kleinen Dateiübertragung. Protokolle, Screenshots, Verträge und andere sensible Dokumente wandern als Anhänge und E-Mails an der Datenrichtlinie vorbei. Externen Zugang zur ServiceNow AI Platform zu geben ist teuer und vergrößert die Angriffsfläche; laut Verizon Data Breach Investigations Report 2026 gehen **48 % der Sicherheitsverletzungen** auf Dritte zurück.

Die Lösung

Kiteworks für die ServiceNow AI Platform ergänzt Incident-, Problem-, Change-Request-, Service-Catalog-Request- und Knowledge-Datensätze um einen kontrollierten Kiteworks-Ordner. Teams versenden sichere E-Mails, speichern Dateien in kontrollierten Ordnern und fordern Dateien von Anbietern, Prüfern und Kunden an, ohne den Datensatz zu verlassen. Die Kiteworks Data Policy Engine bewertet jede Datei; Übertragungen sind bis 16 TB möglich.

Wo Teams ServiceNow einsetzen und was Kiteworks ergänzt

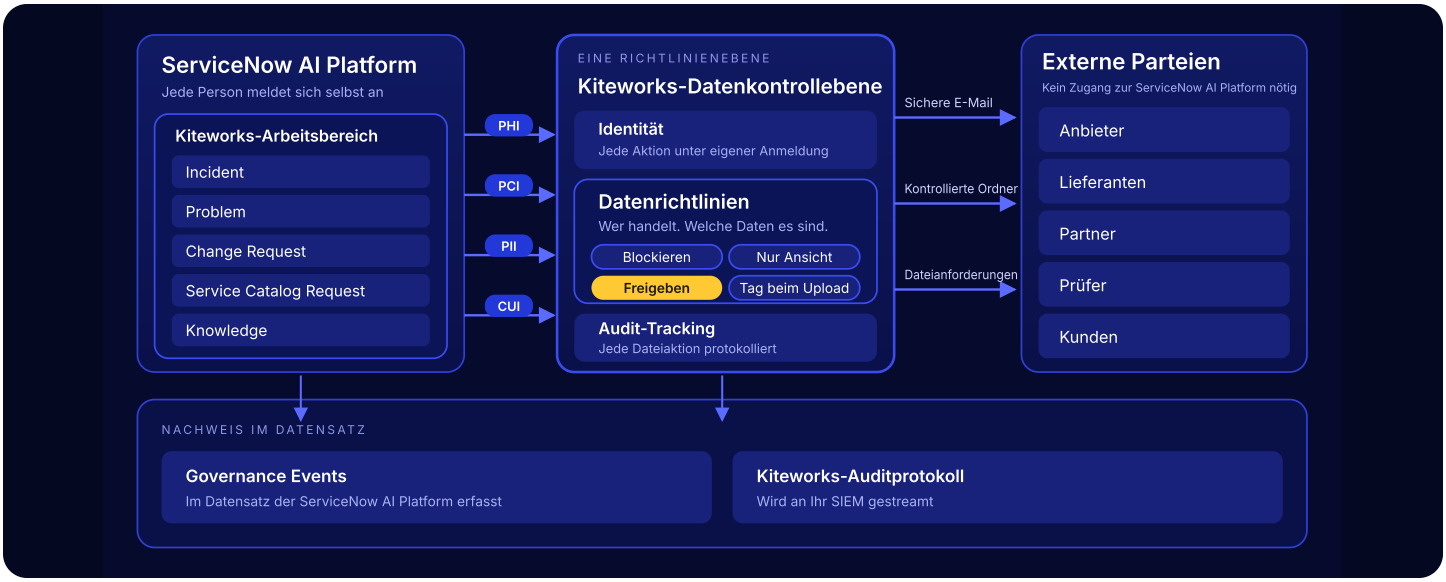
ANWENDUNGSFALL UND DATENSATZ	WAS TEAMS IM DATENSATZ TUN	WAS KITEWORKS ERGÄNZT	WARUM ES WICHTIG IST
IT Service Management Incident Service Catalog Request	Service-Desk-Mitarbeitende bearbeiten Incidents und Katalog-Anfragen von Beschäftigten und Anbietern, mit Screenshots, Protokollen und Dokumenten.	Agenten sammeln Protokolle und Screenshots im kontrollierten Ordner des Incidents statt in Anhängen. Sensible Dokumente zu einer Katalog-Anfrage gehen per sicherer E-Mail direkt aus dem Datensatz.	Die Datenrichtlinie gilt für jede über die App ausgetauschte Datei; eine große Datei ist kein Grund mehr, den Datensatz zu verlassen.
Change Management Change Request	Change-Manager holen vor einer Änderung Nachweise und Freigaben von Anbietern ein.	Der Change-Manager fordert Dateien beim Anbieter an, der sie über einen sicheren Link hochlädt, ohne die ServiceNow AI Platform zu berühren. Die Richtlinie greift beim Eingang.	Nachweise von Anbietern erreichen den Datensatz ohne Anbieter-Lizenz. Anforderung und Upload werden jeweils protokolliert.
Problem Management Problem	Problem-Manager klären die Ursache mit Ingenieuren der Anbieter und teilen Ergebnisse.	Der Ingenieur des Anbieters tritt dem Ordner als Downloader oder Collaborator bei. Mit dem Schließen des Problems entzieht der Problem-Manager den Zugriff.	Anbieter bearbeiten das Problem ohne Konto in der ServiceNow AI Platform; ihr Zugriff endet mit der Arbeit.
IT Operations und AIOps Incident Problem	Betriebsteams machen aus Ereignissen Incidents und senden Diagnose- und Konfigurationsdateien an Anbieter.	Diagnosepakete und Mitschnitte bis 16 TB laufen über einen kontrollierten Ordner; das Scan-Ergebnis wird vor dem Download geprüft.	Konfigurationsdateien beschreiben die Umgebung. Die Suche nach einem Weg, einen großen Mitschnitt zu senden, verlängert einen Ausfall.
Knowledge Management Knowledge	Autoren erstellen Artikel aus Quelldokumenten, teils mit Zugriffsbeschränkung.	Der Autor legt kontrollierte Quelldokumente im Ordner des Artikels ab, den ein Klick erzeugt; die Richtlinie bestimmt, wer sie öffnen darf.	Quellmaterial bleibt kontrolliert, der Artikel bleibt leicht zu teilen.

Die ServiceNow AI Platform steuert den Workflow. Kiteworks sorgt für die Governance der Daten, die ihn durchlaufen.

Zertifizierungen. Kiteworks Secure Gov Cloud: FedRAMP Class D, Agency Authorization in Bearbeitung; Kiteworks Federal Cloud: FedRAMP Class C zertifiziert. Zudem SOC 2 Typ II, ISO 27001 und FIPS 140-3 validiert. Unterstützt Organisationen bei der Erfüllung der Anforderungen von PCI DSS, HIPAA, DSGVO, CMMC 2.0 und NIST SP 800-171.

So funktioniert Kiteworks für die ServiceNow AI Platform

Die Kiteworks Data Policy Engine regelt E-Mail und Dateifreigabe und jetzt auch Dateien im Datensatz.



Kiteworks für die ServiceNow AI Platform: Kontrollierter Datenaustausch in jedem Datensatz.

01
Sichern
Wo liegt die Datei, und wem gehört sie?

Dateien liegen in einem kontrollierten Ordner in der gehärteten virtuellen Appliance von Kiteworks, mit Single-Tenant-Architektur, kundeneigenen Schlüsseln und Geofencing.

02
Steuern
Folgt jede Datei der Richtlinie?

Die Data Policy Engine entscheidet nach Akteur und Dateninhalt: blockieren, nur Ansicht, Freigabe verlangen oder taggen. Das Scan-Ergebnis wird vor dem Download geprüft.

03
Nachweisen
Können Sie einem Prüfer zeigen, was geschehen ist?

Governance Events erfassen im Datensatz, was Personen über die App tun. Das Kiteworks-Auditprotokoll erfasst alle Dateiaktivitäten und streamt sie an Ihr SIEM.

04
Bewegen
Hält es die Menschen arbeitsfähig?

Sichere E-Mail, kontrollierte Ordner und Dateianforderungen aus dem Datensatz. Bis 16 TB pro Übertragung, praktisch ohne Größenlimit. Externe benötigen keinen Zugang zur ServiceNow AI Platform.

ServiceNow, the ServiceNow logo, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries.

Bereit für Governance im Dateiaustausch der ServiceNow AI Platform?

www.kiteworks.com

Kiteworks

in f X ig yt

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

© 2026 Kiteworks LLC. All rights reserved.