Kiteworks | servicenow

SOLUTION BRIEF

FOR SERVICENOW AI PLATFORM OWNERS, IT SERVICE MANAGEMENT, AND SECURITY TEAMS

GOVERNED DATA EXCHANGE, INSIDE THE SERVICENOW AI PLATFORM

Files exchanged on ServiceNow AI Platform records follow company data policies, with the evidence on the record

The Challenge

Teams run IT service, operations, and change on the ServiceNow AI Platform, and every ticket becomes a small file transfer. Logs, screenshots, contracts, and other sensitive documents travel as attachments and email, outside company data policy. Giving outside parties ServiceNow AI Platform access is costly and widens exposure, and Verizon's 2026 Data Breach Investigations Report attributes **48% of breaches** to third parties.

The Solution

Kiteworks for the ServiceNow AI Platform adds a governed Kiteworks folder to Incident, Problem, Change Request, Service Catalog Request, and Knowledge records. Teams send secure email, keep files in governed folders, and request files from vendors, auditors, and customers without leaving the record. The Kiteworks Data Policy Engine evaluates each file, and transfers run up to 16 TB.

Built for ServiceNow AI Platform owners and security leaders at regulated organizations.

Where Teams Use ServiceNow, and What Kiteworks Adds

IT Service Management is the core product for most of ServiceNow's roughly 8,700 customers, with an estimated 44.4% share of the ITSM market, and IT Operations Management was part of 18 of ServiceNow's top 20 deals in Q2 2026.

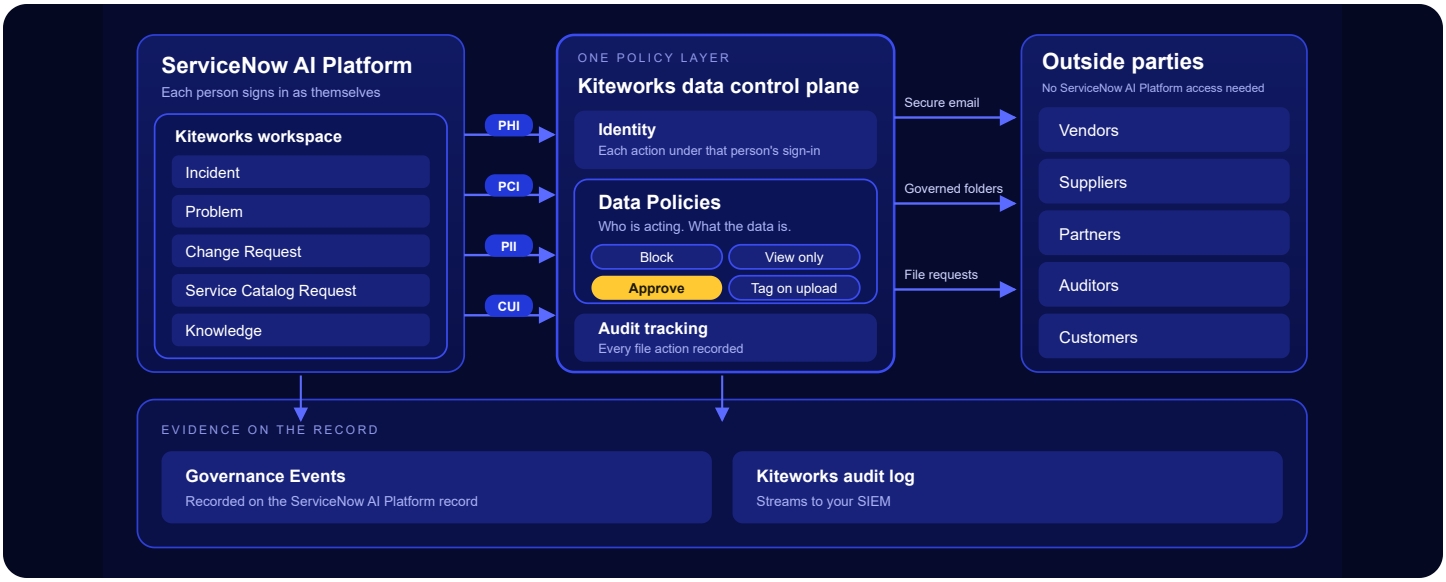
USE CASE AND RECORD	WHAT TEAMS DO ON THE RECORD	WHAT KITEWORKS ADDS	WHY IT MATTERS
IT Service Management Incident, Service Catalog Request	Service desk analysts work incidents and catalog requests for employees and vendors, with screenshots, logs, and documents attached.	Agents collect logs and screenshots in the incident's governed folder instead of attaching them. Fulfillment sends sensitive documents on a catalog request by secure email from the record.	Data policy applies to each file exchanged through the app, and a large file is no longer a reason to leave the record.
Change Management Change Request	Change managers collect vendor evidence and approvals before a change goes ahead.	The change manager requests files from the vendor, who uploads through a secure link and never touches the ServiceNow AI Platform. Policy applies on arrival.	Vendor evidence reaches the record without a vendor seat. The request and the upload are each recorded.
Problem Management Problem	Problem managers work root cause with vendor engineers and share findings.	The vendor's engineer joins the folder as a Downloader or Collaborator. The problem manager revokes the outside party's access when the problem closes.	Vendors work the problem without a ServiceNow AI Platform account, and their access ends when the work does.
IT Operations and AIOps Incident, Problem	Operations teams turn events into incidents and send diagnostics and configuration files to vendors.	Diagnostic bundles and captures, up to 16 TB, move through a governed folder with the scan verdict checked before download.	Configuration files describe the environment. Time spent finding a way to send a large capture extends an outage.
Knowledge Management Knowledge	Authors build articles from source documents, some of them restricted.	The author keeps controlled source documents in the article's folder, created with one button, where policy decides who can open them.	Source material stays governed while the article stays easy to share.

The ServiceNow AI Platform runs the workflow. Kiteworks governs the data that moves through it.

Credentials. Kiteworks Secure Gov Cloud is FedRAMP Class D Agency Auth In Process; Kiteworks Federal Cloud is FedRAMP Class C Certified. Also SOC 2 Type II, ISO 27001, and FIPS 140-3 validated. Helps organizations meet PCI DSS, HIPAA, GDPR, CMMC 2.0, and NIST SP 800-171 obligations.

How Kiteworks for the ServiceNow AI Platform Works

The Kiteworks Data Policy Engine that governs email and file sharing now governs files exchanged on the record.



Kiteworks for the ServiceNow AI Platform: Governed data exchange on every record.

01
Contain
Where does the file go, and who owns it?

Files live in a governed Kiteworks folder, not in ServiceNow AI Platform attachment storage, encrypted in transit and at rest. Choose on premises, self-hosted, Kiteworks-hosted, FedRAMP, or IRAP, with single-tenant architecture, customer-owned keys, and geofencing.

02
Control
Does every file follow policy?

The Data Policy Engine decides by who is acting and what the data is, then blocks, limits to view only, requires approval, or tags the file. The scan verdict is checked before download.

03
Prove
Can you show an examiner what happened?

Governance Events record what people do through the app, on the record. The Kiteworks audit log records all file activity and streams to your SIEM.

04
Move
Does it keep people working?

Secure email, governed folders, and file requests, all from the record. Transfers run up to 16 TB, so there is no practical size limit. Outside parties need no ServiceNow AI Platform access.

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.

Ready to Govern File Exchange Inside the 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.