

Kiteworks

Protecting Sensitive Data in Customer Support Processes

Five Compliance Best Practices for Salesforce Service Cloud® Solutions



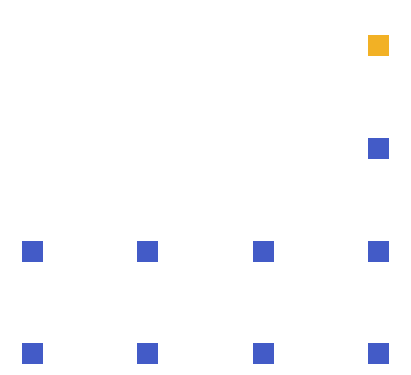


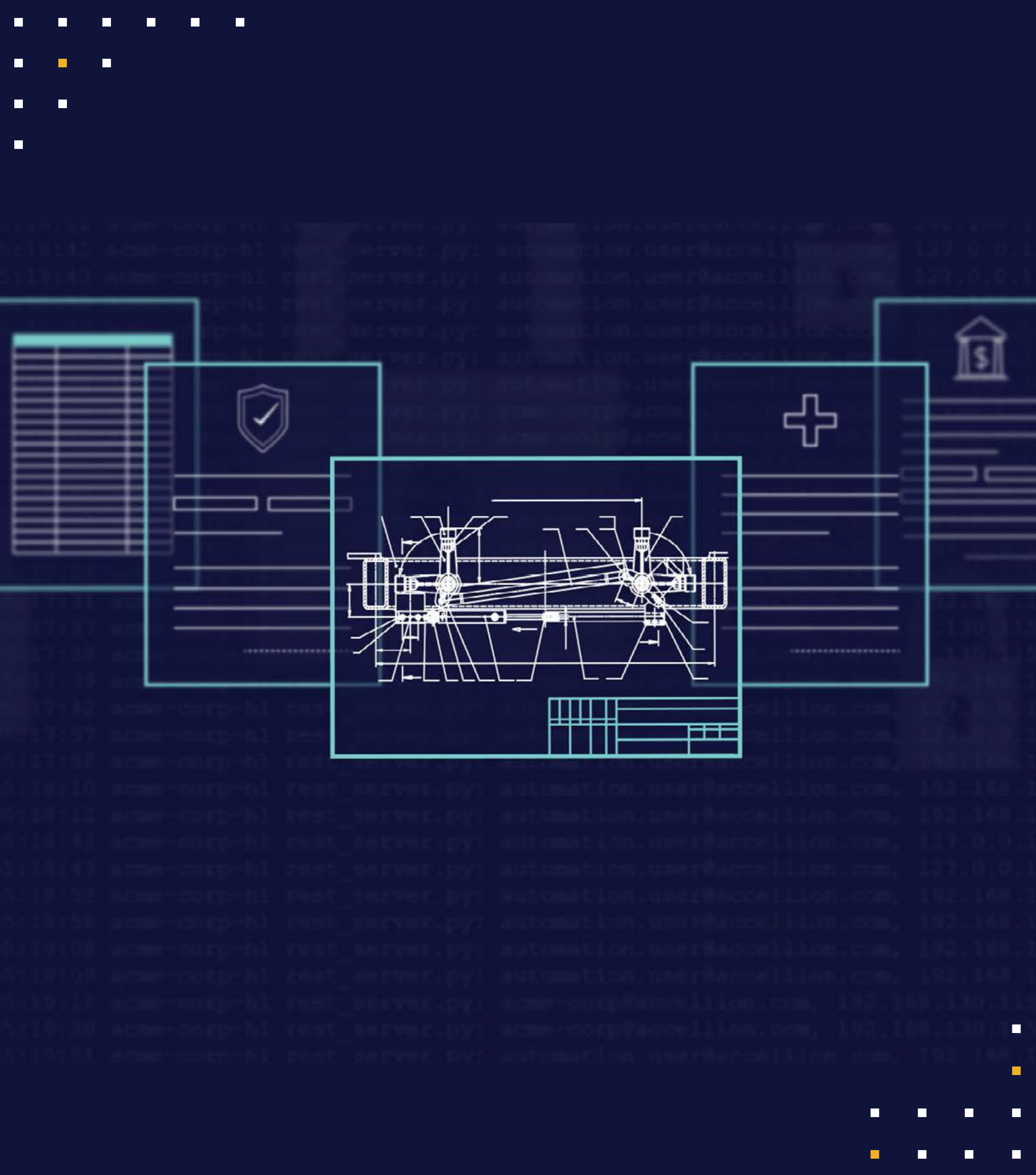
Introduction

Customer support agents have to move fast to elevate customer experiences and prevent churn. They may rotate personnel around the clock like firefighters to resolve a complex case, or individually handle numerous small cases in a day. But executives can't let up on protecting their organizations and customers from compliance fines, security breaches, and reputation loss—even as they deliver this speedy customer experience.

You risk privacy violations during the customer support process because customers share data riddled with personally identifiable information (PII), protected health information (PHI), and private financial data. Does your CISO know how your service agents receive and store customer information? Do agents know and follow your privacy policies—even under pressure? Can you prove it to an auditor?

Leading organizations maintain compliance while providing exceptional customer and employee experiences. Here are five best practices for integrating customer data with your governance policies right where your support agents work: in their Salesforce® cases.





01 Stay Out of Compliance Trouble

Treat All Customer Data as Confidential

Every industry handles customer data containing PHI, PII, financial information, or IP, requiring compliance with HIPAA, GDPR, and other regulations. You risk privacy violations every time customers send your support agents a file.

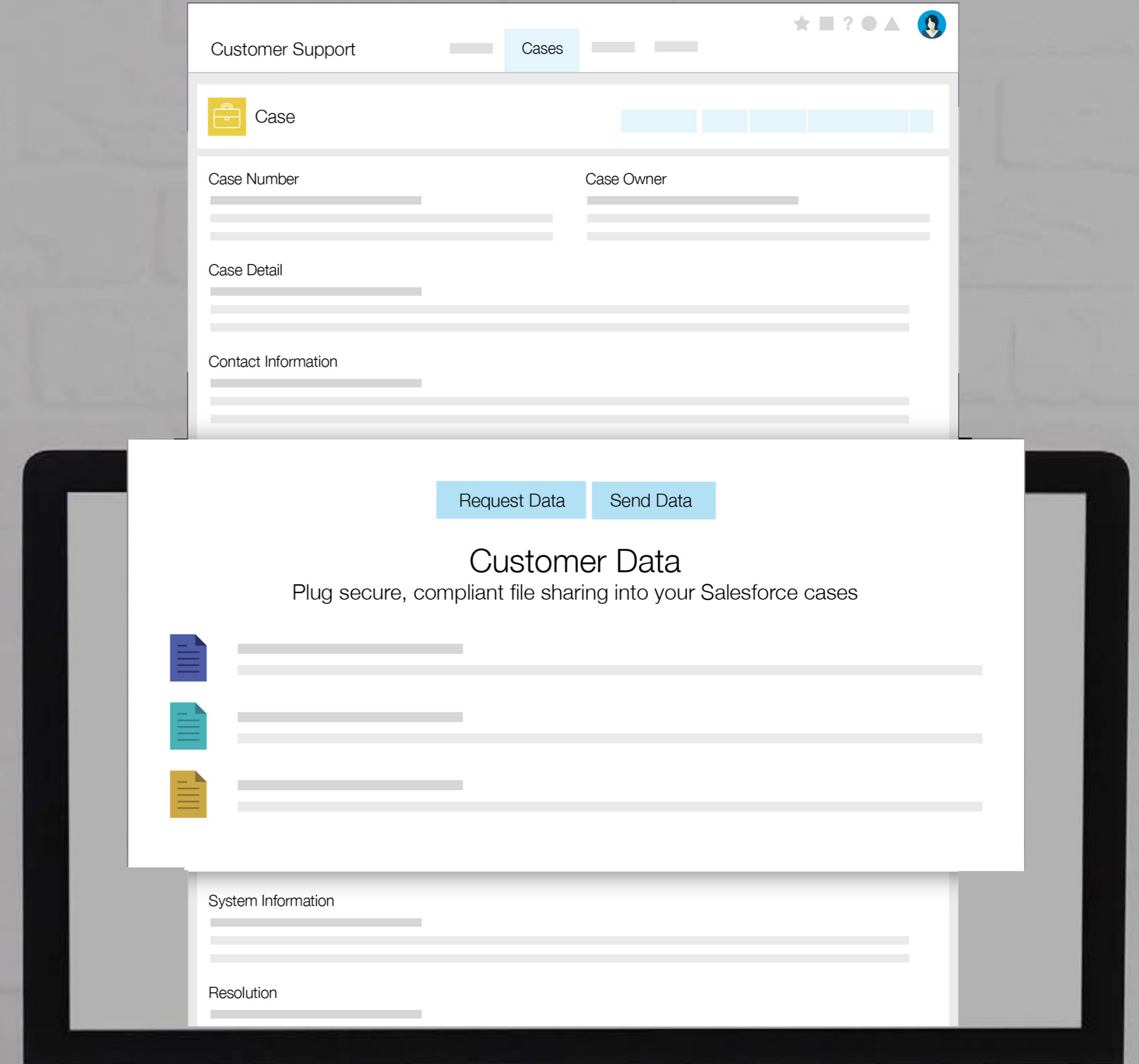
- Healthcare and insurance: test results, claims, patient records
- Manufacturing and engineering: computer aided designs (CAD), plans, budgets
- Financial services: tax histories, account details, fraud affidavits, collections letters
- Government: tax documents, criminal evidence, business registrations, health provider data
- Technology: logs, screenshots, plans, designs

Your support agents must handle customer data in compliance with data privacy laws, but you can't afford to slow them down. Tick the compliance box by automating governance enforcement, and leveraging your enterprise security infrastructure to lock down your data-sharing software.

02 Maintain a 360 Degree View

Link Customer Data to Cases

Agents can access a single view of the customer in their Salesforce solution, enabling them to personalize the customer experience. But if you provide a traditional portal or cloud file share for customers to send their data, it ends up in a disconnected silo. Instead, give agents a Salesforce case plugin to request data from their customer contacts. Let the plugin automatically link the data to the case and provide matching security permissions.





DATE/TIME	USER	ACTIVITY	IP ADDRESS	SIZE
14 Jun 2018 05:40:44	mak00@ing.ir	Downloaded file Security Architecture.docx	213.144.123.456	1.77 MB
14 Jun 2018 05:34:32	mak00@ing.ir	Downloaded file ini_script.bat	213.144.123.456	45.12 KB
14 Jun 2018 05:23:05	mak00@ing.ir	Downloaded file sys10738-01.VMDK	213.144.123.456	42.32 GB

User: mak00@ing.ir
Location: USWest
Node IP: 54.75.226.180
File Name: sys10738-01.log
Client Name: Accellion for iPhone
Client Device: iPhone 8
User Agent: kiteworks/46 CFNetwork/976 Darwin/18.2.0CFNetwork/976 Darwin/18.2.0
Size: 45440753992
Full Path: Backups/VMs/CAD03

03 Prevent Breaches

Provide Visibility Into All Support Process Data

Defending against the security threats and compliance risks that impact your support processes is a tall order. You must have visibility of every file entering and leaving your Salesforce cases. And you have to make it easy for your security, compliance, and support teams to zero in on the problems within that data deluge.

Begin by implementing an audit trail of all data transfers between your support organization and your customers. Once you have this metadata, create clear and complete real-time visualizations that answer the most important security questions about your customer support data. Where is it coming from? Where is it going to? Who is sending it? Who is receiving it? Is it sensitive?

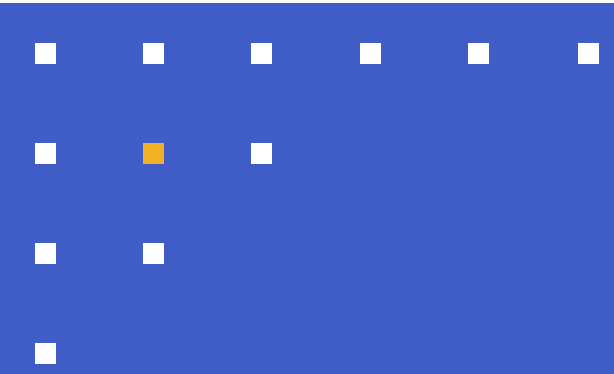
04 Avoid the End-around

Provide Simple Tools Users Want to Use

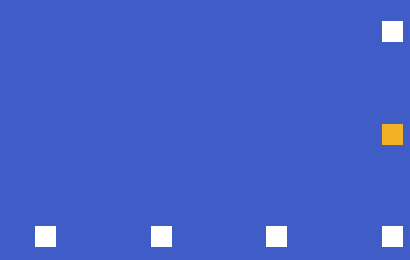
Support agents will overcome any obstacle to solve a customer problem. They may heroically circumvent a data transfer roadblock with a consumer-grade file sharing tool, or even email in the clear. But now you can't answer when the auditors ask: What confidential customer data do you have? Is it encrypted? Who intercepted it?

Prevent this end-around by enabling agents to send and receive customer data without leaving their Salesforce case screen. Support unlimited data sizes, and make sure it is reliable, even when your customers' networks aren't. And remember that your customers aren't trained: Make their uploads and downloads foolproof.





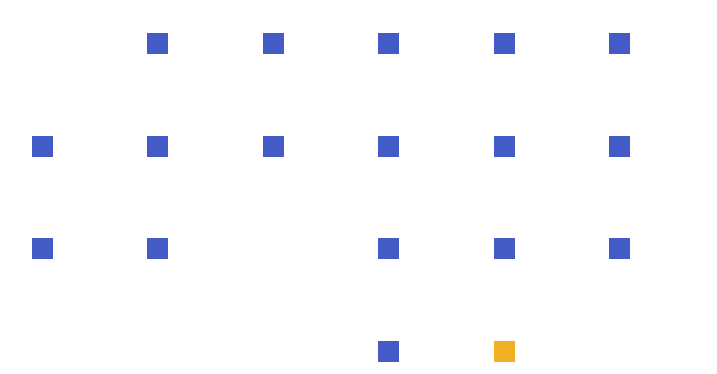
CISOs impose strict data storage policies in response to privacy regulations and constant cyberattacks, often constraining agents to store case data in Windows file shares or SharePoint folders.



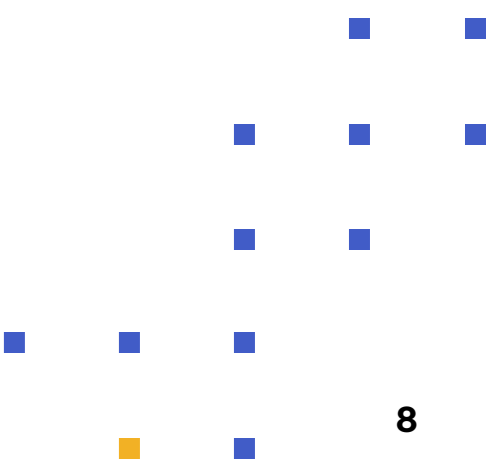
05 Reduce Costs and Ensure Compliance

Control Where Data Is Stored

CISOs impose strict data storage policies in response to privacy regulations and constant cyberattacks, often constraining agents to store case data in Windows file shares or SharePoint folders. This gives you control over the cost, but it also adds extra steps for agents, impacting the customer experience and requiring manual compliance processes. Instead, let them manage the data directly in their Salesforce cases with a plugin connected to storage you control on-premises or in a private cloud or FedRAMP Authorized environment. Now you control the costs and the compliance.



Kiteworks-enabled Private Content Network





Kiteworks

www.kiteworks.com

July 2022

Copyright © 2022 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.

