

Kiteworks

FedRAMP Private Cloud:

The Gold Standard for
Sensitive Content
Communications

**5 Reasons Why Security-first
Businesses Choose FedRAMP**



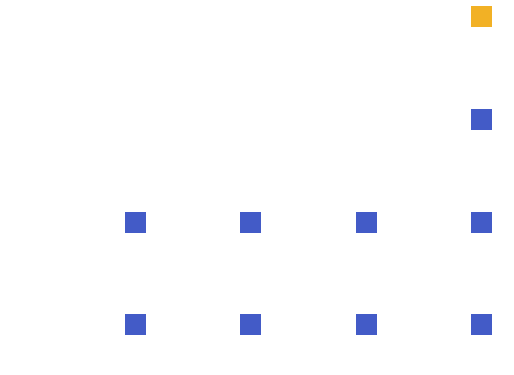
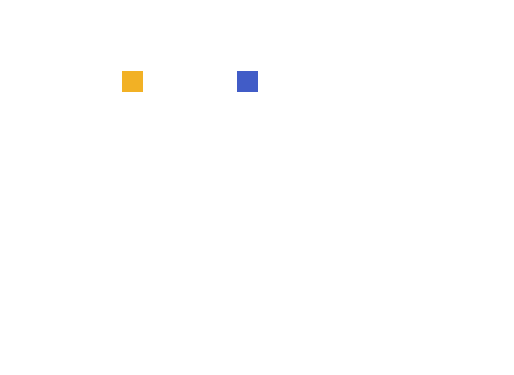



Introduction

CISOs and security professionals often think they are stuck between the rock of a cloud-first mandate and the hard place of ever-escalating security and compliance requirements. This is a false choice: The U.S. government maintains a catalog of cloud services proven to meet the highest security standards of most industries.

In 2011, then-Federal CIO Steven VanRoekel announced the Federal Risk and Authorization Management Program (FedRAMP) to address cloud security challenges. Hundreds of organizations have benefited from the genius of this program, the reusability of its strict, transparent, security risk evaluation, and approval process—or “authorization” in government-speak.

Your organization can take advantage of the marketplace, even if it has no tie to the federal government, or even a U.S. presence. You’ll even save time and money. Read on to understand the five reasons why you should implement FedRAMP private cloud as a business best practice.





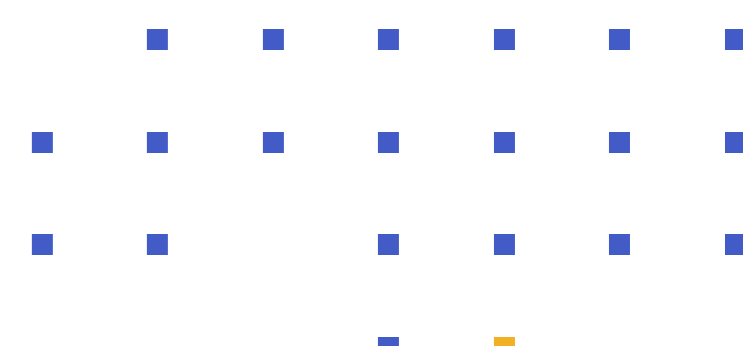
“Most security and privacy regulations are built on top of the NIST 800-53 controls that FedRAMP implements.”



01 Get the Best Possible Security at the Lowest Cost

Trust the security of FedRAMP authorized services, which employ the security development process and controls you would apply yourself. Most security architects assess the security of a system using the risk-based framework specified in NIST 800-37, identifying and prioritizing individual risks and severities. Next, they mitigate these risks by implementing controls per NIST 800-53, such as protection of information, personnel screening, physical access controls, and incident monitoring. Security organizations monitor systems continuously for incidents and deviations from the documented security architecture, and regularly perform security tests and audits. The FedRAMP process applies all of these industry standard disciplines so you don't have to.

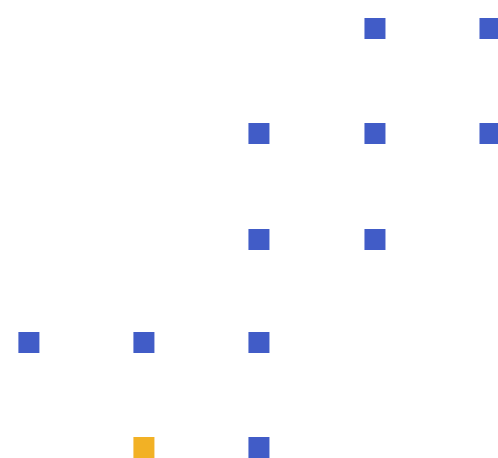
FedRAMP helps reduce your costs during the buying cycle, and long after. It brings you the economies of the cloud, and it dramatically cuts down the resources and time you need to apply in the product evaluation phase because its security is proven. It also reduces the resources you need to apply ongoing, because its continuous monitoring, reporting, and auditing makes life easy for your staff who would otherwise have to provide the functions.





02 Get the Best Possible Compliance at the Lowest Cost

Leverage a FedRAMP private cloud to save yourself time, expense, and heartache on compliance projects. Many regulatory bodies reused NIST 800-53 controls to form the security foundation of their own specifications. Look at any of these requirements—from HIPAA, PCI, and SOC 2, to FERPA, ITAR, and NIST 800-171—and you will see the common controls. Your staff will avoid repeating that body of work, since FedRAMP includes these controls in its authorized package. You will also reduce your workload for periodic compliance audits, since you can take advantage of FedRAMP’s continuous monitoring and yearly third-party audits. Finally, you will avoid the overhead of separately integrating FIPS 140-2 compliant cryptology, since it is included in all FedRAMP authorized packages.

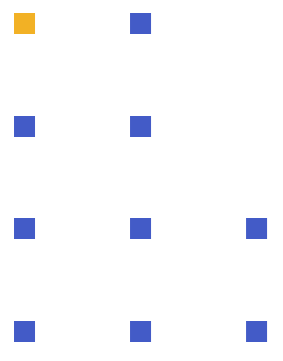


03 The Seal of Approval You Can Rely On

Use a FedRAMP private cloud service, the easiest path to cloud security and compliance peace of mind. The Federal CIO created FedRAMP so any cloud solution could be authorized just once and all other agencies could reuse that work. You can reuse it, too.

A software vendor, known in FedRAMP as a Cloud Security Provider (CSP), starts the process by partnering with a government agency to deploy its service and undergo the authorization process. A Third Party Assessment Organization (3PAO) reviews and tests every step along the way. They validate plans based on NIST 800-53 (325 controls for FedRAMP Moderate or 421 controls for FedRAMP High) covering system security, vulnerability management, configuration management, contingencies, incident responses, and other categories. They perform thorough audits to ensure the controls are properly executed. They perform state-of-the-art pen tests for internet-facing vulnerabilities, as well as on-site pen tests for vulnerabilities facing the vendor's corporate network. When it is ready, the 3PAO submits the CSP to the FedRAMP Joint Authorization Board (JAB), who publishes the service in the FedRAMP Marketplace only if its risk posture attains their very high bar.

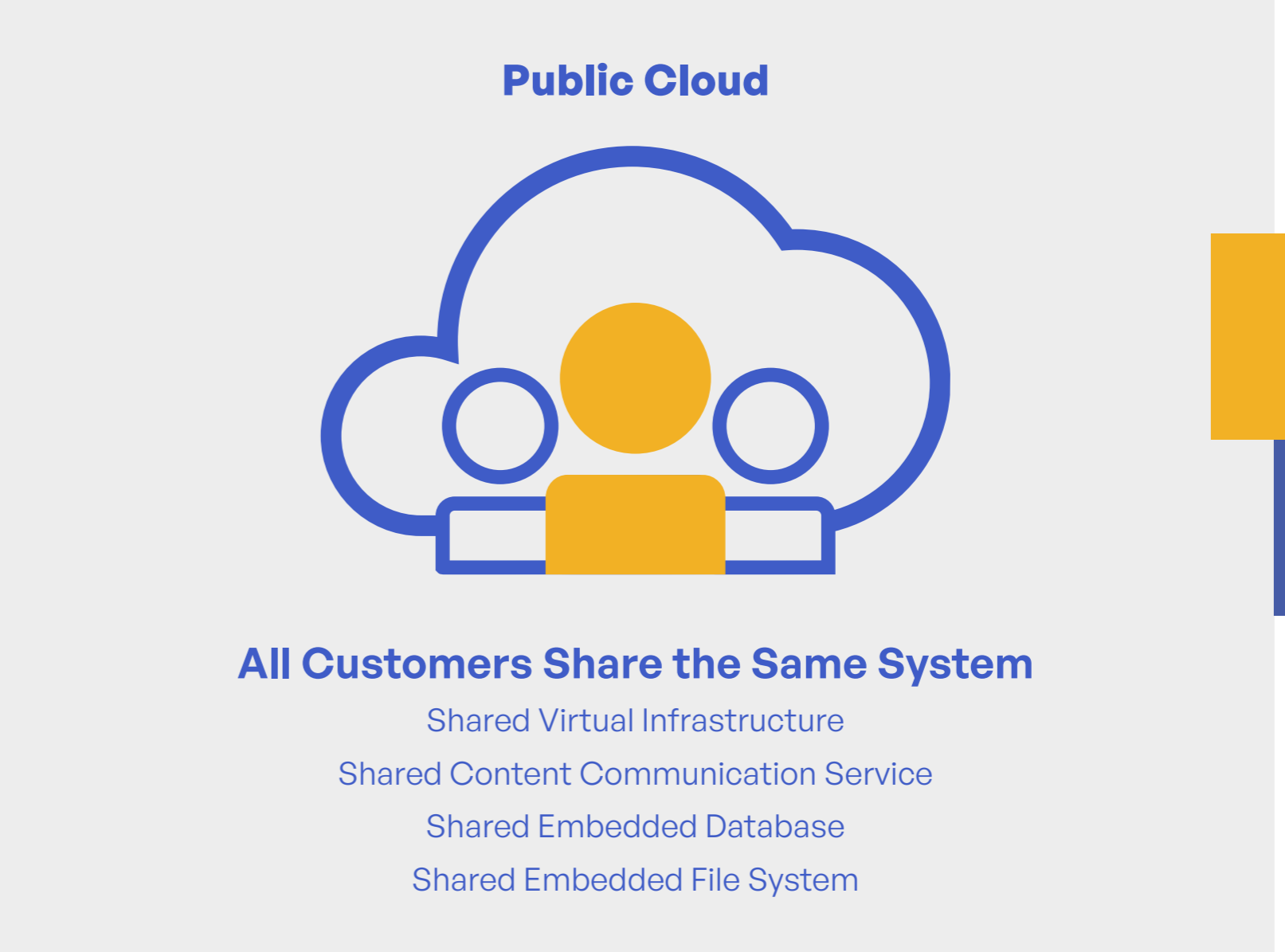
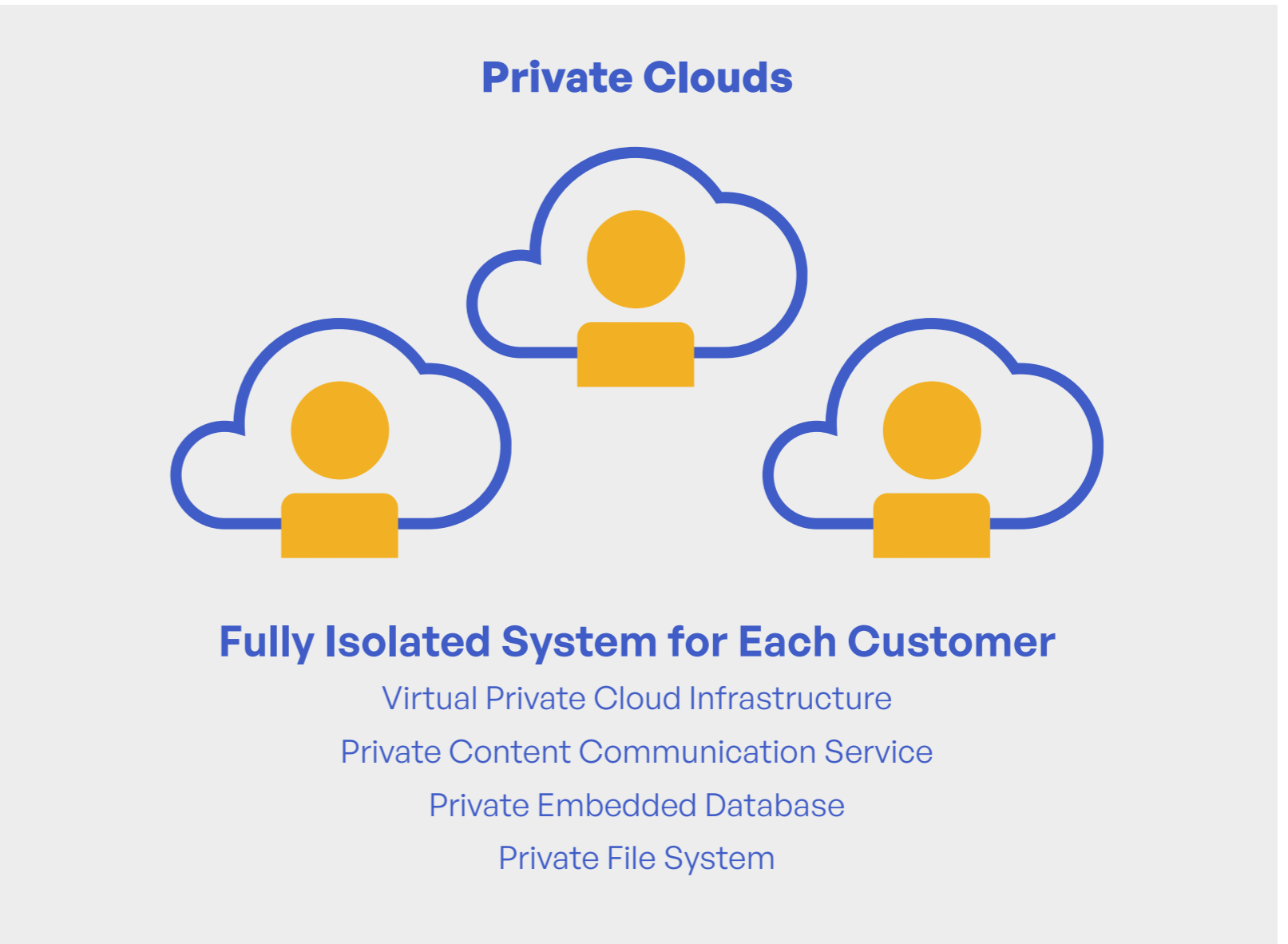
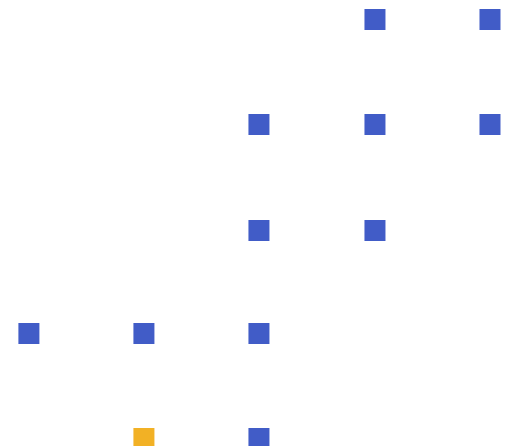
Of course, a security team's job is never done: As things change, even the strongest security posture can slump. FedRAMP CSPs undergo continuous monitoring to keep the security level high. They provide monthly reports to verify that the secure configuration is within spec, and any incidents were resolved per the documented processes. They also submit to yearly audits, where they must prove all documented controls are still in place and tests still run clean.

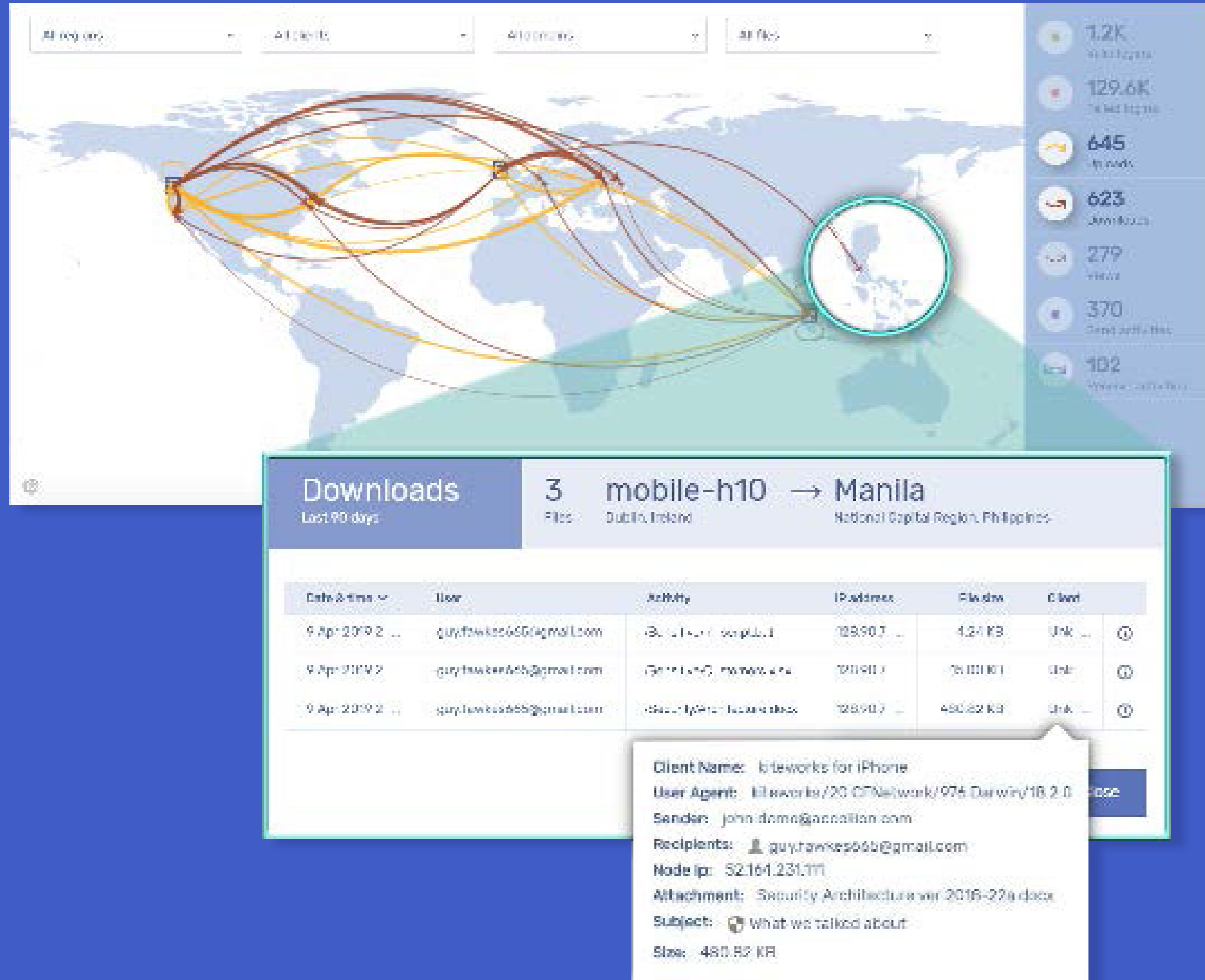


04 Minimize Your Attack Surface With a Private Cloud

CISOs and compliance officers often worry that public cloud services increase their risks. Consider a FedRAMP private cloud deployment to eliminate these concerns. Since it serves only your organization, utilizing a private cloud service minimizes the attack surface and eliminates intermingling of information.

After all, in a public cloud, your organization's data and metadata are intermingled with information from the vendor's entire customer base. Customers share the same infrastructure, from networks to storage to memory and compute resources. Your data shares the same file system, and the metadata shares the same database and tables. Security professionals may fear malware and attacks spreading across shared resources. Infrastructure managers may face less predictable performance due to other customers' load spikes affecting shared resources. Use a FedRAMP private cloud deployment to isolate yourself from other people's problems.





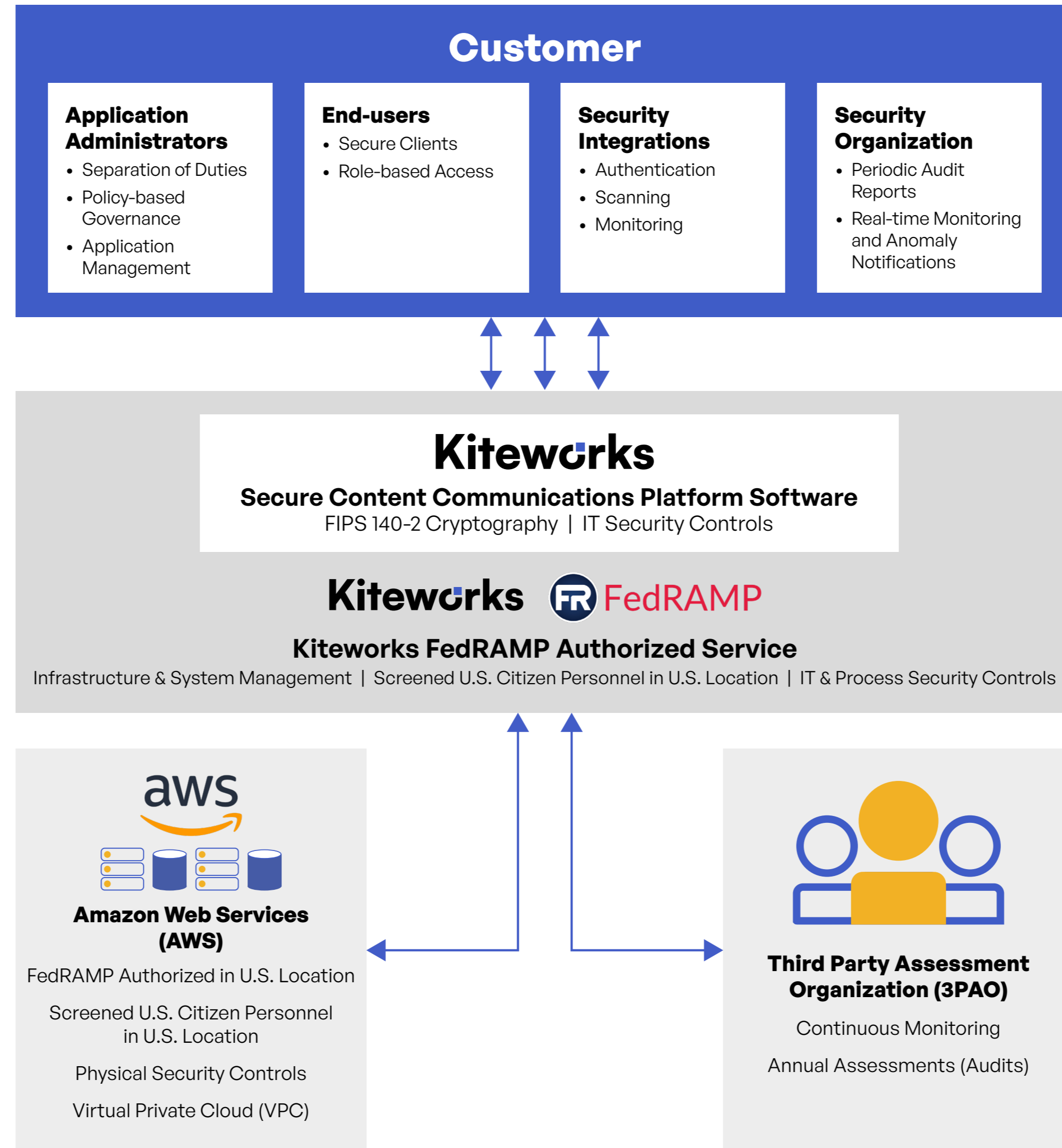
05 See Where Your Intellectual Property Is Going

CISOs know that even conscientious insiders make inadvertent content communication mistakes, while malevolent insiders attempt to enrich themselves or support foreign powers. Use a FedRAMP private cloud content communication service to ensure you can visualize where your IP is in the world, and who has it, so you can protect it.

FedRAMP authorized content communication services enable you to comprehensively monitor third-party traffic for breaches and compliance violations, starting with a complete, centralized log of all file, user, and administrator activity. Use the log data to create clear and complete real-time visualizations that answer the most important security questions about the information entering and leaving the organization. Provide forensic reporting to aid investigators. Finally, invest in emerging machine learning technology that alerts your staff to anomalies in communication patterns—content, users, domains, seasonality—and helps them reduce false-positive indications. Is an employee who is getting ready to quit downloading company secrets? Are unknown parties downloading product design files to a country where you don't do business? Use this technology to answer not just the who, what, where, and when, but also to answer questions you didn't know to ask!

Kiteworks-enabled Private Content Network

FedRAMP Authorized Secure Content Communications Platform



Agencies Using Kiteworks

- [Corporation for National & Community Service \(CNCS\)](#)
- [Council of the Inspectors General on Integrity and Efficiency](#)
- [Department of Agriculture](#)
- [Department of Commerce](#)
- [Department of Energy](#)
- [Department of Labor](#)
- [Department of State](#)
- [Department of the Interior](#)
- [Department of Veterans Affairs](#)
- [Federal Housing Finance Agency](#)
- [FHFA Office of the Inspector General](#)
- [National Science Foundation](#)
- [VA Office of the Inspector General](#)



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.

