Kiteworks

SOLUTION BRIEF

IL6 Zero-trust File Sharing for SIPRNet

Leverage Air Force Experience With Kiteworks

Mission-critical Information Sharing Demands New Safeguards

Defense personnel must share classified information quickly and efficiently across services and commands to execute their missions. While the Secret Internet Protocol Router Network (SIPRNet) provides an air-gapped environment for protecting information up to the Secret classification level, network access controls alone cannot prevent insider threats from accessing and exfiltrating sensitive content that is outside their need to know.

Recent incidents highlight these vulnerabilities. Massachusetts Air National Guard Airman Jack Teixeira leaked classified military documents on social media in 2023. Similar breaches occurred when Army intelligence analyst Chelsea Manning exposed 700,000 classified files in 2010, and NSA contractor Edward Snowden accessed over a million files in 2013, leaking 7,000 classified documents to journalists. These incidents demonstrate how excessive access permissions can dramatically expand the impact of insider threats.

Content-based Zero Trust: The Missing Layer of Defense

Traditional network security focuses on controlling access to systems and networks. However, once inside, legacy content systems often give users lenient access to information far beyond their need to know. This gap requires implementing zero-trust principles at the content layer—ensuring every content access request is verified based on need-to-know, regardless of network access.

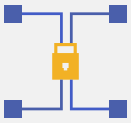
IL6 Solution: Content-centric Security for Secret Communications

A major federal systems integrator deployed Kiteworks to enable secure file sharing and email communications for a U.S. Air Force command. They built a private cloud solution and achieved Impact Level 6 (IL6) accreditation for transmitting Secret-level content, leveraging Kiteworks defense-in-depth and zero-trust capabilities:

Strong Identity and Access Management: Robust authentication for all content access, supporting standards for PIV/CAC cards, MFA, SSO, LDAP, Kerberos, SMS, authenticators, certificates, and others.

Solution Highlights

Simple, secure user interface



Least-privilege secure by default

Built-in audit log feed and reports

Built-in hardening

Mission-based Access Controls Enforce Least Privilege: Precise access controls align with job duties and enforce automated, dynamic risk policies based on data classification, user role and attributes, folder location, and other factors. These settings are secure by default and automate file expiration policies, dramatically reducing the opportunity to inadvertently expose secret or sensitive data to personnel who lack a need to know.

Next-generation Digital Rights Management (DRM) Reduces Risk While Promoting Productivity: Possessionless editing and view-only access options reduce the risks of sharing content.

Built-in Hardening Reduces Vulnerability Risks: The Kiteworks hardened virtual appliance builds defense in-depth directly into the architecture, including an embedded network firewall, web application firewall (WAF), intrusion prevention system (IPS), and double encryption, while minimizing the attack surface by using only required libraries and drivers on top of a bare Linux operating system. Its development team enforces secure software development life cycle best practices, and utilizes frequent pen tests and an active bounty program. This results in dramatically reduced vulnerability exploit potential and impact severity as demonstrated by reducing the CVSS score of the Log4Shell vulnerability from 10 to 4. The product also features automatic patching and updates, helping customers manage vulnerabilities quickly and efficiently.

Automated Integration With Data Loss Prevention (DLP) Servers Reduces Leak Risks: Kiteworks supports a variety of DLP servers, automatically blocks transfers of potentially sensitive documents, and enables straightforward overrides by administrators.

Comprehensive Audit Logging and Reporting Monitors for Insider and Outsider Threats: Kiteworks provides a unified, comprehensive audit log that tracks and records all system activities including user and admin actions, file interactions, and security events, while offering seamless SIEM integration with platforms like ArcSight and Splunk. Specialized reports help admins monitor policy execution, threats, and compliance.

Familiar User Interfaces Speed Adoption and Mission Success

Even as Kiteworks delivers sophisticated security controls, its user interface mirrors standard file sharing and email applications that defense personnel use daily. This familiar experience minimizes training requirements and user resistance. Personnel can securely share classified content as easily as sending a regular email or moving files in Dropbox or Microsoft OneDrive, ensuring security measures don't impede operational tempo or mission success.

By implementing zero trust at the content layer, defense agencies can ensure classified information remains protected while allowing authorized personnel to quickly and effectively share and access the content they need to complete their missions.