Kiteworks

COMPLIANCE BRIEF

Kiteworks Advances NSA's Zero Trust Maturity Model Across Data Layers

Addressing zero trust maturity in all seven data pillars

The "Advancing Zero Trust Maturity Throughout the Data Pillar" information sheet, created by the National Security Agency (NSA), provides recommendations for maturing data security within a Zero Trust framework. It is primarily intended for National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) networks, though it may be useful for other system owners and operators targeted by sophisticated threat actors. The guidance aligns with federal directives for agencies to adopt Zero Trust architectures. Failure to properly implement data security controls leaves organizations vulnerable to costly data breaches. The information sheet covers key data security capabilities including data cataloging, governance, labeling/tagging, monitoring, encryption, loss prevention, and granular access control. It provides a maturity model to help organizations progress these capabilities over time as part of a comprehensive Zero Trust strategy. Kiteworks is uniquely situated to support organizations in adopting this maturity model with its content-defined zero trust embodied within the Private Content Network (PCN). Here's how:

Classify Content With Risk Policies for Data Catalog Risk Alignment

Data Catalog Risk Alignment involves identifying and assessing risks to all data types, creating a comprehensive data inventory, and facilitating data governance activities. The maturity levels progress from manual identification of critical data (Basic), to automated processes for data discovery and monitoring (Intermediate), and ultimately to continuous risk analysis and protection based on data tagging and prioritization frameworks (Advanced). Kiteworks provides asset management features that classify content based on risk policies, considering factors such as folder path, sensitivity labels, file type, and creator. The consolidated activity log for compliance and audits, captures details like user actions, IP addresses, and content-related metadata. Importantly, Kiteworks logs when users add, update, or remove tags from content, enabling administrators to track activities and maintain a comprehensive data inventory.

Solution Highlights

Automated content classification

Strong double encryption

Granular access controls

Data labeling and tagging

Comprehensive audit logs

Next-gen DRM capabilities

Robust authentication options

Double Encryption and Granular Controls Provide Enterprise Data Governance

Enterprise Data Governance ensures data is controlled, accessed, and shared according to defined policies, aligning with Zero Trust principles. The maturity levels progress from developing enforceable data labeling/tagging and access control policies, to tagging, labeling, and encrypting data in compliance with these policies, automating rules and access controls through central policy management, with regular policy reviews and updates. Kiteworks' comprehensive authentication options and integration with identity providers and role-based access controls and least-privileged defaults ensure users have only the necessary permissions. Granular collaboration roles at the file and folder level enable secure data sharing. These features, combined with Kiteworks' secure architecture and double encryption, provide the foundation for implementing and enforcing enterprise data governance policies.

Automated Classification Capabilities Enable Data Labeling and Tagging

It is crucial to implement machine-enforceable access controls, risk assessment, and situational awareness with Data Labeling and Tagging in the Zero Trust framework. This moves from defining tagging standards and tools, to manual tagging by data owners, automated access controls and tooling, to fully automated tagging with continuous analysis. Kiteworks' automated classification capabilities identify sensitive content based on keywords, patterns, and machine learning. These labels and tags enforce granular access controls and data protection policies, ensuring that sensitive information is only accessible by authorized users and devices. Kiteworks also logs all tagging activities, providing a consolidated audit log.

Audit Logs Provide Robust and Real-time Data Monitoring and Sensing

Based on the model, data needs to be detectable and observable by authorized individuals and management systems. Maturity levels begin at identifying and capturing metadata for data access, sharing, and use, to feeding all monitoring logs and analytics to SIEM, and the incorporation of additional data attributes. Kiteworks supports organizations through comprehensive logging and auditing capabilities. Administrators have customizable access to tracking data, ensuring separation of duties. Dashboards provide system-level activity logs, reports, storage and bandwidth consumption, and user rankings. Kiteworks captures all log messages without throttling, and the consolidated, normalized activity log enables real-time monitoring and immediate feeding to external SIEMs like Splunk.

Next-gen DRM Features Support Data Encryption and Rights Management

Combining technology and policies to protect data from unauthorized access, modification, or redistribution supports Data Encryption and Rights Management. This means organizations need to progress from establishing an encryption strategy to initial DRM implementations, to automatically encrypting data based on tags, and using machine learning for anomaly detection. Kiteworks customers retain full control over their encryption keys, preventing unauthorized access and the platform employs double encryption, minimizing the attack surface even if an intruder breaches outer layers. Kiteworks' DRM capabilities, SafeVIEW and SafeEDIT, enforce content-based risk policies, enabling secure viewing and editing of sensitive files without allowing them to leave the secure enclave. Additionally, Kiteworks maintains an evolving library of patterns that detect suspicious activities on the network and within Kiteworks application code within the virtual appliance.

WAF and Zero Trust Principles Support Data Loss Prevention

Detecting and preventing data leakage, unauthorized use is a critical strategy for Data Loss Prevention (DLP). This begins with scoping enforcement points and establishing techniques for identifying sensitive data automating data tagging, extending DLP scope, and identifying additional enforcement points through monitoring. The platform's DLP engine identifies sensitive content based on predefined policies and data tags, automatically enforcing protective actions like blocking, quarantining, or encrypting data. Kiteworks logs system activities related to DLP, such as file locking, virus scanning, and tagging, and the embedded web application firewall (WAF) and IP address blocking provide additional layers of protection against intrusion attempts and suspicious activities. Kiteworks also employs open-source library sandboxing and tiered internal services with Zero Trust principles to isolate and secure critical components.

Least-privilege Defaults and Authentication Strengthen Data Access Control

Enforcing granular access policies and utilizing all available data attributes for access decisions is crucial for Data Access Control. Organizations are expected to progress from developing organizational policies and integration plans to fully automating access controls and refining ABAC for more granular regulations. Kiteworks offers multi-factor authentication (MFA), single sign-on (SSO), and attribute-based access control (ABAC) options. Theis enables organizations to enforce context-aware access policies based on user roles, device attributes, and environmental factors. Kiteworks supports various authentication methods, including credentials, certificates, MFA (RADIUS, PIV/CAC, OTP), SSO (SAML, Kerberos), OAuth, LDAP/AD, and Azure AD. The platform enforces least-privilege permissions and file and folder access is governed by predefined collaboration roles, which can be delegated and limited based on user profiles.

The NSA's "Advancing Zero Trust Maturity Throughout the Data Pillar" framework provides a roadmap for organizations to enhance data security within a Zero Trust architecture. Kiteworks, with its content-defined Zero Trust approach embodied in the Private Content Network (PCN), is well-positioned to support organizations in aligning with this framework. By offering features such as automated content classification, double encryption, granular access controls, comprehensive audit logs, advanced DRM capabilities, and robust authentication options, Kiteworks enables organizations to progress through the maturity levels outlined in the NSA framework. Kiteworks customers can expect to benefit from improved data governance, enhanced risk assessment, real-time monitoring and threat detection, and strong data loss prevention measures, all while maintaining compliance with stringent security and privacy regulations. Adopting Kiteworks' PCN solution empowers organizations to achieve the highest levels of Zero Trust maturity in data security, ensuring the protection of sensitive information in an increasingly complex threat landscape.

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.

May 2024