Kiteworks

SOLUTION BRIEF

Secure Your Organization's Sensitive Information Over Email to Mitigate Human Error

Leveraging Automated Policy Enforcement and Anomaly Detection to Protect Controlled Unclassified Information (CUI)

The advent of CMMC means that leaks of controlled unclassified information (CUI) can now have devastating consequences, including the loss of multimillion-dollar contracts. This risk is particularly acute with low-level employees, contractors, and consultants, who often have access to CUI as part of their daily tasks and may not fully understand the sensitivity of the content they handle. The challenge lies in ensuring that every individual in every process across your organization is protected from inadvertently or intentionally sending CUI, every time.

The threat of CUI leaks stems from several sources. Human error, such as forwarding sensitive emails to unauthorized external recipients, is by far the most common issue, especially among new, busy, or low-level employees. Insider threats, where employees knowingly leak sensitive content due to personal grievances, monetary incentives, or external pressure, are another significant concern. Additionally, these employees may be particularly vulnerable to social engineering attacks, where threat actors manipulate individuals into divulging sensitive information.

To address these challenges, the Kiteworks Email Protection Gateway (EPG) offers a feature set designed to protect your organization's CUI effectively.

Automated Policy Enforcement: Ensuring Encryption Without User Intervention

Our automated policy enforcement ensures that users can't forget to use encryption when emailing sensitive content. This feature eliminates the need for any intentional steps, as the system automatically applies the necessary safeguards for legitimate transfers of CUI.

Transparent Gateway: Secure Email Encryption Without User Training or Additional Software

Our transparent gateway allows users to encrypt sensitive emails without any onboarding, training, setup, or additional software. It ensures that every email leaving your organization is secure, regardless of the sender's location or position within the organization.

Solution Highlights

Automated Encryption: No User Intervention Needed

Transparent Gateway: Effortless Secure Communications

Corporate-wide Coverage: Universal Policy Enforcement

Proactive Anomaly Detection: Early Threat Identification

Comprehensive Audit Log: Pass Audits With Minimal Effort

Corporate-wide Coverage: Universal Application of Security Policies Across the Organization

Our solution provides corporate-wide coverage of the gateway. This feature ensures that the email gateway applies policies to every email leaving your organization, eliminating the need to predict who needs protection.

Comprehensive, Unified Audit Log: Simplifying Compliance and Issue Identification

Our comprehensive, unified audit log allows you to demonstrate compliance to auditors with minimal effort. This feature provides a clear and concise record of all data transfers, making it easy to identify and address any potential issues.

Anomaly Detection: Proactive Alerting for Unusual Behavior and Potential Threats

Our anomaly detection feature sends alerts on violations or behavior deviations, such as sending a file to a location where you don't do business. A continuous SIEM feed of the comprehensive Kiteworks audit log also allows you to quickly identify and respond to potential threats, further enhancing the security of your organization's CUI.

With our comprehensive solution, you can mitigate the risks of insider threats and human error, ensuring that your organization's CUI communications remain secure. By leveraging automated policy enforcement, a transparent gateway, corporate-wide coverage, a unified audit log, and anomaly detection, you can protect your organization's CUI and thus protect your multimillion-dollar contracts.

Kiteworks