Cyber Essentials Plus

Meeting Cyber Essentials Plus Requirements With Kiteworks: A Comprehensive Solution for Protecting Your Organisation From Cyber Threats

Cyber Essentials is a UK government-backed scheme that aims to protect organisations from common cyber threats. It comes in two levels, Cyber Essentials and Cyber Essentials Plus. The former is a self-assessment certification that provides protection against common cyber threats. The latter requires an external testing and certification process that demonstrates an organisation's secure handling of sensitive and personal information and is required for organisations to bid for central government contracts. Both levels are based on a set of controls that organisations must implement to mitigate vulnerabilities and prevent unwanted attention from cybercriminals. Kiteworks is pleased to meet these requirements to ensure customers who deploy a Kiteworks-enabled Private Content Network (PCN) are in compliance with Cyber Essentials and Cyber Essentials Plus while communicating sensitive content within the system. Here's how:

Securing Your Organisation With Defence-in-Depth Approach

Kiteworks utilizes a defence-in-depth approach consisting of comprehensive encryption for sensitive data in motion and at rest, an embedded and optimized network firewall and web application firewall (WAF), multiple layers of server hardening, zero-trust communications between internal services and cluster nodes, and internal tripwires. The embedded network firewall limits entry points to defined interfaces only and ensures that only approved accounts gain access to content. This perimeter protection minimizes the external attack surface, reduces risk of external attacks, and saves resources in defending their organisation against potential external attacks.

Ensuring Security and Compliance Through Role-based Controls and Rigorous Audits

Kiteworks' administrators use role-based controls to enforce security and compliance policies and to configure simple connections to security infrastructure components such as MFA. Kiteworks has passed rigorous yearly audits by certified third parties that validate, among others, 325 NIST 800-53 security controls, as well as having incidents and configuration changes continuously monitored, providing customers best-in-class security.

Granular Policy Controls and Secure Authentication

Kiteworks allows you to have granular policy controls like view-only access and watermarking to protect sensitive content and enforce compliance policies, and enables business owners to easily manage content, folders, invitations, and access controls. Kiteworks also allows you to set policies for password complexity while allowing administrators to reset user passwords and enforce password changes during login. This ensures least-privilege access and authentication, restricting the potential damage caused by a security breach and making audits much faster and more effective.

Advanced Threat Prevention, Encryption, and Real-time Reporting

Kiteworks protects from incoming malware with embedded antivirus (AV) or an organisation's advanced threat prevention (ATP) server, both with automatic quarantine and notification. Ensure encryption of all content at rest (with AES-256 encryption) to protect data from unauthorized access, data corruption, and malware. Real-time reporting and log exporting ensure an external copy remains complete to audit any attacks and understand exactly what happened, and what was compromised. This allows an organisation to respond quickly and with full details in hand of what was exfiltrated, allowing them to recover from the loss that much faster.

Automated Security Testing, Patching, and More

Kiteworks uses an OWASP secure development life cycle with automated security testing, white box and black box testing, regular penetration testing, and a continuous bounty program for unearthing vulnerabilities. Kiteworks also rapidly alerts with a single point of truth report log that details every activity of all access globally. All activity is fully logged and visible via reporting and the CISO Dashboard, and exportable to a syslog and SIEM. With update services and patching along with one-click appliance updates being pushed to customers annually, Kiteworks works tirelessly to ensure threats are mitigated. This allows customers to focus on growing their business, not protecting it.

Cyber Essentials and Cyber Essentials Plus are essential for organisations to protect themselves from common cyber threats. Kiteworks provides a comprehensive solution that meets the requirements of both levels, with a defence-in-depth approach, role-based controls, secure authentication, advanced threat prevention, encryption, and real-time reporting. Automated security testing, patching, and one-click appliance updates ensure customers can focus on growing their business without worrying about protecting it. With Kiteworks, organisations can be confident that their data is secure and compliant with Cyber Essentials and Cyber Essentials Plus.