Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Essential Eight Implementation for Australian Organizations

Safeguard Sensitive Data and Maintain the Trust of Customers and Stakeholders

The Essential Eight model, a cybersecurity framework established by the Australian Cyber Security Centre (ACSC), outlines critical controls to mitigate cyber risks. Compliance with this regulation is crucial for organizations handling sensitive data, including government agencies, financial institutions, and healthcare providers, and is recommended for all Australian organizations to enhance cybersecurity measures. Specifically, compliance with the Essential Eight is mandatory for all Australian non-corporate Commonwealth entities (NCCEs) as per the Protective Security Policy Framework (PSPF) Policy 10. While compliance is mandatory for NCCEs, it is highly recommended for non-corporate Commonwealth entities and federal government agencies. Adhering to the Essential Eight demonstrates a commitment to best practices, enhances customer trust, and safeguards against potential data breaches and financial losses. Noncompliance can result in severe consequences, such as reputational damage, legal penalties, and loss of business. The model defines three maturity levels: Level 1 (basic controls), Level 2 (advanced measures and regular assessments), and Level 3 (proactive defense and strong security culture). Achieving higher levels of compliance requires increasing resources and expertise, making it challenging for some organizations, but ultimately necessary to effectively combat ever-evolving cyber threats. Kiteworks supports compliance for all three levels. Here's how:

One-click Updates Support Patch Application

Kiteworks supports most of the Patch Application mitigation strategies of the Essential Eight through its comprehensive security features. The platform automatically checks for updates and allows system administrators to download, cryptographically verify, and apply updates to the entire solution with a single click. This streamlined process ensures that the operating system, databases, web servers, application code, and other services are always up to date, eliminating the need for separate compatibility checks or integration testing. Furthermore, Kiteworks' embedded web application firewall (WAF) and intrusion detection system (IDS) receive continuous updates to address new threat patterns discovered through internal research, market research, bounty programs, and evolving known threat patterns. These updates can be automatically downloaded and applied by default for non-air-gapped systems, reducing the workload on IT departments while maintaining a robust security posture. For air-gapped deployments, Kiteworks provides a secure offline update process to ensure all installations remain protected against the latest vulnerabilities.

Solution Highlights

Immutable audit logs

Granular controls

Double encryption

Embedded web application firewall

One-click updates

Continuous Updates Streamline Patch Operating Systems

The Patch Operating Systems mitigation strategy recommends a streamlined and automated update process. The platform continuously releases updates to address newly discovered threat patterns, which are based on internal research, market research, bounty programs, and evolving known threats. These updates can be automatically downloaded and applied by default for non-air-gapped systems, ensuring that the operating system, databases, web servers, and other components are always up to date. For air-gapped deployments, Kiteworks provides a secure offline update process. System administrators can easily download, cryptographically verify, and apply updates to the entire solution with a single click, eliminating the need for separate compatibility checks or integration testing. This comprehensive approach to patch management helps organizations maintain a strong security posture and comply with the Essential Eight's requirements for timely patch application, reducing the risk of successful cyberattacks on both internet-facing and non-internet-facing systems.

MFA and Enterprise Connect Enable Access

Kiteworks enables compliance throughout all three levels within the Muli-factor Authentication mitigation strategy with native email-based and SMS-based one-time passwords (OTP), as well as support for RADIUS protocol, PIV/CAC cards, and time-based OTP (RFC 623Eight). These multi-factor authentication methods add an extra layer of protection by requiring users to provide at least two forms of identification before accessing their accounts, such as a password and a mobile device or fingerprint. Kiteworks logs all successful and unsuccessful authentication events, including user ID, login time, and IP address, in a centralized, tamper-proof manner. These event logs can be analyzed in a timely manner to detect and report cybersecurity incidents to the appropriate personnel, enabling swift enactment of the organization's cybersecurity incident response plan.

Restrict Administrative Privileges With Role-based Access Controls

Kiteworks supports the Restrict Administrative Privileges mitigation strategy by implementing role-based access controls and the principle of least privilege. All users are assigned a set of permissions that control access to features and resources, with users automatically given the least permissions necessary. Administrators must explicitly enable elevated permissions. Kiteworks has a separate set of admin roles that control access to administrative features, with a hierarchy of permissions set to either no access, view only, or full access. Privileged access events, including account and group management events, are centrally logged and protected from unauthorized modification and deletion. These event logs can be analyzed in a timely manner to detect and report cybersecurity incidents to the appropriate personnel. Kiteworks also supports time-based access controls, such as deactivating user accounts after a period of inactivity, further restricting administrative privileges.

Application Control Verification via Detailed Audit Logs

The Application Control mitigation strategy recommends strict controls to manage applications. The Kiteworks virtual appliance contains all the necessary files and software to run securely, with multiple layers of protection that minimize the attack surface. This includes an embedded network firewall, web application firewall (WAF), and intrusion detection system (IDS), which restrict the execution of unauthorized applications and detect anomalous activities. Kiteworks logs all relevant events, including successful and failed logins, file uploads, downloads, edits, shares, and administrative activities. These event logs are protected from unauthorized modification and deletion, and can be analyzed in a timely manner to detect and report cybersecurity incidents to the appropriate personnel, such as the Chief Information Security Officer or their delegates. The centralized, standardized nature of Kiteworks' logging ensures that organizations can quickly identify and respond to potential security threats.

Centralized Reporting Monitors User Application Hardening

Kiteworks logs a wide range of user and system events, including successful and failed logins, file uploads, downloads, edits, shares, and administrative activities. These event logs are protected from unauthorized modification and deletion, ensuring the integrity of the data for security and compliance purposes. Kiteworks feeds these logs to security information and event management (SIEM) systems in real time, enabling organizations to analyze the data promptly to detect cybersecurity events and incidents.

The centralized nature of Kiteworks' logging, along with its ability to normalize and standardize the data, allows security teams to efficiently identify potential threats across internet-facing and non-internet-facing servers, as well as workstations. When cybersecurity incidents are detected, Kiteworks' logging and reporting features facilitate timely notification to the Chief Information Security Officer or their delegates, as well as to the Australian Signals Directorate (ASD) when necessary.

Enable Regular and Automated Backups

Kiteworks supports all three levels of the Regular Backups mitigation strategy through its built-in disaster recovery and data protection features. Customers can create snapshots of their storage node virtual machines (VMs) at regular intervals, capturing the entire system state, including code, metadata, and data, at a specific point in time. These snapshots can be securely stored and used to restore the system in the event of a disaster, such as a system failure or data center outage. Additionally, Kiteworks allows customers to configure automatic replication between storage nodes located in different data centers, ensuring that data is synchronously backed up and can be quickly restored to a common point in time. The system's role-based access controls and least-privilege principles ensure that unprivileged accounts cannot access, modify, or delete backups belonging to other accounts or their own backups. Similarly, privileged accounts, excluding backup administrator accounts, are prevented from accessing, modifying, or deleting backups. These features help maintain the security, resilience, and integrity of the backup data, enabling organizations to meet their business continuity requirements and comply with the Essential Eight guidelines.

Kiteworks provides a comprehensive solution that supports organizations in achieving compliance with all three levels of the Essential Eight model. By offering features such as one-click updates for patch management, multi-factor authentication, role-based access controls, application control verification, centralized reporting, and regular automated backups, Kiteworks enables organizations to implement proactive defense measures and cultivate a strong security culture. These capabilities are crucial for industries handling sensitive data, including government agencies, financial institutions, and healthcare providers, as they help mitigate cyber risks, protect customer information, and maintain business continuity. Compliance with the Essential Eight not only demonstrates a commitment to best practices and enhances customer trust but also safeguards organizations against potential data breaches, financial losses, and reputational damage. As cyber threats continue to evolve, leveraging Kiteworks' robust security features becomes increasingly important for organizations striving to maintain a resilient security posture and meet the stringent requirements of the Essential Eight framework.