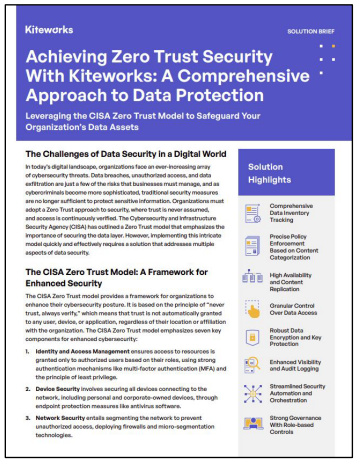
Kiteworks

carahsoft.


Kiteworks SOLUTION BRIEF

Achieving Zero Trust Security With Kiteworks: A Comprehensive Approach to Data Protection

Leveraging the CISA Zero Trust Model to Safeguard Your Organization's Data Assets

The Challenges of Data Security in a Digital World

In today's digital landscape, organizations face an ever-increasing array of cybersecurity threats. Data breaches, unauthorized access, and data exfiltration are just a few of the risks that businesses must manage, and as cybercriminals become more sophisticated, traditional security measures are no longer sufficient to protect sensitive information. Organizations must adopt a Zero Trust approach to security, where trust is never assumed, and access is continuously verified. The Cybersecurity and Infrastructure Security Agency (CISA) has outlined a Zero Trust model that emphasizes the importance of securing the data layer. However, implementing this intricate model quickly and effectively requires a solution that addresses multiple aspects of data security.

The CISA Zero Trust Model: A Framework for Enhanced Security

The CISA Zero Trust model provides a framework for organizations to enhance their cybersecurity posture. It is based on the principle of "never trust, always verify," which means that trust is not automatically granted to any user, device, or application, regardless of their location or affiliation with the organization. The CISA Zero Trust model emphasizes seven key components for enhanced cybersecurity:

1. **Identity and Access Management** ensures access to resources is granted only to authorized users based on their roles, using strong authentication mechanisms like multi-factor authentication (MFA) and the principle of least privilege.
2. **Device Security** involves securing all devices connecting to the network, including personal and corporate-owned devices, through endpoint protection measures like antivirus software.
3. **Network Security** entails segmenting the network to prevent unauthorized access, deploying firewalls and micro-segmentation technologies.

Solution Highlights

- Comprehensive Data Inventory Tracking
- Precise Policy Enforcement Based on Content Categorization
- High Availability and Content Replication
- Granular Control Over Data Access
- Robust Data Encryption and Key Protection
- Enhanced Visibility and Audit Logging
- Streamlined Security Automation and Orchestration
- Strong Governance With Role-based Controls

Achieving Zero Trust Security With Kiteworks: A Comprehensive Approach to Data Protection

Thank you for downloading this Kiteworks Solution Brief. Carahsoft is the reseller for Kiteworks' cybersecurity solutions available via GSA 2GIT, CMAS, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Kiteworks' solutions, please check out the following resources and information:

For additional resources:
carah.io/KiteworksResources

For upcoming events:
carah.io/KiteworksEvents

For additional Kiteworks solutions:
carah.io/KiteworksSolutions

For additional cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Kiteworks@carahsoft.com
703-871-8548

To purchase, check out the contract vehicles available for procurement:
carah.io/KiteworksContracts

For more information, contact Carahsoft or our reseller partners:
Kiteworks@carahsoft.com | 703-871-8548

Kiteworks

SOLUTION BRIEF

Achieving Zero Trust Security With Kiteworks: A Comprehensive Approach to Data Protection

Leveraging the CISA Zero Trust Model to Safeguard Your Organization's Data Assets

The Challenges of Data Security in a Digital World

In today's digital landscape, organizations face an ever-increasing array of cybersecurity threats. Data breaches, unauthorized access, and data exfiltration are just a few of the risks that businesses must manage, and as cybercriminals become more sophisticated, traditional security measures are no longer sufficient to protect sensitive information. Organizations must adopt a Zero Trust approach to security, where trust is never assumed, and access is continuously verified. The Cybersecurity and Infrastructure Security Agency (CISA) has outlined a Zero Trust model that emphasizes the importance of securing the data layer. However, implementing this intricate model quickly and effectively requires a solution that addresses multiple aspects of data security.

The CISA Zero Trust Model: A Framework for Enhanced Security

The CISA Zero Trust model provides a framework for organizations to enhance their cybersecurity posture. It is based on the principle of "never trust, always verify," which means that trust is not automatically granted to any user, device, or application, regardless of their location or affiliation with the organization. The CISA Zero Trust model emphasizes seven key components for enhanced cybersecurity:

1. **Identity and Access Management** ensures access to resources is granted only to authorized users based on their roles, using strong authentication mechanisms like multi-factor authentication (MFA) and the principle of least privilege.
2. **Device Security** involves securing all devices connecting to the network, including personal and corporate-owned devices, through endpoint protection measures like antivirus software.
3. **Network Security** entails segmenting the network to prevent unauthorized access, deploying firewalls and micro-segmentation technologies.

Solution Highlights

- Comprehensive Data Inventory Tracking
- Precise Policy Enforcement Based on Content Categorization
- High Availability and Content Replication
- Granular Control Over Data Access
- Robust Data Encryption and Key Protection
- Enhanced Visibility and Audit Logging
- Streamlined Security Automation and Orchestration
- Strong Governance With Role-based Controls

4. **Application and Workload Security** focuses on protecting applications from vulnerabilities through regular scanning, patching, and secure development practices.
5. **Data Security** safeguards data through encryption, access controls, and data loss prevention (DLP), with data classified based on sensitivity.
6. **Visibility and Analytics** provide insight into network activities, utilizing security information and event management (SIEM) systems and behavioral analytics.
7. **Automation and Orchestration** streamline security processes, automating threat detection, response, and policy enforcement.

The Kiteworks Solution: A Holistic Approach to Data Protection

Kiteworks offers a comprehensive solution that addresses the data layer of the CISA Zero Trust model, enabling organizations to achieve robust data protection. The key components of the Kiteworks solution include:

1. **Data Inventory Management:** Kiteworks inventories and tracks content, preventing data exfiltration by integrating with data loss prevention (DLP) solutions.
2. **Data Categorization:** Policies are applied based on AIP sensitivity labels, content properties, users, and actions, ensuring that data is appropriately protected based on its category.
3. **Data Availability:** The high availability cluster provides automatic data replication and failover, ensuring that data is always accessible when needed.
4. **Data Access:** Kiteworks applies access, sharing, retention, and other security controls based on risk categories, providing granular control over data access and transfer.
5. **Data Encryption:** Advanced encryption is applied to all content in transit, and double encryption is used for data at rest. Kiteworks also protects encryption keys, supports Hardware Security Module (HSM) key protection, and facilitates key rotation.
6. **Visibility and Analytics Capability:** Comprehensive audit logging captures all actions on content, structure, usage, and permissions, with continuous feed to SIEM systems via syslog and Splunk Forwarder.
7. **Automation and Orchestration Capability:** Kiteworks automates policy enforcement for creation, sharing, and transfer, as well as data disposal, retention, and archiving.
8. **Governance Capability:** Role-based access controls and permissions are applied for internal and external sharing, transfers, and forwarding, ensuring compliance with governance requirements.

Securing Your Organization's Future With Kiteworks

In an era where data security is paramount, organizations must take proactive measures to safeguard their information assets. Kiteworks provides a holistic solution that aligns with the CISA Zero Trust model, delivering comprehensive data protection. By implementing Kiteworks, organizations can achieve greater visibility, control, and security over their data, mitigating the risk of cyber threats and ensuring business continuity.