HELYX™

Helyx™ Data Security White Paper

HELYX DATA: A SECURE, COMPLIANT, AND SCALABLE DATA TRANSACTION AND STORAGE SOLUTION

Table of Contents

Executive Summary

As organizations increasingly store and manage sensitive data, safeguarding this information while ensuring compliance with regulatory standards has become more critical than ever. Helyx Data offers a secure, user-centric solution for data transactions and storage, guaranteeing compliance with GDPR and HIPAA. The platform enables seamless access and management through trusted cloud technologies.

Helyx Data integrates robust security features, granular access controls, and policy enforcement, all aimed at protecting your most valuable asset—your data. This whitepaper outlines the security architecture and compliance features of Helyx Data and explains how it enables your organization to securely manage data transactions and storage while adhering to essential industry regulations.

Introduction

Data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), establish high standards for organizations that store and process personal data. Helyx Data is our secure solution for data transactions and storage, designed to help organizations comply with these regulations.

Built on reliable and scalable cloud infrastructure, Helyx Data utilizes advanced security measures and a user-friendly design to provide your organization with a seamless and highly secure experience. Whether you are an IT Director, a compliance officer, or an executive seeking a clear overview, this white paper explains how Helyx Data safeguards your data and simplifies compliance.

Security Architecture

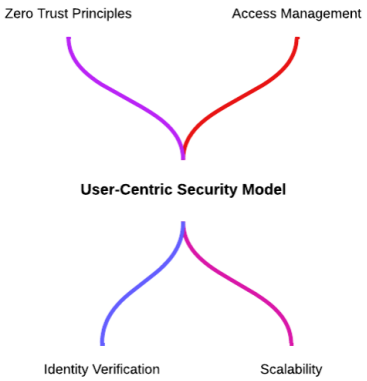
1. User-Centric Security Model

Helyx Data is built around a user-centric security model that prioritizes security controls and access based on user identity rather than relying on

device or network trust. This approach adheres to the principles of Zero Trust, where trust is never assumed, and access is continuously verified according to the user's identity and role. By linking security controls directly to each user's identity, Helyx Data ensures that only authorized individuals can access specific data and resources according to their assigned roles and access levels. This eliminates reliance on the security of the user's device or network, guaranteeing that every interaction with the platform is rigorously validated, regardless of the user's location or device.

This identity-based model promotes scalability; no matter how many users are added, security controls are consistently enforced across the platform. Each user's identity is continually authenticated, reducing the risk of unauthorized data access and maintaining security as the user base expands. The platform utilizes Microsoft Entra ID for identity and access management, providing centralized control over user permissions and authentication and streamlining the process of securely managing access.

Users can be quickly invited to the platform, with access granted based on their identity and specific role within the organization. This ensures access is managed securely and aligned with each individual's responsibilities without depending on device-based trust. Single Sign-On (SSO) capabilities allow users to securely access the platform with a single authentication, enhancing their experience while reinforcing security. This identity-driven approach enables Helyx Data to scale securely, upholding Zero Trust principles as the user base grows and ensuring that access remains tightly controlled and aligned with each user's role and responsibilities.



2. Granular Role-Based Access Control

Access to resources and data within the platform is managed through advanced access controls, ensuring that each user is assigned the appropriate level of access based on their role. The platform utilizes role-based access control (RBAC) to assign permissions that align with users' responsibilities. Roles include Reader, Writer, and Contributor, along with specific portal permissions that manage access to administrative and audit functions. These roles and permissions ensure that users can only perform the necessary tasks while minimizing the risk of unauthorized data exposure or system misuse.

- **Reader:** This role allows users to view data but prohibits them from modifying or deleting it, ensuring access is limited to information necessary for their tasks.
- **Writer:** Users in this role can view and modify data but are restricted from deleting it. This offers a higher level of interaction while still limiting potential harm.
- **Contributor:** This role gives users full access to create, modify, and delete data within the platform, granting them complete control over the data they manage.

In addition to these core roles, Helyx Data includes portal-specific permissions that further refine access control within the platform, enhancing both flexibility and security. These permissions enable users to interact with the platform's administrative interface without directly accessing the underlying data stored in the system. The key portal roles include:

- **User:** This role is limited to read-only operations within the portal. Users can view the system's interface, data, and resources without administrative access or the ability to modify any configurations or data. This ensures users can access necessary information without harming the platform's integrity.

- **Auditor:** Users in the Auditor role are granted complete read access to the platform, allowing them to review all data and activities for compliance, reporting, and auditing purposes. However, they are restricted from writing operations, such as editing or deleting data. This role is crucial for organizations that need transparency and compliance without granting full administrative privileges.

- **Tenant Administrator:** This role provides users full read and administrative access to the platform. Tenant Administrators can view all data and modify the platform's configuration, including adding or changing resources and users. This role is intended for trusted individuals who require comprehensive environmental control while ensuring security and compliance.

It is important to note that portal permissions are separate from data access mappings, meaning that users with administrative or auditing roles do not necessarily have direct access to the data stored within the platform. This separation allows auditors or administrators to review the platform and system configuration without compromising data security. For instance, an Auditor may need complete visibility into audit logs and platform usage. Still, he would not be able to alter or delete any data, thus preserving the integrity of the information. Similarly, a Tenant Administrator may have complete administrative control over the system's configuration but may not be authorized to access specific sensitive datasets unless explicitly granted permission through data access mappings.

3. Data Access and Filtering

When users are authenticated, they gain access to platform resources relevant to their specific roles and responsibilities. Data access is carefully segmented to ensure that users only see the information pertinent to their position. This approach provides a high level of dynamic access control that maintains strong security while enhancing the user experience. Users are presented only with the data and tools necessary for their tasks.

The platform minimizes the risk of unnecessary data exposure by segmenting access based on roles and user identities. This role-based

segmentation ensures that users can only view and interact with data relevant to their responsibilities, preventing unauthorized access to sensitive or unrelated information. For instance, a Reader may have visibility into specific datasets but cannot modify or delete them. In contrast, a Contributor can view and modify data but is still restricted from seeing other users' data unrelated to their role.

This dynamic access control model adapts to each user's identity, allowing the platform to scale efficiently. As the number of users increases, the access control system maintains secure, role-based data isolation and ensures each user experiences a personalized interface based on their specific permissions. This segmentation reduces potential security risks and streamlines the user experience. Users can focus solely on the data and tasks relevant to their work, avoiding navigating through unnecessary or restricted resources.

4. Access Management and Controls

Data access within the platform is strictly controlled, with security mechanisms designed to ensure that only authorized users can interact with sensitive resources. The platform's security architecture enforces best practices in data security, guaranteeing that access to critical information is governed by clearly defined roles and permissions. By implementing these robust security protocols, the platform minimizes the risk of unauthorized access or modification, thereby protecting the integrity and confidentiality of sensitive data.

User access is carefully managed based on individual roles within the system, ensuring that only users with the appropriate permissions can interact with specific resources. This control is essential in preventing unauthorized modifications or exposure of sensitive data, which could lead to serious compliance and security issues. Access controls are achieved through granular role-based permissions that restrict what users can view and do, from simply accessing data to performing more advanced actions such as editing or deleting information. The platform employs multi-factor authentication (MFA), further enhancing security by ensuring that only legitimate users can access the system.

 842 Main St. Redwood City, CA 94063 | +1 650.374.2121

By consistently adhering to best practices in data security, including the principle of least privilege, the platform ensures that users only have access to the resources necessary for their roles. This approach reduces the likelihood of security breaches and guarantees that data is handled securely throughout its entire lifecycle—from storage to access and modification. As a result, the platform effectively protects sensitive data from unauthorized access and misuse while maintaining compliance with regulatory requirements.

5. Enforced Security Policies

Helyx Data implements several advanced security measures to ensure that only authorized and adequately authenticated users can access the platform. Each user interaction is carefully examined to verify that the request is legitimate and complies with security best practices.

A core component of the platform's security is Multi-Factor Authentication (MFA), which requires all users to authenticate using multiple factors. This process ensures that only legitimate users who successfully pass the multi-factor verification can access the platform, providing additional protection against unauthorized access.

Moreover, the system enforces secure authentication methods, eliminating the vulnerabilities associated with basic authentication. By requiring more potent, more secure authentication techniques, the platform reduces the risk of compromise due to weak or easily bypassed credentials.

The platform continuously monitors suspicious login patterns. Any unusual or potentially malicious login activity, such as logins from unexpected locations or devices, triggers an automatic review process. This proactive monitoring ensures that any suspicious behavior is flagged for further investigation, allowing for timely threat detection and response before unauthorized access can occur.

Compliance and Regulatory Framework

1. GDPR Compliance

The General Data Protection Regulation (GDPR) sets strict guidelines for collecting, storing, and processing personal data within the European Union (EU). Helyx Data fully complies with these regulations, allowing organizations to use the platform while confidently meeting their GDPR requirements.

The platform employs robust security measures, including data encryption, to protect sensitive information when stored and during transmission. This encryption prevents unauthorized access to personal data and safeguards it at all times. Furthermore, Helyx Data follows the principle of data minimization by collecting only the data necessary for its operations. This approach reduces the risk of exposing unnecessary personal information and ensures that only data required for business purposes is retained.

Access control within the platform is managed through user-centric permissions, ensuring that only authorized individuals can access personal data. Access rights are granted based on each user's role and responsibilities, minimizing the risk of unauthorized access to sensitive information. Additionally, the platform maintains detailed audit logs that track all access and modification events related to personal data. These logs are crucial for conducting compliance audits, providing transparency, and ensuring accountability, which helps organizations demonstrate their adherence to the stringent requirements of the GDPR.

2. HIPAA Compliance

Helyx Data fully complies with the Health Insurance Portability and Accountability Act (HIPAA), establishing high standards for protecting healthcare information in the United States. The platform ensures that Protected Health Information (PHI) is securely stored and managed according to HIPAA guidelines. Helyx Data's security framework includes strict access controls that restrict access to PHI based on user roles and responsibilities. Only authorized personnel can access and modify

sensitive healthcare data, protecting it from unauthorized exposure and preserving confidentiality.

In addition to access controls, Helyx Data maintains audit trails that monitor all activities related to PHI. These logs are crucial for providing transparency and accountability, ensuring that any actions involving PHI can be reviewed for compliance purposes. The detailed audit trails enable organizations to oversee and report on their compliance with HIPAA while facilitating ongoing monitoring to ensure that healthcare data remains secure.

3. ISO 27001-2013 Compliance

Helyx Data operates within a cloud infrastructure compliance-ready with ISO 27001:2013, the globally recognized standard for information security management systems (ISMS). ISO 27001 provides a comprehensive framework for managing and securing sensitive data. Helyx Data's environment is continuously monitored for potential security threats and vulnerabilities, ensuring that the highest information security standards safeguard data.

The platform employs proactive measures to identify and address risks in real time, ensuring that sensitive data remains secure. It also enforces strict policy controls and best practices as outlined by ISO 27001, consistently covering all aspects of information security, including access management, risk assessment, and incident response.

Furthermore, Helyx Data adopts a comprehensive approach to risk management, regularly assessing potential security threats and implementing corrective measures to protect data from breaches or unauthorized access. This commitment to continuous monitoring and rigorous policy enforcement ensures that Helyx Data remains compliance-ready with ISO 27001 controls, providing users with a secure, reliable, and globally recognized environment for their data management needs.

Together, these compliance frameworks—GDPR, HIPAA, and ISO 27001-2013—demonstrate Helyx Data's commitment to offering a secure and compliance-ready platform for managing sensitive data. The platform's approach to data protection, access control, and audit tracking ensures

that organizations can maintain regulatory compliance while safeguarding data throughout its lifecycle.

Continuous Monitoring and Threat Protection

The platform significantly enhances security through real-time monitoring and threat protection mechanisms that operate continuously to keep your data safe from emerging threats. These security measures are designed to identify potential vulnerabilities within the system, enabling the platform to respond quickly to any security risks before they can compromise data integrity or availability. The system monitors unusual activities and potential threats, ensuring deviations from established security standards are flagged and investigated.

In addition to threat identification, the platform enforces security policies and compliance checks, essential for maintaining a secure and compliance-ready environment. These policies are created to uphold the highest data protection standards, ensuring that security controls are consistently implemented and that any violations are addressed promptly. The platform minimizes the likelihood of data breaches or security lapses by continuously monitoring the environment for potential risks and ensuring compliance with industry regulations.

This proactive approach to security protects your data from emerging threats and ensures that your environment remains compliance-ready with relevant industry regulations, such as GDPR, HIPAA, and ISO 27001-2013. With real-time threat detection and continuous policy enforcement, Helyx Data provides peace of mind, knowing that your data is safeguarded against evolving risks while maintaining regulatory compliance.

Conclusion

Helyx Data is a secure and scalable data transaction and storage solution that complies with GDPR and HIPAA regulations. It utilizes trusted cloud technologies and advanced security controls to protect sensitive information.

With user-centric access management and detailed data access controls, Helyx Data ensures that your organization's sensitive data always remains secure. Whether you are managing healthcare data or personal information within the EU, Helyx Data provides the necessary tools and features to meet compliance requirements and reduce the risks associated with data storage and transactions.

By choosing Helyx Data, your organization can access a reliable, secure, and compliance-ready data solution that meets the highest security and regulatory standards.

Contact us today to learn how Helyx Data can help your organization securely manage its data while staying compliant.

 842 Main St. Redwood City, CA 94063 | +1 650.374.2121