zluri

Zluri's Trust and Security Deep Dive

Published Date: 25th January 2024

Table of Contents

Table of Contents

Introduction

Our Client's Data Guardian: Zluri's Commitment to Trust and Security

Welcome to Zluri, where safeguarding the data is not just our mission; it is our unwavering commitment. Our client's trust is our greatest asset, and we partner with global security experts to protect the information with the utmost care. This comprehensive whitepaper provides a deep dive into Zluri's robust security framework, compliance details, and the measures we have implemented to ensure their data safety.

This whitepaper is more than a document; it is a testament to our commitment. Get a deep dive into our robust security framework, compliance practices, and the measures we have in place to ensure our client's data safety.

Our Commitment to Data Security

At Zluri, our commitment to data security is unwavering and multifaceted. It is underpinned by key compliance certifications covering SOC 2 Type II, PCI DSS, GDPR, and more. Security is integrated at every stage of our product development, from concept to implementation, with Privacy Impact Assessments, security testing, and robust data encryption at rest and in transit. We rely on a secure cloud infrastructure, primarily Amazon Web Services (AWS), bolstered by AWS KMS, Secure PII Data Vault, and Secrets Manager services.
Zluri's transparent approach to data processing ensures client involvement, secure authentication, and role-based access controls. Regular audits, third-party testing, and security tools ensure we maintain robust security. Our comprehensive agreements are tailored to client's needs, and GDPR compliance guides our purposeful data processing and transparency. Disaster recovery and supplier management protocols are in place, and employee security is a priority, with stringent background checks and training. Our platform architecture further fortifies security, and data processing includes thorough quality control steps. In a nutshell, Zluri is dedicated to safeguarding data through comprehensive, proactive measures and a commitment to transparency.

Our Guiding Principles

The cornerstone of our approach lies in our guiding principles, which shape every feature we design and every decision we make.

Minimum Data Collection

All the metadata we collect is meticulously vetted to ensure what is essential is gathered. This minimizes potential vulnerabilities and upholds our commitment to our client's privacy.

> We collect information on logins, and app usage but only gather essential personally identifiable information (PII) when necessary. The approach minimizes potential vulnerabilities.

Transparency

In an era where data privacy is paramount, we lay all our cards on the table. We openly detail the data we collect and its use, ensuring our clients are never in the dark.

> We transparently share the data report we collect and how it is used. Our approach ensures they are always aware of what is happening with client's data.

Security

At Zluri, we adopt a multi-faceted approach to security encompassing various aspects, including robust compliance certifications, comprehensive security integration, rigorous encryption measures, a secure infrastructure on AWS, transparent communication.

> We strongly focus on data governance and retention, disaster recovery, supplier management, and employee security protocols.
>
> Our architecture includes advanced security features such as Secure PII Data Vault Firewalls, encryption at rest, and protection against DDoS attacks, ensuring data protection at every level.

Compliance and Certifications

We take client's data security seriously and have obtained various certifications and accreditations. These certifications are not just badges on our website; they represent our commitment to the highest global standards of information security management.

Tailored Compliance to Our Client's Needs

We understand that every organization has unique compliance requirements. At Zluri, we have blended industry standards with custom assessments to ensure our compliance measures align with our client's needs.

Merged Industry Standards and Customized Risk Assessments

Our compliance strategy goes beyond checkboxes. We seamlessly merge industry standards with tailored risk assessments, creating a compliance approach that is as unique as our client's business.

Our Key Compliance Certifications

Let's delve into how Zluri adheres to each critical control relevant to essential compliance.

SOC 2 Type II

Zluri's approach to critical controls within the SOC 2 Type II framework to secure our client's valuable information:

- **Change Management:** Our rigorous change management process authorizes, documents, tests, and implements changes in infrastructure, data, software, and procedures. This meticulous approach guarantees that any alterations meet our objectives while adhering to documented policies and procedures.
- **Access Control:** We strictly restrict access to change the production environment to authorized DevOps Engineers. Furthermore, we enforce the physical and logical separation of development and test environments from production.
- **System Monitoring:** We employ advanced monitoring software that evaluates system performance, security threats, resource utilization needs, and typical system activity. We configure this software to alert our security committee when thresholds exceed, ensuring swift responses to potential threats.
- **Business Continuity:** Zluri takes business continuity and disaster recovery seriously. We maintain documented plans that identify and mitigate risks, define critical systems, assign roles and responsibilities in case of a disaster, and assess and mitigate risks identified during testing.
- **Confidentiality Measures:** Confidential data is essential to our client's operations, and we treat it as such. We have policies and procedures to guide our personnel on confidentiality processes. An inventory log of assets with confidential data is meticulously maintained, and measures are in place to protect this data from erasure or destruction during its retention period.

For a detailed SOC2 report, contact our support team or submit a request here.

PCI DSS

If our clients are utilizing third-party applications for payment prevention, Zluri does not directly handle transaction processes. Our systematic approach to PCI compliance encompasses multiple security measures aimed at safeguarding PII and sensitive data, identifying and mitigating vulnerabilities, and maintaining the highest level of security.

- **Firewall Configuration and Strong Passwords:** To protect client's data, Zluri maintains a robust firewall configuration. We steer clear of default passwords and security parameters provided by vendors, ensuring the use of unique, strong passwords. This approach adds layer of protection, making it significantly harder for unauthorized entities to access sensitive data.
- **Encryption of Data Transmission:** The secure transmission of data is paramount. Zluri encrypts the transmission of all data across open and public networks. This encryption minimizes the risk of interception by malicious actors, further strengthening the security of payment information.
- **Malware Prevention and Secure Systems:** We are committed to preventing malware attacks by regularly updating anti-virus software and programs. Our focus on developing and maintaining secure systems and applications follows industry best practices and vendor recommendations. The approach is integral to protecting the integrity of the data we handle.
- **Access Control and Authorization:** At Zluri, access to data is tightly controlled. Access is granted based on business need-to-know, ensuring that only authorized individuals can access sensitive information. Strict access controls minimize the risk of unauthorized access to sensitive and PII data.
- **Physical Security and Access Monitoring:** Zluri recognizes the importance of physical security in protecting all data. We restrict physical access to data and employ robust tracking and monitoring of all access to network resources and data. The thorough approach guarantees that unauthorized physical access is promptly identified and addressed.
- **Regular Security Testing:** We conduct regular security testing on our systems and processes to identify and address vulnerabilities effectively. The proactive measure ensures that any potential security weaknesses are discovered and rectified promptly.
- **Comprehensive Information Security Policies:** A comprehensive policy that addresses information security for all personnel is meticulously maintained at Zluri. The policy ensures every team member knows their responsibilities and follows the best practices for safeguarding cardholder data.

For a detailed PCI DSS report, contact our support team or submit a request here.

BSI - ISO/IEC 27001 ISMS

Our clients can trust Zluri to securely manage and optimize their SaaS applications without fearing data breaches, ensuring that every piece of data is treated with the highest security protocols of BSI - ISO/IEC 27001 ISMS.

The certification is a testament to our commitment to safeguarding our client's data and ensuring the integrity, confidentiality, and availability of the information we handle.

- **Comprehensive Document Management:** As part of our ISO 27001:2013 compliance, we have meticulously organized and managed a comprehensive set of documents. These documents cover every aspect of information security management and align with the standard's requirements.
- **Rigorous Audit and Assessment:** The audit is carried out with a thorough examination of various aspects, including the effectiveness of our system, risk assessment procedures, incident handling, and management reviews. The results of this audit demonstrated our commitment to the highest standards of information security.
- **Strong Risk Management:** One of the key strengths highlighted in the audit is our robust risk management procedures. We have a documented Risk Assessment Procedure and a Risk Register that identifies and assesses risks related to our ISMS and specific projects. The approach helps us proactively mitigate risks and maintain a secure data environment for our clients.
- **Comprehensive Personnel Training:** The audit report also acknowledges that our employees undergo extensive security awareness training. The training ensures that our team is well-equipped to handle our clients data security.
- **Cloud Security:** Our cloud environment, hosted on AWS, complies with ISO 27001:2013 standards. Additionally, multi-factor authentication (MFA) is enabled for all accounts to add an extra layer of security.
- **Issues Management:** We have documented internal and external issues critical to our information security practices. The knowledge base helps us address challenges and opportunities in our security strategy.
- **Supplier Management:** Our Supplier Management Policy ensures that our suppliers also adhere to stringent security standards, extending the umbrella of protection to all parts of our operation.
- **Continuous Improvement:** Management review meetings are held regularly to evaluate our internal audit reports, set objectives for continual improvement, and drive our commitment to advancing our information security management.

For more, ISO Certificate, contact our support team or submit a request here.

GDPR

For our clients with European customers or with EU citizens' data, we are committed to ensuring compliance with the General Data Protection Regulation (GDPR). GDPR is one of the most stringent data protection regulations globally, and we understand the importance of safeguarding our client's data. The section will outline the key measures we have in place to ensure GDPR compliance and certification.

- **Purposeful Data Processing:** We process Customer Personal Data only per our client's documented instructions, as specified in our agreements. We will not use their data for any purpose other than what is required to provide and support our Cloud Products unless applicable law requires. If any other purpose is legally mandated, we will inform our clients of this requirement unless prohibited by essential grounds of public interest.
- **Data Processing Assessments:** We actively assist our clients in their obligations under GDPR. Our approach includes performing data protection impact assessments when necessary and informing supervisory authorities if such assessments indicate a high risk in the absence of mitigation measures.
- **Data Subject Rights:** We support our clients in fulfilling their obligations under GDPR. We aim to provide our clients with the necessary documentation, or processes to assist them in retrieving, correcting, deleting, or restricting Customer Personal Data when requested.
- **Security Measures:** We implement and maintain technical and organizational measures to protect Customer Personal Data against unauthorized processing and potential risks such as accidental loss, destruction, damage, theft, alteration, or disclosure. These measures are designed to minimize potential harm.
- **Notification of Security Breaches:** If we become aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of our client's Customer Personal Data that we process while providing our Cloud Products (a "Security Breach"), we commit to notifying our clients without undue delay. We take immediate action to address and rectify any Security breaches.
- **Data Transfers under GDPR:** When processing Customer Personal Data under the European Data Protection Law in a country that does not ensure adequate protection, we adhere to GDPR requirements for data transfers via Standard Contractual Cluases.

For more, refer to Our Data Protection Addendum and review our GDPR Certificate.

NIST SP - 800-171

NIST SP - 800-171 guidelines are designed to protect controlled unclassified information. Our compliance with NIST SP - 800-171 ensures that our client's data, even if unclassified, is kept secure. Let's delve into how we adhere to these stringent guidelines:

- **Controls Across Key Control Families:** We have implemented controls spanning various critical control families outlined in NIST SP - 800-171. These include access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity.
- **Zero Data Storage at Our Office:** It is vital to understand that Zluri does not store any data in our office. We have opted for a cloud-first approach, with all our services and data hosted on Amazon Web Services (AWS). AWS, renowned for its rigorous security protocols, is responsible for ensuring the physical security of its data centers. The approach aligns with NIST SP - 800-171 and offers our clients the peace of mind that their data remains secure even at the physical infrastructure level.
- **Annual Risk Assessments:** Risk is an ever-present element in the digital landscape, and we are steadfast in our commitment to assessing and addressing it. We conduct annual risk assessments to identify, evaluate, and mitigate potential risks. Risk owners are promptly informed about open risks and those successfully closed or mitigated. The approach ensures that risks are handled comprehensively and transparently, per NIST guidelines.
- **Governance, Risk, and Compliance Training:** One of the cornerstones of data security is ensuring that our team is well-versed in the best practices. That's why we provide comprehensive security and privacy training to all our employees. Our online Governance, Risk, and Compliance (GRC) platform equips our team with the knowledge and skills required to maintain NIST SP - 800-171 compliance. The approach, in turn, contributes to the robustness of our security measures, ensuring our client's data remains in safe hands.

For a detailed NIST SP - 800-171 report, contact our support team or submit a request here.

ISO 27701

Our client's organization deals with sensitive customer PII data, and they are bound by regulations to protect that data. Our unwavering commitment to data security has obtained the ISO 27701 certification, a hallmark of excellence in privacy information management systems. This certification is a testament to our dedication to ensuring that customer data is handled with the utmost care, diligence, and privacy, going beyond the call of duty.

- **Data Handling with Precision:** We recognize that our clients handle customer data that is valuable and comes with legal obligations to protect. We have established stringent procedures and practices that govern such data's handling, processing, and storage. All sensitive and PII Data is encrypted with a unique key for every customer with the option of BYOK (Bring your own key) and stored in Secure PII Data Stores.
- **Data Privacy Commitment:** Our data handling practices, from data collection to sharing, are designed with an unwavering commitment to protecting the integrity and confidentiality of our client's data.

For a detailed ISO 27701 report, contact our support team or submit a request here.

Our Trust and Security Measures

Product Development

Security is not just an afterthought but embedded in our product's DNA.
We place security at the core of our product development process. Security is embedded at every stage, from conceptualization to design, implementation, and ongoing operations.

Privacy Impact Assessment

We ensure that new features do not create unnecessary privacy implications for our customers. When developing a new feature that collects user data, we conduct a Privacy Impact Assessment (PIA) to identify and mitigate any associated privacy risks.

Comprehensive Security Testing

Security testing is performed with every release, incorporating automated and manual testing. Before rolling out a software update to identify and address potential vulnerabilities.

End-to-End Encryption

Data Security from Every Angle

Our client's data deserves the best protection. Zluri's robust end-to-end encryption ensures that the data is shielded comprehensively.

- **Data in Transit:** When our client's data moves between locations, it is encrypted to prevent interception by unauthorized parties. Even if the data is transmitted over public networks, it remains confidential and secure.
- **Data at Rest:** Data stored on our servers is protected through encryption, ensuring that even if someone gains physical access to our servers, they cannot access the data. Imagine the peace of mind in knowing that our client's sensitive information is safe from both external and internal threats.
- **Client-Side Encryption:** For additional security, we encrypt data on our client's devices before it is transmitted, making it indecipherable even if intercepted in transit. The approach means that even if a hacker gains access to the device, the data they acquire remains unreadable.
- **Secure PII Data Vault:** Secure PII Data Vault adds an extra layer of protection for our client's sensitive personal data. If the organization is handling sensitive employee's information, with our PII Vault, they can be confident that employee data is secure, even in the face of the most determined cyber threats.

AWS-Powered Infrastructure Security

Leveraging Amazon's World-Class Infrastructure
We chose Amazon Web Services (AWS) as the foundation of our platform because of its impeccable reputation for security and high availability. For a deep dive, visit Cloud Security – Amazon Web Services (AWS)

High Availability

Our platform hosted on AWS ensures that our client's data is available whenever needed. AWS provides industry-leading uptime and redundancy.

AWS KMS

AWS Key Management Service (KMS) keeps our client's sensitive data secure. These services protect access to the data and credentials. If the organization relies on Zluri to manage critical customer data. With AWS KMS, they can trust that the data remains confidential and accessible only to authorized personnel.

Secrets Management

Leveraging AWS Secrets Manager, Zluri ensures that our client's sensitive information is not only secure but also optimally beneficial for their organizational needs.

Our platform allows clients to securely store and manage crucial data such as API keys, access tokens, and scopes. Moreover, in a Bring Your Own Key (BYOK) scenario, clients have the flexibility to bring their encryption keys, enhancing the level of control and security over their sensitive data to encrypt the data on Secrets Store.
During the synchronization process, we seamlessly retrieve the necessary secrets from the Secrets Manager to establish a secure connection with the application. This ensures not only sensitive data security but also efficiency and adaptability.

Secure PII Data Vault

We use a Secure PII Data Vault to store and secure client's PII data. Having a separate vault guarantees that PII data is handled with meticulous care and control, thereby augmenting overall data privacy and security.

This vault serves as an extra layer of defense for our client's sensitive personal data. The vault employs advanced techniques such as tokenization and de-identification to replace sensitive PII with unique tokens. This ensures that in the event of an unauthorized access, the data remains unreadable and unusable.

Encryption and decryption keys are stored in a separate ecosystem from the data which ensures other layer of separation and security against any possibility of a leak.

The Data Vault allows for fine-grained access controls, enabling us to define and enforce policies on who can access, view, or modify specific types of data. This reduces the risk of unauthorized access or data misuse. Comprehensive audit trail capabilities provided by the PII Data Vault enables us to track and review all activities related to sensitive data.

In a BYOK scenario, all data is stored in the Vault using the unique client's encryption keys. In this setup, the clients gain the flexibility to oversee their encryption keys, introducing an additional level of control and security to their stored PII data. This allows clients to implement key rotation and manage the lifecycle of encryption keys more effectively. Clients can use their own key management systems (KMSs) to generate, store, and manage encryption keys.

Transparent Customer Metadata Processing

Gaining our Client's Trust through Transparency

At Zluri, transparency is not just a principle but a commitment to safeguarding our client's data. We recognize the significance of critical metadata in our client's business operations and uphold the highest standards of transparency through a Data Processing Agreement (DPA). This agreement outlines our commitment to securely process their data, ensuring trust, accountability, and compliance at every step. For a deep dive, visit Privacy Policy | Zluri

Customer Metadata

We collect only the required metadata as required to provide accurate insights to administrators about SaaS usage in their organization.

Data Transparency

We provide our clients with complete visibility into the processing of critical metadata, which includes nuanced SaaS usage metrics. They are always aware of the reason for processing the data. This transparency builds trust between our clients and Zluri, ensuring they fully understand how the data is managed and processed.

Data Collection Practices

At Zluri, our approach to data collection prioritizes the responsible handling of Personal Identifiable Information (PII). We strictly adhere to the principle of collecting only the PII that is essential for our services. Our robust data minimization policy guarantees the minimalization of data and ensures timely removal when it is no longer necessary. Furthermore, we enhance the security of stored data by applying encryption at rest across all our systems, along with Secure PII Data Stores to provide an additional layer of protection. This commitment reflects our dedication to safeguarding sensitive information and maintaining the highest standards of data security.

Secure Authentication & Access Control

Access to our platform is secure and seamless.

Single Sign-On Controls

- **SAML-Based SSO:** Zluri offers seamless integration with SAML-based Single Sign-On (SSO) providers like Okta, Azure, and G Suite. Our client's organizations can streamline access to Zluri using the client's preferred authentication providers.
- **Whitelisting:** Authorized source IPs are whitelisted for access. Ensures that only trusted sources can access our client's organization's Zluri account.
- **Multi-Factor Authentication (MFA):** Additional layers of authentication provide enhanced security.

Role-Based Access Controls

We implement precise permissions through Role-Based Access Controls (RBAC), ensuring only authorized personnel can access specific data. Consider a scenario where our client's organization uses Zluri to monitor software usage across various departments. With RBAC, they can grant different levels of access to other team leads, ensuring that each department can only view its data.

Regular Credential Rotation

Our approach to security includes regularly patching credentials to prevent unauthorized access. Regularly changing credentials is a standard security practice that helps mitigate the risk of unauthorized access to our client's accounts.

Access Control to Data Processing Systems (System Access Control)

Zluri implements stringent measures to ensure the security of data processing systems. Regular reviews of production access involve user verification, and access requests are meticulously tracked and approved by the Team manager, with quarterly reviews for ongoing scrutiny. Access to AWS read-only and System Admin accounts is carefully controlled, bolstered by SSO and Multi-Factor Authentication (MFA). Additionally, a robust Privileged Access Management system is in place, limiting access to environments hosting user data and reinforcing the overall security post.

Controlled PII Access for Debugging

To maintain the utmost security, access to Personal Identifiable Information (PII) for debugging purposes is strictly controlled through support credentials. Our systems employ robust access logging and reporting mechanisms, generating detailed audit trails for transparent accountability.

Data Access Control

Ensuring authorized access to specific areas of data processing systems is a meticulous process. Approval procedures, granting minimum access rights, and rigorous training protocols are enforced. This includes strict compliance with the Zluri data management policy, Zluri security and privacy policies, GDPR regulations, and comprehensive privacy training. At Zluri, safeguarding Personal Data is not just a practice but a commitment upheld through stringent access controls and adherence to industry-leading data management standards.

Comprehensive Auditing & Monitoring

Vigilant Watchkeepers: Protecting Our Client's Data
We leave nothing to chance regarding safeguarding our client's data. To ensure the highest level of security, we conduct periodic third-party audits and penetration testing.

Third-Party Audits and Penetration Testing

Regular third-party audits and penetration testing ensure that our security practices meet rigorous testing. The approach assures that our security controls and policies protect our client's data. We conduct audits at least once in six months.

AWS Security Hub

We utilize AWS Security Hub for comprehensive internal and external auditing, providing transparency regarding activity associated with our client's data. AWS Security Hub acts as an additional layer of security, ensuring that the data remains safe and any potential vulnerabilities are identified and addressed.

Comprehensive Agreements Framework

Tailoring Security to Our Client's Needs

Master Service Agreement and Data Processing Agreement

We understand that one size does not fit all. Our Master Service Agreement (MSA) and Data Processing Agreement (DPA) structures are meticulously aligned with regulations like GDPR and CCPA.

Business Associate Agreements

We offer specialized Business Associate Agreements (BAAs) that allow our clients to customize our client's security journey to meet their unique requirements. If our client's organization operates in the healthcare sector, they can customize our agreements to ensure compliance with HIPAA regulations.

Data Discovery and Classification

Data is classified based on sensitivity, ensuring appropriate security measures are applied. PII is treated with the highest level of protection.
Our data discovery and classification lay the groundwork for enhanced security strategies and compliance-driven measures. By categorizing employee Personally Identifiable Information (PII), we empower our clients to dictate access and harness enriched analytics, setting the benchmark for comprehensive digital protection.

Data Governance, Retention & Removal

Empowering Our Clients with Data Control
Data governance is a crucial aspect of our service.

Smart Storage Practices for PII

Our approach includes regular reviews and purging of outdated or non-critical data to minimize risks associated with unnecessary information. Furthermore, we maintain a clear distinction between in-scope and out-of-scope elements, explicitly identifying considerations like IP addresses and data in transit.

Versioning and Lineage Tracking

We empower our clients with the ability to track our client's data evolution through versioning and lineage. With Zluri, they can track relevant changes, providing a detailed history of edits and contributors with audit logs.

Flexible, Customer-Driven Data Removal

All PII data would be automatically deleted within 60 days of contract termination. Our clients maintain control over their data, including options for flexible and customer-driven data removal based on request. The approach ensures they can delete data per the organization's data retention policies and compliance requirements.

Secure Internet Connectivity and Data Transmission

Zluri prioritizes the security of data during its journey over the internet. All externally-facing services implemented by Zluri utilize HTTPS coupled with TCP/TLS version 1.2 or higher. This meticulous approach guarantees the encryption of all customer information in transit, regardless of where the connection is established. By implementing these robust encryption standards, Zluri ensures a secure and confidential connection, safeguarding customer data from potential unauthorized access during transmission over the internet.

Corporate Security

Human Resource Security

Our commitment to data security extends to our employees. We maintain strict human resource security protocols, ensuring our team meets the highest standards. All employees undergo background checks to ensure trustworthiness and reliability.

Disaster Recovery

At Zluri, safeguarding our client's data and ensuring uninterrupted service are paramount. Our disaster recovery strategies encapsulate state-of-the-art technology, meticulous planning, and unwavering dedication, ensuring our infrastructure remains robust and reliable.

1. **Data Backup Protocols**
   - **Consistent Backups:** Daily automated backups, coupled with advanced encryption.
   - **Diverse Storage:** Data storage across distinct regions boosts resilience against localized disruptions.
   - **Internal and Third-Party Systems:** A dual-layered backup approach guarantees data accessibility, even during server failures.
2. **Strategic Recovery Planning**
   - **Structured Recovery:** Our plan comprises Notification/Activation, Recovery, and Reconstitution phases, ensuring systematic disaster management.
   - **Priority-based System Recovery:** 'Critical' systems get precedence during recovery, ensuring vital operations resume promptly.
3. **Proactive Threat Management**
   - **Thorough Assessments:** Our comprehensive IT Risk Assessment identifies potential threats, preparing us for various challenges.
4. **Flexible Recovery Solutions**
   - **Versatile Restoration:** We restore operations across platforms promising agility in recovery processes.
5. **Transparent Communication**
   - **Stakeholder Updates:** In recovery scenarios, we maintain open channels with partners and customers, upholding transparency and trust.

Supplier Management

Security is not limited to our walls; it extends to our suppliers. We have strict supplier management processes to ensure that anyone connected to us also adheres to the same stringent security standards.

Organization and People

Security Team and Leadership

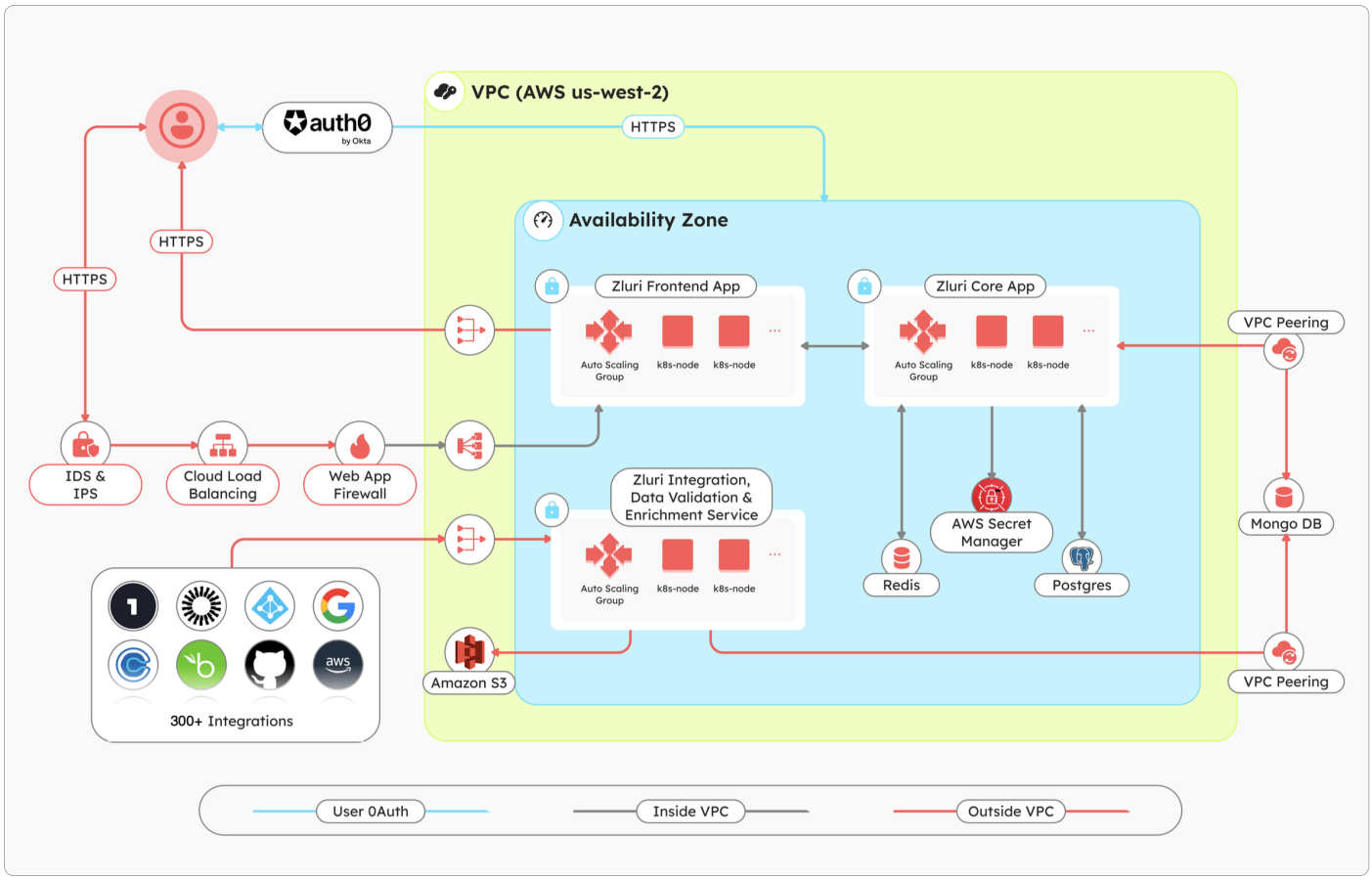
Our security is driven by a dedicated team led by a Chief Information Security Officer (CISO) who reports directly to the CEO. This ensures that security is at the core of our operations and receives the highest leadership commitment.

Employee Onboarding and Security Training

Each Zluri employee undergoes a rigorous background verification process before joining our team. Mandatory security training further equips our staff with the knowledge and skills to protect our client's data.

Zluri Architecture

Our platform architecture forms the backbone of our commitment to data security.



Data Flow Control with Zscaler's ZTNA Firewalls

Zluri takes data security seriously and employs Zscaler's Zero Trust Network Access (ZTNA) as a vital component of our security infrastructure. The ZTNA web app firewall acts like a gatekeeper for incoming and outgoing web traffic, helping us filter and monitor data interactions. This security layer is crucial for identifying and blocking potential cyber threats. Through Zscaler's ZTNA, Zluri ensures that only legitimate data enters or goes out of our system.

Data Protection with Encryption at Rest

Keeping our client's data safe, even when it is at rest, is a top priority for Zluri. We store various sensitive data, including API keys and tokens, in a secure Secret Manager and our client's PII within the secure confines of Secure PII Data Vault. We use robust encryption methods to protect this data. The encryption extends to data stored in AWS S3 which is also encrypted with client specific key.

Secure Communication with HTTPS and TLS

Securing data in transit is necessary for Zluri. We use HTTPS (Hypertext Transfer Protocol Secure) and TLS (Transport Layer Security) to put a protective shield around our client's data as it moves. Whether data comes in or goes out of the system, it is wrapped in cryptographic protection. This extra layer ensures that any attempts at snooping or data interception by bad actors are stopped, preserving their data's confidentiality and integrity.

Authentication via Auth0 and SSO

We have made logging into Zluri simple and secure. We use Auth0 and Single Sign-On (SSO) technologies along with access control to data processing systems. These let our clients use their existing login credentials from services like Google, Microsoft Office 365, SAML v2.0, etc., to access Zluri. The approach means only authorized personnel can get into the system, adding an extra layer of security.

Load Balancing and DDoS Protection

To keep our service running smoothly, Zluri uses something called Application Load Balancer. Think of it as a traffic cop for data. It spreads incoming data across multiple servers, ensuring all the servers get a fair load. But it also has a critical role as the first line of defense against Distributed Denial of Service (DDoS) attacks, which try to overwhelm a system. We achieve this by leveraging Cloudflare's advanced DDoS protection services. By stopping DDoS attacks, Zluri ensures our clients have continuous and uninterrupted access to our platform.

JWT Authentication and Network Security

We use JSON Web Tokens (JWT) for authentication. This means that every request coming into our system needs a valid JWT to be processed. It is a digital badge to make sure only the right requests get through. Our network security is extra solid thanks to scrutiny of network connections through NAT gateways. These gateways keep a close eye on network traffic for potential threats, making sure only safe and verified traffic is allowed.

Integration and Sync Management

At Zluri, our backbone is our integrations. Our system helps us quickly set up new connections with other services. These connections are essential for getting data, but we also check tokens and credentials to ensure everything runs smoothly.

Our data syncing process is quite versatile. We have full syncs for the first-time connection to get historical data, which goes back several months to a couple of years. After that, we use partial syncs to keep the data current. Based on the last successful sync, these syncs fetch data within specific timeframes, so our clients always have the latest information.

We even offer custom syncs to meet unique data retrieval needs, letting our clients specify the date range. Scheduling these syncs is done with an orchestrator. Their data is kept extra secure by using the Secret Manager and Secure PII Data vault to protect sensitive information like PII, API keys and tokens. The raw data is also encrypted with client specific keys to ensure high levels of security.

Data Processing and Quality Control

Data processing at Zluri involves several steps. We take data from various sources, clean it up, store it in AWS S3 with encrypted storage, apply business rules, and then make it available through the Zluri user interface (UI).

Quality control is a big deal for us. We have measures to ensure the Zluri platform's data matches what we get from APIs. The approach includes finding and fixing issues like duplicate users and ensuring data consistency and reliability. Additionally, our commitment to transparency and accountability is evident through comprehensive audit logs. These logs meticulously document key activities, providing an auditable trail for our users and enhancing the platform's accountability.

We prioritize the safety of your data through a robust backup and recovery system. Regular data backups, both internal and external, coupled with a reliable recovery mechanism, ensure the resilience and availability of your data even in unforeseen circumstances. This comprehensive approach to data management exemplifies our dedication to maintaining data integrity, consistency, and accessibility at all times.

General Security Best Practices and General Controls

Zluri prioritizes password protection, stringent access controls, and conscious secure encryption practices for all types of data. Zluri practices corporate and industry policies for governing PII handling.
Our suite of robust general controls:

- Monitoring and surveillance
- Encryption of data at rest
- Adherence to data retention policy
- Governed and pr-approved changes
- Logging system for production changes
- Software development life cycle (SDLC)
- Multiple environment for testing
- Regular redundancy checks

Conclusion

Our Unparalleled Commitment to Our Client's Data Security

At Zluri, our commitment to our client's data security is unwavering. We continuously evolve and adapt to meet the ever-changing landscape of cyber threats. Their trust is our most valuable asset, and we are dedicated to safeguarding it.

This whitepaper, while informative, is just one aspect of our commitment to data security. To experience it in action, explore our platform and discover how we ensure our client's data remains safe and secure. We are ready to be the partner in data security, guiding them through the ever-evolving landscape of digital threats.

Disclaimer

The information provided in this whitepaper is accurate as of the publication date and is subject to change without notice. Zluri makes no guarantees or warranties regarding the information's completeness or accuracy.