Calibo

Calibo Integrated Security Assurance (CISA)

Robust Security Controls for End-to-End Platform Security and Data Protection

LAZSA

The Self-Service Development Platform to Drive Your Digital Innovation

Calibo Lazsa PaaS: The Self-Service Platform to Drive Your Digital Innovation

Calibo is your trusted companion in your digital innovation journey. Calibo's industry-first fully integrated, pro-code Self-Service Development Platform (PaaS) empowers you to deliver digital products and solutions faster while creating long-term technology advantage. It serves as a one-stop platform for your end-to-end digital portfolio and product lifecycle management, data intelligence, and DevSecOps requirements. Customers across industries are truly excited to experience Lazsa and build their products and digital solutions leveraging the platform.

While Lazsa helps accelerate digital innovation, Calibo assures its customers that **Security** is by design, at the heart of everything we do.

Security:
Our Topmost Priority

Lazsa connects multiple stakeholders, cross-functional teams, and an array of tech stack and tool chain. For such a huge collaborative platform, having a robust security control framework in place is a must.

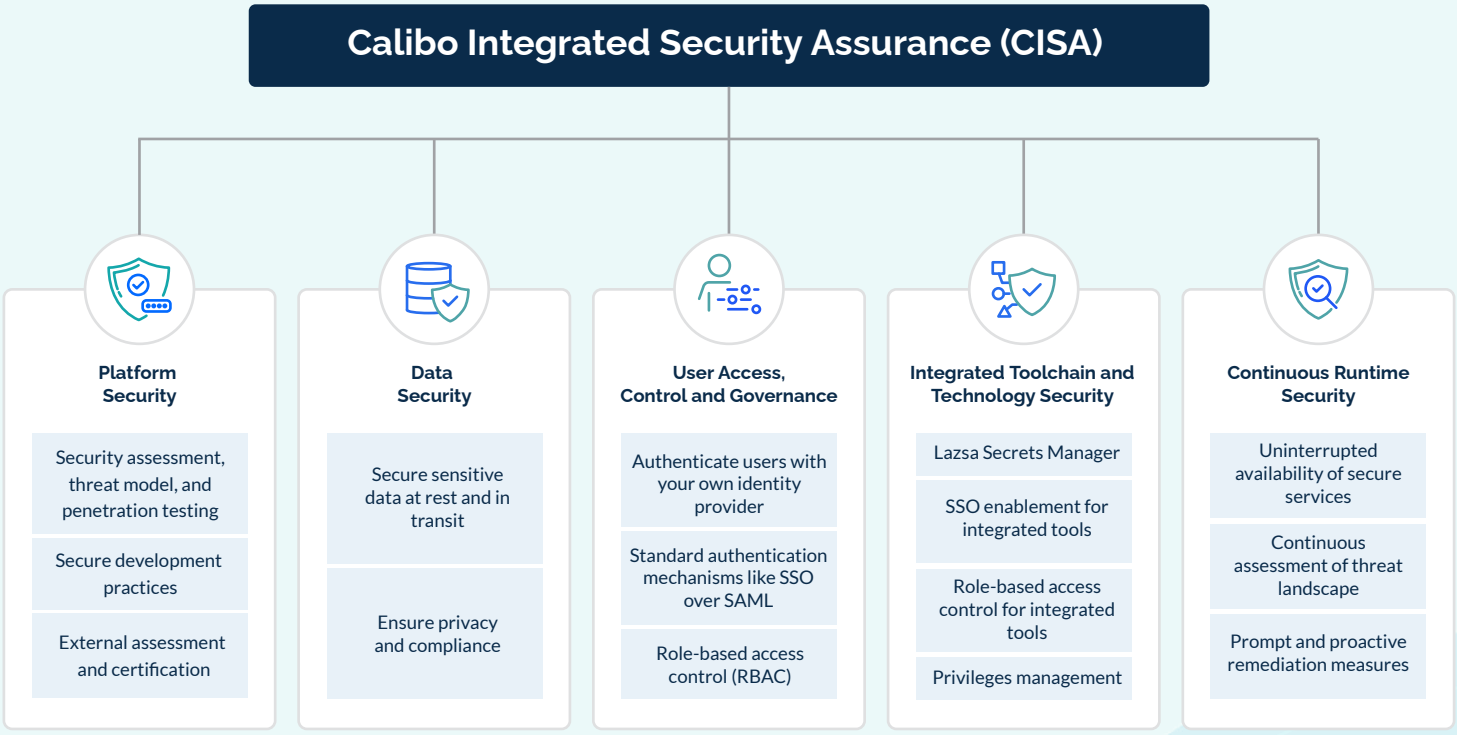
You may bring in your own tools to Lazsa or embrace the built-in technology tools in Lazsa. You may opt for a single-cloud, multi-cloud, or hybrid cloud deployment. You may connect to Lazsa from your trusted corporate network or from a relatively less-managed public network. In any case and at any cost, security of the Lazsa platform, infrastructure, user access, technology and tool chain integration, and the data exchanged through the Lazsa platform is **Calibo's topmost priority and a lifetime commitment!**

Calibo Integrated Security Assurance (CISA)

Calibo takes a holistic approach towards platform security and governance through its unique **Calibo Integrated Security Assurance (CISA) framework**.

The Lazsa self-service platform is designed and developed by considering all your platform and data security requirements and by following the industry best practices. We boast a dedicated team of cyber security experts and we partner with leading cyber security agencies to certify the platform security. We have developed and enforced technological, physical, administrative, and logical security measures to continuously assess the overall security and compliance posture of the Lazsa platform.

CISA framework emphasizes on five major security areas in the Lazsa workflows and ensures comprehensive and continuous security and risk assessment.



Platform Security

- STRIDE-based threat model developed for Lazsa by our security experts
- Periodic security assessment, penetration testing, and certification by leading external cyber security agencies
- Continuous detection and remediation of security issues in product development, deployment, and configuration
- Periodic scanning and reviews of open-source components, source code, third-party tools and technologies, OS and Docker images used in Lazsa to detect newly-reported vulnerabilities
- Training programs for employees and enforcement of secure coding best practices
- Secure development and deployment practices embedded in the work culture
- Use of benchmarked OS images for infrastructure
- Industry-best container security scanners for scanning nodes and containers running in the platform
- Monitoring of cloud infrastructure for security compliance and periodic enforcement of controls
- Periodic rotation of encryption keys as a cryptographic best practice and use of latest secure encryption algorithms for end-to-end data encryption

Data Security

- Role-Based Access Control (RBAC) to authorize users before granting them access to data and services
- Lazsa Secrets Manager for securely storing all the sensitive information like tools configuration
- Adherence to security protocols while storing and transferring data in and out of Lazsa
- Privacy information compliance with adherence to the latest data protection laws, regulations, and general privacy best practices
- Lazsa services isolated from your invaluable IP and production workloads, giving you full control over your data

User Access, Control, and Governance

- Federated authentication based on SAML and OpenID
- Integration with corporate SSO and industry-standard IdPs like Microsoft Active Directory and Azure Active Directory
- Multi-factor authentication to ensure multi-level protection
- User authorization through Lazsa Role-Based Access Control (RBAC) model
- Custom roles to have fine-grained access to resources as per your project requirements
- Comprehensive auditing of all users and system actions for governance and control
- Policy templates to restrict access to underlying cloud infrastructure, resources, and tools

Integrated Toolchain and Technology Security

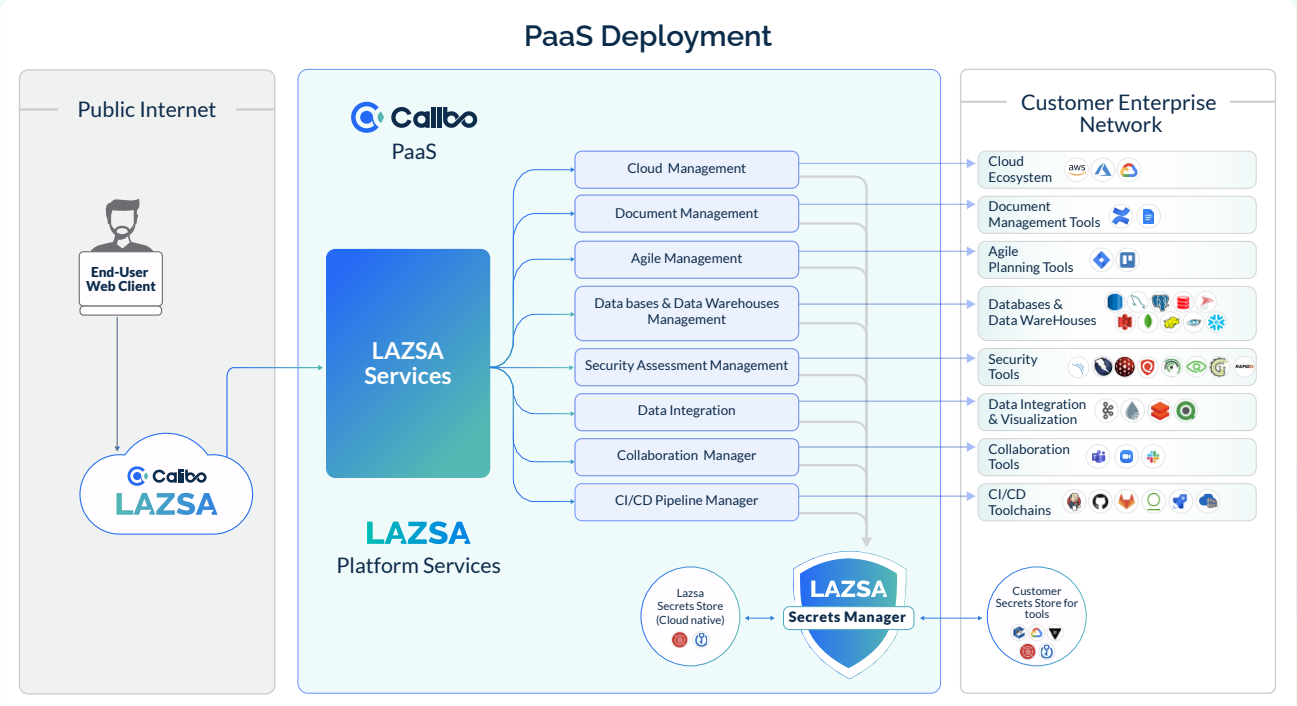
- Lazsa does not store the credentials of the integrated tools and technologies unless explicitly specified.
- Lazsa supports integration with customer's own secrets store like CyberArk, AWS Secrets Manager, HashiCorp Vault, etc. to retrieve credentials for integrated tools and technologies.
- Lazsa Secrets Manager service is deployed within customer's network to connect to customer's secrets management tool and consume credentials in encrypted format as required.
- SSO enablement and role-based access control is provided for integrated tools and technologies.
- User privilege management is used for a granular approach to delegate access rights to users and applications in Lazsa.

Lazsa Deployed as PaaS

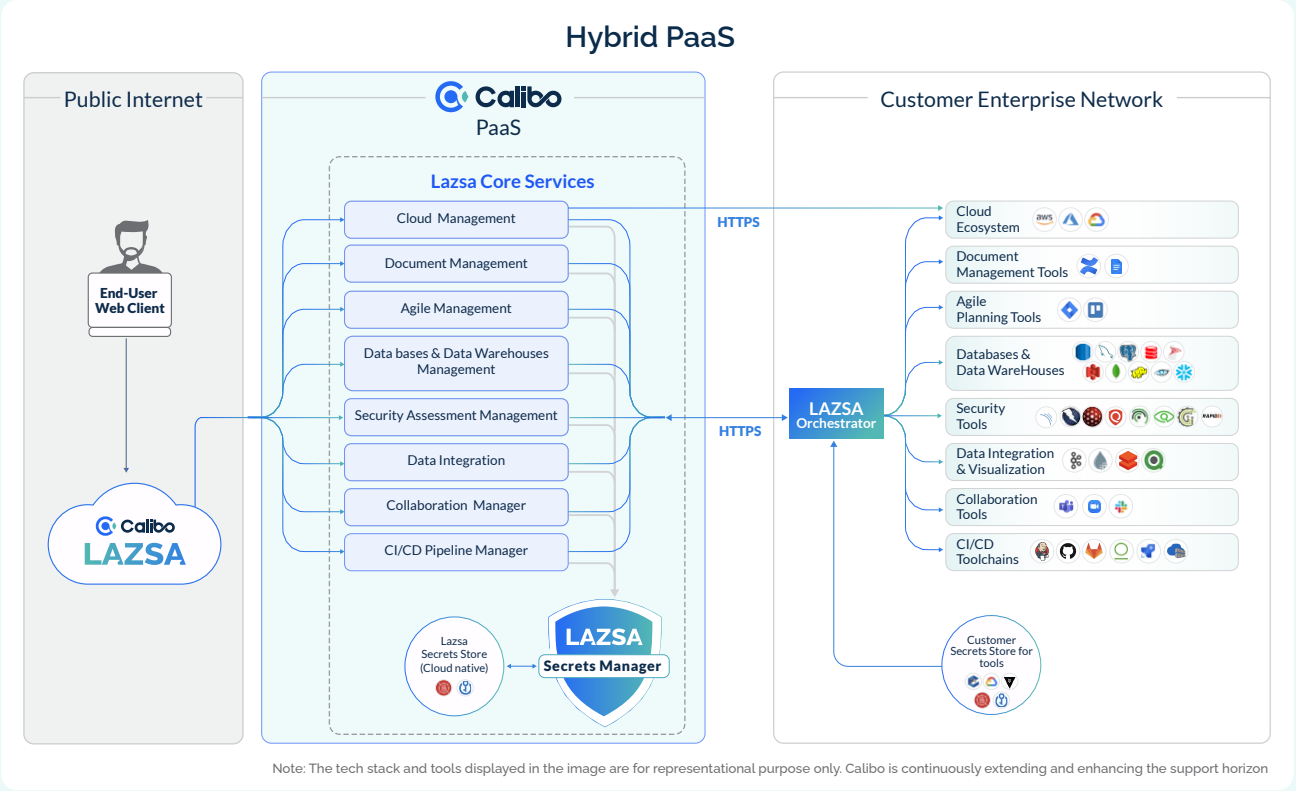
Lazsa is a PaaS offering with safe and secure credential management of the integrated tools and technologies.

- Lazsa core services are deployed in Calibo-managed public cloud.
- Lazsa tools and technologies adapters and Secrets Manager service are deployed in customer-managed public cloud.
- Lazsa Secrets Manager connects with customer's credential managment tools to get credentials for connecting to their tools and technologies.

The following image depicts how Lazsa Secrets Manager ensures safe and secure credential management in a PaaS deployment.



Note: The tech stack and tools displayed in the image are for representational purpose only. Calibo is continuously extending and enhancing the support horizon



Note: The tech stack and tools displayed in the image are for representational purpose only. Calibo is continuously extending and enhancing the support horizon

Continuous Runtime Security

- Continuous monitoring of Lazsa services for health and security
- Uninterrupted availability of services through clustering, auto scaling, and disaster management
- Best-in-class security tools to continuously monitor infrastructure security as well as application security, and to remediate identified issues to avoid security breaches
- Minimum to negligible downtime during remediation
- Established practices for periodic data backup, recovery, and management

Note: If you choose to deploy Lazsa in your own public cloud, it is assumed that runtime security tasks are monitored and governed by your security policies, practices, and tech stack.

Some Frequently Asked Questions Related to Data Security

Who decides where my data resides?

You can decide where your data will reside. You can create your own account with any industry leading public cloud service provider. If you manage your own account, you have full control over your data. If you choose to use a cloud account managed by Lazsa, your data security is our responsibility.

If my cloud account is managed by Calibo, how does Calibo ensure data security?

All the required security controls for a Lazsa-managed cloud account are in place and are managed by our Site Reliability Engineering (SRE) team.

Which authentication methods are used to connect to the Lazsa platform?

You can opt for SSO authentication built on top of your corporate identity service provider or you can choose the Lazsa-managed authentication mode.

- If you choose the first option authentication and security of user credentials are taken care of by your corporate ID provider, and not by Lazsa.
- If you choose Lazsa-managed authentication, Lazsa makes sure that user credentials are stored securely in an encrypted format. Your credentials are safe with us.

Who can access my data?

Your authorized Lazsa Administrator has full control on who can access your enterprise data. The Lazsa Platform uses role-based access control (RBAC) to manage access and authorization for users across various Lazsa objects and processes. Lazsa provides predefined roles that come with a set of default permissions to perform certain actions in Lazsa. Additionally, Lazsa Administrator can create custom roles, grant permissions to custom roles, and assign roles to users.

How does Lazsa ensure security of credentials for tools integrated with Lazsa?

You can choose whether you want Lazsa to manage tools credentials for you, or you want to manage them in your own secrets management tool.

- If you choose the first option, your credentials are securely stored in Lazsa using best secrets management tools.
- If you have a secrets manager installed in your environment, Lazsa securely connects with it to consume credentials in an encrypted format. Lazsa supports all the industry-leading secrets managers like Cyber Ark, AWS Secrets Manager, HashiCorp Vault, etc.

I do not want to share credentials with Lazsa. I have my own secrets management service in place. Can Lazsa connect with my secrets manager?

Of course. The Lazsa Secrets Manager service is a safe, secure, and light-weight connector that resides within your environment. The Lazsa Secrets Manager is responsible for a secure handshake between Lazsa services (in your public network) and your secrets manager in customer' pubilc cloud. So, whenever Lazsa needs to call any application or tool in your environment, the Lazsa Secrets Manager connects with your secrets manager, retrieves credentials in an encrypted format, and shares them with the Lazsa platform. Lazsa uses these credentials to log on to the required application and proceeds with the next steps in the workflow.

How does Lazsa protect the sensitive information like PII and PHI?

Sensitive information like PII and PHI is stored securely and user access to data is fully controlled in Lazsa.
To provide desired functionalities to customers and to ensure the best user experience, Calibo needs to collect, store, and process the following data on Lazsa: *user's first name and last name, business email address, company name, country, job title, and phone number.*

Calibo interprets this data as personally identifiable information (PII) and takes its protection seriously. As a non-negotiable component of PII protection, Calibo uses AES256 algorithm and disk encryption. Calibo does not use any of your sensitive information for Calibo's own business needs.

Multiple stakeholders will collaborate on the Lazsa platform. Can we control the way sensitive data is exchanged through Lazsa?

All the collaborators must be given access through roles and permissions by Lazsa Administrator. Access to sensitive data can be restricted through such controlled access.

Do you follow the Zero Trust Approach to secure data?

Our Role-Based Access Control (RBAC) is a testimony to our Zero Trust Approach.

Data Residency

Where do you host my data? How do you ensure data availability?

If you choose Calibo-managed PaaS offering, we host and store your data in industry-best public cloud along with Lazsa services. We avail services of the underlying cloud platform to securely store data and back it up. We use disaster recovery mechanisms (like data mirroring to different geographical locations) of underlying public cloud platform to ensure continuous availability.

Is my data stored and processed in shared manner with other Calibo customers?

Each customer gets a dedicated set of Lazsa services and data services. This means your data is fully private to you. It is never shared with other Calibo customers.

How do you back up my data?

If Calibo manages your cloud account, Calibo ensures regular data backups.

Monitoring and Compliance

How do you monitor and track the security posture of the Lazsa platform?

We continuously monitor the health status of the platform workflows through security assessments and automated compliance monitoring. Continuous automated detection of misconfiguration or potential vulnerabilities allows us to take remediation measures quickly on a continuous, ongoing basis.

Is your information security and data privacy policy in compliance with industry standards and regulations?

The Calibo Information Security and Data Privacy Policy has been defined to ensure the highest level of information systems security. The platform infrastructure is ISO-compliant. The data security and privacy norms are aligned with industry best practices.

Do you have continuous risk assessment and mitigation framework in place?

End-to-end security is infused in each phase of your PDLC. During development, we make sure the source code is secure. None of the third-party components carries any vulnerabilities. After we deploy the build, we employ best-in-class monitoring and security tools to continuously assess the health status of the deployment.

Do you ensure data compliance with industry standards?

Yes. We are compliant with the latest industry standards.

Calibo

Contact us - **sales@calibo.com**
or visit **www.calibo.com**