darwinbox

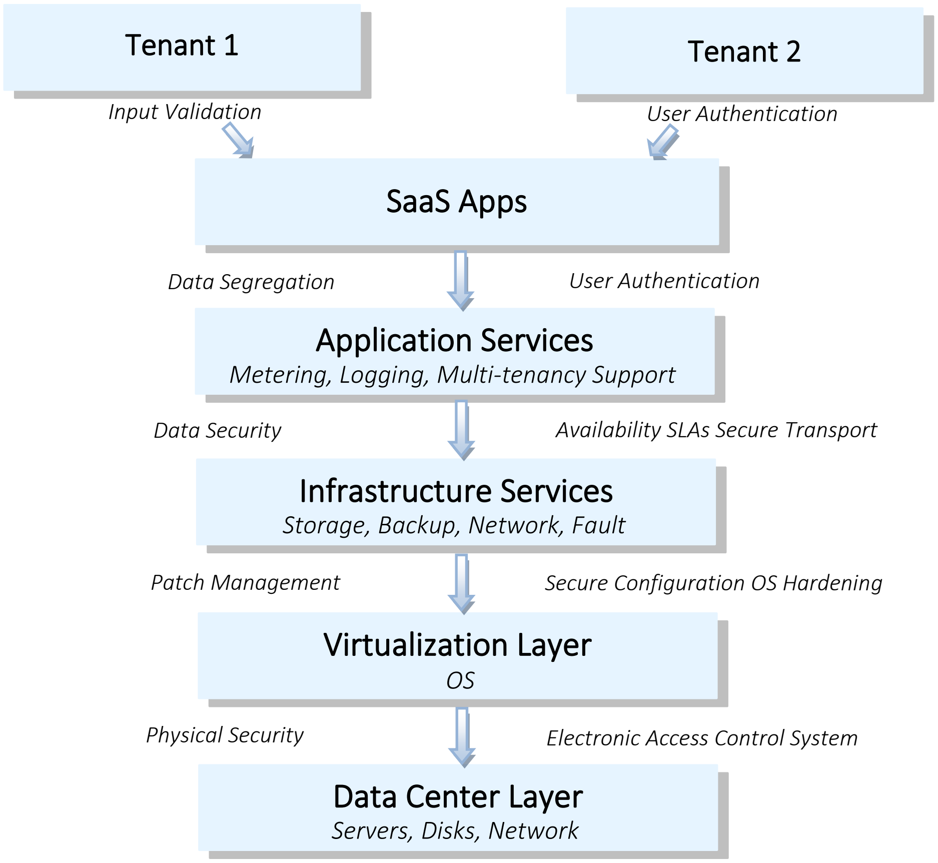
Darwinbox

Data Protection & Privacy

Table of Contents

Darwinbox Data Protection

The following figure illustrates the layered stack of Darwinbox platform and highlights critical aspects that must be covered across layers in order to ensure the security of customers' enterprise data.



High Level Security Considerations

The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- ✓ Deployment model
- ✓ Data security
- ✓ Network security
- ✓ Regulatory compliance
- ✓ Data segregation
- ✓ Availability
- ✓ Backup
- ✓ Identity management and sign-on process

Deployment Model

Below tests are part of Darwinbox platform to validate the security of the infrastructure used to deploy the solution on AWS.

- Host scanning
- Penetration testing
- Perimeter separation for dev/production systems
- Server hardening
- Firewall testing
- Router testing
- Domain name server testing
- Mail Server testing

Darwinbox is deployed on Amazon public cloud that helps to build secure SaaS solutions by providing infrastructure services that aid in ensuring perimeter and environment security. This involves the use of firewalls, intrusion detection systems, etc. A self-hosted SaaS deployment, however, Darwinbox built a custom suite of monitoring and management tools like prometheus, grafana, OpenDLP, ELK stack assess platform for security vulnerabilities.

Data Security

Data in the database is encrypted using SHA512 and AES mechanism is used for encryption and decryption between database and application layer. Darwinbox adopted additional security checks using our monitoring tools to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

In Amazon, the Elastic Compute Cloud [EC2] administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell [SSH] keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service [S3] is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party.

The following assessments test and validate the security of the enterprise data stored at the SaaS vendor -

- ✓ Cross site scripting [XSS]
- ✓ Access control weaknesses
- ✓ OS and SQL Injection Flaws
- ✓ Cross site request forgery [CSRF]
- ✓ Cookie manipulation
- ✓ Hidden field manipulation
- ✓ Insecure storage
- ✓ Insecure configuration

Any vulnerability detected during these tests can be exploited to gain access to sensitive enterprise data and lead to a financial loss.

Application Vulnerability Assessment and Penetration Testing.

Application Vulnerability Assessment and Penetration testing is an integral part of Darwinbox CI/CD pipelines and is done along with every release using owasp tools, however external vendors audit Darwinbox platform once in every 6 months.

Network Security

In AWS the network layer provides significant protection against traditional network security issues, such as MITM attacks, IP spoofing, port scanning, packet sniffing, etc. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, ensuring that data is transferred securely both within AWS and to and from sources outside of AWS.

All Darwinbox data flow over the network is secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer [SSL] and the Transport Layer Security [TLS] for security.

The following assessments test and validate the network security of Darwinbox.

1. Network penetration and packet analysis
2. Session management weaknesses
3. Insecure SSL trust configuration

Network VA is also done to validate the network/host security in the cloud used for deploying the SaaS application in a self-hosted model.

Regulatory Compliance

Access, storage, and processing of sensitive data is carefully controlled and is governed under regulations such as -

ISO 27001/9001

GDPR Compliant

SOC 2 Type 1
SOC 2 Type 2

Data Segregation

Darwinbox is deployed as a multi-tenant SaaS architecture, the application instances and data stores are sometimes shared across multiple enterprises. This allows the Darwinbox to make more efficient use of resources and helps achieve lower costs. At the same time, sufficient security checks are adopted to ensure data security and prevent unauthorized access to data of one tenant by users from other tenants. This involves hardening the data store as well as the application to ensure data segregation using unique tenant ID for each client.

Additional safeguards are adopted so that data of an application tenant is not accessible to other applications. In the case of Amazon, the S3 APIs provide both bucket-level and

object-level access controls, with defaults that only permit authenticated access by the bucket and/or object creator. Write and Delete permission is controlled by an Access Control List (ACL) associated with the bucket. Permission to modify the bucket's ACL is itself controlled by an ACL, and it defaults to creator-only access. Therefore, the customer/tenant maintains full control over who has access to their data. Amazon S3 access can be granted based on Tenant ID, AWS Account ID etc.

The following assessments test and validate the data segregation are done at Darwinbox in a multi-tenant deployment.

1. SQL Injection Flaws
2. Data Validation
3. Insecure Storage

Any vulnerability detected during these tests can be exploited to gain access to sensitive enterprise data of other tenants.

Availability

With Darwinbox account service for instance, the API endpoints are hosted and deployed on a world-class infrastructure using AWS multi region and multi zones distributed architecture using Kubernetes as a service from AWS. Standard Distributed Denial of Service [DDoS] mitigation techniques such as syn cookies and connection limiting are used. To further mitigate the effect of potential DDoS attacks.

These assessments, tests and validations are done at Darwinbox to ensure availability of the platform.

- ✓ Authentication weaknesses
- ✓ Session management weaknesses

Darwinbox platform ensures that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture is adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, are built from the ground up within the application. At the same time, an appropriate action plan for business continuity [BC] and disaster recovery [DR] is considered for any unplanned emergencies. This is essential to ensure the safety of the enterprise data and minimal downtime for enterprises.

Backup

Darwinbox ensures that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters. Also the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information. Data is typically stored in 3 geographies on AWS S3 and data is encrypted by default. Darwinbox application logic encrypts customer data and backups so that it cannot be accessed or tampered with by unauthorized parties.

As part of periodic audits below checks are done on the backups

1. Insecure Storage
2. Insecure Configuration

Identity Management [IdM] and Sign-on Process

Darwinbox allows three ways for Identity management on the platform

Independent IdM stack

Darwinbox platform provides the complete stack of identity management and sign on services. All information related to user accounts, passwords, etc. is completely maintained at the Darwinbox end. The IdM stack is highly configurable to facilitate compliance with enterprise policies, e.g., password strength, etc.

Credential Synchronization

Darwinbox supports replication of user account information and credentials between enterprise and HRMS applications. The user account information creation is done separately by each tenant within the enterprise boundary to comply with its regulatory needs. Relevant portions of user account information are replicated to Darwinbox to provide sign on and access control capabilities. The authentication happens at Darwinbox end using the replicated credentials.
Darwinbox ensures security of the credentials during transit and storage and prevent their leakage

Federated IdM

The entire user account information including credentials is managed and stored independently by each tenant. The user authentication occurs within the enterprise boundary. The identity of the user as well as certain user attributes are propagated on-demand between Darwinbox and vendors using federation to allow sign on and access control. Darwinbox and tenants ensures that proper trust relationships and validations are established to ensure secure federation of user identities.

Insider Threat Mitigation

An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems

Darwinbox has below controls in place to handle any insider threats.

- ✓ Periodic enterprise-wide risk assessments
- ✓ Periodic security awareness training for all employees.
- ✓ Enforce separation of duties and least privilege.
- ✓ Implement strict password and account management policies and practices.
- ✓ Log, monitor, and audit employee online actions.
- ✓ Actively defend against malicious code.
- ✓ Monitor and respond to suspicious or disruptive behavior.
- ✓ Documents insider threat controls.
- ✓ secure backup and recovery processes.
- ✓ Collect and save data for use in investigations.

Darwinbox manage and Audit team behaviours this helps us clear visibility on user actions like user risk scoring, usb tracking, activity alarms, detailed reports and raw data analysis.

Darwinbox SaaS implementation does not allow customers data on employee machines, all data including audits are stored in cloud (with KMS encryption) and is visible only to application logic.

Cookies Policy

To make this site work properly, we sometimes place small data files called cookies on your device.

What are cookies?

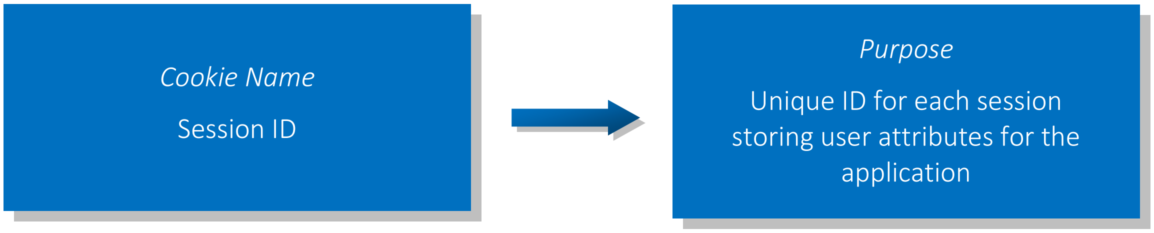
A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language, font size and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

How do we use cookies?

We use cookies for a variety of reasons, including to:

- ✓ Analyze the usage of our Products and Services;
- ✓ Provide a more personalized experience;
- ✓ Allow you to more easily login to use our products services; and
- ✓ Help make your use of Our Products and Services more efficient and more valuable by providing you with a customized experience and recognizing you when you return.

We use the following cookies:



Cookie Name

Session ID

Purpose

Unique ID for each session storing user attributes for the application

You can set Your web browser to warn You about attempts to place cookies on Your computer, limit the types of cookies You allow or refuse cookies altogether; however, You may not be able to use some or all of the features of the Services, or Your experience will be different or less functional if You refuse/disable cookies.

How to control cookies:

You can control and/or delete cookies as you wish. You can delete all cookies that are already on your computer and you can set most browsers to prevent them from being placed. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some services and functionalities may not work.

ABOUT US

Darwinbox is India's fastest growing cloud based HCM platform that is enabling enterprises to achieve strategic HR goals faster and smarter. Leading enterprises have been seamlessly managing their entire employee lifecycle on our unified platform.

One of the most preferred HCM solutions by enterprises in APAC
- Gartner

Arvind
FASHIONING POSSIBILITIES

kotak

adani wilmar

Myntra

NIVEA

Dr.Reddy's

ZILINGO

tokopedia

ZALORA

Paytm

SWIGGY

HT Media

Know more about how Global Organisations enabled a #SmarterWorklife with Darwinbox

Explore Darwinbox