Security Operations

Last Modified on 15.01.2024

Encryption

Data at rest

All databases use a so-called "at rest" encryption. This means that data can only be read if proper authentication takes place on the respective database system. The files in which the data is stored are stored in encrypted form so that they can only be read by database systems that have the appropriate decryption key. Userlane strives to keep its systems up to date with the newest and most secure encryption algorithms. The standard algorithm for encrypting data at rest is currently AES256. Encryption keys are securely managed by Microsoft Azure using Key Vault.

- Read Azure’s principles on Encryption At-Rest

Data in transit

Userlane applies transport encryption whenever data has to be transmitted over an insecure or public network (e.g. outside the virtual private cloud). The type of transport encryption depends on the encryption requested by the client system. Userlane uses HTTPS connections with 256-bit SSL certificates and TLS version 1.2 or newer for all communications with clients. This ensures that data is protected against interception or modification.

Selection of encryption algorithms

Userlane follows the NIST standards for selecting strong encryption algorithms and approving built-in encryption used by a Userlane subprocessor.

- Read the NIST SP 800-175B guidelines

Segregation of traffic in multi-tenant environment

Userlane’s Cloud systems implement multi-tenancy in a shared cluster. Multiple customers are served from a single cluster. Tenant separation is enforced on a logical level, not on a physical level. Userlane ensures strict tenant separation through the following measures:

1. Input sanitization and pre-built queries
2. Request isolation
3. Use of frameworks
4. Extensive manual and automated testing
5. Security scans

6. Penetration testing (see below)

Firewalls

Userlane works with Azure Network Security Groups to ensure that services running within the Azure environment are accessible only to the networks that need it. Access to network ports of various services is restricted to the extent that access is only possible through services that need access.

Penetration Tests

Userlane works with recognized security experts and researchers. Together we aim for the highest possible security of our systems.

We perform penetration tests on a yearly basis. Our contractor Cobalt maintains a core of 200+ highly vetted, certified security researchers.

Upon performing each penetration test, Cobalt provides Userlane with a report containing the list of detected vulnerabilities along with recommended fixes. Userlane commits to implement fixes depending on the severity of the vulnerability. The timeline for such fixes is set as follows:

- Critical vulnerabilities: Fix immediately
- High vulnerabilities: Fix within 30 days
- Medium vulnerabilities: Fix within 60 days

Once a fix is implemented, the vulnerability is re-tested. The cycle is repeated until all vulnerabilities are confirmed to be fixed.

Monitoring

Userlane uses various monitoring tools to ensure maximum availability, performance and security of the application. The monitoring includes but is not limited to the following parameters:

Availability

- Availability of the application
- Accessibility of backend systems and services

Resources

- CPU utilization
- Utilization of network interfaces

- Utilization of persistent and volatile storage

Performance

- Response times of the application
- Response times of backend systems
- Query times for database contents

Security

- Update status of systems
- Error logs
- Access logs (IP address, URL, browser type and version)

Backups

Userlane drives continuous backups of databases. With those database systems that support it, the database state can be restored to a previous state down to the second. Other databases are backed up regularly, e.g. every 24hrs. The backups are stored in the same datacenter region, but a different availability zone. Backups are retained for 30 days. These backups are treated as sensitive data. Only specific personnel can access these backups after an internal authorization process.