Security in xAssets Software

A white paper by : Will Islwyn Lambert, 08 December 2023

xassets
asset management software

Overview

Safeguarding customer data is our highest priority.

We understand the significance of securing your information and ensuring compliance with industry standards. Many of our customers are large and medium sized enterprises who have staff logging into our SAAS servers hundreds of times per day and some manage over 100,000 assets per instance. We do everything in our power to minimize risk and protect your data, knowing that any security breach, downtime, or data loss could have a significant impact on your business and ours.

This document is designed to provide you with insights into the practical and effective security measures that we have implemented at xAssets to keep your data safe. Our approach focuses on creating a secure, scalable, available, and low-risk hosting environment, practical steps to keep your data protected and to keep pace with all forms of emerging threats and risks.

Compliance with Security Standards

We comply with GDPR, SOC 1, SOC 2, HIPAA, and FedRAMP. We try to go far beyond these standards in everything we do.

xAssets applies European Union General Data Protection Regulation (GDPR) standards to all customers, regardless of location. This is compatible with USA, Canadian, UK and Swiss data protection laws. We act as a data processor for our customers, meaning we operate under a legal framework where the role and scope of data processing is clearly defined.

No sub-processing occurs - xAssets does not share customer data with any third parties or contracts, and staff get the minimum level of access necessary to do their work. This means that we cannot use online services such as Dropbox, Google Cloud, AWS storage, or Azure storage, since these services are sub-processors, instead we do the necessary data replication on our own infrastructure. If they haven't got it, it can't be compromised!

Security forms the baseline of our employee training and handbooks, and employees are regularly refreshed on security requirements. All employees with access to servers (physical or remote access) are trained in security best practices and are required to pass a security test.

Our software has passed full testing in a FIPs validated environment, meaning that the software is fully functional in a FedRAMP compliant environment.

We also maintain a CyberEssentials certification. This is a UK standard but the audit covers all our infrastructure including USA locations and hosted servers.

Server Security

Our servers run a standard build Windows Server 2022 and are hardened to US DoD STIG standards. We use a multi-tenant architecture but with a single-tenant database, meaning that each customer has their own dedicated database instance, and no data can be shared between databases. Cross-over of data between customers is not possible since each instance has different credentials - they cannot cross-communicate even with admin access.

Physical security is managed by the datacenters who have been carefully selected as SOC-2 certified providers. The actual physical security includes CCTV coverage, restricted access, 24/7 monitoring, and secure access controls.

Our hardening process includes the following:

- Prebuilt servers are "hardened" to a vanilla Windows Server 2022 with no third-party software installed
- Every server runs an identical configuration
- Only port 443 is allowed in
- Only necessary ports are allowed out, so communication of your data to an external destination is generally not possible
- Lower grade TLS encryption/communication protocols are disabled, only the latest TLS protocol is enabled
- Server disks are encrypted
- Over 460 registry and group policy settings are hardened to STIG requirements
- Administrator accounts are disabled
- Only specific IP addresses can remote into servers, "access from anywhere" is not possible
- Third party software is not permitted. Our permitted software stack only permits software from xAssets, Microsoft and MariaDB

Security Technical Implementation Guides (STIGs) are a set of cybersecurity standards and guidelines developed by the U.S. Department of Defense (DoD). STIGs are recognized for their effectiveness in mitigating cybersecurity risks and are not exclusive to defense. Organizations, including those in sensitive industries, government agencies, healthcare, and private enterprises, adopt STIGs to improve security. By adhering to STIG standards, our servers are better protected against vulnerabilities, hacking and other cyber threats.

Servers are protected by hardware firewalls and windows firewall giving two layers of protection. DDOS protection is also provided at the data center level and the software also has DDOS mitigating services to block repetitive requests.

Servers are inspected, PEN-tested and patched weekly, and vulnerability scans are run during this process. Our auditing software is used to detect and report any changes to the server configuration.

Data Security Measures

Customer data is protected as follows

- Single sign on to all major SSO providers is supported
- Customers can download a compressed backup of their data daily
- Data is encrypted at rest and in transmission
- Single tenant architecture
- Customers have full visibility, control, and ownership of their data when stored in our cloud
- If any breach occurred, we must notify you as soon as we know
- Where possible data is held only in the jurisdiction chosen by the customer
- Servers are firewalled and hardened to US DoD STIG requirements

Our hosted implementations run the MariaDB database. On-premise customers generally run Microsoft SQL Server.

All our servers use disk mirroring and RAID technology to ensure that data is not lost in the event of a disk failure.

Backups are transmitted over secure SSL channels and are encrypted and are then removed from live servers.

xAssets supports several SSO providers including the following:

- Microsoft Azure
- OKTA
- OneLogin
- DUO
- Amazon Cognito

This enables customers to implement two factor authentication and other secure technologies to keep user accounts secure.

xAssets provides comprehensive audit information, recording every change to an asset record in a dedicated history table. This transparency ensures accountability and allows for thorough historical reporting and compliance tracking. Enterprise edition customers can also switch on user activity tracking to record every action a user takes in the system.

Product Security

The US Air Force granted certification in January 2018 for all xAssets Version 7 products to be used on the two main US air force networks - NIPRNET and SIPRNET. Our products are written to the highest standards and specifications and have passed stringent tests covering all aspects of software security in a web-based environment.

This means that the products are safe to use in web environments and best practices have been deployed. xAssets goes beyond these standards, so for example we provide a means for cloud customers to save discovery credentials directly on their network with no transmission over the web, and the product requires high encryption SSL to function, thus disallowing low security communication protocols.

Each release of xAssets products is security tested using the IBM AppScan, a leading security testing tool.

Data Centers and Failover

All our USA data centers are SOC 2 type 2 certified

Failover and resilience measures are in place to permit business continuity when outages occur. Servers are paired with a failover server in a different data center, and a third full backup is transmitted to a third data center in the UK (where customer rules allow this).

Datacenters are required to implement the following high availability measures:

- Redundant power supplies
- Redundant network connections
- Redundant cooling systems
- Redundant firewalls, routers, and switches
- Redundant internet connections

Server redundancy is not handled by the datacenters, instead xAssets manages server redundancy in paired datacenters. There is no dependency on a provider to restore a service

Storage redundancy is excluded from the above list since xAssets manages this through disk mirroring and separately through redundant servers in different datacenters.

User Security

User group permissions and context-specific user profiles allow users to access only the data and functionality they need. This is important not just because of the need to set the minimum access needed for security reasons, but also because users are seeing less functionality and less data, making the system much easier to use.

As mentioned, customers can choose to use xAssets native login or one of the SSO providers mentioned above.

User personal data, whether related to asset records within your instance, or related to user login accounts, is protected by the same security measures as all other data. All user data is encrypted at rest and in transmission, and never rests on third party infrastructure.

Development and Source Code Security

xAssets uses an "air gapped" development environment, meaning that the development environment is not connected to the internet.

Code quality is critical to ensuring that security vulnerabilities are not introduced. We use a combination of automated and manual code reviews to ensure that our 1.2 million lines of code are of the highest quality, written to consistent standards, and test harnesses ensure that previously tested code remains secure.

External libraries are only used under strict conditions:

- We trust pre-compiled libraries which are provided and signed by Microsoft
- Other libraries can only be used as follows:
- We fork each library, audit the source code, re-sign it, and produce our own compilations
- We always fork test harnesses with each library
- Only a limited number of library providers are used
- No libraries are permitted to transmit data

Code backups are encrypted and uploaded to GitHub; however, the code is in a private repository and since it is encrypted, it cannot be directly read by GitHub staff.

Like our hosted servers, our development environment is hardened to US DoD STIG standards, hard disks are encrypted at rest, administrator accounts are disabled, and no laptops are permitted.

Our Track Record

Outages can happen and should be expected. Our attention to detail in security and our experience in hosting has helped us maintain the following excellent track record for many years.

- No SLA outages since we started hosting in 2003
- No unplanned outages of any kind since January 2021
- No data breaches
- No data losses
- All DDOS attacks handled successfully
- No viruses
- No systems compromised in any way

Copyright © xAssets.com Limited 2023-2024.