wizehive

Cloud Security & Compliance

The Importance of Security Features in Cloud-Based SaaS Platforms, and WizeHive's Investment and Committment to Them

Table of Contents

The use of cloud-based services is growing rapidly, and with it the question and concerns from potential users about the security of data on these servers. In fact according to a survey of more than 350 IT executives by Unisys and IDG Research, more than 70% cited security concerns as their biggest hurdle in deploying cloud-based strategies at their organization, while nearly half of respondents (45%) expressed concerns about information governance.

This hesitation however doesn't appear to be slowing down the adoption rate; Gartner predicts the cloud services market to grow to $383 billion by 2019. One reason might be the benefits of cloud-based services, such as lower costs, greater storage capacities, faster development, and the ability to deploy on a global scale.

But another reason might be that initial worry: security and privacy. Cloud adoption and security reports by McAfee show that the percentage of organizations that trust public clouds to keep their data secure has jumped from 13% to 69% in just two years. The explanation is cyclical: as more companies have raised security concerns, cloud platforms and server providers have responded with enhanced features.

Companies are still right to question a platform's security capabilities, but will be increasingly pleased with the responses they receive.

At WizeHive, we are committed to pursuing strong controls in order to protect our customers and their constituents. We subscribe to privacy by design and by default; systems are designed and built with privacy and security in mind at every step.

However, all parties that have access to data play a role in keeping it safe. While

WizeHive can safeguard the data that you and your constituents store with us, we have no control outside our environment, or of actions taken by our customers within the environment. It's important for you to assess your own security policies and procedures, such as how users access your system and what data they are permitted to view or edit.

This paper is divided into several sections that address this shared responsibility. The first three sections outline the controls that WizeHive has in place in order to safeguard the security and privacy of data stored in our systems. The fourth section describes the controls that your administrative team can implement in our platform to safeguard your data. The last section describes some of the compliance frameworks that your organization may be required to comply with, and WizeHive's level of implementation or tools available that allow you to comply.

The controls outlined in this paper apply to the cloud-based Zengine suite of products: Zengine API, Zengine platform, Standard and Vault versions, and Zengine portals, identified by a URL beginning with https://webportalapp.com/. Used by organizations worldwide, from large banks and government organizations to small family foundations, Zengine is designed to to safely allow people to manage, track, and make decisions around data, regardless of their location.

WizeHive Has a Strong Security & Privacy Culture

Security and privacy both play an integral part of WizeHive's culture for all personnel. This is especially apparent during the hiring process, onboarding and offboarding, and as part of ongoing training.

Background Checks & Confidentiality Agreements

Before new team members join our staff, WizeHive conducts criminal background checks where local regulations permit.

All personnel are required to sign confidentiality agreements, which include clauses that require confidentiality of all customer data both during and after their relationship with WizeHive terminates.

Security and Privacy Training

All WizeHive personnel undergo security and privacy training as part of their orientation process and receive comprehensive training on at least an annual basis. Special topics in security and privacy are regularly presented at company-wide meetings to reinforce key concepts.

Depending on their job role, additional training on specific aspects of security may be required. For example, engineers and network administrators attend technical presentations on security-related topics specific to software development and networking.

Designated Security and Privacy Team

WizeHive has a designated Security Officer and Privacy Officer who lead all efforts on security and training compliance, with additional resources allocated as appropriate.

The team regularly attends conferences and trainings, as well as reviews OWASP and industry specific blogs, to keep up to date on best practices.

To keep up to date on potential security vulnerabilities, the team subscribes to security updates from the specific vendors, libraries, and tools that it relies on. More generally, the team monitors the general security landscape via third party sites such as Twitter, Hacker News, and CVEdetails.com.

Security Policies and Procedures

WizeHive maintains a robust set of security policies and procedures, modeled after the NIST 800-52 security framework, moderate level.

Privacy Policies and Procedures

WizeHive also maintains a public privacy policy, along with internal procedures to ensure compliance with this policy.

Two key provisions of this policy are:

- WizeHive stores, but does not own customer data.
- We do not apply different standards based on data type, which means that non-identifying pieces of customer data are treated with the same high level of security as government data, personal health information (PHI) protected by HIPAA laws, and special category data protected by GDPR.

Technology with Security at its Core

WizeHive's Zengine platform runs on technology platforms that are conceived, designed, and built to operate securely and reliably in the cloud.

Data Hosting

WizeHive uses Amazon Web Services (AWS) to store data for its Zengine platform; WizeHive does not maintain any of its own servers on-premise. Customer data is secured by AWS's industry-leading security measures, quick scaling, and high availability rates. Data is stored in the AWS US-East region and is replicated to a second data center for disaster protection. Data is stored in a multi-tenant environment protected by logical access controls.

Several other vendors are used to transmit or transform data as part of Zengine's services. We perform a risk assessment with each vendor and sign a data sharing agreement prior to transmitting any customer data.

Encryption

All data traffic is encrypted in transit, at rest, and in backups. All TCP traffic occurs over TLS 1.2 and is 256-bit encrypted when possible.

Operational Security

Security is an essential part of our daily operations.

Access Control

WizeHive implements role-based access using the principle of least privilege, granting only the information necessary for a person to do his or her job. Access is monitored and removed when no longer appropriate.

When possible and appropriate, we require multi-factor authentication (MFA) and IP whitelist controls.

We also have a policy that prohibits password sharing unless the system only provides single user access. In those rare instances, we use a password management tool that manages access via buckets. Personnel are required to use unique, strong passwords for every system they have access to.

Logging

WizeHive has a web log system in place for Zengine that logs important metadata around all web requests including API read, write, update, and delete operations. In

addition, many server-level details such as logins and system events are logged.

Logs are retained a minimum of 7 years, and protected by access controls. Logged audit events are reviewed in response to incidents.

Monitoring

Zengine is monitored for uptime and availability, with automated alerts to the production support team if a potential incident is detected.

The network is also monitored using Amazon GuardDuty for intrusion threat detection.

Risk Assessment

WizeHive conducts, documents and/or reviews its risk assessment every three years, or more often if significant change occurs. This assessment is conducted against all security and privacy policies described in this document. Risk assessment results are disseminated to management and to individual teams on an as needed basis.

Third-Party Penetration Testing

WizeHive subscribes to Cobalt.io, a third-party penetration testing service that uses a mix of automated and manual testing. Scans are performed twice a year, with results immediately reviewed and prioritized by the product team. Once a vulnerability is fixed, Cobalt.io re-tests to confirm resolution.

Configuration and Code Change Management

WizeHive has a documented policy that follows industry best practices for configuration and code changes. During development, code is continuously pushed to a staging branch for quality assurance review. Code is also reviewed for security vulnerabilities prior to release.

Releases are scheduled every two weeks, with immediate hotfixes for any major security issue or urgent bug.

Security Patches

WizeHive maintains a system maintenance policy that includes policies and procedures for both critical and noncritical system maintenance.

When we become aware of a potential security issue that may affect the confidentiality, integrity, or availability of systems or data, we immediately assess the risk and impact and schedule accordingly. High risk of impact items are addressed as soon as possible, generally within hours.

Incident Management

WizeHive has policies in place for handling security or privacy incidents that include procedures for identification, remediation, notification, and lessons learned.

Automated processes and tools are in place to automatically detect certain incident types and automatically notify the on-call team members to more quickly address incidents. Additionally, all company personnel are trained to report suspected security incidents to our incident response team as soon as they are detected via monitoring tools, internal notification, or self-discovery.

The incident response team schedules daily on-call resources that have access to the database and logging systems to assist with the handling and reporting of security incidents. Incident response training is required of all users identified as having a role in incident response prior to commencing that role, when required by any information system changes, and then on at least an annual basis.

To date, we have not had any security or privacy incidents that require notification, but procedures are in place to notify clients in accordance with their contractual service level agreement.

After any reported incident, the team performs a lessons learned retrospective and follow-up activities to incorporate those learnings into implemented changes.

Business Continuity and Disaster Recovery

WizeHive maintains a contingency plan for WizeHive Systems designed to respond to disaster, compromise, disruption, or failure in a manner that preserves core business functionality and minimizes adverse impacts to users.

The plan identifies essential missions and business functions and associated requirements. In its first step, a meeting of disaster recovery team members confirms recovery goals and priorities, defines roles and responsibilities, and reviews execution steps.

WizeHive conducts real-time and daily backups of user and system-level information stored in Zengine that are stored, encrypted, for 30 days. In the event of an incident requiring disaster recovery for all customers, WizeHive would use these backups to restore data. Recovery would use these backups and configurations defined in an automated deployment system so as to recover without deterioration of security safeguards normally implemented. The recovery systems are reviewed by Network Administrators and the Security Administrator prior to becoming operational.

Empowering Administrators to Improve Security and Compliance

As a Zengine administrator, you have complete control of your data and data access policies. Below are some key features that can help customize Zengine to meet your organization's security and compliance needs:

User Authentication and Authorization

Zengine has a variety of features for administrators to manage data access across the Zengine administrative platform and portals.

Platform Permissions & Workspace Member Management

Zengine workspace administrators can create custom roles to create a variety of permission levels. These roles can restrict a user's ability to view, add, modify, or delete data for each form in the workspace. Roles can even be created to restrict a user's permissions based on whether they created a record in a particular form, or a record member field matches the logged in user.

Administrators can easily invite members, review and edit role assignments, and remove access from any workspace member from one screen. This includes insight into which WizeHive implementation and support personnel have access to view, add, or modify data.

Workspace member accounts are secured by strong password requirements that require at least 8 characters and at least one uppercase, lowercase, and number.

Portal Permissions & Portal Member Management

Zengine application forms and submission portals are generally targeted at applicants, who only have access to data that they've entered into the system or that is linked and explicitly shared by the administrator with that particular applicant.

Zengine review portals use administrator-driven manual, batch, or automated assignments to explicitly share data with the reviewer logging into the portal. When a reviewer signs up, email confirmation is required to confirm their identity prior to providing access to the shared data. Administrators have additional tools to confirm reviewers.

Administrators can also link portals with their SAML 2.0 single sign on system to further manage portal permissions. By integrating in this manner, administrators can take advantage of their organization's security requirements regarding MFA and password policies, along with quicker provisioning of accounts.

Audit History

Zengine's audit history features enable an administrator to review changes to data records. This includes who created or modified a record, as well as what changes were made at a field level.

Administrators can also create custom reports or notifications based on workspace activity using the activities API, notifications API, or webhooks API.

Data Backup

Although WizeHive automates data backup for disaster recovery reasons, we also provide administrators with a variety of tools to backup their data or sync with other systems. This includes CSV exports and the ability to manually download files uploaded into the system. Saved views make it easy to pull up a report and export it to CSV. Custom scripting is also available via the Zengine API for automated backups or synchronization with other systems.

Privacy Compliance

Zengine has enabled tools to help organizations comply with privacy regulations, such as the EU General Data Protection Regulation (GDPR).

Data Retention and Deletion

Any data entered into a workspace is retained indefinitely until deleted by an authorized user. Upon deletion, the data will be immediately unavailable to all workspace users. When specifically deleting a form, all records contained within that

form will be deleted also. When deleting a workspace, all forms and their records are deleted. Data is permanently deleted from all downstream systems and backups within 60 days.

Consent

Portals have a consent feature that allows an administrator to provide notice of data collection and planned use, gain an affirmative opt-in, and log the consent prior to allowing a portal user to submit any data.

Regulatory Compliance & Certifications

Our customers have a variety of compliance needs across industries and countries.

E.U. General Data Protection Regulation (GDPR)

WizeHive is compliant with GDPR, which protects the personal data of EU citizens, for customer and prospect data, as outlined in our privacy policy.

WizeHive also supports customers' compliance with GDPR, as outlined above. Customers who require GDPR compliance must sign a data processing agreement with WizeHive.

Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

WizeHive is committed to enabling its customers to fully comply with all applicable Canadian privacy laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial privacy regulations.

U.S Health Insurance Portability and Accountability Act (HIPAA)

WizeHive supports customers' compliance with HIPAA, which governs the privacy of protected health information (PHI). Customers who are subject to HIPAA and wish to use Zengine must sign a business associate agreement with WizeHive and use the Vault version of Zengine.

Note that certain features are excluded from this version. If you require HIPAA compliance, please contact us to determine fit.

Children's Online Privacy Protection Act of 1998 (COPPA)

Protecting children's privacy is important to us, and we contractually require our customers to obtain parental consent that COPPA calls for in order to use our services to collect applications from minors protected by COPPA.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a U.S. government-wide program that standardizes security assessments for agencies adopting cloud services.

WizeHive works with a variety of government agencies and has successfully passed agency level reviews. We are investigating paths to FedRAMP ATO, and would welcome the opportunity to work with any agency willing to sponsor us.

Conclusion

Protecting user data is an integral part of WizeHive's business that goes beyond the controls built into our platform. From hiring and employee training, to vendor selection, to the design of our systems, privacy and security is part of every decision.

For these reasons and more, over 750 organizations trust WizeHive with their valuable information. WizeHive will continue to invest in security and privacy best practices to allow our customers and their constituents to benefit from our services.

Verion 1.1 | Last Updated: September 2018