Copilot for Mechanical Engineers

Bananaz Platform Suite Hybrid Solution

Enterprise cloud Hybrid Solution
Deployments in AWS

Overview

Bananaz Platform Suite can be deployed in the Amazon Web Services (AWS) cloud in an Hybrid configuration, to enable the customer to fully owner of his critical buisness data.
Deployments to a customer's own cloud hosting service are managed by the customer based on their infrastructure standards.

Customers who contract with Bananaz to manage their cloud deployment in AWS receive end-to-end support.
Bananaz provisions the cloud services, installs and configures the Bananaz Platform and related products, and maintains the solution.

The following are some of the features and benefits of deploying the Bananaz Platform to AWS:

- Fully managed deployment available across the globe to any AWS Region.
- Physical access to the AWS data centers and networks is strictly controlled, monitored, and audited.
- Multi-factor authentication - together with Identity and Access Management (IAM) and fine-grain permissions - are used to access the infrastructure.
- Your data is segregated with dedicated servers and logically isolated networks.
- Your data is secured in motion and at rest with industry standard encryption.
- Your data is protected with tight controls at the firewall and policy/procedure level to ensure there is no unauthorized access or compromise of your data.
- Your data is backed up and retained on a 90 day sliding window.

bananaz

- Systems are managed with integrated auto-recovery from hardware failures.
- 99.95% service availability.
- Infrastructure and user activity logging and monitoring.

The following sections provide an overview of the security policies and procedures applied to the Bananaz Platform. Please also refer to the AWS Cloud Security site for information on the security provided by AWS.

Facility security

Deployments of the Bananaz Platform utilize AWS for all customer systems; there are no systems located onsite in Bananaz offices.

Access to the Bananaz facilities are controlled through electronic key card access. Bananaz guests are greeted in the lobby and must sign in to enter the facility. Guests require escort by a Bananaz employee while in the facility.

System security

the Bananaz Platform customer systems are deployed and managed on AWS in line with the security policies outlined in the AWS Cloud Security site. The Technical Operations Team is responsible for all systems management. Access to systems – corporate and customer – is controlled and limited to specific identified employees. The Technical Operations Team at Bananaz utilizes multi-factor authentication to secure access to systems.

Network security

Customer systems are configured and managed in a dedicated Virtual Private Cloud (VPC). The VPC provides fine grained control and monitoring of all network interactions between the outside world and your managed instance, as well as internally between infrastructure components. Security policies are implemented for each customer, defining all the rules for how data flows and who has access to the systems.

Data security

the Bananaz Platform employs the industry standard AES-256 encryption algorithm to encrypt your data at rest. All data residing in the database or on file systems are encrypted. the Bananaz Platform encrypts data in transit, ensuring that all communication with the managed instance is secure using industry standard 256-bit encryption with a 2048 bit public key (TLS 1.2^). Direct access to data stored in customer databases is restricted.

Application access

The Bananaz Platform supports modern authentication mechanisms to ensure secure and streamlined user access. Single Sign-On (SSO) is supported through industry-standard protocols including SAML 2.0, OAuth, and OpenID Connect. Integration with enterprise identity providers is available, including Microsoft Active Directory, Okta, Google Workspace, Azure AD, Auth0, and Ping Identity. This enables centralized access management and enforcement of corporate policies.

bananaz

The Bananaz Platform customers are provided with the option of limiting access to their application instance by IP restriction or allowing access from the Internet.

Secure coding practices

the Bananaz Platform utilizes secure coding practices based on best practices prescribed by the Open Web Application Security Project (OWASP). All the Bananaz Platform, Software Engineers are required to complete yearly training and testing on secure coding practices. the Bananaz Platform leverages tools to assess the security of the code and employs a secure coding audit as part of code reviews.

Logging

the Bananaz Platform utilizes a log management system which logs IT infrastructure activity as well as user activity, including successful and failed user authentication attempts. The log management system is used to review the logged activity and alert the Technical Operations team on the detection of suspicious activity. Log data is retained for up to one year.

Monitoring

the Bananaz Platform actively monitors all systems, networks, applications, and supporting infrastructure using multiple commercial tools. Systems and infrastructure are monitored using Amazon CloudWatch. Alerts from monitoring are routed to VictorOps for management by support teams.

Bananaz has contracted with an independent third party for penetration testing and vulnerability assessment services.

Change management

Bananaz employs a Change Management Policy to record all changes to systems and infrastructure. Changes are reviewed to mitigate risk and recorded for accounting purposes. Bananaz utilizes CloudTrail to track all changes to systems and infrastructure. CloudTrail captures all maintenance and management activity supporting continuous audit of changes.

Disaster recovery

the Bananaz Platform has a standardized deployment architecture and associated procedures. This standardization allows the Technical Operations Team to easily stand up new environments as needed. Bananaz manages services for customers across all AWS regions and availability zones (refer to Regions and Availability Zones). The Bananaz Platform has the ability to be deployed into any region or availability zone as needed. Bananaz maintains backups of all customer services separate from the deployed environment (refer to “Backup and Recovery” section of this document). In the event of a disaster scenario, Bananaz will evaluate the risk and impact of the event and contact affected customers. An Incident Manger for Platform for Science software will develop a plan to restore services, focusing on risk and impact to the customer.

bananaz

The customer will be apprised of the reason for the restoration, the risk and impact, and the plan. The customer will be included in the restoration process to ensure that expectations are met. Technical Operations will execute the plan to restore services.

Backup and recovery

the Bananaz Platform leverages Amazon's comprehensive infrastructure to execute a backup and restoration process in order to maintain system availability for all hosted systems.

- Systems and data are backed up on a standard schedule and stored separate from the systems.
- Restoration due to data or system corruption or loss is deemed an incident and is managed under the Incident Management Policy.
- Restoration due to data or system corruption or loss is deemed an incident and is managed under the Incident Management Policy.
- Technical Operations will restore systems and data to address unrecoverable system failure, data corruption, or data loss.
- Customer stakeholders are notified prior to a planned execution of a system or data restore. The customer will be apprised of the reason for the restoration, the risk and impact, and the plan.
- Technical Operations will verify restored systems and data. The customer is required to verify that the restoration meets their expectations.
- All restoration procedures will be executed under established change management procedures.

Find out more at:
trust.bananaz.ai

bananaz