CloudBerry Security Whitepaper

Introduction

CloudBerry Lab (CloudBerry) recognizes the importance of privacy, security and data protection to our customers and is committed to safeguarding your privacy online.

This document describes the security policies and procedures in effect at CloudBerry. It provides an overview of the security controls implemented by the company and is proprietary information, intended to be shared with current or potential clients directly.

The intent of this document is to provide a brief overview of the security measures implemented to help protect the information and systems used by the company to conduct normal business. It does not represent all efforts made by the company to mitigate potential security risks related to Information Technology. The statements in this document do not constitute a guarantee against any security breaches.

Privacy Policy and Procedures

The CloudBerry Privacy Policy describes how CloudBerry collects and process personal information of our customers. It also describes how users can control that collection and use. This policy is available at https://www.cloudberrylab.com/company/privacy-policy.aspx

CloudBerry does not process customers' backup data through the hosted service. We only log backup/restore/auditing activity, along with managing the metadata provided, to manage the service on behalf of our clients. Backups are stored in a customer's controlled storage (local or cloud) and are owned by the customer. We do not offer private cloud storage under our control, nor does CloudBerry hold customer backup data for any reason.

Learn more about the legal information here.

Scalability & Reliability of Architecture

CloudBerry hosts its services with outsourced cloud infrastructure provider - Amazon Web Services (AWS), and as such, has the benefit of the included AWS security protections detailed in this following AWS Cloud Security information from Amazon: https://aws.amazon.com/security/.

Benefits include:

- Automatic Scaling while maintaining a secure environment
- Penetration testing
- Updated security bulletin posting
- Amazon Web Services Cloud Compliance to maintain security and data protection
- Certified with SOC 2 Type II and ISO 27001.

AWS CloudWatch monitors and notifies on a set of performance and operational stats.
The database is replicated synchronously so that we can quickly recover from a database failure. As an extra precaution, we take regular snapshots of the database and securely move them to a separate data center so that we can restore them elsewhere as needed, even in the event of a regional Amazon failure.

Service Level Availability

We use AWS CloudWatch to monitor and report on any service outages in AWS. In case of required server maintenance, which would take the service offline temporarily, CloudBerry notifies customers in advance about any planned downtime, and that activity is limited to off-hours to minimize any customer impact.

Authentication & Authorization

CloudBerry implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Customer personal data is stored in multi-tenant storage systems accessible to customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of CloudBerry's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Encryption & Key Management

CloudBerry stores hashes of the passwords (on server side) and encrypted passwords (on client side) following policies that follow industry standard practices for security. CloudBerry has implemented technologies to ensure that stored data is encrypted at rest. The SHA-256 secure cryptographic hash is used.

Our products and services use end-to-end encryption when communicating between customer assets and the cloud. This includes using secure HTTPS using TLS 1.2 for encryption over the internet or within a cloud data centre. All of our backup products support using the Advanced Encryption Standard (AES-256) encryption - that is FIPS 140-2 compliant - for any stored data with user supplied keys.

CloudBerry also supports cloud storage encryption options like Amazon AWS S3 Server-Side Encryption. Cloud encryption wraps all data in a secondary layer of AES encryption to protect the data at rest.
Our application security design provides granular control over access to limit who can see what data. This helps control and prevent unwanted or unnecessary access to customer's data from within the customer's environment.

Certification & Compliance

- HIPAA

In order to comply with HIPAA requirements, our methodology is described here:
https://www.cloudberrylab.com/blog/hipaa-compliant-backup-solution-cloudberry-backup/

- GDPR

CloudBerry is compliant with new regulation requirements. It acts as a data processor for customers personal data; processing necessary personal data in accordance with privacy rights and regulations following the GDPR. Our GDPR policy can be seen here:
https://www.cloudberrylab.com/company/gdpr.aspx

Change Control & Configuration Management

CloudBerry monitors and documents the installation, configuration, and use of products and services in the interests of quality control. We monitor third-party sites, security sites, and perform our own security tests on any incorporated source code. All software development is in-house, and all code changes occur via our version control software. A Changelog is available to customers, consisting of brief information about all the releases, and links to the detailed information for each release, with a list of known issues. CloudBerry has a

procedure to remedy reported bugs and security vulnerabilities, and to remove all debugging and test code elements from released software versions.

CloudBerry leverages the built-in .NET automated source code analysis tools to detect security defects in code prior to production.
CloudBerry validates API parameters and formatted output for each function to prevent manual or systematic processing errors or corruption of data.

Network Security & Access Control

Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

CloudBerry utilizes several different access control measures to ensure only authorized persons have access to the system, including software-driven restrictions, password and account policies, centralized authentication, restricted access to corporate resources, physical security of company locations, and strict procedures for user account provisioning.

A subset of CloudBerry's employees have access to the products and to customer personal data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Endpoint Protection

Part of protecting the infrastructure involves protecting each of the machines connected to that infrastructure. In order to deal with threats aimed at individual endpoints, we have embraced several industry standard practices and technologies including filtered and restricted web access, use of anti-virus and anti-malware tools, patch management, and limited end-user privileges.

Patch Management

CloudBerry strives to apply the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they become available.

For the AWS Cloud hosted services system admins perform patch management to the needed systems when needed. For employees, patches are applied automatically via Microsoft's SCCM (System Center Configuration Manager). In order to scan for vulnerabilities, we use Windows Server Defender / Endpoint Protection on all Windows Servers in AWS.

Business Continuity and Disaster Recovery

We have a BCDR plan in place; we test it with every version of our software. We use Amazon CloudWatch for monitoring and alerting: https://aws.amazon.com/cloudwatch/

We run a regular backup of sources and test recovery procedures on a regular schedule as servers / software change.

We continually monitor system performance and make changes to our EC2 instances in anticipation of growth or resource need. It is important to note the CloudBerry servers perform authentication and

monitoring / reporting and job management. All intensive operations, like backup and restore, including scheduling, are at the client level. All customers can define as many cloud storage providers and accounts and regions as needed.

Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) are available to authorized personnel to ensure correct configuration, installation and operation of the information systems.

CloudBerry has implemented backup and redundancy mechanisms, according to Amazon recommendations, with improvements planned. These are tested regularly.

Incident Management

We publish a Security Incident Response Plan (available upon request).

Governance and Risk Management

CloudBerry provides security control health data in order to allow customers to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status). All employees are trained on security procedures and educated on what resources they have access to and which ones they have no access. All IT operations are logged. Employees do not have access to customer-related data. Employees are trained on procedures. Logs are maintained for review. Security access is limited to those who need it.

Human Resources

All CloudBerry employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

We provide our employees with IT policies and guidelines that outline individual responsibilities with respect to acceptable use of IT systems and safeguarding corporate resources. These policies global survey are readily available to employees on the corporate Intranet and changes to these policies are emailed to employees.

Acceptable Use

Employees connecting to the CloudBerry network are required to conduct themselves in a manner consistent with corporate policies regarding, among other matters, confidentiality, business ethics and professional standards. All CloudBerry employees must participate in CloudBerry's annual Compliance training which emphasizes individual responsibility for the security of CloudBerry's information to which employees have access and reminds employees to take due care to identify and protect any sensitive data. As part of annual certifications, CloudBerry employees are required to accept and acknowledge adherence to the CloudBerry Code of Ethics, including information handling policies.

CloudBerry regularly trains its employees on information security awareness and tests them regularly. CloudBerry grants its employees access to systems based upon an established need, least privilege necessary basis. Accounts with privileged access are tightly controlled and logged, with user rights being under periodic review and passwords controlled for complexity, length and regular replacement. CloudBerry immediately rescinds any terminated employee's access rights.

Summary

The salient take-away concept behind our offerings is this: You own and control your data; we provide tools and mechanisms, which enable you to manage your backups securely and efficiently. You choose where and how to host your backups, and you control the encryption keys.

If you need additional information, please contact us at legal@cloudberrylab.com.