Deep Freeze Cloud

Architecture and Security Overview

Faronics

UNITED STATES
5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA
Call Toll Free: 1-800-943-6422
Fax Toll Free: 1-800-943-6488
Email: sales@faronics.com

CANADA & INTERNATIONAL
1400 - 609 Granville Street
P.O. Box 10362, Pacific Centre
Vancouver, BC, V7Y 1G5
Phone: +1-604-637-3333
Fax: +1-604-637-8188
Email: sales@faronics.com

SINGAPORE
20 Cecil Street, #104-01,
Equity Way, Singapore,
049705
Phone: +65 6520 3619
Fax: +65 6722 8634
Email: sales@faronics.com.sg

EUROPE
8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, England
Phone: +44 (0) 1344 206 414
Email: eurosales@faronics.com

www.faronics.com

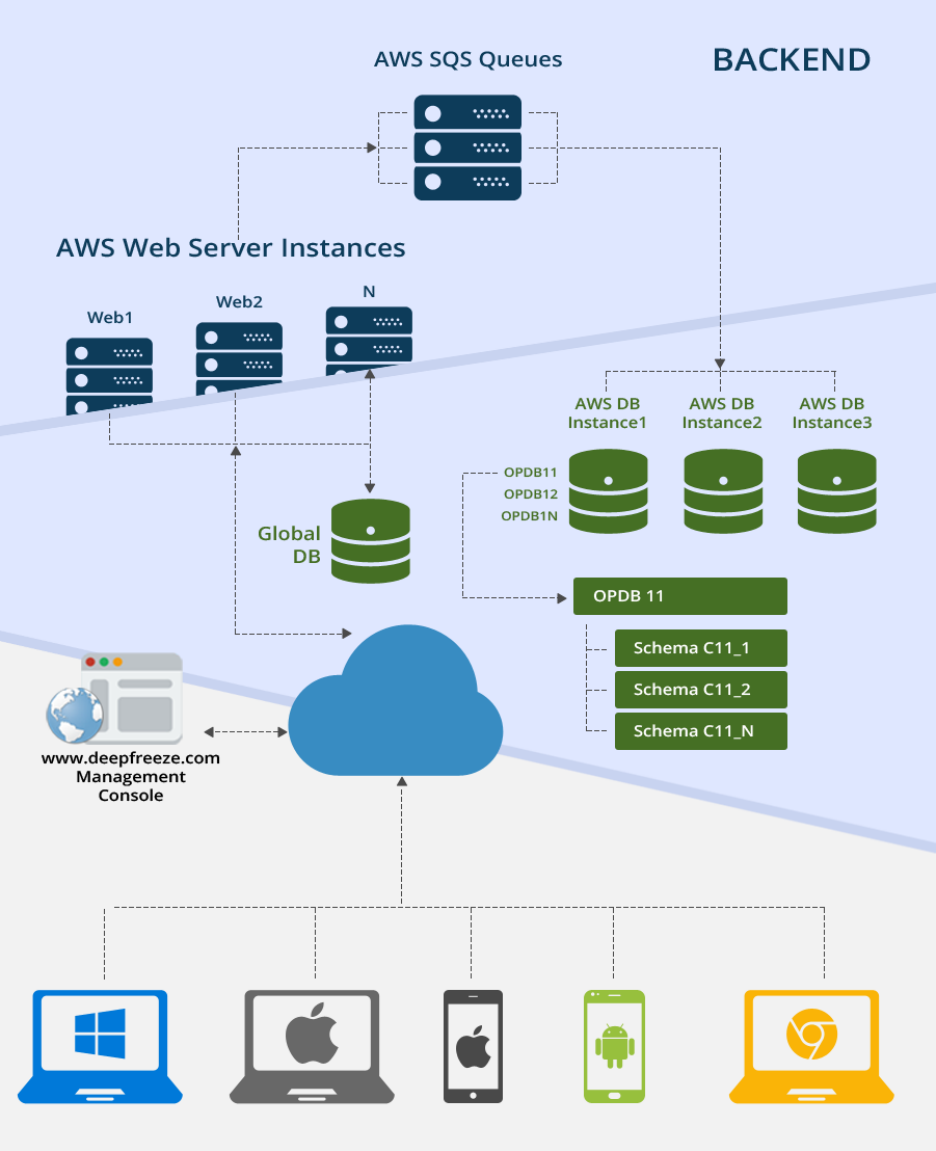
Introduction

This document provides a high-level overview of the Deep Freeze Cloud architecture. It describes how the security and privacy of customer data are protected by all parties involved under the shared responsibility model. This document also outlines the security policies, processes, and practices the Faronics team follows to fulfill its own responsibilities for the security of Deep Freeze Cloud Service.

Architecture overview

Deep Freeze Cloud is a unified service platform that enables customers to access Faronics Deep Freeze software via the Internet. It includes a broad set of services, such as PC and Mac management, mobile device management, antivirus, application whitelisting, data protection, asset administration, power management, and more.

Deep Freeze Cloud Service is composed of two major parts: *Client-side components and Backend components.*



Client-side components

Each managed computer (client) contains a *Cloud Agent* and various *Services* as specified in the client's policy settings. For some specific services, the customer can optionally set up a *Cache Server* computer within their local network to save bandwidth. System administrators access *Deep Freeze Cloud Console* via their internet browser.

Backend components

Deep Freeze Cloud backend components are hosted on Amazon Web Services (AWS). The production environment is hosted at two AWS regions: US West (Oregon) and EU (Ireland). The backup replica environment is hosted at two AWS regions: US East (N. Virginia) and EU (Frankfurt) for disaster recovery. A farm of *Web Servers* receives and responds to all queries from managed clients and Cloud Consoles, passing queries to the *Database Server* via AWS Simple Queue Service (SQS) for processing. A global database hosted on AWS Multi-AZ RDS instances stores globally required system data. A separate database contains the isolated database schemas created for each customer.

Deep Freeze Cloud Service security and privacy protection

Information security and customer privacy is paramount to Deep Freeze Cloud Service customers. By following industry security best practices, Faronics aims to protect customer data and privacy from accidental or deliberate theft, leakage, integrity compromise, and hacking.

Shared responsibility model

As a cloud solution, responsibility for data security is shared by AWS (the cloud service provider of Faronics Deep Freeze Cloud Service), Faronics (cloud service provider to its customers), and Deep Freeze Cloud Service customers.

AWS infrastructure and services meet several industry-specific standards, including:

- HIPAA
- Cloud Security Alliance (CSA)
- Motion Picture Association of America (MPAA)

AWS provides detailed information regarding their IT control environment through white papers, reports, certifications, accreditations, and other third-party attestations. For more information, see the Risk and Compliance whitepaper available on their website: http://aws.amazon.com/security.

Faronics is responsible for the security of the backend OS, network, firewall configurations, platform & application management, and customer data. Our security policies and practices are described in Customer data & privacy protection and Security policies and practices, below.

Deep Freeze Cloud Service customers are responsible for their own data security by managing access and permissions for their Deep Freeze Cloud Service accounts, and by keeping credentials safe and using strong passwords.

Customer data & privacy protection

Customer data collected

Faronics only collects personal information for the following reasons:

- To develop, manage and deliver our products and the Services to our customers
- To contact customers with product and service updates, upgrades and enhancements
- To contact our customers, either directly or through one of our resellers, to offer them the option to renew the services
- To contact our customers directly about products and services that may be of interest
- To ensure high standards of service to customers

- To verify a customer's identity
- To meet regulatory requirements

In the Deep Freeze Cloud Service system, the following customer data may be collected depending on the services that the customer uses:

- Customer identity and account information, including Organization Name, User Name, Password, Title, Phone Number, Email Address, and the like.
- Customer device information, including device name, IP Address, MAC address, date/time connected to Deep Freeze Cloud Service server, and the like.
- Customer device usage information, including date/time user log on/off, software installed on the device, software usage on the device, and the like.
- Deep Freeze Cloud Service configurations and selections.
- All data used to populate the Campus Affairs app, including customer staff info, course info, contact info, events info and notifications, and the like.

Customer data segmentation

Deep Freeze Cloud Service segments customer data (including device details but no personal information) into dedicated database schemas in which all tables belong to a specific customer. Each customer-specific database schema is hosted on a shared database instance in AWS. The architecture is sufficiently flexible that customers can request a dedicated database instance for their data. Note that additional costs may be chargeable to the customer to segregate the data.

Protection for customer data in transit

Deep Freeze Cloud Service servers use HTTPS (TLS 1.2) encryption.

Protection for customer data at rest

Faronics encrypts at-rest sensitive customer data, such as password, policies, and database connection strings, according to data type:

- Passwords hashes use SHA1 one-way encryption.
- Database connection strings are encrypted using a 256-bit Rijndael algorithm.
- Policies (partial) are encrypted using a non-standard, home grown cypher, or an RC4 stream encryption algorithm supported by the Microsoft Base Cryptographic Provider, depending on the specific service.

Protection for customer data in storage

Deep Freeze Cloud Service backup data is stored in AWS with encryption enabled. Sensitive data is always pre-encrypted.

Security policies and practices

Development & QA security policies and practices

Faronics development and QA processes are designed with the awareness of security risks and vulnerabilities. Relevant best practices include, but are not limited to, the following:

- Source code builds are scanned for malware and all security code is reviewed prior to deployment.
- The development team conducts application-level penetration tests on a regular basis as prescribed by industry best practices and guidance.
- The Operations team tests business continuity and disaster recovery plans for critical services per a defined testing schedule and for different loss scenarios.
- Security tests are conducted against all releases prior to deployment.
- Continuous security improvement within the Systems/Software Development Lifecycle (SDLC) using both Prevent Breach and Assume Breach security postures.

Faronics has established software development and release management processes to control implementation of major changes, including the following:

- Planned changes are identified and documented, including the creation of feature specifications and component designs
- Business goals, priorities, and scenarios are identified during product planning
- Operational readiness is reviewed according to pre-defined criteria, assessing overall risk and impact
- Testing, authorization, and change management based on entry and exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production) and PROD (production) environments as appropriate
- Faronics ensures database input and user input sanitization using the following best practices:
  - Inputs are constrained by basic validation and proper escaping
  - Use of .NET SqlCommand and SqlParameters
  - SQL Queries are never directly manipulated or concatenated

Operation security policies and practices

By following industry security best practices, Deep Freeze Cloud Service operations are designed to provide robust protection and privacy for customer data. Relevant policies include, but are not limited to, the following:

- AWS IAM (Identity and Access Management) service is used for user, group, and roles authentication management in the backend environment.
- AWS VPC (Virtual Private Cloud), Network ACL (Access Control List), and Security Group is used to protect the backend infrastructure (EC2 instances and RDS instance).
- Activities on the AWS platform are audited using AWS CloudTrail.
- Changes to the DFC production site are made in conformance to the guidelines in the "Deep Freeze Cloud Service Change Management" document.
- Components and processes are provided the minimum user privileges necessary to perform their duties.
- Faronics Internal authorized personnel with access to customer data in Deep Freeze Cloud Service are required to use MFA (Multi-Factors Authentication) login.
- System infrastructure is configured for redundancy and smooth fail-over handling.
- Data is regularly backed up, and backups are periodically validated for restoration for disaster recovery purposes. Backup standards, policies, procedures, and controls are verified and documented.
- Cloud services can be restored in a different availability zone within the same AWS region, or in different AWS region, in the event of a data center power failure, network failure, or other disaster situation. Restoration processes are defined and documented.
- Operations are subject to regular internal security audits based on traces, logs, and other information performed by a system administrators and other parties involved in routine operation.

References and further reading

– AWS Security Best Practices (by Amazon Web Service)

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

– Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights (by Cloud Security Alliance (CSA))

https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/

– OWASP Top 10 2017 - The Ten Most Critical Web Application Security Risks (by OWASP (The Open Web Application Security Project))

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf