FARONICS™ Cloud

Architecture and Security Overview

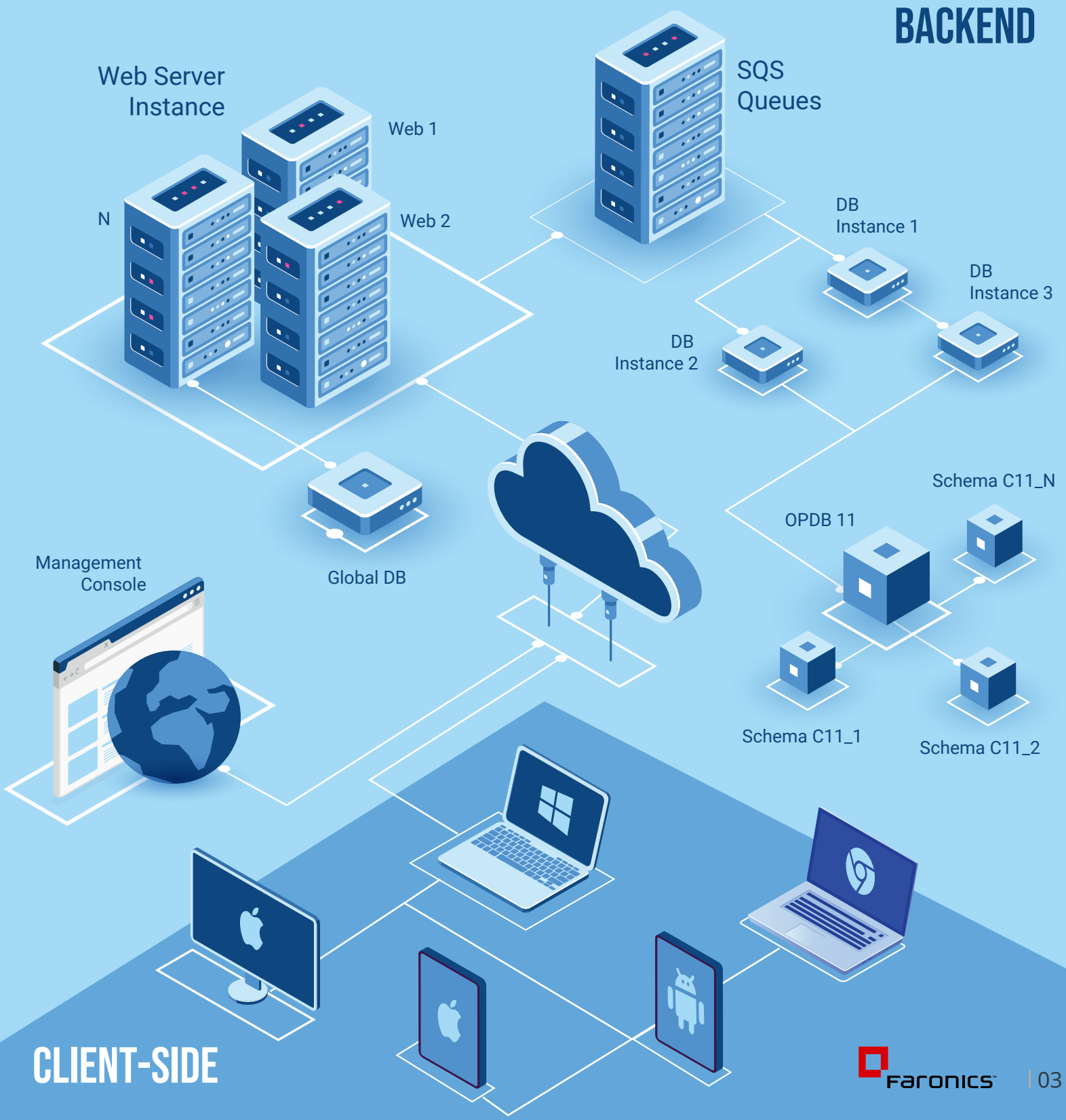
Introduction

Faronics Cloud refers to both **Faronics Cloud Deep Freeze** and **Faronics Cloud Deploy** (henceforth referred to as "Faronics Cloud"). Faronics Cloud is a unified platform that simplifies endpoint management over 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.

Faronics Cloud is hosted in two primary environments: **Amazon Web Services (AWS)** and our **Colocation facility**. These environments provide a robust, scalable, and secure infrastructure for managing endpoints, with hosting determined by customer and operational needs. This document outlines Faronics Cloud architecture, how customer data security and privacy are protected under the **Shared Responsibility Model**, and the security policies, processes, and practices Faronics follows to secure the platform.

Architecture Overview

Faronics Cloud 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. Customers may optionally set up a **Cache Server** within their local network to save bandwidth. System administrators access the management console via a web browser, enabling remote management of endpoints.

Backend Components

Faronics Cloud backend components are hosted either in **Amazon Web Services (AWS)** or in one of our **Colocation facilities**.

- **AWS-based infrastructure is hosted in** the **US West (Oregon)** and **EU (Ireland)** regions, with backup replication for disaster recovery in the **US East (N. Virginia)** and **EU (Frankfurt)**. Web Servers handle incoming queries from managed clients and Cloud Consoles, passing them to the Database Server through AWS Simple Queue Service (SQS). Global data is stored on **AWS Multi-AZ RDS instances** with isolated customer schemas.

- **Colocation-based infrastructure** is managed in a carrier-neutral data center located in **Vancouver**, **Canada**.

Web Servers

A farm of Web Servers receives and responds to all queries from managed clients and Cloud Consoles. These queries are then passed to the appropriate **Database Server** for processing, ensuring efficient request handling and system performance.

Database Servers

The **Faronics Cloud Database Server** manages and processes customer data. All data is stored in isolated schemas to ensure data separation and protection. This setup is replicated in both AWS and Colocation environments, maintaining uniform data management practices across all hosting options.

Shared Responsibility Model

Faronics follows the **Shared Responsibility Model** for security. Faronics is responsible for securing the cloud infrastructure, including the integrity of servers, data, and networks. This responsibility includes:

- **Physical security** of data centers.
- **Infrastructure security** across all layers.
- **Backup and disaster recovery processes** for business continuity.

Customers are responsible for securing their usage **in the cloud**, including managing access controls, securing their applications, and defining their endpoint policies.

Security and Privacy

Security is paramount at Faronics. We implement stringent security policies to protect customer data across both AWS and Colocation environments:

- **Data encryption**: All data in transit is encrypted using HTTPS/TLS, and data at rest is protected using **Advanced Encryption Standards (AES)**.
- **Network security**: Firewalls, intrusion detection, and prevention systems safeguard our network infrastructure.
- **Regular security audits**: Our environment undergoes regular audits to maintain compliance with industry standards and best practices.

Data Backup and Disaster Recovery

Faronics ensures comprehensive **data backup** and **disaster recovery** strategies across both AWS and Colocation environments:

- **AWS-hosted customers**: Backups are stored in alternate AWS regions **(US East and EU Frankfurt)** for fast recovery.
- **Colocation-hosted customers**: Similar backup strategies are employed to recover data efficiently and ensure continuity.

Customer Data & Privacy Protection

At Faronics, we are committed to responsible data usage and protection. When using Faronics Cloud, data is collected to improve services, stored securely, and erased when no longer needed.

Key Points:

- **Data collection**: Faronics Cloud collects hardware and software configurations, user activities, and system state data to ensure service functionality and enhancement.
- **Data retention**: Data is typically retained for **12 months to 2 years** after a customer stops using the services, allowing time to safely remove cloud clients. Customers may request earlier removal.
- **Data storage**: Data stored in the Faronics Cloud is encrypted both in transit and at rest.
- **Data privacy**: Faronics does not use customer data for targeted advertisements and only uses it to deliver and improve services.

For more information, please visit the relevant **Faronics Cloud Product Data & Privacy Policy**:

- **Faronics Cloud Deep Freeze**
- **Faronics Cloud Deploy**

Compliance

Both AWS and Colocation environments comply with global data protection standards, including **GDPR** for customers in the European Union. Faronics is dedicated to ensuring data residency and compliance needs are met, regardless of the hosting environment.

Network and Port Security Configuration

To ensure secure and smooth communication between managed clients and Faronics Cloud services, network ports and domain access must be correctly configured. Ensure **port 443** is open for outbound traffic and review the required ports and hostnames to avoid service disruption.

For detailed security requirements, please refer to the relevant Knowledge Base articles:

- → **Faronics Cloud Deep Freeze**
- → **Faronics Cloud Deploy**

Development & QA Security Policies and Practices

Faronics follows stringent **Development & QA Security Policies**:

- **Source code builds** are scanned for malware, and security code is reviewed before deployment.
- Regular **application-level penetration tests** are conducted following industry best practices.
- **Business continuity** and **disaster recovery plans** are tested for critical services.
- **Security tests** are performed on all releases before deployment.
- Continuous security improvements are integrated into the **Systems/Software Development Lifecycle (SDLC)**, using both Prevent Breach and Assume Breach postures.

Operations Security Policies and Practices

Faronics Cloud operations are designed to ensure robust protection and privacy for customer data through industry best practices:

- **Identity and Access Management (IAM)** controls access across both AWS and Colocation environments.
- **Network security** uses VPCs, ACLs, and Security Groups in AWS, with similar protections in Colocation environments.
- **Activity audits** are performed using AWS CloudTrail and similar tools in the Colocation environment.
- **Change Management guidelines** ensure secure updates to production systems.
- **Multi-Factor Authentication (MFA)** is required for personnel with access to customer data.
- **Redundancy and fail-over handling** are configured across both hosting environments.
- Regular **backups** are taken, and recovery procedures are periodically validated for disaster recovery purposes.

Conclusion

Faronics Cloud offers flexible and secure hosting options. Customers can be assured of high levels of security, availability, and performance, regardless of their hosting environment. Faronics Cloud's infrastructure is built to scale with customer needs while maintaining the security and reliability standards that have made Faronics a trusted provider for endpoint management.

To learn how your computing environments can benefit from Faronics Solutions, visit www.faronics.com

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

sales@faronics.com

CANADA & INTERNATIONAL

609 Granville Street, Suite 1400
P.O. Box 10362, Pacific Centre
Vancouver, BC, V7Y 1G5

Phone: +1-604-637-3333
Fax: +1-604-637-8188

sales@faronics.com

EUROPE

8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, United Kingdom

Phone: +44 (0) 1344 206 414

eurosales@faronics.com

SINGAPORE

6 Marina Boulevard
#36-22 The Sail At Marina Bay
Singapore, 018985

Phone: +65 6509 4993
Fax: +65 6722 8634

sales@faronics.com.sg