Sitrion ONE

Infrastructure & Security
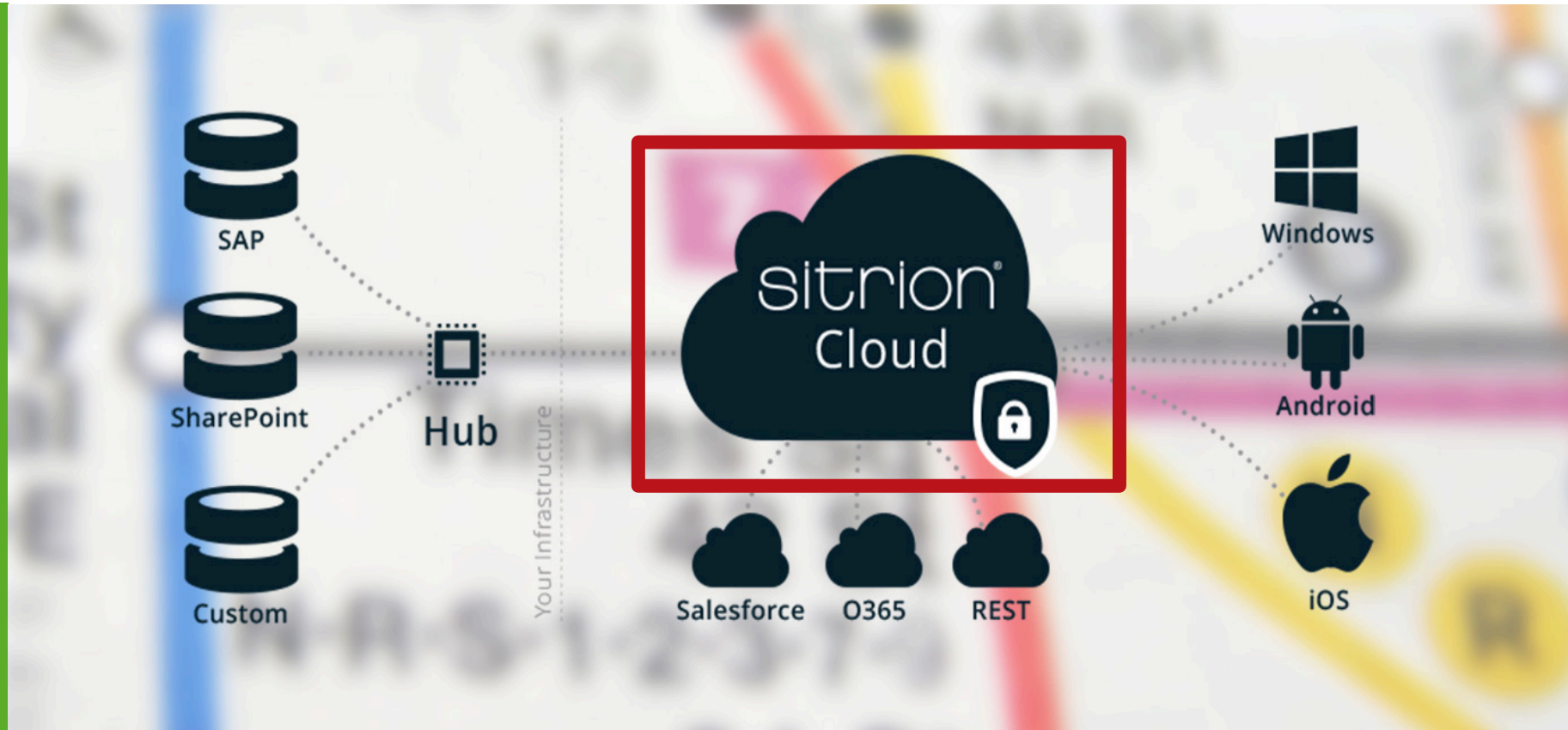
sitrion

Sitrion ONE Infrastructure (Overview)

Your Infrastructure

SAP
SharePoint
Custom
Hub

sitrion® Cloud

Salesforce   O365   REST

Windows
Android
iOS
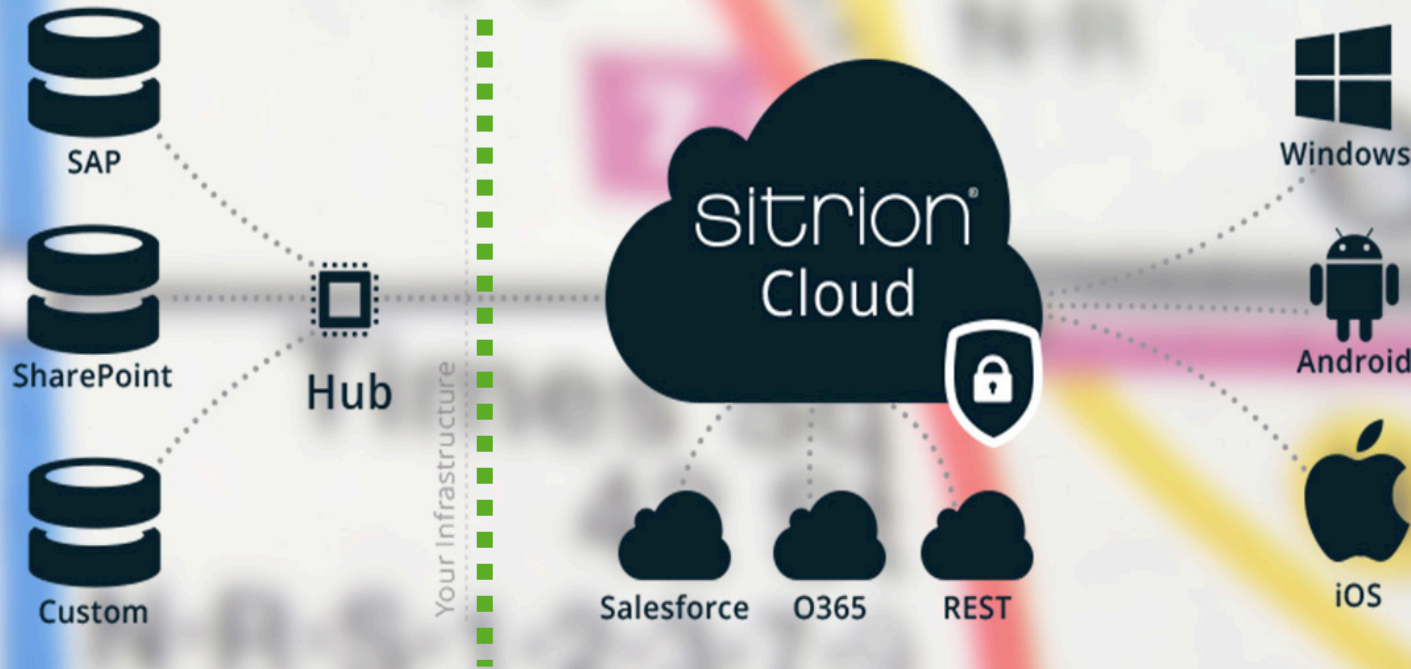
- Hosted on Microsoft Azure
- Isolated Tenants for every Customer
- No data storage on mobile devices and the cloud (except Push-Content-Cache)
- Encryption of all communication and messages
- Real-Time access, no Offline storage

sitrion

Sitrion ONE Infrastructure (Hosting)

- No replication of backend data, no data storage (except Push-Content-Cache)

- Cache-Content of Push-Data (Cards) leverages Rijndael (AES 128 Bit) Encryption. Dynamically generated keys per tenant-> Sitrion doesn't know the keys and has no access to the customer tenant
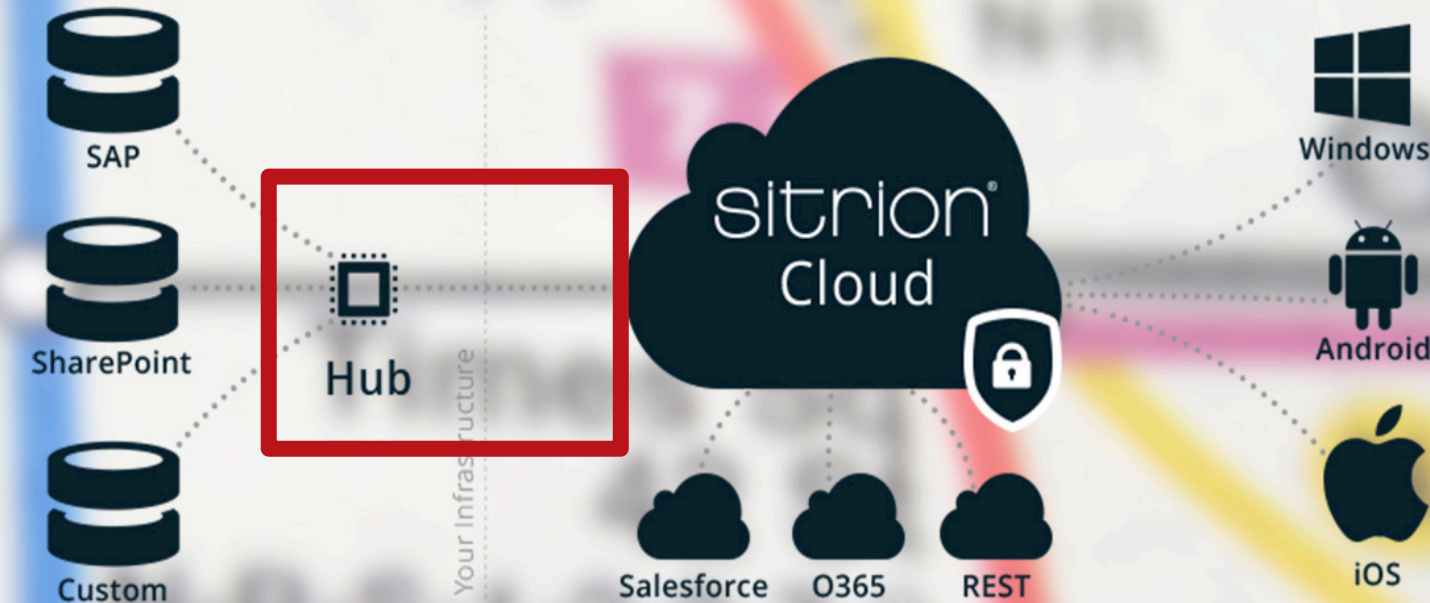

Microsoft Azure Certifications:
https://azure.microsoft.com/en-us/support/trust-center/compliance/

sitrion

Sitrion ONE Infrastructure (Hub)

SAP

SharePoint

Custom

Your Infrastructure

Hub

sitrion® Cloud

Salesforce   O365   REST

Windows

Android

iOS

- The hub contains the connectors to the backend systems (SharePoint, SAP etc.)
- Connectivity from the hub to the customer tenant via Azure Service Bus (Outbound only TCP to dedicated Azure IP ranges)
- Encrypted communication between Hub and Cloud via Secure Relay Access Token
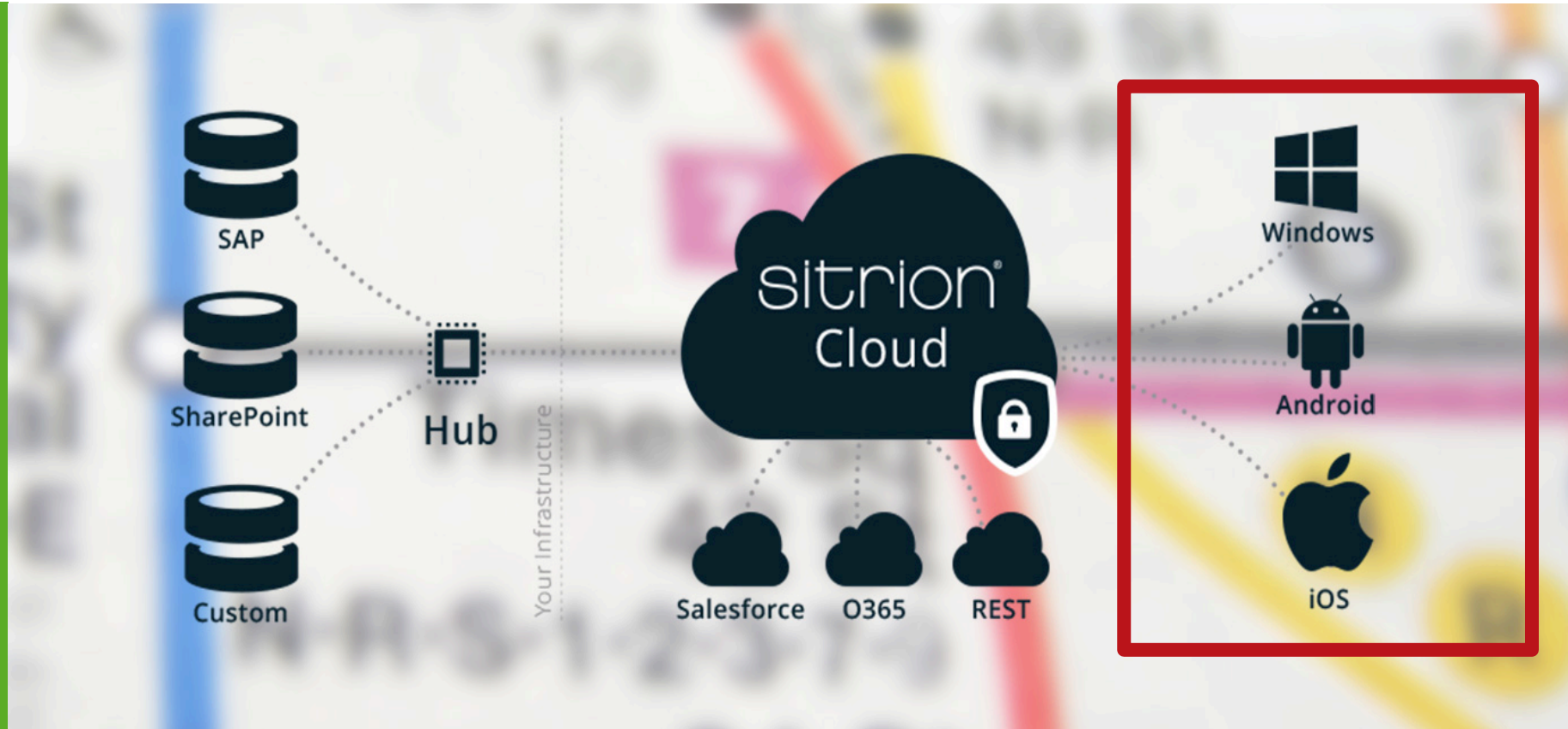
Microsoft Azure Service Bus:
https://azure.microsoft.com/en-us/services/service-bus/
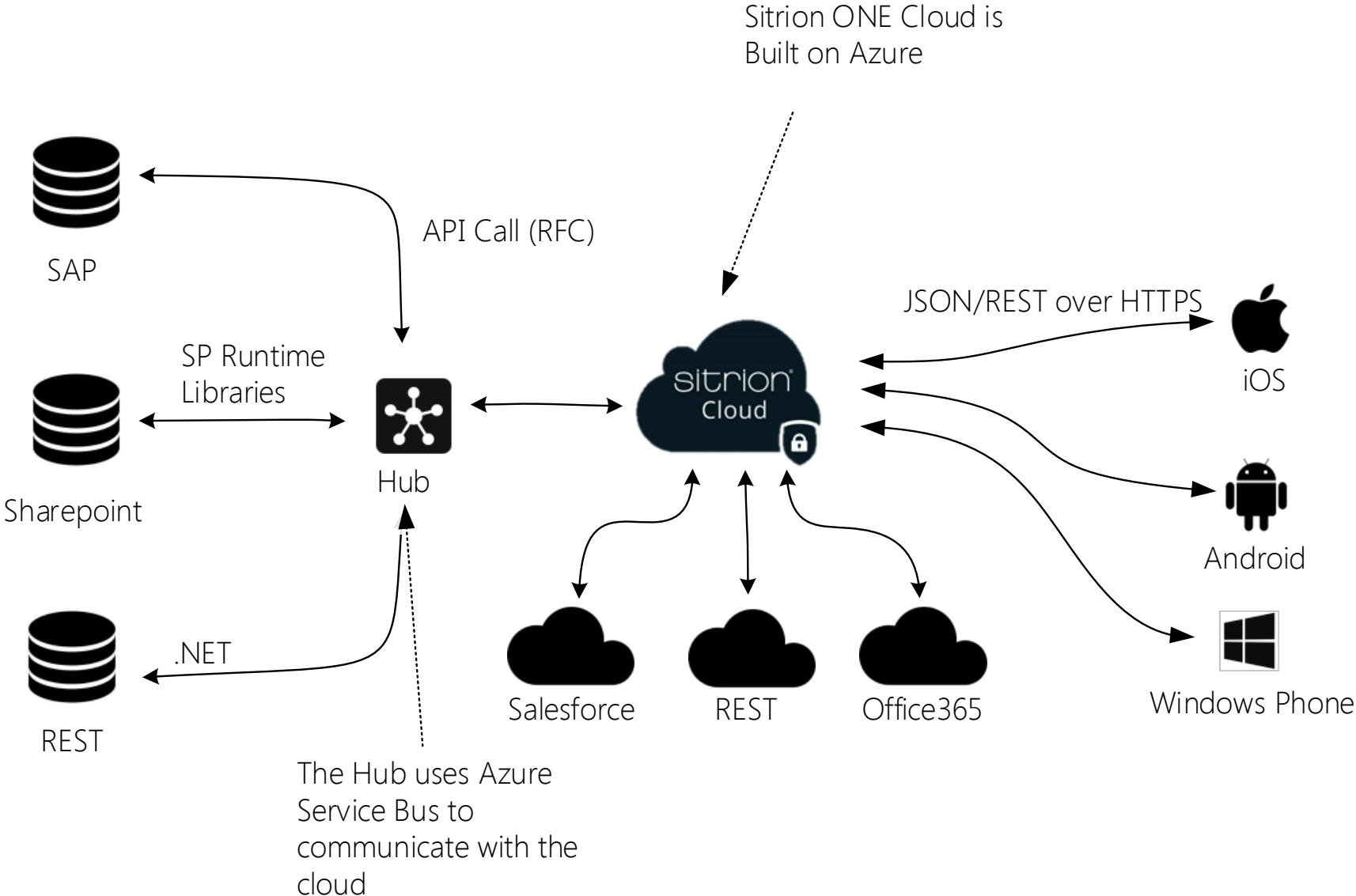
sitrion

Sitrion ONE Infrastructure (Device)

- No data storage on the mobile device
- No offline access
- Encrypted communication with the customer tenant via SSL (TLS 1.2, AES 256 CBC, SHA1 & ECDHE RSA)
- Authentication of users leveraging ADFS or Generic Sitrion ONE-Login

sitrion

Backend Integration

Integration Details

Sitrion ONE Cloud is
Built on Azure

API Call (RFC)

SAP

SP Runtime
Libraries

JSON/REST over HTTPS

iOS

Sharepoint

Hub

sitrion
Cloud

Android

.NET

REST

Salesforce   REST   Office365

Windows Phone

The Hub uses Azure
Service Bus to
communicate with the
cloud

sitrion

Authentication

Option 1: Sitrion ONE-Authentication

2 User Logs into the App

3 User provides any other credentials required for Third Party Systems

1 User is provisioned

SAP

SharePoint

Hub

REST

4 Authentication through credentials provided by the user

Salesforce

REST

Office365

iOS

Android

Windows Phone

sitrion
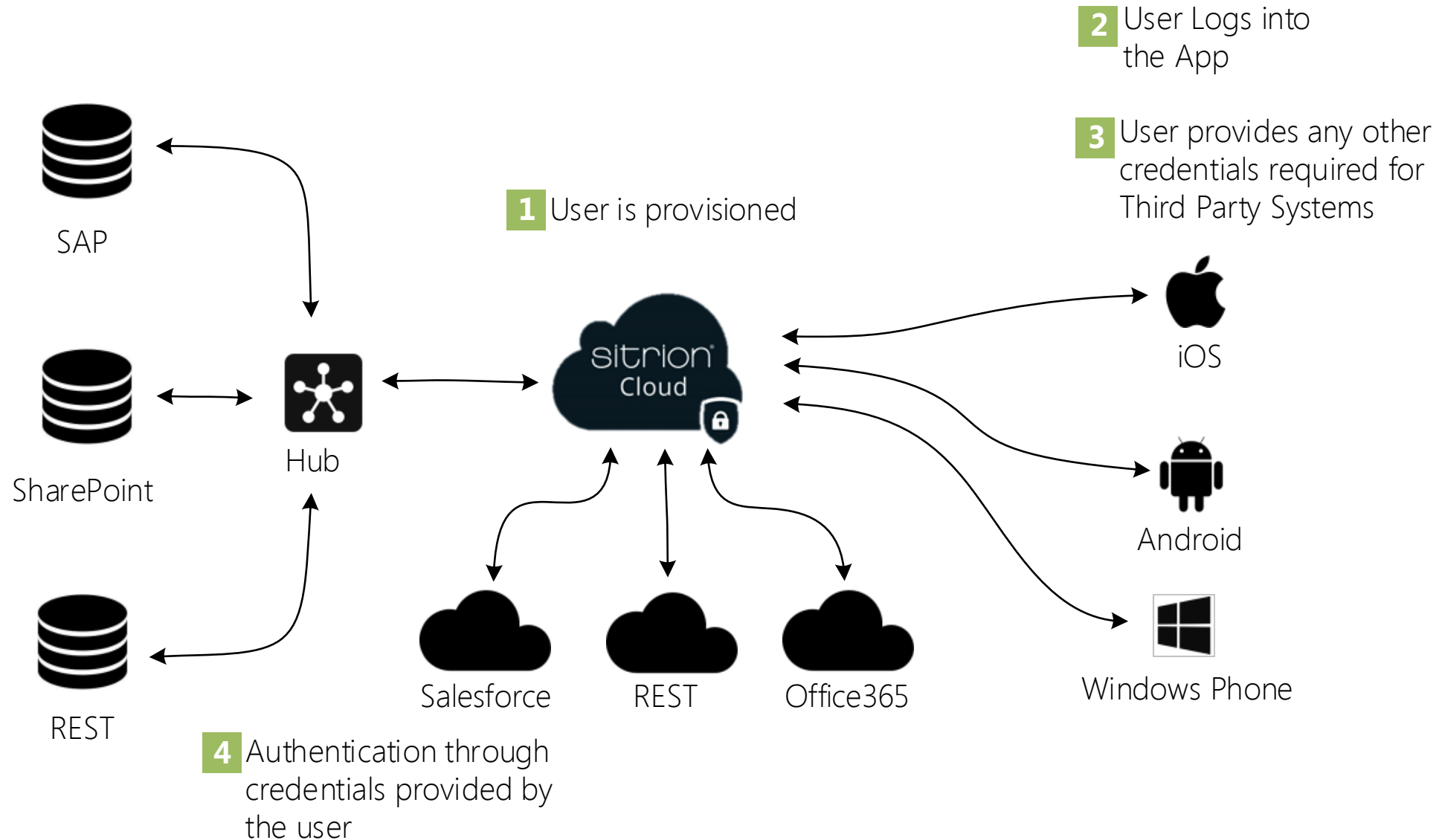
Option 2: Microsoft ADFS-Authentication

SAP

SharePoint

Hub

REST

1 Technical Team intergrates with ADFS (Trusted Relationship)

2 User logs into ADFS on the app

sitrion Cloud

Salesforce

REST

Office365

iOS

Android

Windows Phone

3 ADFS Tokens Used to Log Into Other Systems
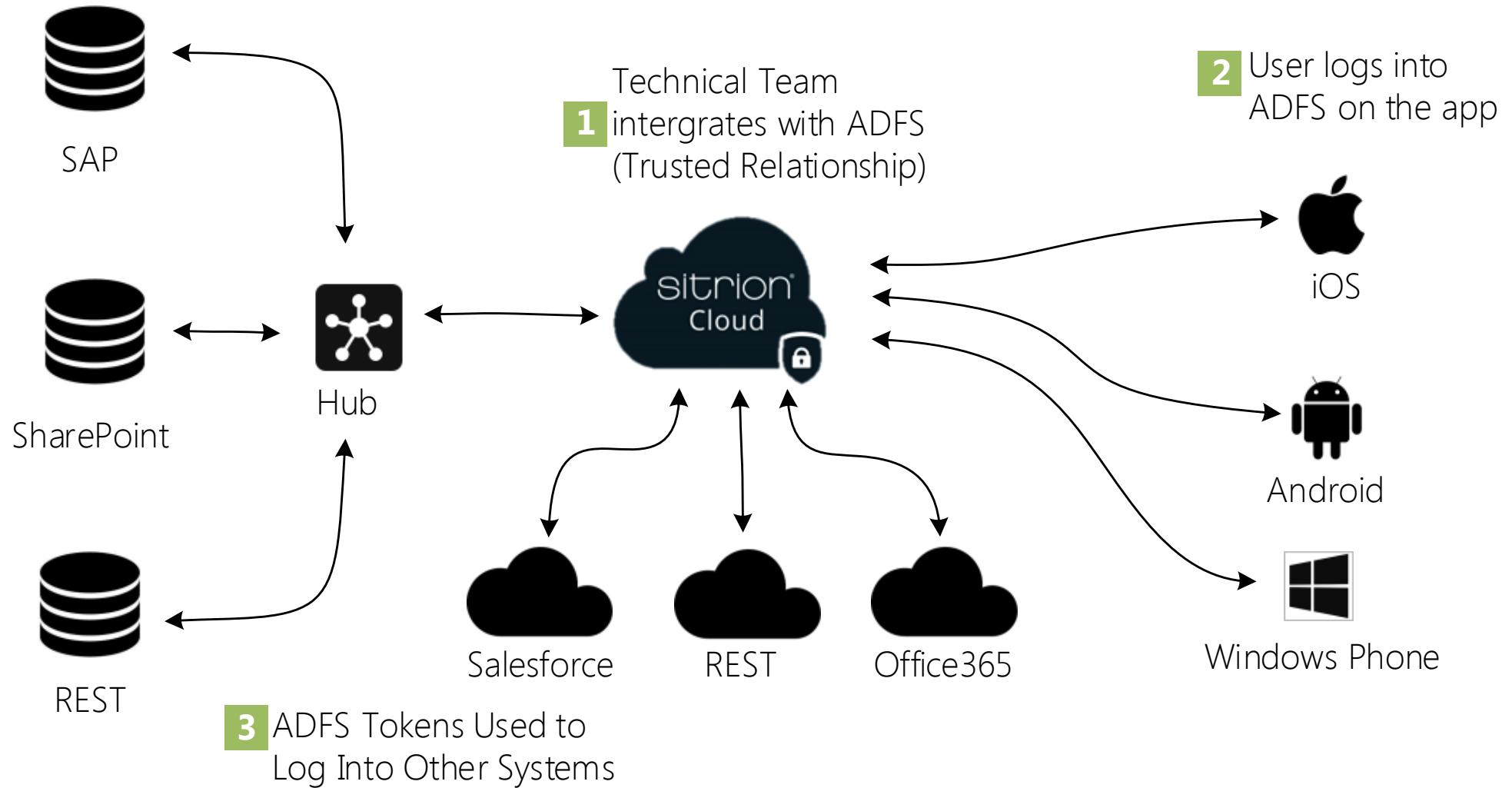
(depending on the backend configuration)

sitrion

Technical Resources

General Technical Overview
http://devcentral.sitrion.com

Security/Architecture
http://www.sitrion.com/one/developer/documentation/security-guide
http://www.sitrion.com/one/developer/documentation/integration-guide

Development
http://www.sitrion.com/one/developer/documentation/getting-started/build-your-first-app
http://www.sitrion.com/one/developer/documentation/development-guide

Application Owners
http://www.sitrion.com/one/developer/documentation/integration-guide

sitrion