

Loftware Cloud Details

March 2026 | Revision 19



Contents

CONTENTS	2
1 INTRODUCTION	3
2 SOFTWARE CLOUD ARCHITECTURE	5
2.1 Introduction	6
2.2 Multitenancy	7
2.3 Authentication	7
2.4 High Availability	8
2.5 Hybrid Cloud and Edge Computing with Loftware Cloud	9
2.6 Environments	12
2.7 Local Sites	12
2.8 Printing in the Cloud	14
3 SOFTWARE CLOUD INTERNALS	15
4 RELEASE CYCLE	17
4.1 Upgrades	17
5 SLA	18
6 SECURITY	19
6.1 SOC2 Type II Certification	19
6.2 Fundamentals	19
6.3 Role-based Access	20
6.4 Database Security	20
6.5 Data Encryption	21
6.6 API Security	21
6.7 Printer Connection Security	22
6.8 Client requirements for connecting to Loftware Cloud	22
7 DATA LOCATION	23
8 EXIT STRATEGY	23
9 GLOSSARY	25
10 REFERENCES	26

	Software Cloud Details				
			Revision	19	Number of pages

1 Introduction

Software Cloud is the world's first public cloud-based labeling software as a service. It includes everything you need to manage your labeling, from design, quality review and approval to printing and data management.

Software Cloud is scalable to many thousands of label templates, graphical images, users, and printers and can be extended to remote locations, suppliers, and contract manufacturers.

Software Cloud

- Eliminates hardware, software, and database infrastructure costs
- Removes the need to install, monitor and manage
- Speeds implementation, rollout, and scale
- Simplifies upgrades to new versions
- Offers seamless high availability with failover
- Aligns with corporate initiatives

Software Cloud's three core pillars include

- **Reliability.** Software labeling solutions need to be available 100% of the time. We ensure high availability using appropriate cloud architecture utilizing Microsoft Azure features and services like availability zones for web services and redundancy in databases and storage.
- **Scalability.** Software Cloud solutions are designed to operate on a web scale, exceeding the needs of our largest global users.
- **Security.** Software Cloud offers secure solutions with least privilege access, encryption of the data at rest and transit, as well as adhering to required laws on data storage and policy (e.g., GDPR).

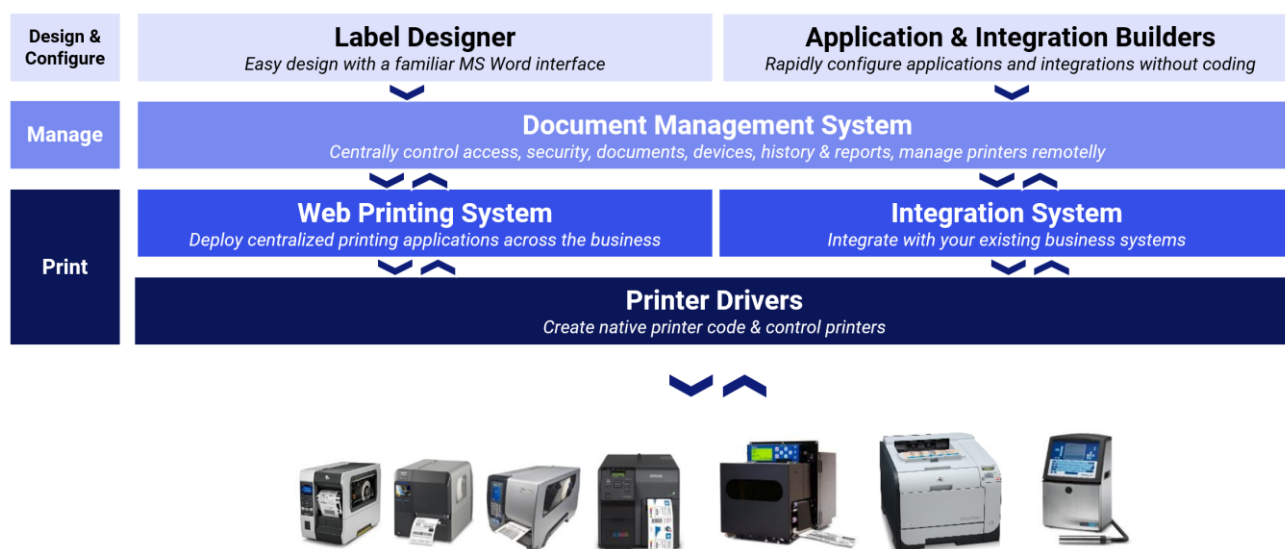


Figure 1 - Software Labelling Platform

	Software Cloud Details				
			Revision	19	Number of pages

Label Designer provides the following benefits:

- **Familiar Microsoft Word-like user experience.** Anyone can quickly design professional labels without barcoding, design, or advanced computer skills.
- **Next-generation label design software** enables business users to design and maintain customer specific and regulatory compliant label templates. Every Software template is optimized for over 5,000 printer models, reducing the number of label variations.
- **Improved speed and flexibility in making label changes.** Use the same template with any printer brand and model, even printers with different resolutions. There is no need to design different labels for different printers to get the same consistent output and fast printing performance.
- **Streamlined compliance with regulatory requirements.**
- **Faster global optimization and expansion into new markets.**

Document Management System (DMS) delivers the following management and control benefits:

- **Label lifecycle management** built to streamline the label creation and approval process.
- **Secure centralized storage** with version control, approval workflows, and audit trails of all revisions.
- **Full traceability** and transparency of all labeling transactions and print history.
- **Instant deployment** of label templates and printing applications. The time needed for a new user to print the first labels is measured in minutes. Changes to label designs and printing applications are made quickly and deployed globally in seconds.

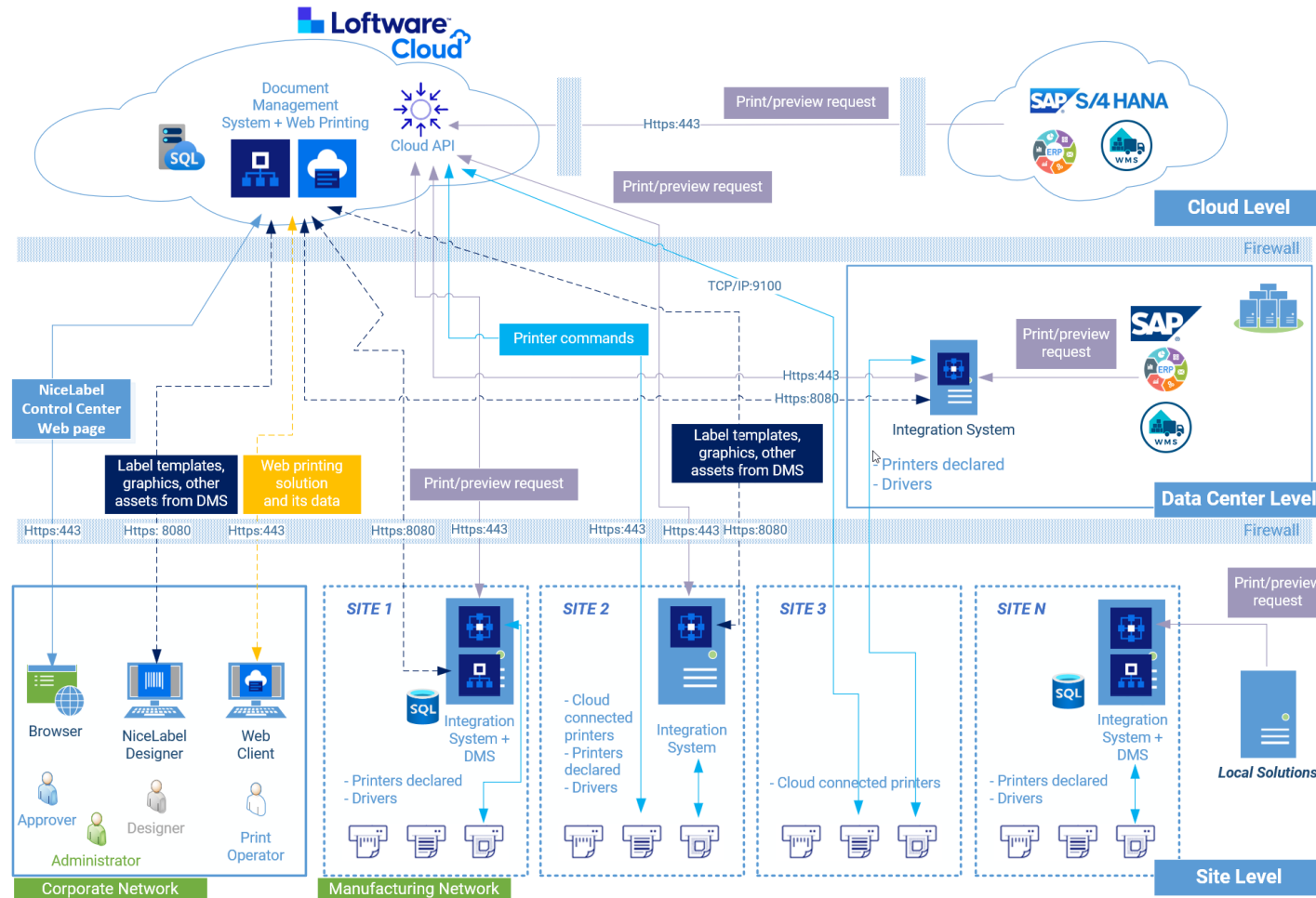
Software Cloud's **Integration System** delivers the following benefits:

- **Best in class performance and reliability.** Software solutions handle printing of billions of labels to thousands of printers securely, offering the best performance.
- **High availability and reliability.** Software's design, architecture and implementation ensures operational continuity without disruption of mission critical work.
- Designed to meet the integration needs of businesses of all sizes, our integration system provides **unrivalled connectivity** to any application or source data via web services, event-based integration, and certified pre-built integrations to SAP®, Oracle®, Microsoft® and many other leading MES, ERP and WMS applications.
- **Single Source of Truth** principles are adhered to ensure reliable labeling content using master data.
- **On-demand "instant" printing.** Rapid printing requires label and document on-demand printing.
- **Real-time status feedback.** Take on-demand printing to new levels of efficiency with real-time status notifications. You no longer need to check the spooler, printer, or job error state. Confirmed delivery reduces help desk calls.

Software Cloud also delivers the following accessibility benefits:

- **Easy web-based access** allows print users to connect from anywhere without requiring administrators to install local software. This streamlines deployment, saves costs, and eliminates the need for IT to manage individual workstations.
- **Web-based administration** of the entire Label Management System across any device or platform. This provides administrators with easy access, oversight, management, and control.

2 Software Cloud Architecture



	Software Cloud Details				
			Revision	19	Number of pages

The architectural diagram above shows a few possible architectures for centralized Label Management Solution utilizing Software Cloud.

2.1 Introduction

Software Cloud is the world's first public cloud-based labeling software as a service. It includes everything you need to manage your labeling, from design, quality review and approval to printing and data management. It was introduced back in 2011 and enables users to print tens of millions of labels per month.

Software Cloud consists of cloud hosted software (Control Center and Web Printing) and clients that connect to the cloud. Client modules are both fat (Software Designer, Software Print and Software Automation) and thin clients (Software Web Printing Client).

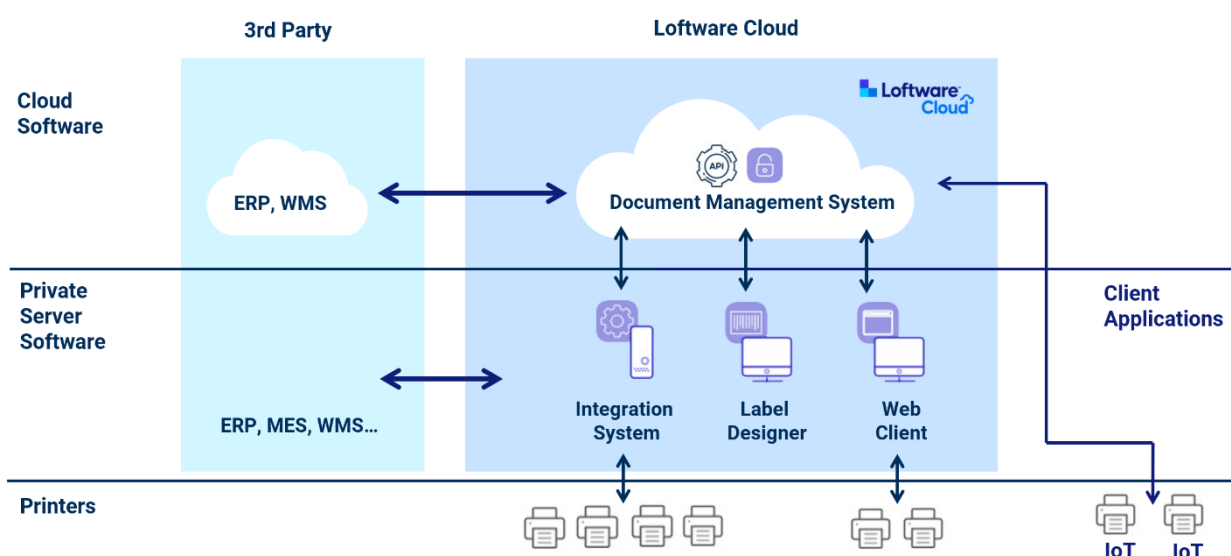


Figure 2 - High level overview of Software Cloud

Software Cloud consists of the following entities on the cloud side

- **Control Center**
Control Center delivers a secure central storage repository, file archiving, file versioning, label approval workflows and audit logs. Control Center aggregates print history, label metadata, user credentials and more.
- **Web Printing Backend**
Server-side component of the Web Printing where Web Client connects to.
- **WebDAV for Document Management System**
Used for file management for client applications via WebDAV protocol.
- **Cloud printing**
Used for directly printing to cloud connected printers without any local infrastructure.
- **APIs**
 - **Document API**
Used to access documents in Document Management System

	Software Cloud Details					
			Revision	19	Number of pages	26

- **Rendering API** (for internal usage only)
Used to render label templates in the browser.
- **Help API** (for internal usage only)
Used to access product help system.
- **Cloud trigger** (Cloud API)
Used for cloud integration with Loftware Automation clients and other cloud business systems and applications.

Deployment location runs one or multiple versions of deployments. Each customer account is assigned to run under a specific deployment.

2.2 Multitenancy

One of the primary benefits of cloud computing is the concept of a shared, common infrastructure across numerous customers simultaneously, leading to economies of scale. Loftware works continuously to ensure that the multi-tenant architectures of our cloud services support enterprise-level security, confidentiality, privacy, integrity, and availability standards.

Loftware Cloud was designed with security measures to prevent the actions of one tenant from affecting the security or accessibility of content of another tenant.

The two primary goals of maintaining tenant isolation in a multi-tenant environment are:

- Preventing unauthorized access to customer content across tenants; and
- Preventing the actions of one tenant from adversely affecting the service for another tenant

Multiple forms of protection have been implemented to prevent customers from compromising Loftware Cloud services or gaining unauthorized access to the information of other tenants.

Loftware Cloud customers get one or multiple accounts, or “tenants”. Each tenant gets its own database and a unique DNS entry (example: customer.onnicelabel.com). Database separation is important to our users as we have an additional layer of security. No data from one customer can ever be accessible to another customer.

In basic usage scenarios, computing and database processing power are shared between multiple users. For some of our customers this is not acceptable, so we offer options where specific customers can run in separate cloud deployment, if required.

2.3 Authentication

During the early development of Loftware Cloud, it was decided to use only OAuth2 (and OpenID Connect) for authentication, without implementing custom authentication logic, in alignment with current industry standards. In the first phase Microsoft and Google authentications were supported. Integration with Microsoft

	Software Cloud Details					
			Revision	19	Number of pages	26

Entra ID (previously known as Azure Active Directory - AAD) is also supported for Microsoft (via Microsoft Graph API) accounts.

User authentication runs in a separate sign-in web site and handles authentication logic. Software Cloud redirects unauthorized access to a sign-in site and after the user is authenticated, they get redirected back to the page of origin. User authentication is validated via authentication cookie.

2.4 High Availability

Software Cloud achieves high availability through a robust, multi-layered architecture built on Microsoft Azure, designed to ensure resilience, redundancy, and uninterrupted service.

1. Azure-Based Global Infrastructure

Software Cloud is hosted on Microsoft Azure, leveraging its global infrastructure to ensure high availability (HA) and disaster resilience. Key architectural elements include:

- **Availability Zones:** These are physically separate locations within Azure regions. Software Cloud services are distributed across zones to protect against datacenter-level failures.
- **Redundant Clusters:** Web services run on clusters of virtual machines across different zones. If one node fails, others continue operating without disruption.
- **Geo-Replication:** System databases are geo-replicated, allowing automatic failover to a secondary location in case of a primary failure.

2. Database Resilience and Performance

- **Azure SQL Database:** Software Cloud uses Azure SQL Database, which offers 99.99% availability and is always running on the latest stable version of SQL Server.
- **Separation of Compute and Storage:** This design ensures that failures in one layer do not impact the other, enhancing fault tolerance.
- **Backup Strategy:** Full backups weekly, differential backups every 12 hours, and transaction log backups every 5–10 minutes ensure data recoverability.

3. Local Site High Availability

For hybrid or distributed deployments:

- **Active-Active or Active-Passive Application Servers:** Local sites can be configured with multiple application servers to ensure continuity.
- **SQL Server Always On Availability Groups:** Recommended for local database failover, ensuring no single point of failure.

4. Offline Printing Capability

Software Cloud supports offline printing for up to 5 days:

- **Cached Templates:** Label templates are cached locally, allowing uninterrupted printing even during internet outages.
- **Automatic Sync:** Once reconnected, offline print records are synchronized with the cloud backend.

5. Monitoring and Maintenance

- **Automated Maintenance:** Azure handles patching, backups, and upgrades without affecting workloads.

	Software Cloud Details					
			Revision	19	Number of pages	26

- **Performance Monitoring:** Loftware monitors system performance and can scale resources or migrate workloads to maintain service levels.

6. SLA and Risk Mitigation

- **Service Level Agreement (SLA):** Guarantees high service availability as defined in the Master Software Subscription and Services Agreement.
Risk Mitigation: Includes proactive scaling, geo-replication, and failover strategies to handle overloads and failures.

2.5 Hybrid Cloud and Edge Computing with Loftware Cloud

Hybrid cloud is an IT infrastructure design that integrates a company's internal IT resources with Loftware Cloud infrastructure and services. With hybrid cloud, you can store your data and run your applications across multiple environments – including on-premises, cloud and edge locations. This architecture enables you to provision, scale, and centrally manage compute resources while optimizing performance, latency, and connectivity.

Loftware Cloud's hybrid deployment model is designed to support environments with limited or no internet connectivity. It enables **modules to run offline for extended periods**—typically with **yearly re-activation**—while still reserving printer seats and maintaining license compliance through the cloud. When combined with edge computing, this model empowers localized processing at or near the source of data generation, reducing latency and ensuring uninterrupted operations even in remote or bandwidth-constrained environments.

This model is particularly useful for:

- **Remote or isolated production sites** where edge nodes can operate independently.
- **Highly secure environments** where external connectivity is restricted and edge devices enforce data sovereignty.
- **Customers transitioning from on-premises to cloud** who need a phased approach with edge-enabled continuity.

Key capabilities of the hybrid deployment model are:

- Remote activation
 - Allows **offline operation** of Loftware Cloud modules.
 - Supports **autonomous operation** with periodic cloud check-ins (e.g., once a year).
 - Ensures **license compliance** even when disconnected.
- Localized distributed deployment
 - Enables **local processing** of labeling operations, ensuring **operational autonomy**.
 - Ideal for **multi-site enterprises** with decentralized infrastructure.
 - Reduces latency and improves responsiveness by processing data closer to the source.
- Local failover
 - Provides **resilience** during cloud outages by allowing local systems or edge nodes to take over.
 - Ensures **business continuity** in case of internet disruptions.

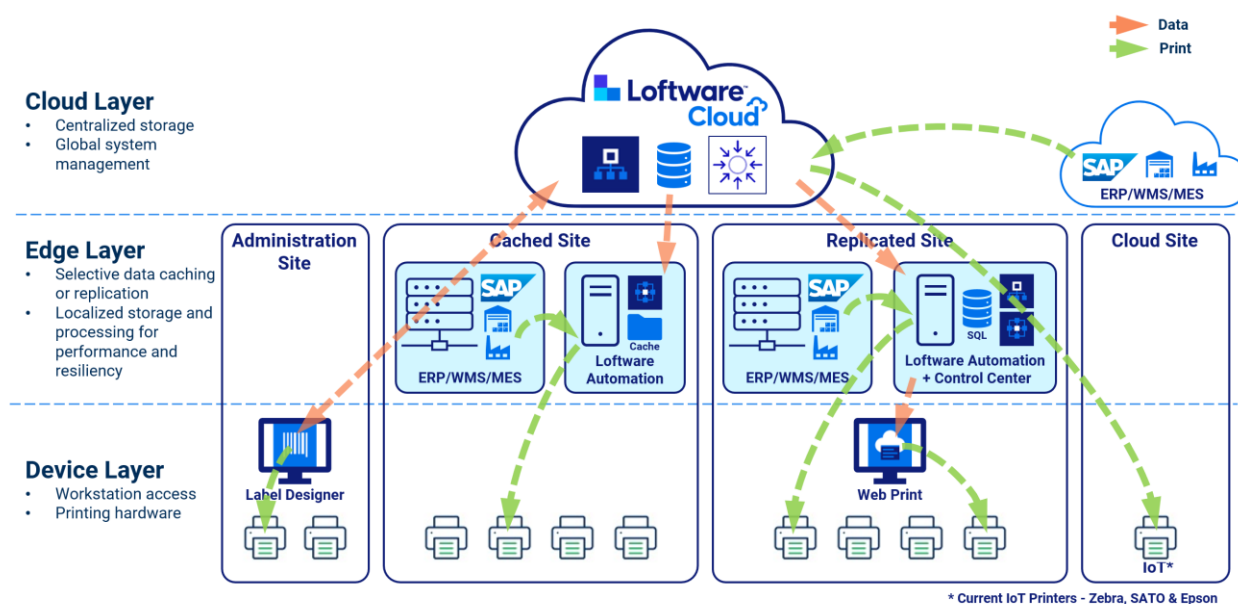
	Software Cloud Details				
			Revision	19	Number of pages

The full hybrid architecture includes:

- Local installation of Control Center and Software Automation at edge locations.
- Local authentication and UI access.
- Local data storage and replication (e.g., rules, label templates).
- Cloud synchronization for licensing and updates.

From Software Cloud 24.10 on Software Cloud offers remote activation that allows this hybrid-edge deployment. Remote activation provides an elegant solution for Software Cloud clients in the air gapped systems by providing extended offline operation, enabling them to operate autonomously with yearly re-activation.

The remote activation is available with Software Cloud Business, Software Cloud Compliance and Software Cloud Enterprise products with the Hybrid add-on. More details about remote activation can be found in Software Cloud [on-line help article](#).



	Software Cloud Details			
		Revision	19	Number of pages 26

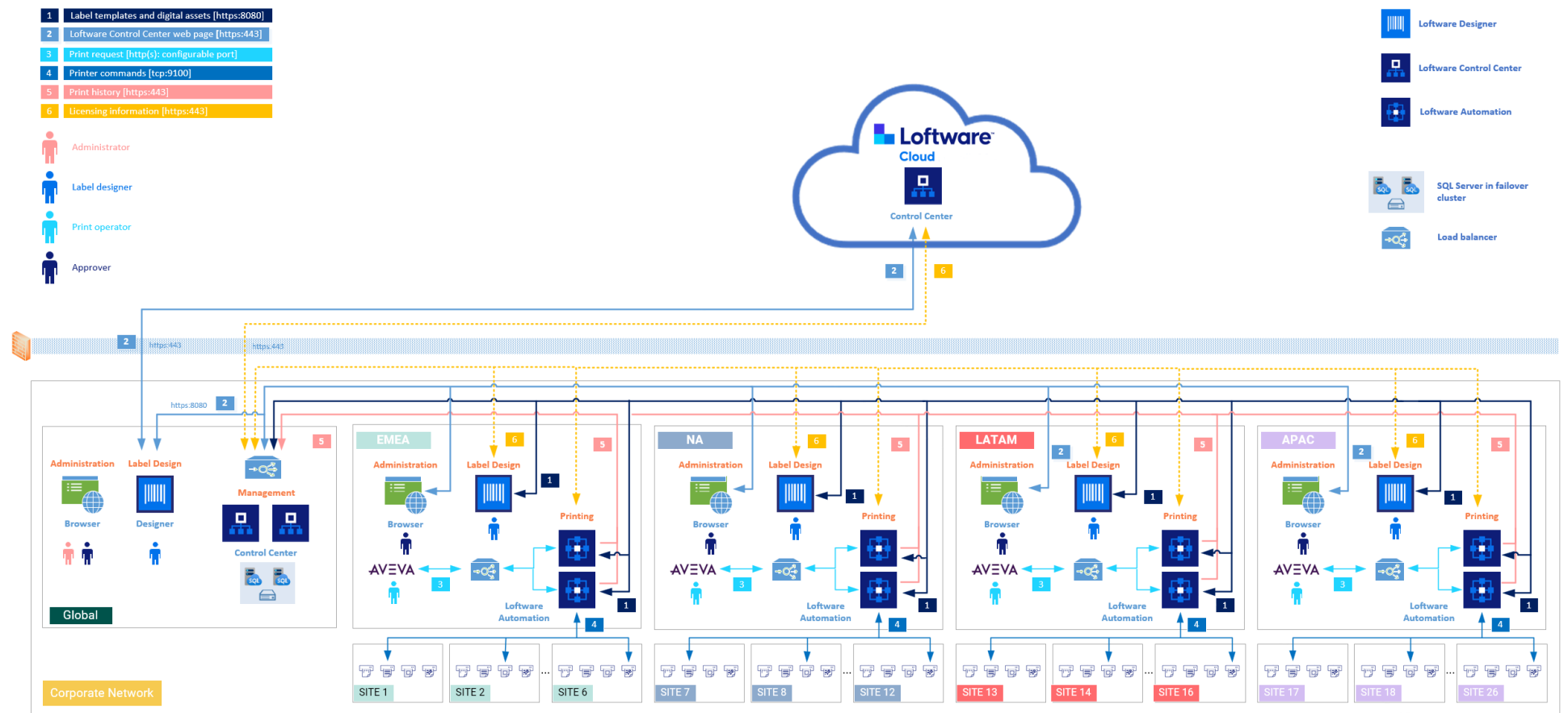


Figure 3 - Example of Hybrid Deployment

	Software Cloud Details					
			Revision	19	Number of pages	26

2.6 Environments

Based on selected Software Cloud edition, customers get different number of environments. Software Cloud Enterprise for life science customers and Software Cloud Compliance include three different environments: development, QA, and production. Software Cloud Enterprise (for non-life science customers) and Software Cloud Business include two environments: non-production and production. Software Cloud Essentials comes with production environment only.

Software change and transport system (CTS) can automatically transport changes between environments, or centralized production and local production environments.

2.7 Local Sites

In the architectural diagram at the beginning of this chapter, you can see four different possible deployments to local sites:

- Local installation of Software DMS and integration system with connection to Software Cloud (*Site 1 on the diagram*)
For sites where it is desired to keep a local copy of the Document Management System. Label templates can be synchronized from centralized Software Cloud DMS or designed, stored, and managed locally. Printing or preview generation is triggered via Software integration system utilizing one of numerous possibilities (SOAP web service, HTTP REST call, file drop to a folder, etc.). Printer drivers can either be installed locally or cloud-connected printers that require no local footprint can be used. All the traffic to Software Cloud is encrypted and uses ports 443 (standard HTTPS port) or 8080 (for access to label templates and images; also, over HTTPS).
- Local installation of Software integration system (*Site 2 on the diagram*)
For sites that can utilize centralized Document Management System in the cloud, only Software integration system is installed on-premises. Printer drivers can either be installed locally or cloud-connected printers that require no local footprint can be used. The diagram also shows the possibility to securely trigger printing to these local printers via our Cloud API utilizing on-premises cloud trigger running in Software integration system
- Local installation of printers (*Site 3 on the diagram*)
In cases where integration is handled by centralized integration system running for example in customer's data center, nothing needs to be installed locally on such sites. Server where Software Automation is running has drivers installed and handles requests coming from local ERP and other systems or requests coming from cloud applications via Software Automation Cloud trigger.
- Hybrid deployment with local installation of Software DMS and integration system without connection to Software Cloud (*Site N on the diagram*)
On sites where connection to the internet or even to customer's corporate network is not possible all the necessary building blocks (Software DMS, MS SQL Server, Software integration system, printer drivers) are installed locally.

	Software Cloud Details				
			Revision	19	Number of pages

Label designers, label approvers and system administrators are expected to access Software Cloud from customer's corporate network. It is also possible to print manually from a web printing solution.

2.7.1 High availability of local sites

The high availability solution on local sites is designed to ensure that committed data is never lost due to failures, that maintenance operations do not affect your workload, and that the database will not be a single point of failure in your software architecture. There are no maintenance windows or downtimes that would require you to stop the workload while the database (or any other on-premises component) is upgraded or maintained.

To ensure the best possible performance and high availability even on a site level having an appropriate number of properly sized servers is a must. There are typically at least two application servers that can be set up in Active-Active or Active-Passive configuration (depending on customer preferences and the expected load).

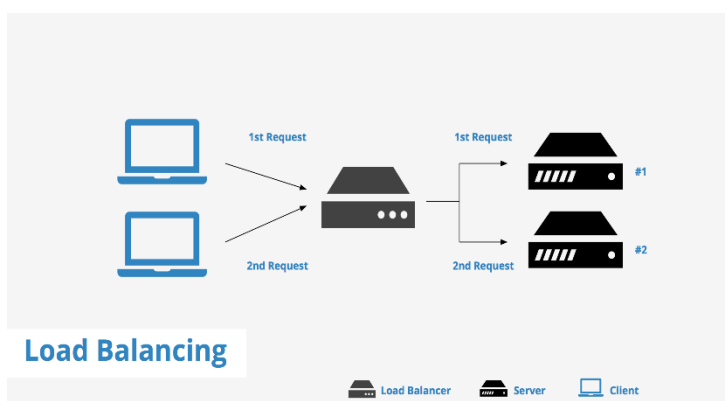


Figure 4 - Load balancing for application servers

For hybrid deployments where Software Control Center is installed on-premises, database server is set up in a failover cluster and separate from application servers. We recommend using SQL Server Always On Availability Groups (please see <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server> for more information).

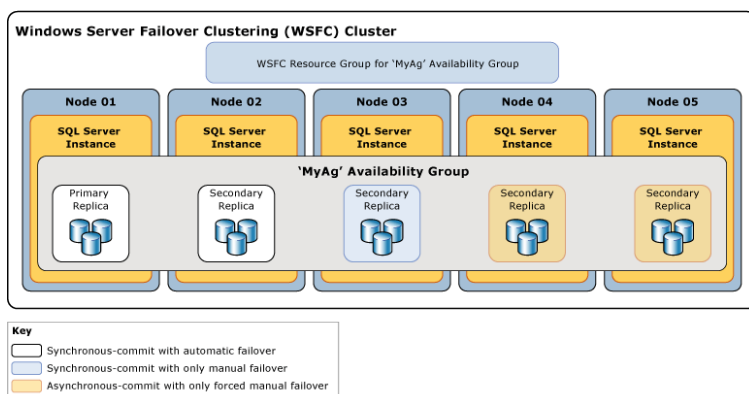


Figure 5 - MS SQL Server Always-on Availability Group

	Software Cloud Details				
			Revision	19	Number of pages

2.8 Printing in the Cloud

2.8.1 Printing via Cloud Print API

Software Cloud supports printing directly to cloud-connected printers (e.g., Zebra printers with LinkOS, SATO CLNX printers, or Epson CW series printers). Only the printer needs to be installed on-premises.

In this scenario, cloud-connected printers initiate secure web socket connection (web socket over HTTPS) to Software Cloud API. Cloud API utilizes Azure API Management as the gateway to prevent API abuse.

There are two steps that need to be taken before this:

1. Administrator assigns a unique name to each cloud printer when registering it Software Cloud. The name is then used when calling Cloud Print API (e.g., from SAP S/4 HANA) to indicate which printer labels should be printed on.
2. The Cloud Print API address needs to be configured on the printer and is specific to each Software Cloud tenant (e.g., wss://customer.zebracloudprint.onnicelabel.com).

Connection is kept open while the printer is powered on. If for some reason the connection is closed, the printer automatically reconnects. The connection is closed when the printer is powered off.

Printer devices are identified based on their serial number. Currently they are not authenticated. Zebra printers connect only to the servers that have a certificate issued by Zebra (Software Cloud does have it).



When the user in a client application (e.g., SAP S/4 HANA) initiates printing from the GUI, payload in XML or JSON format is sent via HTTPS request to Software Cloud API. Cloud API processes the request, determines which label template to use and which printer to print to. Then it opens the appropriate label template from the Document Management System (DMS), maps the variable fields and create printer specific commands. These commands are then sent to the right printer (via already established connection that is initiated from on-premises) and are printed.

Note

The latest information about cloud-connected printed printers can be found at [Cloud Printers](#).

2.8.2 Printing via Cloud Trigger

Printing via Cloud trigger works slightly differently and allows users to print from cloud applications like SAP S/4 HANA, Workday, and others, to on-premises printers even if these printers are not cloud-connected.

In this scenario, Software Automation is deployed on-site (e.g., in customer's data center or in specific site) and its Cloud trigger is used to communicate with Software Cloud and printer. Administrator needs to

	Software Cloud Details					
			Revision	19	Number of pages	26

register the cloud integration in its Cloud Dashboard (accessible only to authorized users) where unique key is generated. This key is used as part of Cloud trigger configuration in Software Automation.

Software Automation service connects to Azure Service bus. Connection is established when the Cloud trigger in Software Automation is started. The connection itself is a secure Azure Service Bus connection (again via Azure API Management). Azure service bus itself decides which connection to use (HTTPS or secure TCP). Connection is authenticated using SAS (Shared Access Signature). Software Automation service receives access key from Software Cloud on startup. The connection is established on port 443 or on one of the ports between 9350-9354 (whichever is available). When the Cloud trigger in Software Automation is stopped, or Software Automation service is stopped, the connection is closed.

When the user in a client application (e.g., SAP S/4 HANA) initiates printing from the GUI, payload in XML or JSON format is sent via HTTPS request to Software Cloud API that routes it to the appropriate Software Automation (via already established connection that is initiated from on-premises). Software Automation then parses the incoming data to get the information about the printer, label template, quantity and variable fields that need to be mapped with the fields on the label template. The label template is opened from the cloud based DMS, variable fields are filled with the values from the payload coming from the client application and printed to the label. All label templates from DMS are cached on a local drive (done automatically) to ensure the best possible performance and prevent printing outages.

3 Software Cloud Internals

Software Cloud applications are hosted by Microsoft Azure. We utilize the following Azure products.

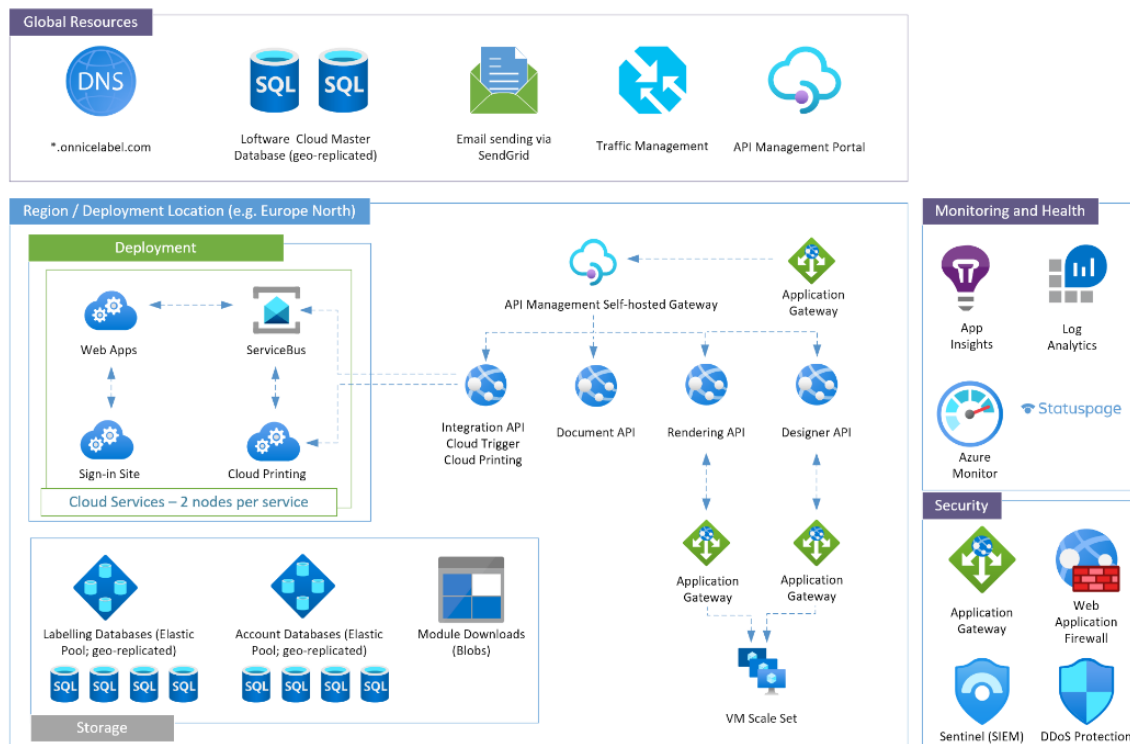


Figure 6 - Microsoft Azure services utilized by Software Cloud

	Software Cloud Details					
			Revision	19	Number of pages	26

- **Azure Cloud Services** used for hosting of:
 - Sign in pages,
 - Dashboard, Print and Document storage,
 - Cloud Printing
- **Azure App Service**

To host Docker instances used for API deployment.
- **Azure SQL Storage**
 - Master database

This is the most important part of Loftware Cloud. All customer information required for running Loftware Cloud is stored in this database. Database is geo replicated in multiple regions which means that Loftware Cloud is operational even if one Azure datacenter is offline.
 - Application databases

Each account has one database where all application data is stored. This database stores files for document storage, print history, access roles and all other configurations.
 - User databases

Optional user databases that hold any data required for labeling.
 - Application and user databases are stored in Elastic Pool. This means that database processing power is shared between multiple databases. We can increase processing power as needed if monitoring detects high load.
- **Azure Storage**

Client application installations and other common assets are stored in blobs.
- **Azure API Management**

Main entrance points for all integrations (cloud printing and cloud triggers). Traffic limits are set here to prevent abuse of APIs.
- **Azure functions**

API calls Azure functions for some additional processing which then calls correct service bus end point.
- **Azure Traffic Manager**

Used to redirect users to the closest API Gateway.
- **Azure virtual machine scale sets**

To create and manage a group of load balanced VMs that host Loftware code used for print stream and label preview generation.
- **Azure Service Bus**

Used for communication with local infrastructure that is either cloud connected printer or cloud trigger. Service Bus creates outbound connection from customer backend and makes it possible to call the backend from cloud.
- **Azure Application Insights**

Constant health monitoring of all hosted entities. We have visibility over request lengths and any errors happening in the backend.
- **Azure Web Application Firewall**

Web Application Firewall (WAF) provides centralized protection of web applications from common exploits and vulnerabilities.

	Loftware Cloud Details				
			Revision	19	Number of pages

- **Azure DDoS Protection Standard**
Provides enhanced DDoS mitigation features to defend against DDoS attacks.
- **Microsoft Sentinel (SIEM)**
Intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

Currently we utilize Microsoft Azure data centers in 5 regions across the world (North Europe, West Europe, South Central US, West US, and Southeast Asia).

4 Release Cycle

Loftware keeps Loftware Cloud up to date.

Our controlled process updates Loftware Cloud automatically, providing you with seamless hassle-free updates with no platform downtime.

We typically update with major product releases every two years, minor releases twice per year, and service releases in between (as needed).

For Loftware Cloud Enterprise, Loftware Cloud Business and Loftware Cloud Essentials, we provide new Loftware Cloud deployments for every software release. We prepare and test each new deployment before we update your subscription, allowing you to upgrade seamlessly without downtime. We update your subscription by simply moving you from your previous deployment version to your new one. If you experience any unexpected problems, we will return you to your previous version while we solve any problems. We have transparent update plans and clearly defined procedures in place for all release types (major, minor, and service). You receive email notifications before any Loftware Cloud version updates, allowing you to prepare for, test, and track every upgrade.

Loftware Cloud Compliance comes with a compliance software release cycle. Typically, our on-premises and cloud software are updated two or three times per year. However, to reduce the validation burden for regulated companies, Loftware Cloud Compliance is updated only once a year. And when it's time for the new release, we also give our customers a three-month testing period and during this time each customer can decide on their own when they are ready to update the production environment as well. This way, you benefit from a continuously updated and maintained labeling solution, while minimizing the validation workload on your staff.

4.1 Upgrades

A lot of effort is invested to support seamless upgrades of our customers to newer versions of the Loftware Cloud. We can pick and choose individually which customers need to be upgraded.

Upgrade procedure includes the following steps:

- Create new deployment
- Create a test customer to see if everything is working as expected

	Software Cloud Details					
			Revision	19	Number of pages	26

- Move all internal accounts to this deployment
- Move all development accounts
- Move all QA accounts
- Move all production accounts

Move of each account again runs completely automatically in multiple steps:

- Decrease DNS TTL to some low amount
- Wait 1 hour for TTL to propagate
- Upgrade database
- Assign account to new deployment
- At this stage account is active on two deployments (depending to which DNS record it points to).
- Increase DNS TTL to default
- Unassign account from the old deployment

These steps allow us to move account to new version without any down time.

Application databases are also backwards compatible. If any customer detects any issue after upgrading, we can quickly move them back to previous version. This allows customers to stay online without any issues affecting their production and allows us to have time to properly fix any issues.

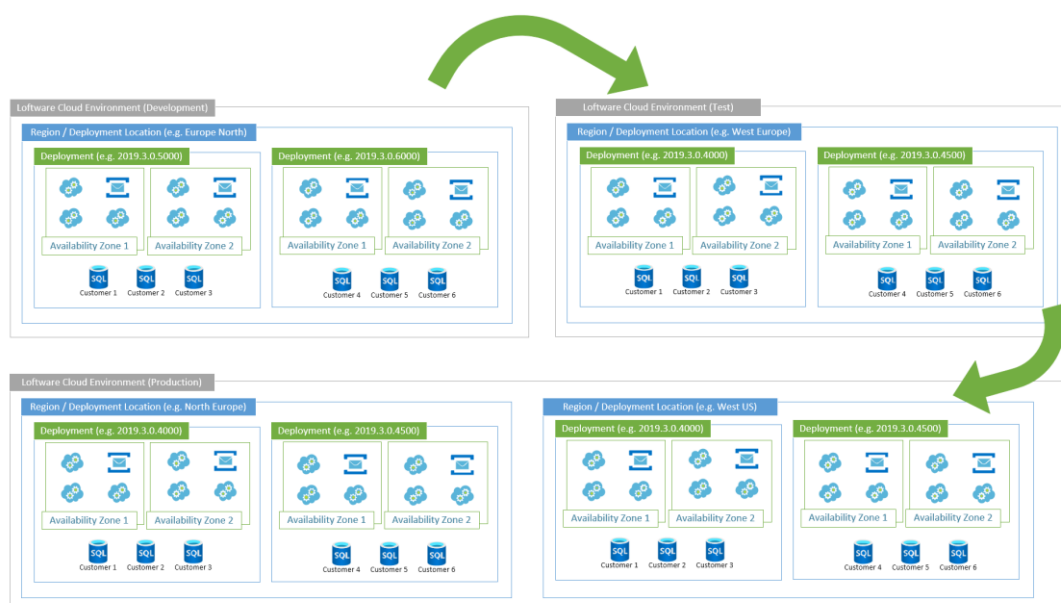


Figure 7 – Software Cloud Upgrade Process

5 SLA

Software guarantees 99,8% uptime for the whole Software Cloud. Each part of the platform was analyzed to see how we could support the required SLA.

- Cloud services
 - At least two nodes are running at any time in each cloud service.

	Software Cloud Details				
			Revision	19	Number of pages

- Master database geo-replicated and set up for high availability
- Azure functions for cloud trigger and cloud printing (created anywhere even if one data center goes down)

In practice, Software Cloud has achieved consistent > 99,95% uptime.

Software continuously monitors your hosted system health with Azure Insights. Insights automatically detect performance anomalies and include powerful analytics tools to help us diagnose issues and improve products by understanding how our customers use Software Cloud. We use Insights to:

- Monitor abnormal traffic and respond quickly to possible threats.
- Detect and respond to higher demands for services.
- Continuously improve performance and stability

Customers can at any time check [Software Cloud status page](#) that is a public-facing webpage that shows the stability and availability of our Software Cloud.

6 Security

6.1 SOC2 Type II Certification

Software Cloud is SOC2 Type II certified. SOC 2 is an auditing procedure that ensures your service providers (i.e. Software) securely manage your data to protect the interests of your organization and the privacy of its clients. With Software's service-driven landscape, your organization's data does not exist only in your IT environment but also in the Software Cloud.

SOC 2 Type II compliance is specifically designed for service organizations. The earned SOC 2 Type II certification verifies that Software has the proper controls in place for data compliance and security. As a customer, a big part of choosing which vendor to trust that data with is made with the help of certifications, which can demonstrate adherence to certain standards for security and confidentiality.

6.2 Fundamentals

Software keeps your systems and data secure in multiple ways. Most security breaches don't occur from someone breaking into cloud data centers. Instead, attackers typically exploit cloud application vulnerabilities. To prevent attacks, we combine multiple mitigation strategies and security controls to protect your resources and data. Our layered security includes:

- Employee education
- Physical security
- Network security
- Web security
- API-based cloud security
- Data encryption
- Monitoring

	Software Cloud Details				
			Revision	19	Number of pages

By running on Microsoft Azure, Software Cloud inherits many platform and infrastructure security approaches and best-practice implementations. Microsoft handles core data center security and inspects dataflows from the internet to help protect against intrusions and malware attacks.

We design cloud applications following modern security-conscious programming practices. We use encryption techniques and execute testing procedures to develop code and launch products. Our development teams complete IT security-related training on software development to strengthen their information security awareness and experience.

We integrate best security practices into our software development lifecycle (from inception to design to development and testing). This practice ensures our products are resistant to attack by malicious or mischievous people or programs. Secure coding helps protect our user's data from theft or corruption. We are using static analysis tools like Microsoft's FxCop to check for security issues (and others) during every build (multiple times per day).

Our software has undergone extensive security vulnerability scans by our existing customers using automated tools like Veracode. Additionally, we regularly perform internal security reviews and external penetration testing of our products. The last external penetration test was done in April 2025 by HackerOne.

Also, we utilize Azure's DDoS Protection Standard service that monitors Software Cloud application traffic patterns 24 hours a day, 7 days a week, looking for indicators of DDoS attacks. DDoS Protection Standard instantly and automatically mitigates the attack once it is detected.

Finally, we use Microsoft Sentinel. Microsoft Sentinel is a scalable, cloud-native, **security information and event management (SIEM)** and **security orchestration, automation, and response (SOAR)** solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

6.3 Role-based Access

Software Cloud authenticates with Microsoft and Google (OAuth2/OpenID Connect) accounts. We integrate trusted providers into Software Cloud security to authenticate your user identities and protect your users from attacks. This allows Software to focus on core features and leaves identification to experts you know. You can define your users with LDAP directory services or use your Microsoft Office 365 or Active Directory (AD) accounts (available as Entra ID for cloud applications). Software Cloud does not include authentication mechanisms or custom authentication logic.

6.4 Database Security

Database separation is essential and ensures you get additional layers of security. You can only access your own assigned application database. You cannot access application databases directly with management applications or via API. Database ownership prevents other customers from accessing or reading any of your data.

	Software Cloud Details					
			Revision	19	Number of pages	26

Depending on your Software Cloud subscription, you can access user-based cloud databases to store printing data and for daily intermediate master data exports from ERP systems. You do not need user-based cloud database access to run Software Cloud web applications.

User database access is entirely customer specific. When you claim your user database, we create your first administrative account so you can manage your database and grant user access yourself.

6.5 Data Encryption

Software Cloud encrypts your data to keep your business safe. Your data can occupy two states in Software Cloud - data in transit and data at rest. Your data can be exposed to risks in both states. Software Cloud uses encryption to protect data in transit and at rest from unauthorized access or theft.

Data actively moving between devices or networks across the internet is data in transit. We protect your data in transit from local storage to Software Cloud storage. We encrypt your data in transit on one end and decrypt it on the other to prevent eavesdropping from unauthorized clients. Software Cloud uses modern data encryption communication protocols (TLS and HTTPS) for privacy and data integrity.

We encrypt your data when you connect to Software Cloud with:

- Browsers. You can use any modern web browser to interact with our web applications.
- Software clients. All our clients, including Designer, Print, Automation, and Web Client, use secure encrypted channels to request Software Cloud data and to send back logs and updates.

Data not actively moving between devices or networks across the internet is data at rest. Software Cloud receives and stores your data in Azure SQL databases unique to you. We follow protective security measures to prevent anyone from accessing, modifying, or stealing your data:

- Only you have access to product databases you own.
- Your Azure SQL databases use transparent data encryption (TDE). TDE gives you real-time database encryption and decryption using AES 256 encryption algorithms.

All backups are automatically encrypted.

6.6 API Security

Software software uses Azure APIs for secure data exchanges and inter-application communication.

- **Service Bus:** The communication system between mutually interacting software applications in service-oriented architecture. We use Service Bus to communicate with your on-premises infrastructure, either through cloud-connected IoT printers or cloud triggers (running in Software Automation). Service Bus creates outbound connections from your backend to Software Cloud and makes it possible to call your backend from the cloud.
- **Azure functions.** Our published APIs for Software Cloud (Cloud Print API and Cloud Trigger API) call Azure functions for additional processing, which in return call the correct Service Bus endpoints. For example, when you execute "print" in Cloud Print API, Software Cloud generates a print job, knows where your IoT cloud printer is, and delivers your print job to your printer. We have traffic limits in place to prevent the abuse of APIs.

	Software Cloud Details					
			Revision	19	Number of pages	26

6.7 Printer Connection Security

Software Cloud supports client-side certificates on printers for printer models that have such functionality.

6.8 Client requirements for connecting to Software Cloud

These are requirements for the clients to be able to connect to Software Cloud.

- Outbound Internet connectivity to <your_account>.onnicelabel.com
 - Port 443/TCP to access Control Center's user interface in the browser.
 - Port 8080/TCP to access label assets in document storage from locally installed Software clients.
- Outbound Internet connectivity to lmscloud-bus-trigger-production.servicebus.windows.net to connect Automation Cloud triggers or Cloud printers to the Software Cloud backend.
 - Ports for Cloud Trigger API (all TCP):
 - 9350 to 9354 or
 - 5671 or
 - 443
 - Ports for SQL database connection:
 - 1433/TCP
 - 1434/TCP&UDP
 - Port number for Cloud printers:
 - 443/TCP

Make sure your firewall doesn't close the idle outbound connections to lmscloud-bus-trigger-production.servicebus.windows.net.

- Outbound Internet connectivity to labelcloudapi.onnicelabel.com
 - Port 443/TCP to consume the Software Cloud APIs. See the list of Software Cloud APIs in our Developer Portal.
- Add the following sites to your Trusted sites (Internet options > Security settings):
 - For Google authentication:
 - https://*.onnicelabel.com
 - <https://accounts.google.com>
 - <https://ssl.gstatic.com>
 - For Microsoft authentication:
 - <https://aadcdn.msauth.net>
 - https://*.onnicelabel.com

	Software Cloud Details					
			Revision	19	Number of pages	26

- <https://login.microsoftonline.com>
- <https://aadcdn.msftauth.net>
- <https://login.live.com>
- Support for WebDAV protocol: supported by Windows 10 out of the box. You must add support for Windows Server operating systems. Read more details in this [KB article](#).
- Recommended browsers: Use the latest editions of Edge, Chrome, Firefox, or Safari.

JavaScript available: Enable **Active scripting** under **Internet options** > **Security** > **Internet zone** > **Custom level...** > **Scripting**.

7 Data Location

Currently we utilize Microsoft Azure data centers in 5 regions across the world:

- The US (West US and South Central)
- The EU (North and West)
- Southeast Asia

Data resides in the Azure data center appropriate for the customer's location. For example, data for customers in the European Union (EU) will always reside in an EU data center. Customers can choose where they would like their data to reside.

8 Exit Strategy

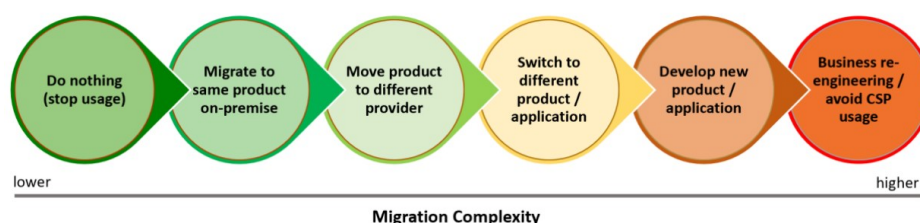


Figure 8 - Typical exit scenarios

Cloud exit strategy is a corporate plan developed to ensure that the cloud services that support business activities can be replaced or replicated efficiently and without significant disruption to the company.

Software Cloud supports two exit scenarios:

- Do nothing (stop usage)
- Migrate to same product on premises

In both cases customers can download all their labeling assets (e.g., label templates, graphics, logos, etc.) stored in the Document Management System. When migrating to on-premises installation of Software LMS

	Software Cloud Details				
			Revision	19	Number of pages

Enterprise it is also possible to configure automatic synchronization of labeling assets from Software Cloud to on-premises.

Additionally, customers can directly download print and other logs from Software Control Center in MS Excel format. It is also possible to manually download data archives of the previously archived logs.

Archive Files List

⚠ We archive your database data older than 1 year(s). We delete your archives after 6 months.

Download

Search...

	File name	From	To	File size
☒	Archive2022-04-30	4/23/2022	4/30/2022	488 KB
☐	Archive2022-04-23	4/16/2022	4/23/2022	488 KB
☐	Archive2022-04-16	4/9/2022	4/16/2022	488 KB
☐	Archive2022-04-09	4/2/2022	4/9/2022	488 KB
☐	Archive2022-04-02	3/26/2022	4/2/2022	488 KB
☐	Archive2022-03-26	3/19/2022	3/26/2022	488 KB
☐	Archive2022-03-19	3/12/2022	3/19/2022	488 KB
☐	Archive2022-03-12	3/5/2022	3/12/2022	488 KB
☐	Archive2022-03-05	2/26/2022	3/5/2022	488 KB

10 items per page
Selected: 1 | 1 - 10 of 24 items

Close

Figure 9 - Downloading data archives

If the customer also utilizes Software Cloud database as part of labeling solution for their own content (e.g., product information) they have full access to the database and can transfer it to their own systems or to on-premises installation of Software LMS.

	Loftware Cloud Details					
			Revision	19	Number of pages	26

9 Glossary

Term/Acronym	Definition
Environment	Environment contains all resources needed to run Loftware Cloud. Each environment is separate from another. Currently Loftware Cloud has three environments: Production, Test, Development
Deployment location	Geographical location / Azure Region = Set of datacenters deployed within latency-defined perimeter and connected through a dedicated regional low-latency network.
Deployment	Web site cluster running one version of Loftware Cloud (utilizing multiple availability zones).
Availability zone	Unique physical location within a region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
Exit strategy	A high-level description of an institution's ultimate risk mitigation strategy when dealing with a failing cloud provider or when terminating the outsourcing. This might include exit and transition of outsourced functions and data to an alternative provider (in part or completely), the return of these functions on-premises, or even discontinuation of the process.
Exit plan	An underlying element to the exit strategy. A high-level document describing how to implement the exit strategy including a description of all its phases, involved roles and responsibilities and various plan features. A plan is to be enacted in case of pre-defined events following a long-term strategy approach. It does not include short-term incident management, since the business implications of enacting an exit plan can be considered severe. The exit plan ensures business continuity in case of the pre-defined events, aiming at response times appropriate to the severity of the triggering event.
Testing of an exit plan	Activities to be performed to ensure that an exit plan is well documented and actionable when necessary. A table-top exit plan test involves a 'paper evaluation' to ensure that the exit plan is fully documented, understood by stakeholders, realistic and achievable in line with business and regulatory requirements. This includes checking on the availability of resources identified in the plan

	Software Cloud Details					
			Revision	19	Number of pages	26

10 References

#	Document ID	Description
[1]	Getting started with Software Cloud	Getting started with Software Cloud guide
[2]	Software Cloud Infrastructure, Security, and Maintenance	Describes Software Cloud infrastructure, security, and maintenance processes
[3]	Software Cloud Data Integration	Describes how data integrations with Software Cloud work
[4]	System Requirements	List of minimum and recommended system requirements
[5]	Software Cloud Overview.pdf	Provides high level overview of Software Cloud, its benefits, and some details of its modules.