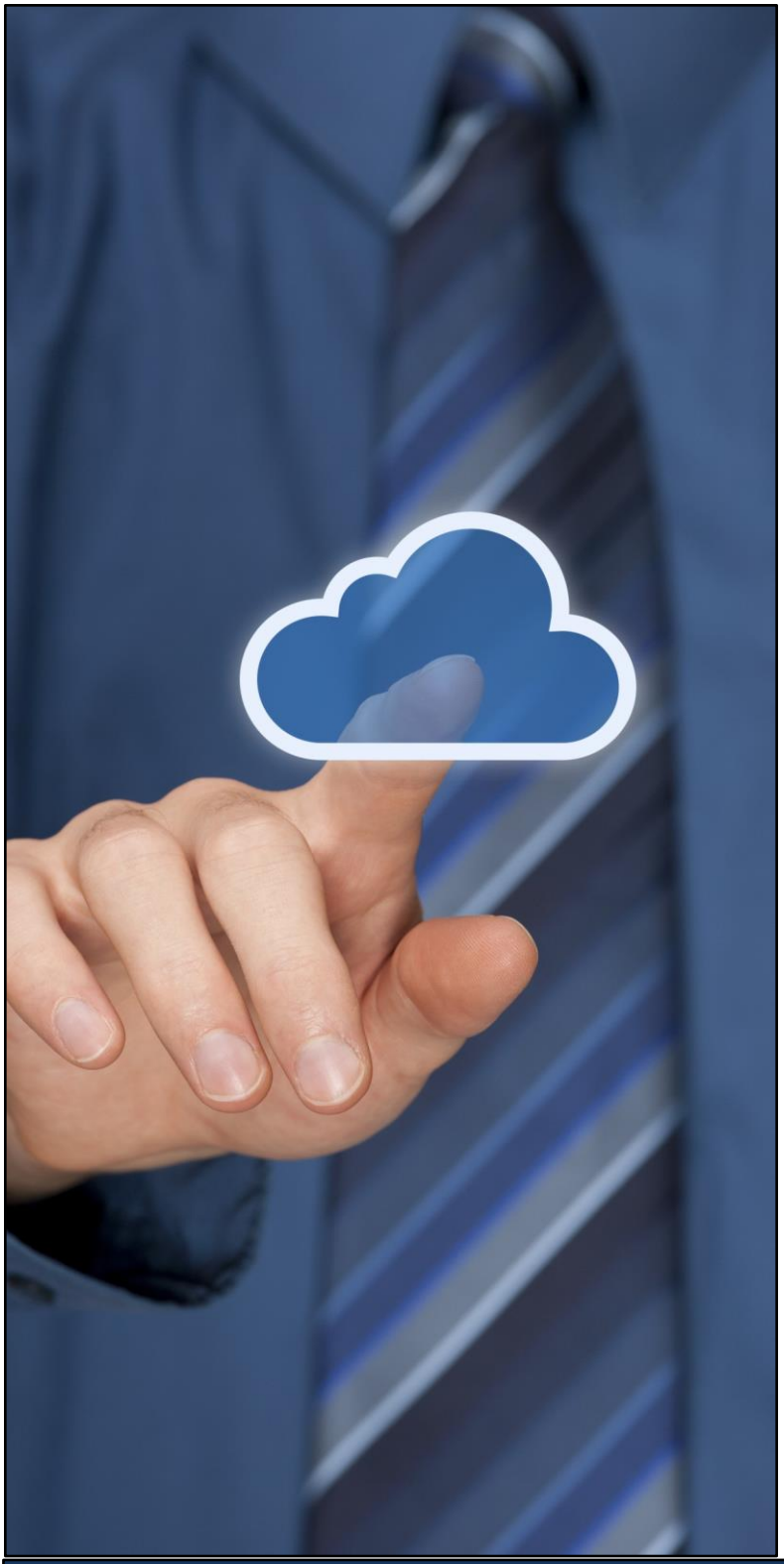

myEZClaim

Software as a Service

myEZClaim Cloud

CELEBRATING 21 YEARS TranSolutions

Food Logistics 2017 FL 100+

AICPA SOC 2 Formerly SAS 70 Reports

BENEFITS

- Purpose Built Environment
- Who Knows myEZClaim Better
- Data Retention
- Disaster Recovery
- Business Continuity
- Distributed Data Centers
- Leveraging Cloud Resources
- Data Retention
- Monitoring
- Business Continuity

Introduction

What is the most important aspect of your myEZClaim application? Availability.

The functionality and usefulness of the **myEZClaim** application provides impressive monetary value to your organization's bottom line, but only if the application is up and running smoothly.

That's why you need ***myEZSaaS*** from the ***myEZClaim Cloud***.

We have years of ***myEZSaaS*** hosting experience and a purpose-built environment designed to ensure your **myEZClaim** application has the highest availability, because that's what you need to be successful.

The ***myEZClaim Cloud*** hosts only myEZClaim applications for customers who demand the best performance and highest availability. That's what we are here for… to make your life easy.

Sure, you can host it internally, but if you're honest with yourself and include all the expenses involved with running any application, not just the server acquisition costs, you'll find you're not saving nearly as much as you think and have taken on all the responsibility for yet another application on your network.

We can take that load off you and off your IT Staff. Backups, application upgrades, data management all add up to FTE utilization and when that is included in your monthly running costs you will find ***myEZSaaS*** is not overpriced, and in fact will be less expensive if you actually provided the level of backup redundancy and increased availability we include out-of-the-box with ***myEZClaim Software as a Service***.

We have the experience. We have the robust, distributed environment. We have the high availability solutions. So how does your company benefit from running your **myEZClaim** application internally instead of leveraging our years of experience and purpose-built environment?

Why not simply turn on ***myEZSaaS*** and have **myEZClaim** professionally delivered to your business?

Thank you… The myEZClaim Cloud Staff

Compliance

The myEZClaim Cloud Platform is SOC 2 Type 2 compliant. Our annual audit report window runs from October 1st through September 30th each year, with the audit report generally available by January 1st.

Because we maintain our own SOC 2 Type 2 audit report, we seamlessly fold right into your compliance objectives and efforts, and your auditors do not have to spend your money examining our controls.

Your security department can also rest easy that our environment is on par with your internal environment and your data is safe when trusted to our ***myEZClaim Software as a Service*** platform.

Customers who have an executed NDR with TranSolutions may request a copy of our current SOC 2 Type 2 Audit Report. The audit report is proprietary and not to be disclosed with anyone outside of your company without our knowledge and express consent.

CERTIFICATE OF COMPLETION

AT-C Section 205 (SOC 2) TYPE II

AICPA SOC aicpa.org/soc4so — SOC for Service Organizations | Service Organizations ™

This is to certify that **TranSolutions, Inc.** has been assessed by Skoda Minotti and received an unqualified opinion of its MyEZClaim Cloud Platform System and on the suitability of the implementation and operating effectiveness of its controls relevant to security, availability, processing integrity, and confidentiality.

TranSolutions, Inc.

www.transolutionsinc.com

Engagement Type: **SOC 2 Type II**

Examination Period: **October 1, 2017 to September 30, 2018**

CONDITIONS:

1. Skoda Minotti has issued this certificate to indicate that the aforementioned company has completed an examination of its MyEZClaim Cloud Platform System and on the suitability of the implementation and operating effectiveness of its controls relevant to security, availability, processing integrity, and confidentiality.
2. This certificate offers no guarantee or warranty to any third party for ongoing compliance.
3. Please contact Skoda Minotti Risk Advisory, LLC at 866.669.6561 for additional information. This certificate is valid for one year from October 3, 2018.

Skoda Minotte — Signature

October 3, 2018 — Date

SKODA MINOTTI RISK ADVISORY SERVICES

The remainder of this document is a high-level overview of some of the many security controls in place for the myEZClaim Cloud Platform. This document is intended to be an overview document to support sales initiatives and not a deep dive. The audit report is the deep dive into our total security posture.

Contents

Data Centers

Locations

A single data center is a single point of failure. That is why we leverage three data centers, two physical separated by over 1000 miles, and one in the cloud. With your data mirrored to all three locations, data loss is non-existent, and recovery options are multiplied.

Primary Data Center

The primary data center is located in a Tier-3, fully compliant data center in Dallas, Texas.

Standby Data Center

The secondary data center is located in a Tier-3, fully compliant data center in Phoenix, Arizona. Data centers are connected via a high-speed fiber inter-connect, allowing for the standby data center to be maintained to just minutes behind the primary data center.

Cloud Data Center

Should both physical data centers become unable to sustain operations, we maintain backup copies of all severs in the Azure Cloud and can spin the environment up virtually in the cloud, or physically into any data center in the world we choose to put hardware into.

Physical Separation

The physical data centers are over 1000 miles apart, making it highly unlikely the same 'event' could affect both data centers.

Power Systems

Being a Tier-3 data center means full N+1 redundancy on all power connections, generators, and UPS systems to ensure a power event never impacts availability.

HVAC Systems

Being a Tier-3 data center provides N+1 redundancy on all HVAC systems to ensure equipment is always operating at optimal temperatures and humidity to assist in preventing premature hardware failures.

Fire Suppression Systems

Air flow, smoke, and particle monitoring systems provide early detention of potential fire threats (e.g. overheating power supplies, etc.) where combustion can be adverted before they become actual fires, but should a fire break out, the proper fire suppression systems and operational protocols are in place to handle the situation at the Tier-3 datacenter level.

Security

Security Administrators

The following individuals have been named as the respective administrators of the various security environments.

	Administrator	Immediate Contact
Network Security	Mike Goodwin	mike.goodwin@myezclaim.com
Host Security	Mike Goodwin	mike.goodwin@myezclaim.com
Application Security	Andy Celestina	andy.celestina@myezclaim.com

Security Escalation

In the event of a security incident the following workflow will be used to work through the issue. The first thing to be done is to engage the appropriate security administrator to drive the process. Every incident will be different, so we need the human intelligence of these trained personnel to determine who will perform each of the following steps.

Containment

The breach must be isolated to the affected server as quickly as possible. In most cases, this will include removing the server from the network and stopping all replication to the warm site. The warm site will have to be analyzed to determine if the compromise has affected it and taken offline also, if impacted.

Identification

The next step is to identify what the breach is, what it has affected, what the remediation process will be, and where the breach originated if possible. This information will determine next steps.

Correction

Based on the outcome of the identification step, the corrective action is applied to the affected system(s).

Re-Deploy

After system remediation the system will be put back into production. The re-deploy will be timed to have the least amount of impact and will be determined by whether we rolled to the DR facility or not.

Communication

This step happens in parallel during each of the above steps, but is called out separately as a place holder. All owners and parties of interest will be informed of decisions and progress as each step is handled.

Network Security

Firewall

We use load-balanced, fault-tolerant FortiNet firewalls. These state-of-the-art firewalls provide the ultimate in packet inspection to ensure we are doing more than just dropping packets on a closed port. They provide real-time perimeter security and threat neutralization to protected systems.

Intrusion Prevention

The FortiNet firewall includes Intrusion Prevention with signatures updated hourly. Constantly checking for all known types of attacks ensures the attacker is stopped at the perimeter.

Perimeter Anti-Virus

The FortiNet firewalls also provides packet level anti-virus scanning with signatures updated hourly. This perimeter defense can stop viruses and Trojans before they ever get to the server environment.

Incoming Connections

Incoming connections to servers behind the firewall are limited to IP to IP connections where possible. We prefer to only open the ports required by the client to access their application(s), from the clients IP address(es) only. However, we will work with the client to establish the best mix of security and usability. Since we are a fully-managed hosting facility, that only supports the **myEZClaim** application, clients are not provided physical access to the environment, access is through web interface only.

Two-factor VPN Access

Access to the platform for application and systems management is reserved for myEZClaim staff only, and access is performed from remote locations over a VPN that has two-factor authentication required.

SSL

All application traffic between the end user community and the application if done over SSL/TLS encrypted data streams.

Wireless

There are no wireless access points on the production or standby networks.

Host/Server Security

Physical Access

Servers are kept in locked cabinets in a Tier-3, fully compliant datacenter that has all of the industry prescribed security policies and procedures in place to ensure physical security. Datacenter SOC II audit report available upon request.

Console Access

Pre-approved individuals may access system consoles to perform application and system maintenance and upgrades. Access is logged and monitored, as well as routinely examined for accuracy. See Appendix A – Policy Changes for the security measures applied to user logon accounts.

User Accounts

Each staff member who needs access to a server is granted their own account and password, with rights tailored for what they need to do on the server.

Password policy is set to reduce the chances of a brute force attack succeeding in less time than our passwords change. Our password policy is spelled out in Appendix A – Policy Changes.

Administrator accounts are renamed via Group Policy to assist in preventing attackers from using it to gain access. An attacker has to crack both the username and the password before gaining access, so even though the Administrator is generally a "known" account… it is not "known" on our servers.

Access Audits

Auditing is enabled on each server. We log and monitor all login events for success and failure. Our auditing policy settings can be seen in Appendix A – Policy Changes.

Anti-Virus

Anti-virus scans run daily on platform servers to back up the perimeter anti-virus provided by the firewall. Anti-virus signatures are updated daily on each server.

Running Services

Non-essential operating system services are disabled to increase security of the servers as well as to reduce operating overhead and provide the fastest processing environments.

OS Hotfixes

All systems have the Windows OS and any third-party tools patched monthly to ensure all of the available latest security patches are protecting the platform.

Physical Security

Building Access

Access to the Tier-3 datacenter requires two-factor authentication utilizing a key card and bio-metrics. One

Video Cameras

Video surveillance cameras are positioned throughout the building to capture snapshots of events such as key card use, and door openings. This surveillance is stored and reviewed each morning by the Operations Manager on site.

Personal Escorts

Vendors have to be either pre-approved or escorted by IT Management to be allowed access to the datacenter. Sign-in and temporary access badges are required.

Systems Monitoring

Vulnerability Assessments

We actually have two tools in use that provide vulnerability assessments and point out new or existing weaknesses in the platform that may need to be addresses. Both tools pull updates from external data sources to ensure we are always polling for all known vulnerabilities.

SIEM/Logging/IDS

Systems are in place to provide real-time logging and analysis of logs generated on servers and network devices, and to couple those log events with NIDS and HIDS events happening across the environment and to correlate those findings with a pre-defined intelligence to determine if an known attacks have penetrated into the platform.

Host/Server/Application

Multiple internal and external systems and application monitors are in place to ensure we are fully aware of issues as soon as they occur.

Change Control

Changes to systems or the applications must pass through the change control process where it is published, discussed as needed, approved, and scheduled.

Disaster Recovery & Business Continuity

Leveraging the latest in snapshot, de-duplication, compression, and replication technologies we have engineered a bulletproof backup and disaster recovery solution that will ensure we are ready and able to recover quickly and easily from the smallest glitch to the largest disaster.

By duplicating your data between two data centers in near real-time, plus maintaining a nightly versioned copy in a cloud storage facility, we provide nearly unlimited recovery options. We have "ready-to-fly" mirror copies of your servers sitting in a standby data center that we can bring up quickly if the primary data center is taken offline. We can even pull your data out of the cloud to any data center in the world if both the primary and standby data centers are impacted severely at the same time… or we can just spin those servers up in the cloud.

But most of the time it is not major disasters we are fighting… it's the accidental deletion of a few files that threatens our data integrity… and we can recover from those little hiccups as well.

Much thought has been put into engineering a backup solution that will provide the best RPO and RTO options to ensure your business is minimally impacted by even a severe disaster. There are several components involved in building a solution of this caliber. This is not your 20th century tape backup solution, where recovery options where limited, slow, and prone to failure.

Replication and Multiple Data Centers

Our environment consists of physical and networking equipment located in two complete, self-sufficient data centers located 1000 miles apart, supported by different power grids and different Tier-1 Internet providers, but connected via high-speed fiber inter-connects.

We leverage several technologies to maintain a near real-time copy of the platform at the standby data center. Hyper-V replication, clustering, mirroring backups, and Active Directory help ensure the standby datacenter is just minutes behind the production facility and ready to be failed over too if needed.

Take a look at Appendix B – Data Center Replication Environment for a diagram of the replication.

Cloud Storage Backup

In addition to maintaining mirror copies of your servers and data in a standby data center, we also push a daily copy of it up to cloud storage locations on AWS and Azure. We can rebuild the entire platform form these sources either on one of the cloud platforms or on hardware in any data center we choose.

This third-level of protection is far beyond what most companies can or do provide for themselves, but this is why we exist… our sole focus is keeping your application available under any circumstances.

The Greener Option

Leveraging data movement over wires burns far less fossil fuel and emits none of the environmental pollutants that having a vehicle carrying tapes back and forth to a facility does. Embracing our services helps you add the "green" moniker to your business model.

It's All About Options

When you need recovery, a stiff-necked solution where you have one and only one way to do things many times doesn't help. We engineered our approach to provide the maximum amount of versatility when it comes to recovering your data. For all but the most severe of outages, we can recover in less than as few hours to within minutes of the outage event.

By leveraging all of today's best technologies we can provide a Recovery Time Objective of 2-4 hours in most circumstances, even up to losing the primary data center, with data that is no more than 1 hour old.

If both data centers we rendered offline and we would have to fail over into the cloud the Recovery Time Objective could be up to 1 day, and the Recovery Point Objective would be within the last 24 hours as well. Compared to most legacy solutions that would have to request tapes be brought to some location where new hardware existed… our cloud tertiary backup alternative is far superior.

Data Retention

We maintain all client data indefinitely, mirrored between the redundant HA data centers. It is up to the client to define how long this data will be kept in the production environment and when it should be archived down to the client's location for long term archiving.

Appendix A –Policy Changes

Policy	Change From Default
Enforce Password History	6 passwords remembered
Maximum Password Age	60 days
Minimum Password Age	10 days
Minimum Password Length	7 characters
Account Lockout Threshold	5 failed attempts
Account Lockout Duration	30 minutes
Account Lockout Reset After	30 minutes
Audit Account Logon Events	Success, Failure
Audit Logon Events	Success, Failure
Access Computer from Network	Remove Everyone, Add Authenticated Users
Shutdown the System	Remove Power Users, Remove Backup Operators
Rename Administrator Account	Yes
Rename Guest Account	Yes
Restrict CD-ROM Access to Local User	Enabled
Restrict Floppy Access to Local User	Enabled
Display User Information When Locked	Do not display user information
Do Not Display Last User Name	Enabled
Logon Message Title	Authorized Access Only
Logon Message Body	Authorized Access Only!
Prompt User To Change Password	7 days before expiring

Appendix B – Data Center Replication Environment