SoftExpert Cloud Services

ODC-EN0020

REV.13

Info. Clas.: Public

Table of contents

Introduction

With the SoftExpert Cloud Services, you can use SoftExpert Excellence Suite in cloud, allowing you to cut your time-to-market or raise user satisfaction without the usual infrastructure and IT administration costs.

SoftExpert Cloud Services takes advantage of cloud-oriented services and technologies to bring the best experience for our customers, giving them reliability, performance, and security.

The solution is deployed in our world-class cloud environments, located in several locations around the globe, using Amazon AWS as the official Infrastructure as a Service (IaaS) partner.

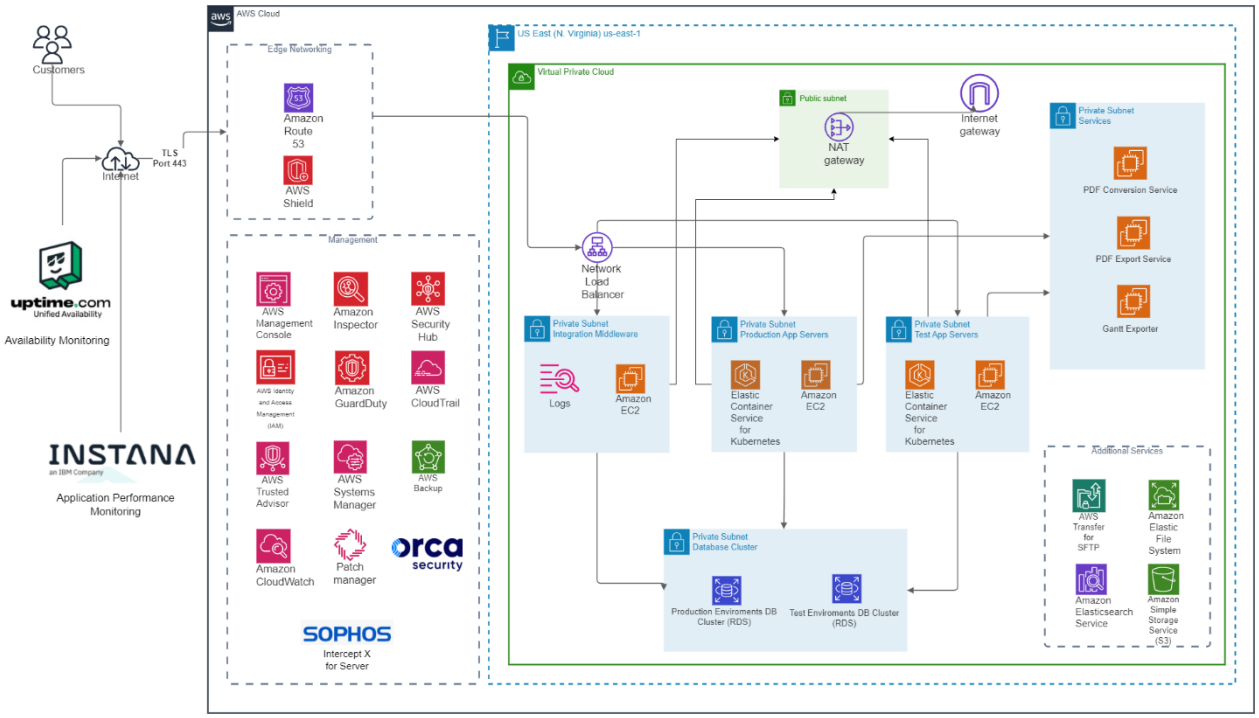
SoftExpert Cloud Services provides significant business benefits by helping with:

- Improve speed to market by relying on our expertise in designing, building, and running large-scale environments/instances.
- Reduce upfront costs by subscribing to infrastructure and management as a service, rather than investing in assets and hiring new personnel.
- Mitigate risk in an environment of rapidly changing technology and security issues.
- Gain the flexibility to embrace innovation as it emerges.
- Software performance optimization including load-balanced application and web servers.
- Environment operating system purchase, maintenance, and licensing
- Solution availability, optimization and assurance needed to support the application.
- Database software purchase, maintenance and licensing are needed to support the application.
- Provide secure and hardened environments built with
    - Host-Based FW & IDS
    - Anti-Virus & Anti-Malware
    - Resiliency & Backup services built in
    - Management of Operating System
    - Network and Firewall configurations
    - Encryption of Data-At-Rest and Data-In-Transit

SoftExpert professionals will maintain the infrastructure necessary to support the solution and will deploy and upgrade your solution, freeing up your IT resources for other strategic initiatives. Plus, you can change and grow your cloud solution when and how you need to.

	On-Premises	**Cloud**
Software Licenses & Annual Maintenance	Customer	SoftExpert
Hardware Purchase, Maintenance & Installation	Customer	SoftExpert
Data Center Costs & Backup	Customer	SoftExpert
Server Software & Installation	Customer	SoftExpert
SoftExpert's Solution Installation & Maintenance	Customer	SoftExpert
IT Staff & Training	Customer	SoftExpert

Cloud Architecture Overview



Architecture Diagram by Region (US)

SoftExpert has Amazon AWS as the certified Cloud Datacenter provider for all of its cloud services.

Access to the application instances/tenants/environment is made through the internet, using secure Internet connection (TLS). SoftExpert constantly updates the TLS protocol version and its ciphers according to the evolution of technologies and security reports.

The connection from end users to our services starts at the domain entry registered in AWS Route 53 (https://<example>.softexpert.com). A Network Load Balancer (NLB) in every region (datacenter location) is associated to the DNS and routes the connection to an application server private subnet.

Only the application servers and our integration middleware servers can be accessed through the internet (NLB routing the requests). All other servers and services support only local network connections between the private subnets.

Security communication for customer's third-party system Integrations

Most clients need to integrate their SoftExpert Cloud Environment with other in-house or third-party systems. SoftExpert provides different rule types to help facilitate integration with our clients' other enterprise systems.

SoftExpert Excellence Suite running on our Cloud includes support for multiple Application and File/Content Integration methods to support both inbound and outbound integration. A full list of currently supported integration methods can be found in our documentation (Integration Guide and Directory Authentication Guide).

When integrations between SoftExpert Cloud Instances and customer´s on premise services are needed, all the services needed for integration MUST be accessible from the public Internet, because you can´t access VPN from SoftExpert Cloud Network. That said, there are many ways to secure your services from unintentional or malicious outside transactions, including:

- **Client Ip Filtering**: SoftExpert maintains a list of their IP Addresses. Customers can configure their firewall/proxy to only allow transactions from this list of approved IP addresses.
- **Authentication**: Customers can use SSL, basic authentication, Oauth and tokens to harden their services against access.
- **Logging and IDS**: Customers may use a logging system and train an Intrusion Detection System to detect unusual patterns. This will help identify and mitigate attacks.

Application Servers

Our application servers are containerized using Elastic Kubernetes Services (EKS) running Linux with autoscaling. The production and test environments are separated into different EKS clusters.

Database Servers

SoftExpert uses the Amazon RDS database as a service, as the official database mechanism for our cloud operation (https://aws.amazon.com/rds/). The database instances are scalable and safe since they are executed in a private and separate subnetwork with data at rest encryption using KMS key.

The data in transit between our application servers and our database servers are all encrypted with SSL/TLS.

Infra-as-a-code

The cloud infrastructure is managed through Infrastructure as a Code (IaC) and stored with revision in our GIT repository. Every cloud server (application and database) is created and maintained using automated pipelines.

- Covers all aspects of software, infrastructure, and client-specific settings.
- Faster time to deploy new environments.
- All change flows through the deployment engine
- Redeploy at any time to exact specs.

Customer Data Storage

SoftExpert uses different cloud services from Amazon to store user data, including:

- Database: All records, configuration and users from the customer's instance are stored in a database.
- Object Storage: Electronic files uploaded in SoftExpert Solution are stored in an Object Storage.
- Full text Search Engine: SoftExpert indexes all content published in customers tenants in an Elastic Search Service.

To check more detailed information about data security, check the "Data Segregation" topic in "Server Models" section of this document.

The backup policy can be checked in the "Data Backup" section of this document.

Deployment Regions

SoftExpert provides you with complete details of where all copies of your data and systems are stored and operated through a completely transparent data location policy. Customers have a designated location in one of Amazon AWS worldwide data centers— typically in the data center physically closest to them (but accommodated to their preferences if necessary).

SoftExpert Cloud Services are currently available to be deployed in the following regions:

Region	**Datacenter Location**
South America	São Paulo
East America	Virginia
Europe	Frankfurt
Asia	Singapore

Instance Models

SoftExpert has 4 different instance models to support all customer needs.

Standard	**Premium** (1)	**Enterprise** (2)	**Regulated** (3)
20 users limit (4)	No user limit (4)	No user limit (4)	No user limit (4)
Multi-Tenant architecture	Multi-Tenant architecture	Single-Tenant architecture	Single-Tenant architecture
One application server running multi-instances	One application server running multi-instances	One application server for each tenant/instance	One application server for each tenant/instance
A single database for each tenant	A single database for each tenant	A single database for each tenant	A single database for each tenant
System updates scheduled by SoftExpert	System updates scheduled by SoftExpert	Customer can decide when software updates will be made(5)	Customer can decide when software updates will be made(5)
Customizations are not supported	Customizations are not supported	Customer can apply customizations	Customer can apply customizations
IP whitelist not available	IP whitelist not available	IP whitelist available	IP whitelist available
No test environment available	Test environments available(6)	Test environments available(6)	Test environments available(6)
			Installation Qualification (IQ)

1 – Former Shared model; 2 – Former Dedicated model; 3 – Former Lifescience model

4 – For all models, the customer MUST provide the max number of concurrent users that will use the solution. Just for the standard model, there is a user max limit.

5 - SoftExpert does not support released versions older than 12 months. For customers with extended support (additional cost), SoftExpert will extend the support for 24 months max. For emergency maintenance (critical issues and vulnerability issues), SoftExpert can require customers with Dedicated and LifeScience servers to approve the maintenance in the same day with the option to block user access to the instance until the maintenance approval.

6 - Additional Cost

Data Segregation

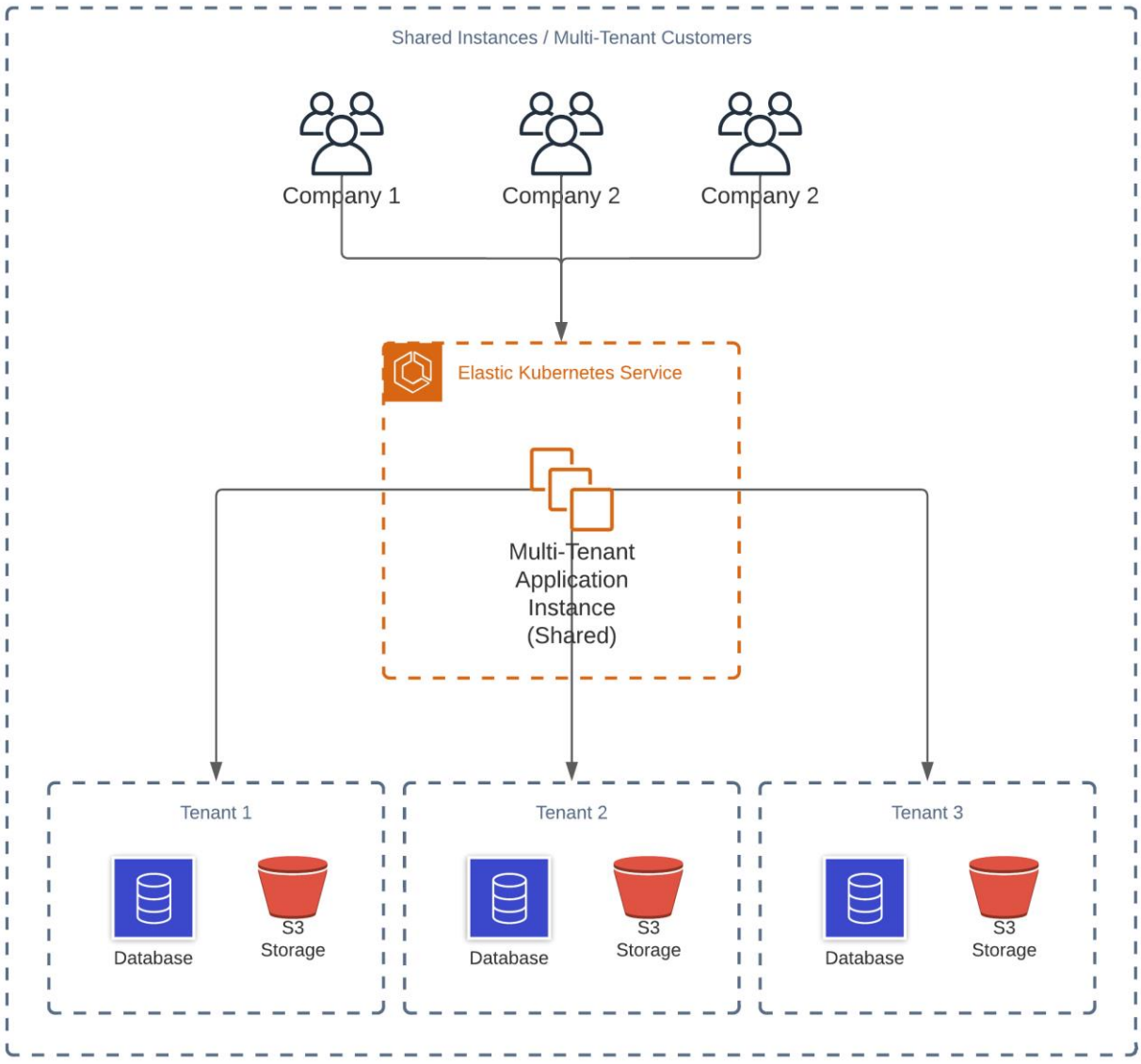
Security and Data Privacy is something SoftExpert takes very seriously.

Considering this concern, all customer data (documents, files, and database records) are segregated in a different database and storage folder/bucket with a credential for each tenant. We do not share the same database using a tenant schema approach. Every instance/tenant has its own database file and credentials.

All customer data is stored within the same region (Datacenter Location) as selected in the contract. Considering Data Privacy compliances, SoftExpert does not transfer customer's data to different regions.

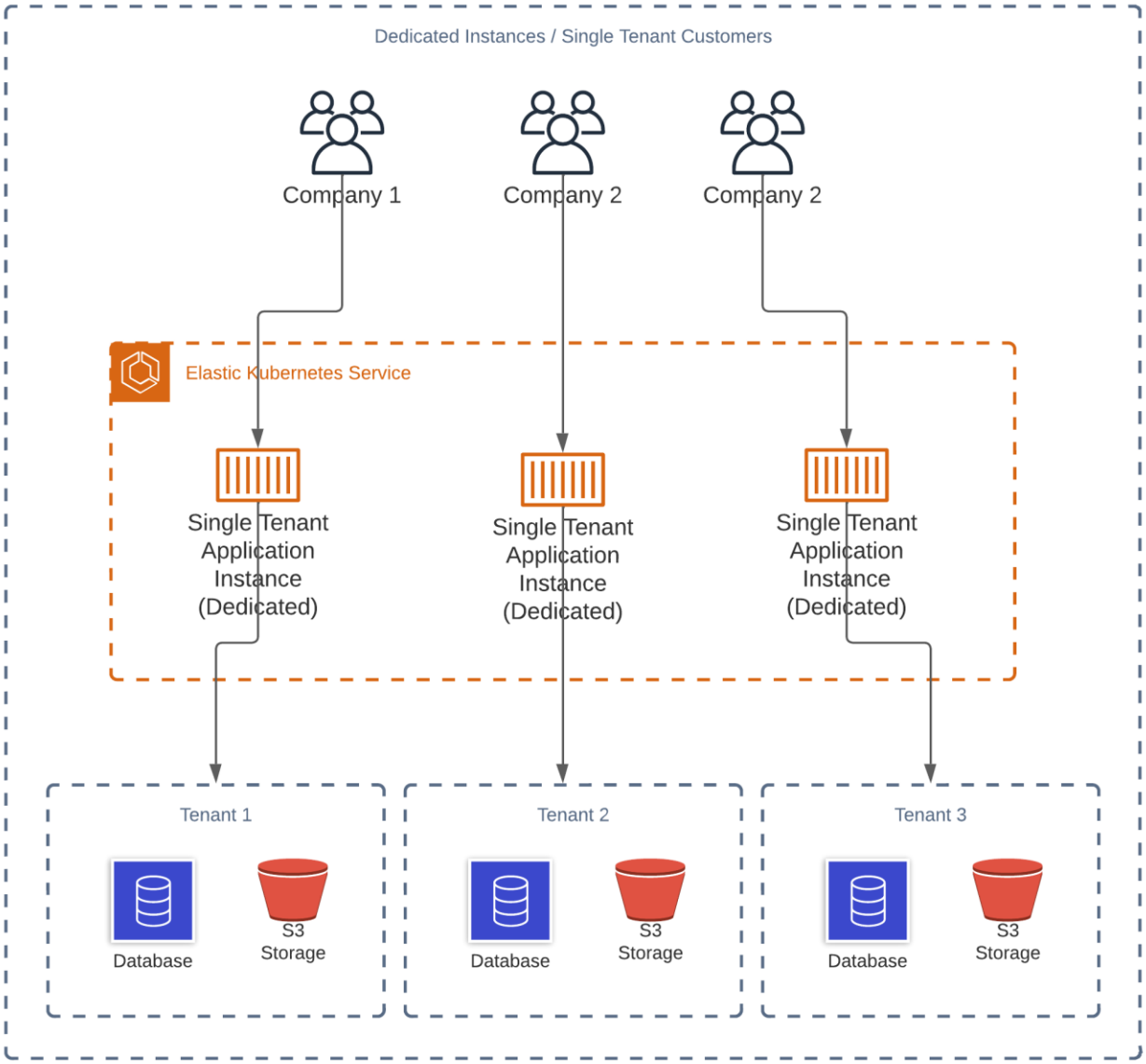
Standard / Premium instances

In these models, the solution runs in a multi-Tenant model, where the applications servers are shared throughout all customers. We run our multi-Tenant servers as container Pods and each application server running in these pods supports multiple instances/tenants sharing the same Pod and application server.



Enterprise / Regulated instances

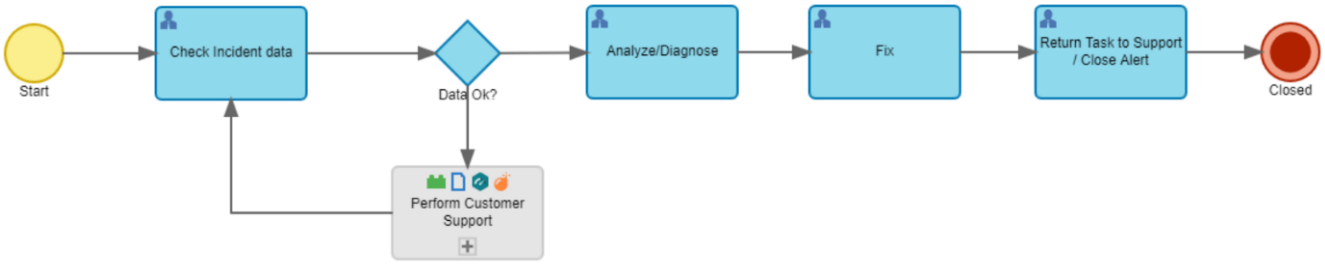
In these models, the solution runs in a Single-Tenant model, where there is an application server running as a container Pod for each tenant. This model gives more flexibility to our customers to decide when they want to update their system.



Incident Management

SoftExpert Cloud Services incidents can be triggered by our monitoring operation (check the “System Monitoring” section) or customers using our support channel.

SoftExpert Cloud Services relies on IaC (infrastructure as a code), and we have a lot of automation scripts that can be triggered to put tenants online if something goes wrong with the infrastructure.

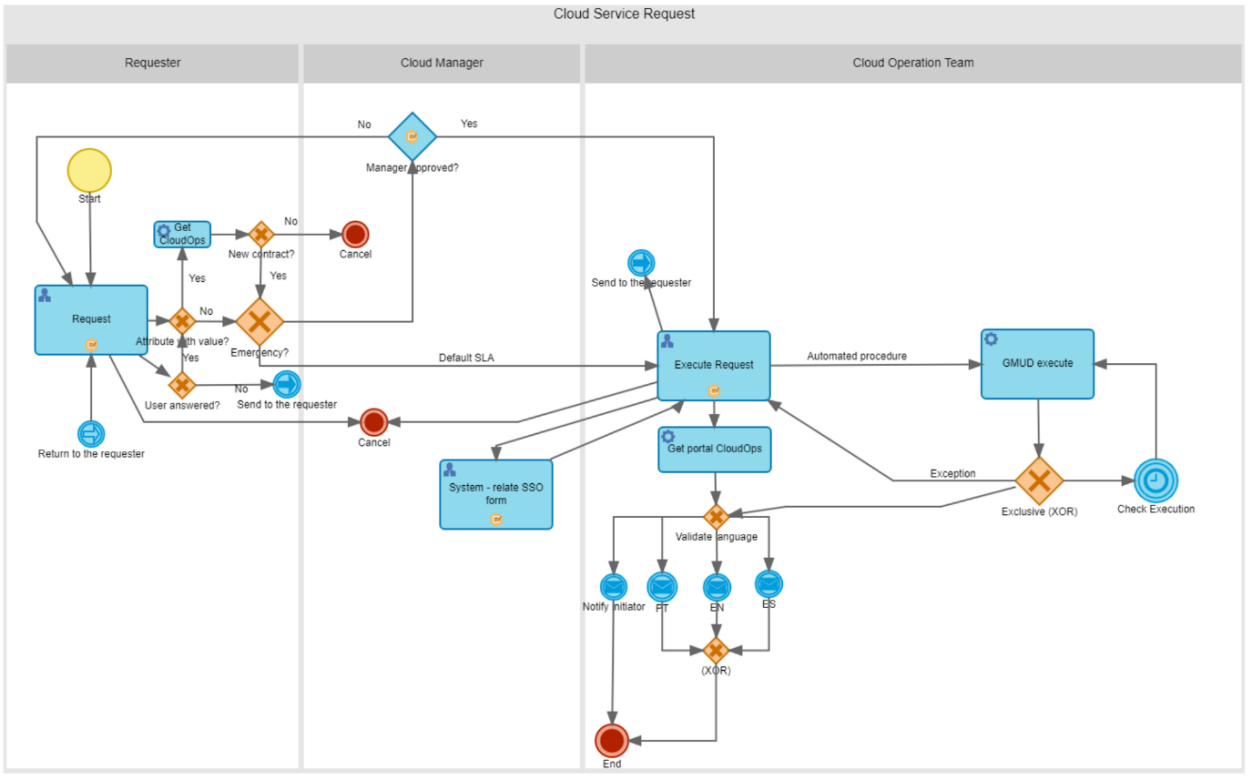


Change Management

Periodic system maintenance is essential to maintaining the on-going stability and security of your SoftExpert Cloud Services environments, as well as to the evolution of SoftExpert Excellence Suite. Periodic maintenance ensures your cloud environments stay up to date with software updates and patches and can make use of the latest features and services included in the new released versions.

SoftExpert is responsible for the administration and for executing every change in customers environments/instances, including applying software updates/patches, or any change in cloud infrastructure. SoftExpert will strive to minimize the impact of maintenance to your cloud environment and its availability.

SoftExpert has a formal process for change management that is certified and audited every year. Every change in cloud environments has a process instance for traceability and compliance.

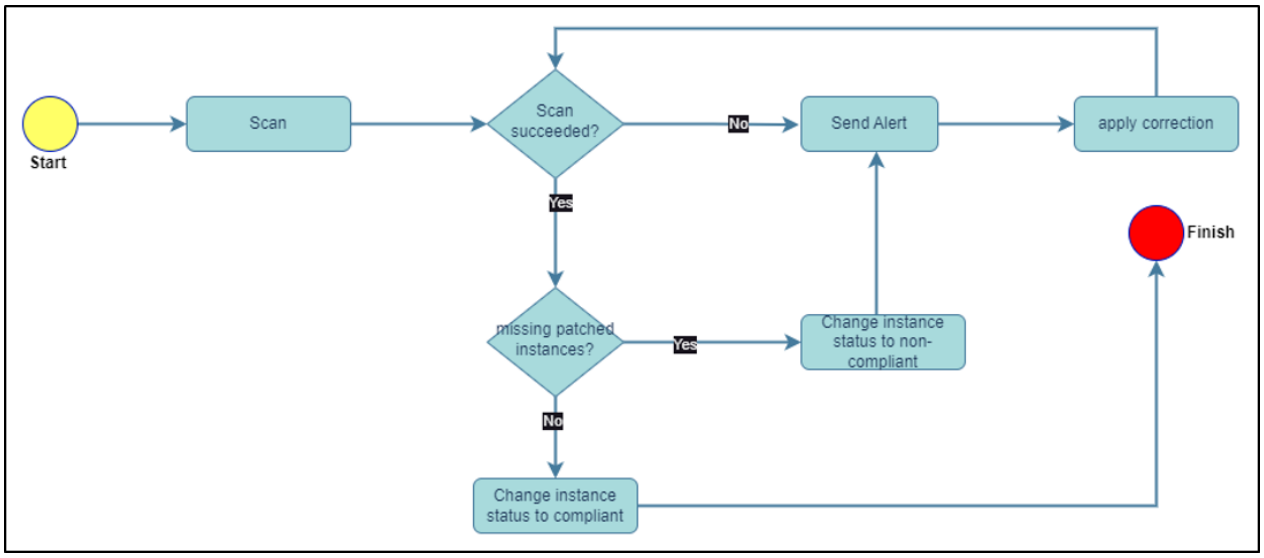


Change control process

The changes / maintenance requests can be started by SoftExpert or the Customer. To request a change in your environment (ex: Apply patch fix, or update major version of the solution), the customer must open a Support Ticket. Check the list of the available change requests in the section “Change Requests and Service Level Agreement”.

Patch Manager

We use automated resources for patch application, update, and corrections of vulnerabilities in our infrastructure, maintaining the instances in compliance with the last available security recommendations.



Patch Manager Fluxogram

The Patch Manager generates alerts when there is a new update of patches available to be applied; they are applied recurrently when there is no need for downtime. When some unavailability is identified in advance, a notice is sent to the affected customers, for execution on a technical window with prior scheduling.

Maintenance types

There are two types of maintenance for SoftExpert Cloud Services: standard maintenance and emergency maintenance. This section describes the differences between the two types of maintenance.

Standard maintenance includes all scheduled SoftExpert Cloud Services update and upgrade events including:

- Cloud infrastructure updates: Updates the supporting infrastructure services of each environment, including the database, to include the latest security and performance benefits, service enhancements, and new capabilities. Infrastructure updates do not change the SoftExpert software running in the Cloud environment. Some changes that usually are made: Copy production data to the test environment, Apply server software updates (web server, app server, requirements, protocols). If downtime is scheduled outside the technical windows, any Enterprise/Regulated or Standard/Premium customer (production and testing) that will be affected must be informed of it at least 2 working days in advance and be provided with information concerning date, time, and reason.
- SoftExpert Software Updates: SoftExpert applies cumulative SoftExpert Excellence Suite patches or Major version updates to your environments. Some changes that usually are made: Apply patch fix, update major version, apply customization, Execute Database script.

Emergency maintenance includes all maintenance performed with immediate or near-immediate timing to remediate or avoid an incident, or to address modifications as mandated by SoftExpert. This maintenance may be performed outside of a maintenance window. SoftExpert will attempt to provide but cannot guarantee delivery of advanced notification for an emergency maintenance event. Examples of emergency activities include:

- Critical Hotfix Deployment: SoftExpert installs software hotfixes that SoftExpert deems critical to the continued availability and security of your SoftExpert Cloud Services. Critical hotfixes address issues that may compromise the availability, stability, or security of the system, and your installation is not optional. Critical hotfixes may be deployed with little to no advance notice to remediate or avoid an incident. While these hotfixes are not optional, SoftExpert will take reasonable steps to reduce the disruption of these changes to your SoftExpert Cloud Services systems.

Customers approval for maintenance tasks and change control

For Standard maintenance, customers with Enterprise or Regulated instance models **MUST APPROVE** the change/maintenance. SoftExpert will not execute any changes in these environments (for standard maintenance) without explicit approval of customers.

For customers with Standard or Premium instance model, the standard maintenance and changes will be made without the need for any approval.

> Emergency maintenance will be made without the need of approval of our customers, even when the customer has Dedicated or LifeScience server model.

All necessary changes performed within the Cloud infrastructure, due to customer requests or technical needs of the Cloud administration team, can be traced.

Maintenance Window

SoftExpert makes a reasonable effort to not undertake scheduled standard maintenance that falls outside of your standard maintenance window and will try to not undertake scheduled standard maintenance for more than 8 hours a month.

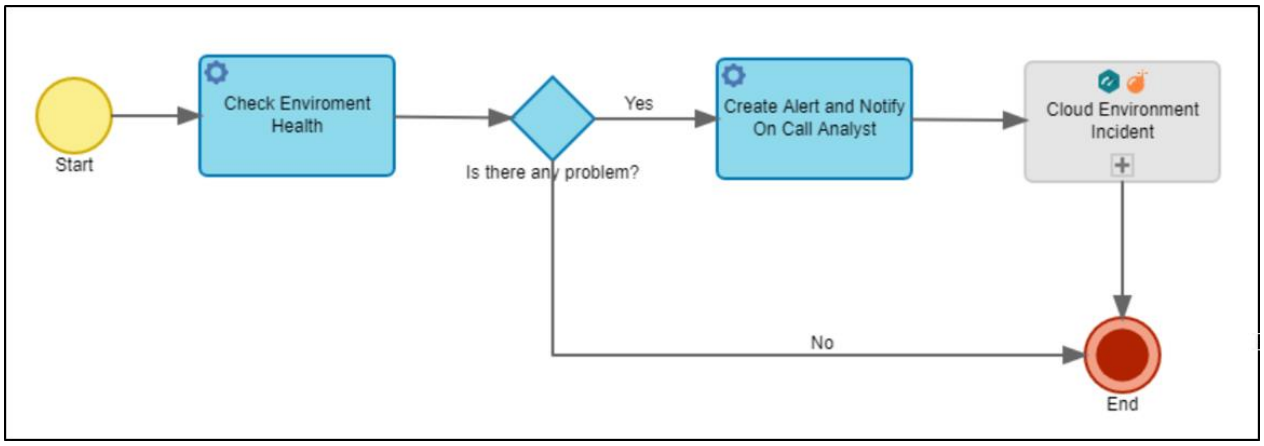
SoftExpert performs maintenance activities that are near zero-downtime during the scheduled standard maintenance window on weekdays between 08:00 p.m. and 5:00 a.m. or weekends between 09:00 am and 12:00pm local time in the Amazon AWS Region of the deployed environment. Most maintenance activity typically last a few hours.

Change Requests and Service Level Agreement

Service	SLA
Apply Patch FIX (4º digit)	same day
Update Major Version (1º, 2º e 3º digit)	2 days
Apply Customization Package	1 day
Execute Database Script	2 days
Refresh Database (copy prod data to test env)	1 day
Provide Database Backup for Download	15 days
Restore Database Backup(1)	5 days
Change Server Configuration	same day
Reset Admin Password	same day
DNS Configuration	same day
Configure mail server settings	same day
Restart Environment	same day
Increase Storage Size	2 days
Request Installation Qualification IQ	10 days
Request Availability Reports	2 days

1 - The Restore Database Backup is a service available only when a customer did a change in his application data that needs to be restored. If there is a problem with SoftExpert Cloud Services and the data needs to be restored, the SLA will be different as described in “Data Backup” and “Disaster Recovery” sections. Note: Only full database restore backup will be made.

System Monitoring



SoftExpert maintenance, monitoring, and support are managed by our Cloud Operation Team.

The cloud operation team provides:

- Environment monitoring and management with proactive response to infrastructure issues and failures, resource utilization issues and tuning of environments.
- Network monitoring and management, including firewall and security group configuration and network and system level access monitoring.

We monitor the health of all services, performance, availability, and security, using:

- Amazon AWS CloudWatch for server and database monitoring
- Amazon RDS Performance Insights to monitor database performance.
- IBM Instana for application performance monitoring - APM
- Uptime.com to check each customer's instance/tenant availability using different locations.
- Amazon GuardDuty for intelligent threat detection
- Amazon Security Hub to aggregate and give a security report using some compliance frameworks.
- Amazon Inspector for automatic vulnerability management, software vulnerability Search, and unintentional network exposure.
- Sophos CloudOptix to aggregate all security alerts coming from all sources including amazon services, endpoint security and firewall.
- Amazon Config for configuration manager in accordance with compliance frameworks

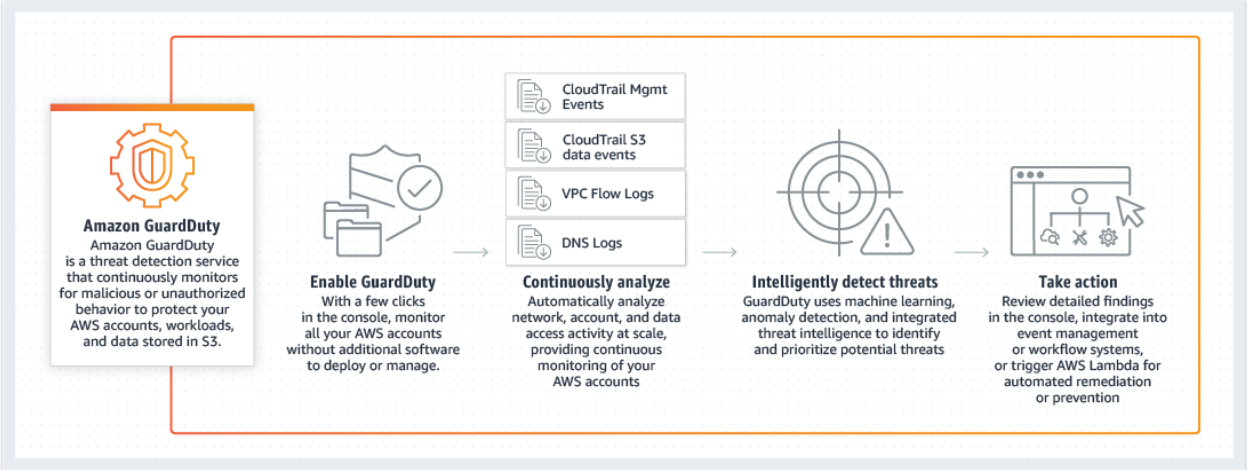
- Orca Security is a Cloud-Native Application Protection Platform (CNAPP) that stands out in the industry that identifies, prioritizes and fix safety and compliance issues in the entire cloud workload, without need for an agent.

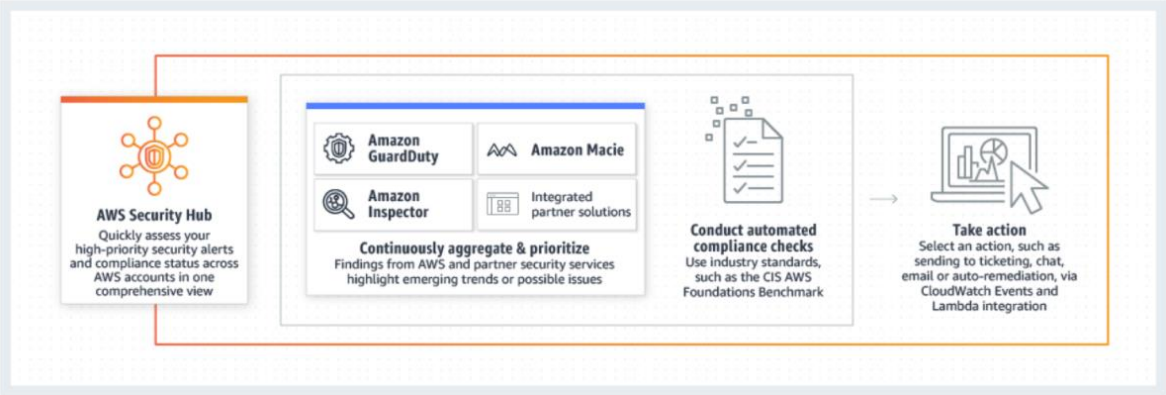
Security Monitoring

SoftExpert uses the best tools and services provided by our cloud partner (Amazon AWS) to monitor infrastructure security threats. These services are continuous monitoring all logs and data traffic using AI and machine learning, as detailed in the next diagrams.

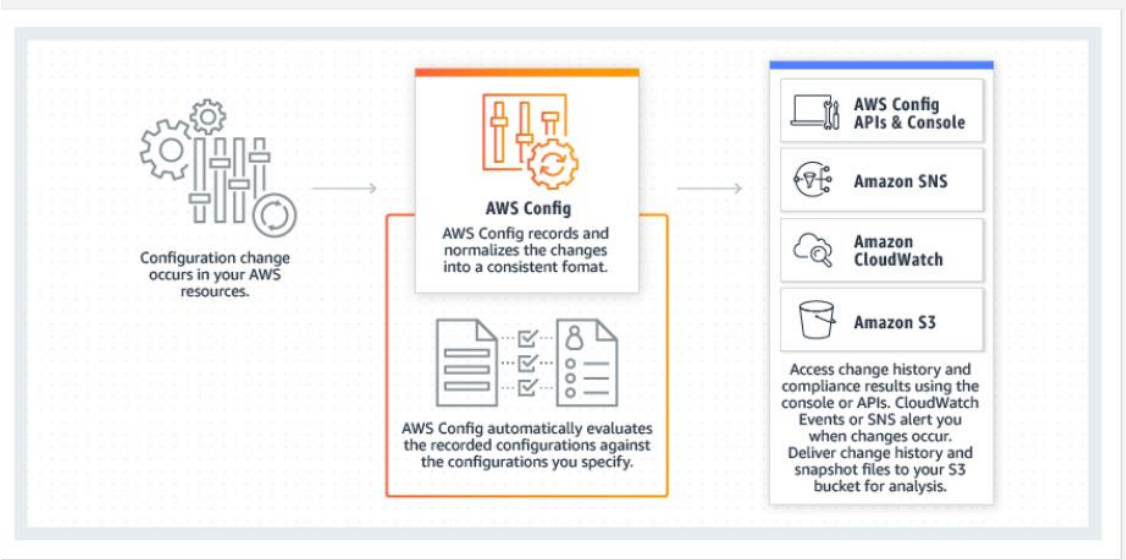
The security control frameworks that SoftExpert currently uses are the CIS, ISO 27001, and Amazon AWS Foundational Security Best Practices.

- https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cis-controls.html
- https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp-controls.html




AWS Security Hub
Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view
Amazon GuardDuty
Amazon Macie
Amazon Inspector
Integrated partner solutions
Continuously aggregate & prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues
Conduct automated compliance checks
Use industry standards, such as the CIS AWS Foundations Benchmark
Take action
Select an action, such as sending to ticketing, chat, email or auto-remediation, via CloudWatch Events and Lambda integration


Amazon Inspector
An automated security vulnerability management service that continually evaluates your resources for software vulnerabilities and unintended network exposure
Enable Amazon Inspector
Get started with a few clicks and use AWS Organizations for multi-account management
Automated workload discovery
Continual scanning
Maintained vulnerability database
Near real-time results
Discover and scan
Auto-discover AWS workloads and continually scan them for vulnerabilities
Contextualize findings
Consider many factors to create a meaningful Inspector risk score
Amazon Inspector
AWS Security Hub
Amazon EventBridge
Amazon ECR
APN Partners
Take action
Use detailed findings to automate workflows like ticketing and remediation


Configuration change occurs in your AWS resources.
AWS Config
AWS Config records and normalizes the changes into a consistent fomat.
AWS Config automatically evaluates the recorded configurations against the configurations you specify.
AWS Config APIs & Console
Amazon SNS
Amazon CloudWatch
Amazon S3
Access change history and compliance results using the console or APIs. CloudWatch Events or SNS alert you when changes occur. Deliver change history and snapshot files to your S3 bucket for analysis.

Data Backup

SoftExpert Cloud relies on Amazon AWS backup procedures and tools to safeguard customer data. All backup policies and procedures are configured using Amazon AWS Backup (https://aws.amazon.com/backup).

For database data, SoftExpert uses the automated backup feature of Amazon RDS (https://aws.amazon.com/rds/features/backup). The default retention policy used for the tenant's production databases is 10 days + 3 monthly copies (1st day of the last 3 months). The default retention policy used for the tenant's test databases is 10 days. The Recovery Point Objective (RPO) is approximately 10 minutes (RPO is the targeted amount of time during which data is at risk for loss in the event of a failure).

For electronic files, SoftExpert uses Amazon AWS S3 versioning feature and the default retention policy for the tenants / customer instances is 180 days.

Both Database and electronic files backups have high levels of resiliency, with 99,999999999% durability across multiple Availability Zones. The backups are resilient against events that impact an entire Availability Zone, like a fire incident.

The backups are encrypted (data at rest) through the AWS Key Manager Service (KMS). The algorithm used is the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your RDS instance.

To check more detailed information about different ways to store customer the data in our Cloud, check the "Customer Data Storage" topic in "Cloud Architecture Overview" section of this document.

Data Retention Policy after Contract Termination

After the contract is terminated, the customer data is stored for up to 365 days for safeguard reasons (some customers may forget to ask for their data). Within this period, customers may request their data for download (database and electronic files will be made available for download through a private link valid for 10 days).

During the 365-day period, the customer may request the definitive deletion of their data. Their data will be automatically deleted after a period of 365 days, without the possibility of recovering it.

Disaster Recovery

SoftExpert Cloud Service delivers two important elements to support business continuity:

- Recovery Point Objective: If the system unexpectedly goes down without warning, a certain amount of data may be lost between the point of failure and the last backup. The recovery point objective is the amount of time that elapses during which data cannot be recovered.
    - For database, the RPO is 10 minutes. And the electronic files are the last version of the file.
- Recovery Time Objective: When a system experiences downtime, the relevant technical team requires a period of time to not only restart the systems, but also to identify and fix any lingering issues with the infrastructure. The recovery time objective represents the time required to restore the SoftExpert Cloud services.

SoftExpert is committed to the preventive safeguarding of the SoftExpert Cloud Services network and the high availability of SoftExpert Cloud Services client applications. This commitment includes working to prevent Severity 4 incidents for databases and electronic files that could have significant business impact for multiple SoftExpert Cloud Services clients.

- SoftExpert´s cloud operation disaster recovery is audited by external auditors, and we can share the certificate with our customers.
- We will not provide disaster recovery reports with any customers for safety reasons, since it may have sensitive data of our cloud infrastructure.

Data recovery

The SoftExpert Cloud Services data recovery has the recovery point objective (RPO) of approximately 10 minutes. This is the maximum amount of time during which data might be lost. The recovery time objective (RTO) is approximately 4 hours. This is the targeted time to restore the client's cloud service.

Physical disasters

SoftExpert Cloud Services client environments are hosted by Amazon Web Services (AWS). Physical disaster impacts on SoftExpert Cloud Services client environments are extremely unlikely.

In case of a physical disaster, considering that all backups are stored in multiple Availability Zones using point-in-time recovery, SoftExpert will deploy new services and servers in a different physical site.

Plan information

SoftExpert Cloud Services has disaster recovery plans that include roles, responsibilities, activation, response, recovery, reconstitution, and validation of SoftExpert Cloud Services environments. SoftExpert Cloud Services regularly test these plans.

Prepared response

SoftExpert Cloud Services offers 24x7x365 situational awareness monitoring and is prepared to activate disaster recovery plans with disaster recovery team response within moments of any disastrous incident. Response bridge calls would include disaster recovery responders and clients, as appropriate.

Announcements for major events

In case of any events that generate major unavailability, impacts, and require SoftExpert Cloud Services to issue a notice, the message will be sent by e-mail to all affected customers.

As the entire structure of SoftExpert Cloud Services is in IaC and pipelines, the entire restoration process in the event of a disaster is also done in IaC and pipelines. This guarantees a standardized re-creation as implemented like application, database, firewall and network structure.

Security standards and Compliances

SoftExpert has testing routines incorporated into its product development cycle to ensure compliance with best security practices, using static code analysis tools and pen testing (application and Cloud Infrastructure) through independent companies.

We follow best practices and apply tests recommended by the OWASP organization (https://owasp.org/).

The Information Security and Privacy policies are revised once a year (or more, if needed) and trained at each revision. The trainings Personal Data Protection and Fundamentals of Information Security include tests at the end of the training.

We are ISO 9001 and ISO 27001:2022 certified, guaranteeing compliance and quality standards required by the norm, including risk management as well as procedures for all operations performed in our cloud environment.

SoftExpert works following the best practices recommended by Amazon AWS Well-Architected Framework. This guideline/framework assures operational excellence, security, reliability and efficiency (https://aws.amazon.com//architecture/well-architected/).

Secure communication

All access to the application instances/tenants/environment is made through the internet, using secure connection (TLS 1.3).

Ciphers used for the encryption:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

How SoftExpert treats vulnerabilities issues

All critical and high-risk items (OWASP classification) are analyzed on an emergency basis. The team of engineers (product and cloud operation) will assess how to mitigate the problem and as soon as there is a fix in the product, customers will be informed through release notes or patch bulletin.

For medium and low risk items, SoftExpert will be defining the mitigation schedule as per its product roadmap.

In addition to SoftExpert's proactive work in monitoring vulnerabilities, we encourage customers who identify a security flaw in the solution to create a support ticket.

We know that some vulnerabilities are complex to find a solution and SoftExpert is committed to analyze all vulnerabilities and find a way to mitigate the issue (blocking the feature) even that the product fix would take more time to be released.

For more details on the OWASP risk rating, visit https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Technical and organizational measures implemented

SoftExpert encrypts all data at rest in an Environment using 256-bit AES encryption. SoftExpert Cloud Services provide functionality for data in transit encryption with https (TLS) and digital certificates.

During the term of the Subscription Services, SoftExpert will notify clients without undue delay (unless otherwise required under applicable law) when SoftExpert confirms any actual security incident affecting the confidentiality, integrity, or availability of client data.

SoftExpert is also responsible for:

- Establishing security group configurations for secure client access
- Host-based Intrusion Prevention System (IPS) and File Integrity Monitoring
- Protecting data in transit over the Internet
- Providing host-based virus protection services, scans, and signature updates.
- Monitoring the security of the infrastructure components in each tenant / environment

Third-party vulnerability reports

We use specialist security services companies to complete penetration tests of our products and other systems at least 1 time every year.

Due to the extensive internal information made available to the testers in conducting these penetration tests, we don't provide full reports. Letter of Assessment from our Penetration Testing partners will be available for our customers, proving that security tests are being made every year.

Any findings from these assessments will be triaged and remediated according to "How SoftExpert treats vulnerability issues".

Physical and environmental controls

SoftExpert uses a third party (currently Amazon Web Services [AWS]) as its Infrastructure-as-a-Service (IaaS) provider, which hosts SoftExpert Cloud Services environments in state-of-the-art, large-scale, secure data centers.

The IAAS provides physical and environmental security controls for cloud infrastructure. SoftExpert Cloud Services inherits these controls as part of the shared security model. See the IAAS provider website for summary of controls with current IAAS provider (currently Amazon Cloud Security).

Identity and Access Management

All administration of SoftExpert Cloud environments is done through a control panel, using role-based access control with multi-factor authentication.

Multi factor Authentication (MFA) is required for all SoftExpert's Cloud professionals. With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (username and password) and the OTP to access our Cloud Infrastructure Console.

Network access to the datacenter is only available through VPN, using a bastion host. It is not possible to access Cloud servers directly through our local network.

Network and infrastructure controls

SoftExpert Cloud Services network architecture provides a level of security that provides:

- Virtual network devices to establish the boundaries, network rulesets, and access controls to govern inbound and outbound traffic in any client environment.
- Network security controls that limit access from untrusted sources.
- Network architecture that limits the effects of distributed denial-of-service (DDoS) attacks.
- SoftExpert Cloud Services deploys anti-malware software on the SoftExpert infrastructure level.

Operation System Hardening

Hardening of the OS is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services. This is done to minimize a computer OS's exposure to threats and to mitigate possible risk.

SoftExpert follows CIS (https://www.cisecurity.org/benchmark/amazon_web_services/) guidelines, including:

- Removing all unnecessary and unused programs in OS. SoftExpert disables/uninstall all programs and services that are not used in the operation system.
- Configuring audit trail and logs for every access and changes made, and log protection procedures. SoftExpert relies on Amazon CloudTrail to store and access all operations and configurations that are made in every service and server.
- Network and firewall (security group) configuration to block any protocol that SoftExpert Cloud Services does not use or public access coming from internet.
- Access, Authentication and Authorization hardening, including strong access keys, credentials rotation, individual identities, least privilege access grant.

Encryption Keys

Our key management for services that use and require encryption is AWS-native – KMS (Key Management Service). In our case, as S3 buckets, EBS disks and RDS disks.

Keys are used by AWS services or instances.

All keys are created, rotated, and discarded automatically. Policies are managed by the AWS KMS itself.

AWS KMS integrates with AWS CloudTrail to provide logs containing all key usage to help meet compliance and regulatory requirements.

https://aws.amazon.com/pt/kms/

Internet Egress Ips

If authorization is required for public IPs on calls to restricted destinations originating from our cloud to a customer's resource, such as a web service, API server or DNATs, we have fixed IPs that concentrate internet outbounds, making these releases easier. See below the IPs and their corresponding application datacenter:

FQDN	IP	Datacenter Region
gw1-sa-east-1.softexpert.com	54.207.102.240	South America
gw2-sa-east-1.softexpert.com	54.94.83.9	South America
gw3-sa-east-1.softexpert.com	54.207.164.67	South America
gw1-us-east-1.softexpert.com	34.196.191.124	US East
gw2-us-east-1.softexpert.com	34.196.65.152	US East
gw3-us-east-1.softexpert.com	54.165.49.15	US East
gw1-eu-central-1.softexpert.com	35.156.225.178	Europe
gw2-eu-central-1.softexpert.com	3.67.15.205	Europe
gw3-eu-central-1.softexpert.com	3.71.223.177	Europe
gw1-ap-southeast-1.softexpert.com	52.74.181.166	Asia
gw2-ap-southeast-1.softexpert.com	3.1.147.171	Asia
gw3-ap-southeast-1.softexpert.com	54.151.144.111	Asia