ToolsGroup Cloud Security Overview

toolsgroup | Be ready for anything

Index

Introduction

This document provides an overview of ToolsGroup's regulatory compliance, certifications and supporting processes that are designed to protect and secure data in its Cloud Systems. ToolsGroup is committed to safeguarding its data and measuring its security system's performance against and in compliance with the highest security standards. ToolsGroup tightly integrates vulnerability management with its operations systems by continuously monitoring emerging industry threats and using this information to adapt and improve its day-to-day security policies and procedures.

This document and the information contained within are confidential.

Software as a Service - Overview

ToolsGroup provides the Software as a Service (SaaS) version of its solution in a single-tenant architecture, completely isolated from other customers.

ToolsGroup uses Microsoft Azure as a hosting provider for its solution. Over the years, ToolsGroup, with its close partnership with Microsoft, has developed a specialized architecture that is able to leverage the advantages of the Azure Cloud in order to deliver high performance, scalability and security.

Security is an integral facet of ToolsGroup's Solution and Cloud service. To ensure the highest level of security, ToolsGroup employs multiple layers of authentication, encryption, vulnerability monitoring and scanning, as well as sound, secure and audited operational practices.

+ ToolsGroup Software as a Service (SaaS)

Data Center and Security

ToolsGroup delivers its Software as a Service solution from Microsoft Azure data centers. Microsoft Azure's geographical reach allows us to bring the solution closer to users around the world, thus preserving data residency and offering comprehensive compliance and resilience guarantees for customers.

Microsoft designs, builds and operates datacenters in a way that strictly controls physical access to the areas where your data is stored.

Microsoft has hundreds of Azure datacenters in 54 regions (as of 2019), and each of these has extensive multilayered protections to ensure unauthorized users cannot gain physical access to your customer data. Physical security reviews of the facilities are conducted periodically to ensure the datacenters properly fulfill Azure security requirements.

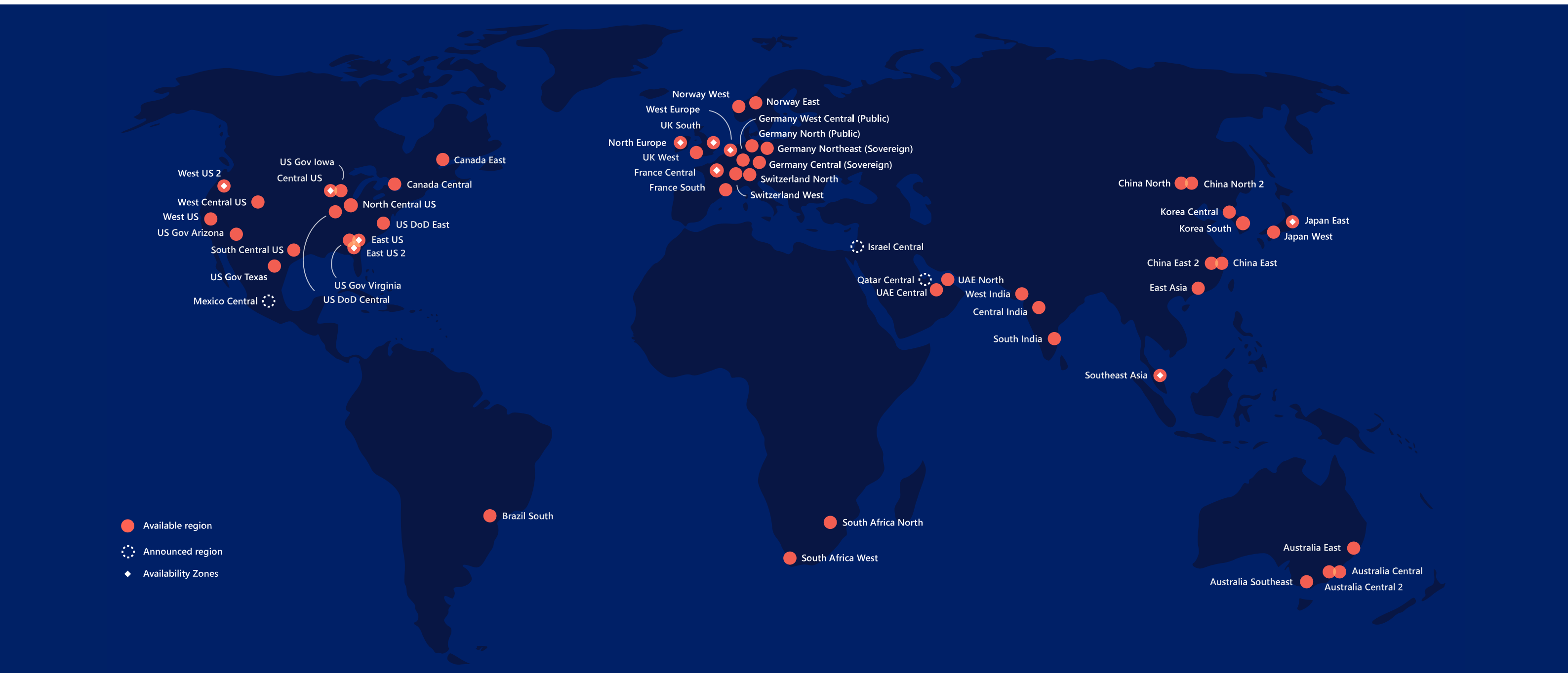
Microsoft Azure meets an extensive set of global and industry-specific standards and key regulations, including for example ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3 Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, and the CS Mark in Japan.

ToolsGroup leverages the extensive capabilities offered by the Azure Cloud to ensure that the Solution is delivered with the highest security standards in the industry.

Microsoft Azure data centers are designed to be fully redundant in terms of network, storage, power and cooling and they are located in areas ofminimal risk as regards natural disasters.

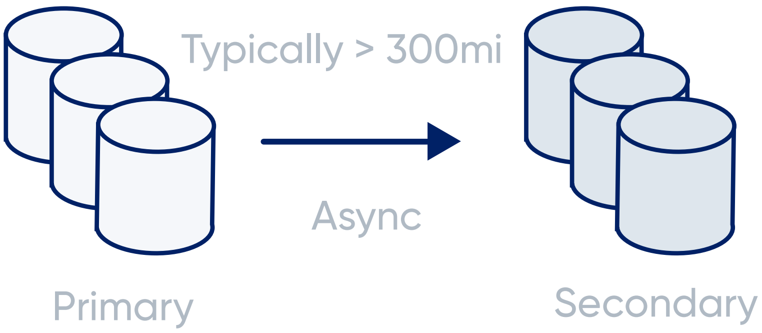
Microsoft takes a layered approach to physical security, so as to reduce the risk of unauthorized users gaining physical access to data and data center resources. For additional details of the security measures implemented by Microsoft, refer to: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Fig. 1 - Microsoft Azure Regions



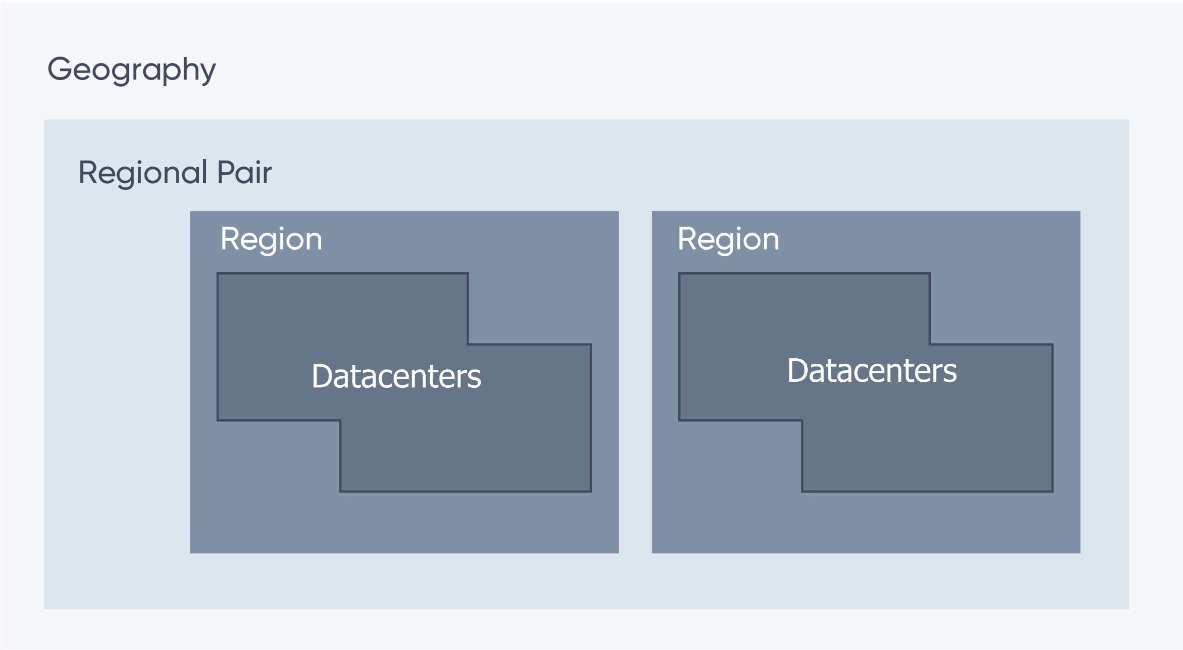
+ Service and Data Redundancy

ToolsGroup ensures, with the support of Azure's capabilities, that each Customer's data is redundant at multiple levels. Any data stored in the Solution is maintained with multiple redundant copies in the Primary Region, as well as Geo Replicated asynchronously to a Secondary Region.



The Secondary Region used for Geo Replication is based on the Affinity to the Primary Region. For more details see: https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions

Fig. 3 Azure Paired Regions



ToolsGroup guarantees the availability and continuity of the service and backs this with service level agreements (SLA). A Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of 24 Hours come standard with any plan.

+ Data Security

Customer Data

The Customer is the exclusive owner of the Customer Data present in the Solution and is responsible for Data Classification and Governance. ToolsGroup Operators will have access to Customer Data only for purposes compatible with providing the contracted services. These may include troubleshooting aimed at improving features, assisting the Customer with specific requests, or preventing, detecting or repairing problems affecting the operation of the Solution.

Subcontractors can access and use customer data only to deliver the services they were hired to provide. ToolsGroup discloses the names of subcontractors who have access to customer data and provides advance notice of new subcontractors.

Data Isolation

ToolsGroup provides Customers with a Single Tenant solution. Each Customer environment is completely separate from other Customers, and ToolsGroup ensures that your Customer Data is not combined with anyone else's.

Data Encryption

ToolsGroup uses strong encryption both for data in transit and data stored at rest. This includes data stored in backups or geo replicated to a secondary region.

All data transmitted from the Solution is encrypted in transit using Transport Level Security (TLS). The list of ciphers and protocols is constantly monitored as part of a Vulnerability Management process to ensure that they meet or exceed industry standards and are not affected by any known vulnerabilities.

/ Data At Rest

All data stored on the Solution is encrypted using AES-256, with Keys controlled by ToolsGroup and separate for each Customer.

/ Data In Transit

All data in transit is protected using TLS, with a minimum key length for certificates of 4096-bit RSA.

+ Operational Security in the ToolsGroup Cloud

Solution Sizing and Scaling

The Solution is sized in standard tiers (small, medium, large) to support the most common deployment scenarios. The Solution can be scaled further beyond those standard tiers based on Customer requirements. The scaling process typically requires a short maintenance window and can be performed off-hours to limit any business impact.

Passwords

When not using federated authentication, any passwords used as part of the Solution will need to meet some complexity requirements. It must contain:

- At least eight characters.
- Both upper and lower case letters.
- At least one number.
- At least one special character.

Additionally, passwords must not be reused, nor may variations of previous passwords be used.

After five consecutive failed login attempts, the account will be locked for 30 minutes as a security precaution against brute force attacks.

Audit Logging

ToolsGroup logs all accesses to the Solution, as well as security activities performed on systems. All logs coming from authentication systems, applications, network devices, servers and other components of the Solution are stored centrally and monitored by a security information and event management (SIEM) that is capable of warning ToolsGroup Operators of any activity exceeding set thresholds.

Audit events (such as logon, logoffs, and security or permissions changes) are stored in an inalterable form for 180 days to assist in security investigations.

Change Management

ToolsGroup maintains structured procedures on how to manage changes on systems supporting the Solution. This includes a change management process that requires formalized requests on the Ticketing Support Portal, a process to evaluate the impact of changes.

+ ToolsGroup Operators

ToolsGroup Operators working on the systems supporting the Solution are working from secured locations, connecting with TLS to the systems and using Multi Factor Authentication (MFA) for all sensitive operations. All ToolsGroup Workstations are using Full Disk Encryption and have no access to Customer Data.

+ Disaster Recovery and Business Continuity

ToolsGroup maintains up-to-date plans to manage the most common scenarios that can affect business continuity. These plans are tested yearly or more frequently if required by any significant change to the affected process and audited yearly as part of ToolsGroup's ISO 27001 certification process.

To support this, and provide resiliency to the Solution, ToolsGroup provides business continuity in the following ways:

- High availability for the underlying infrastructure and components.
- Disaster Recovery in a secondary region.
- Frequent Backups with multiple redundant copies.
- Comprehensive monitoring to detect anomalies and events relating to outages and other events that may require immediate action. The monitoring system collects data from all systems that compose the Solution and can also issue alerts related to hardware and network capacity as well as security events and attacks.

Data that composes the Solution is organized in three layers:

1. **Virtualization layer**

   Data related to the Virtual Machines that support Solution components is encrypted at rest, replicated in multiple local copies and Geo-redundant.

2. **Instance layer**

   Using Azure native functionalities, ToolsGroup performs a full backup for the individual compute note or virtual machine that is kept for 15 days rolling. These backups are stored in multiple copies, Geo-redundant and encrypted at rest.

3. **Application data layer**

   This includes Customer Data stored inside the Solution and is backed up daily and kept for 15 days rolling.

+ Security Incident Management

ToolsGroup maintains policies and procedures to detect, manage and track any security incidents or events. The primary aim is the prompt detection of any incident or potential incident to reduce the risk of information exposure and to promptly communicate any breaches to all affected Parties and Authorities in the shortest time frame possible.

To support this process ToolsGroup has implemented:

- A security incident response plan that clearly defines tasks and activities that need to be carried out to properly evaluate, classify, mitigate and respond to security incidents.
- The definition of security-related roles and responsibilities within the organization, including the role of Information Security Manager and an oversight committee.
- Processes aimed at the continuous improvement of security-related aspects in the Organization that include the period review of existing measures and their effectiveness.

+ Compliance

Compliance plays a critical role in providing assurance for Customers and in securing and bolstering the trust between the Customer and ToolsGroup. ToolsGroup maintains compliance with both local regulations as well as International Standards widely recognized in the industry.

ISO/IEC 27001:2013

ISO/IEC 27001 is a security standard that formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain and continually improve the ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures.

ToolsGroup currently maintains an active Certification in good standing for ISO/IEC 27001:2013. The Certificate as well as the Statement of Applicable Controls can be shared with Prospects and Customers for review upon request. The scope of the certification is "The Information Security Management System for the provisioning of SaaS (Software as a Service) services for Planning and Business Analytics solutions".

As part of this process ToolsGroup has developed an Information Security Management System (ISMS) that is distributed to employees and contains policies, procedures, modules and instructions for internal use.

About ToolsGroup

ToolsGroup is how organizations achieve their target service levels while optimizing inventory, no matter how complex their supply chain is or how much demand changes. In a world that never follows the rules, organizations have to be ready for anything—from the challenges of multi-echelon inventory optimization to the endless surprises of sporadic demand. To do this, they have to predict more behaviors, protect against surprises, and perform more efficiently. Only ToolsGroup makes all this possible. That’s why global leaders like Absolut, BP and Harley-Davidson continue to rely on us year after year.

www.toolsgroup.com and follow us on Twitter @ToolsGroup.

toolsgroup® | Be ready for anything™

toolsgroup.com