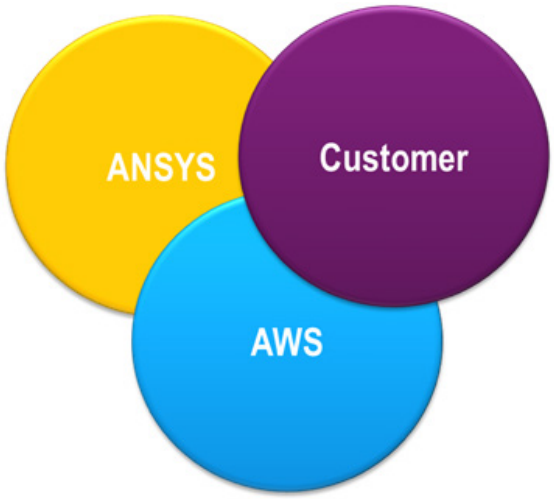
Application Brief

ANSYS Enterprise Cloud Security Overview

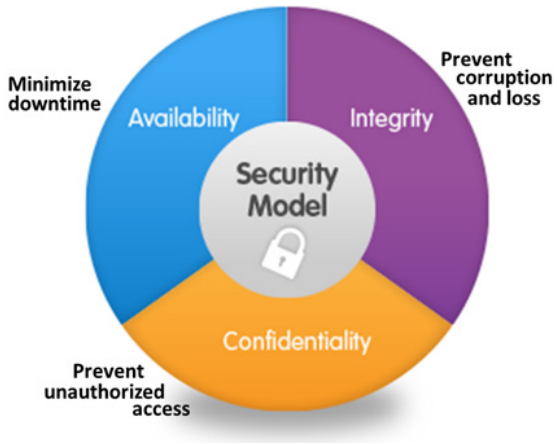
Cloud computing solutions provide value through business agility, ability to focus on core competence and enhanced collaboration. However, organizations may be concerned about data storage in a public cloud infrastructure outside of a company's network. When designed correctly cloud technologies have the potential to be more secure than the on-premises infrastructure of most companies. The security architecture in ANSYS Enterprise Cloud – and the Amazon Web Services-based infrastructure on which it operates – provide a well-engineered and highly secure solution. A framework of confidentiality, integrity and availability provide a holistic view of security.



Shared responsibility

Cloud computing solutions such as ANSYS Enterprise Cloud provide significant value to organizations adopting them. These include business agility, the ability to focus on core competence and enhanced collaboration. But, organizations are rightly concerned about keeping sensitive data outside their company network in a public cloud infrastructure. Security thus becomes a barrier for cloud adoption. But this shouldn't be the case; when designed correctly cloud technologies have the potential to be more secure than the on-premises infrastructure of most companies. There are two main reasons for this. The first is that sensitive IP is centrally managed in the cloud rather than distributed among different, unreliable and unsecured devices. Central data management provides robust security, access control and backup policies. Second, security responsibility in the cloud is distributed among three separate entities: the infrastructure provider such as Amazon Web Services (AWS), the solution provider such as ANSYS and the site administrator which can be either customer IT or a managed service provider. By focusing on their core competence and using economy of scale, each of these entities can ensure that the layer for which they are responsible is made highly secure.

This high-level overview of the security architecture in ANSYS Enterprise Cloud and shows how solution's design and the AWS-based infrastructure on which it operates provide a well-engineered and highly secure solution for any organization. The responsibilities of the site administrator in maintaining a secure environment are highlighted. The well-known CIA triad of **confidentiality**, **integrity** and **availability** is the framework used to provide a holistic view of security.



Security triad

Confidentiality
Confidentiality means that the intended users have access to information and unauthorized access is avoided.

Starting at the physical level where data is stored, ANSYS Enterprise Cloud is hosted on AWS, an industry-leading public cloud platform that complies with variety of IT security standards such as SOC 1, SOC 2, PCI DSS, FIPS, MTCS, etc. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance intrusion detection systems and other electronic means. All physical access to data centers by AWS employees is logged and audited routinely. Before any storage device is presented to a new tenant, any leftover data from the old tenant is wiped clean. AWS follows industry best practices to completely destroy data before decommissioning the storage devices. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity. The AWS network is designed to avoid IP spoofing and packet sniffing by other tenants.

On top of this secure physical layer, ANSYS Enterprise Cloud leverages AWS Virtual Private Cloud (VPC) to ensure a separate and secure network architecture for each customer. The network is broken into a public subnet and a private subnet. The public subnet only contains a few internet- or external-facing instances that require external access. These instances do not store confidential data or run sensitive processes. The private subnet contains all the other instances, including those containing sensitive data and running applications such as web server, license server, authentication server, network file system and simulation jobs. The network connectivity between all instances, especially between public subnet and private subnet, is fine-tuned using AWS Security Groups (SGs) to only allow essential traffic to pass through. All sensitive data at rest is encrypted, whether in the network file system or in AWS Simple Storage Service (S3). Users gain access to the system only after successful authentication against a Windows® Active Directory (AD) server. Rights to the data residing in file systems is regulated using OS file permissions, whereas rights to the data archived in the portal is regulated through the Access Control List (ACL) that allows definition of user/group permissions for any object.

The site administrator is responsible for managing users in the AD server, defining OS-based permissions and defining ACLs in the portal. The site administrator can optionally restrict access to instances in the public subnet to only a limited set of IP addresses or networks. This further reduces the attack vector by disallowing anyone using an unknown IP address to access any part of the infrastructure. The site administrator can apply SSL certificates to ensure any data transferred over the instances in the public subnet is encrypted. Site administrators should also follow AWS security best practices, such as creating Amazon Identity and Access Management (IAM) accounts with specific permissions for those users who directly operate on the AWS infrastructure, and using AWS CloudTrail to setup API/user-activity logging.

Integrity
Integrity involves ensuring the trustworthiness of data at any time, avoiding data corruption and unauthorized alteration, and having the ability to restore data to a consistent state when required.

ANSYS Enterprise Cloud and AWS provide many tools that can be used by the site administrator to ensure data integrity. These include using Secure Socket Layer (SSL) certificates for all data entering and exiting the cloud network, providing defence against man-in-the-middle attacks. The OS permissions and ACLs described previously can also be used to control what data can be read, modified, created or deleted by any user. Version management can be enabled for the data managed in the portal. This allows easy restoration of state to a previous snapshot if data corruption occurs. Each user also has a recycle bin in the portal that can be used in case of accidental data deletion.

All data in ANSYS Enterprise Cloud is stored in two storage systems provided by AWS: Elastic Block Storage (EBS) and S3. All data in EBS volumes is redundantly stored by AWS to reduce the chance of data corruption. Site administrators can also leverage the EBS snapshot feature provided by AWS to take regular backups of data in EBS volumes and restore them to a consistent state in the unlikely event of data loss or corruption. All data archived in the portal is stored in S3. AWS stores S3 data redundantly across multiple devices in multiple facilities, thus providing an industry-leading 11 9's (99.9999999%) of durability. S3 also regularly checks the integrity of stored data using checksums. If corruption is detected, automatic repair is performed using redundant data. ANSYS Enterprise Cloud does not modify existing records in S3. Any modification results in the creation of a new record. Obsolete records can be garbage collected on demand by site administrators. This design ensures data integrity and prevents accidental corruption.

Availability
Availability means that users can access the system and data when required and that downtime or failures are minimized.

The state-of-the-art data centers used by AWS provide the first level of availability. Each data center has automatic fire detection and suppression equipment, fully-redundant power supply, automatic climate control and advanced monitoring for quick identification and resolution of issues.

Redundancy in storage systems, such as EBS volumes and S3, also helps in reducing data outages. AWS security monitoring tools help identify several types of denial of service (DoS) attacks including distributed, flooding and software/logic attacks. In addition to the DoS prevention tools, redundant telecommunication providers at each region, as well as additional capacity, protect against the possibility of DoS attacks.

ANSYS Enterprise Cloud has also been engineered with availability in mind. Some of the components, such as load balancers and the HPC cluster, are

automatically scaled on demand. Most of the other components can be manually scaled out by site administrators to meet expected load or availability guarantees. These components include authentication server, license server, web server, network file system, visualization cluster and database server.

If there is a server failure, comprehensive monitoring capabilities provided by both AWS and ANSYS Enterprise Cloud can be used by site administrators to react quickly and restore operations. AWS provides CloudWatch which can be used to monitor the health and performance of AWS services such as load balancer and database system. ANSYS Enterprise Cloud provides a Ganglia-based monitoring of HPC and visualization cluster nodes. It also provides framework for a Nagios-based health monitoring of other components and essential services. All these monitoring tools provide web-based charting and email based alerting capabilities.

Summary

This is a comprehensive overview of the security architecture designed into ANSYS Enterprise Cloud. Those interested in a deeper understanding of the security architecture of AWS can refer to the Amazon Web Services: Overview of Security Processes white paper.

The reference architecture of the system has undergone comprehensive testing, including detailed vulnerability and penetration testing. But security management isn't a static or one-off activity. Any changes to the deployment may introduce new vulnerabilities. New security threats are encountered regularly and need to be effectively managed. For this reason, it is recommended that site administrators employ similar security practices as those used to protect on-premises infrastructure. These include network log analysis/monitoring for intrusion detection, patch management, anti-virus management and regular vulnerability and penetration testing. By following these practices and using the features provided by AWS and ANSYS Enterprise Cloud, site administrators can provide a highly robust and secure environment for running simulations on the cloud.

ANSYS, Inc.
Southpointe
2600 ANSYS Drive
Canonsburg, PA 15317
U.S.A.

724.746.3304
ansysinfo@ansys.com