WHITEPAPER

AVEVA cloud security: Mitigating cybersecurity risk through good design

Authored by:

-

Neville van der Merwe,
Chief Security Architect, AVEVA

Executive summary

Information security is a key part of AVEVA's business strategy. The security of our cloud offerings is paramount and is achieved using secure cloud platforms, the application of a rigorous Security Development Lifecycle (SDL) and secure DevOps practices.

This whitepaper details the ways in which AVEVA mitigates information security risks in our cloud offerings.

Introduction

Digital transformation is leading to increased adoption of cloud offerings. The benefits of cloud are well known and include:

- Ease of use
- Speed of deployment
- Increased availability and scalabilty
- Reduced IT costs

However, these benefits do have associated costs in increased risks of data exposure and compromise. Cloud products are, by definition, provided on the Internet, and therefore not protected by traditional corporate network boundaries meaning that the vendor offering the cloud solution must engage in proactive practices to ensure that cloud resident data and applications are secure.

At AVEVA, the safety and security of your data is our top priority and is why we follow industry best practices to safeguard our customer's data and AVEVA applications.

Cloud hosting partners

AVEVA cloud offerings are hosted in Microsoft Azure and Amazon AWS, which are two of the leading public cloud service providers. Each company provides a robust global cloud platform that incorporates strong security practices as well as ensuring high availability.

Both Microsoft Azure and Amazon AWS have many security features designed to protect data and applications, ranging from physical and environmental security through network security to data privacy and security controls. This is achieved through compliance with numerous standards including ISO 27001/27017/27018 and AICPA SOC 2 along with transparency in how security is implemented and managed.

AVEVA employees and customers have no physical access to any cloud service provider data center.

See the References for security details of each platform.

Digital transformation requires a new approach to security

Shared responsibility

Our cloud products follow a shared responsibility model to clearly define the responsibilities of all organizations involved in operating a safe and secure cloud environment as shown in Figure 1 below.

Shared responsibility means that the cloud providers are responsible for the security of the cloud infrastructure, and we are responsible for the security our applications, networks and data. At the same time our customers are responsible for configuration of roles and permissions and for protecting their accont credentials.

Separation of environments, access control and administrative privileges

We make use of multiple separate cloud environments for development, testing and production. This ensures that development and operational activities are segregated. It also ensures that development teams do not have access to customer data.

Production environments – which contain customer data – are accessed only for administrative and operational purposes, and only by a limited set of authorized personnel. All changes are logged in order to provide an audit trail.

Development and test environments are used to develop new features and test them before they are rolled out to production and made available to our customers.

Data protection and application security

Data at rest is encrypted using industry standard techniques. For example SQL Databases are encrypted using AES256, as is data in Azure Blobs, Files or Tables. Keys and other application secrets area stored in Azure Key Vault or the AWS Key Management Service (KMS).

Data in motion is encrypted using TLS 1.2 or later to ensure communications security.

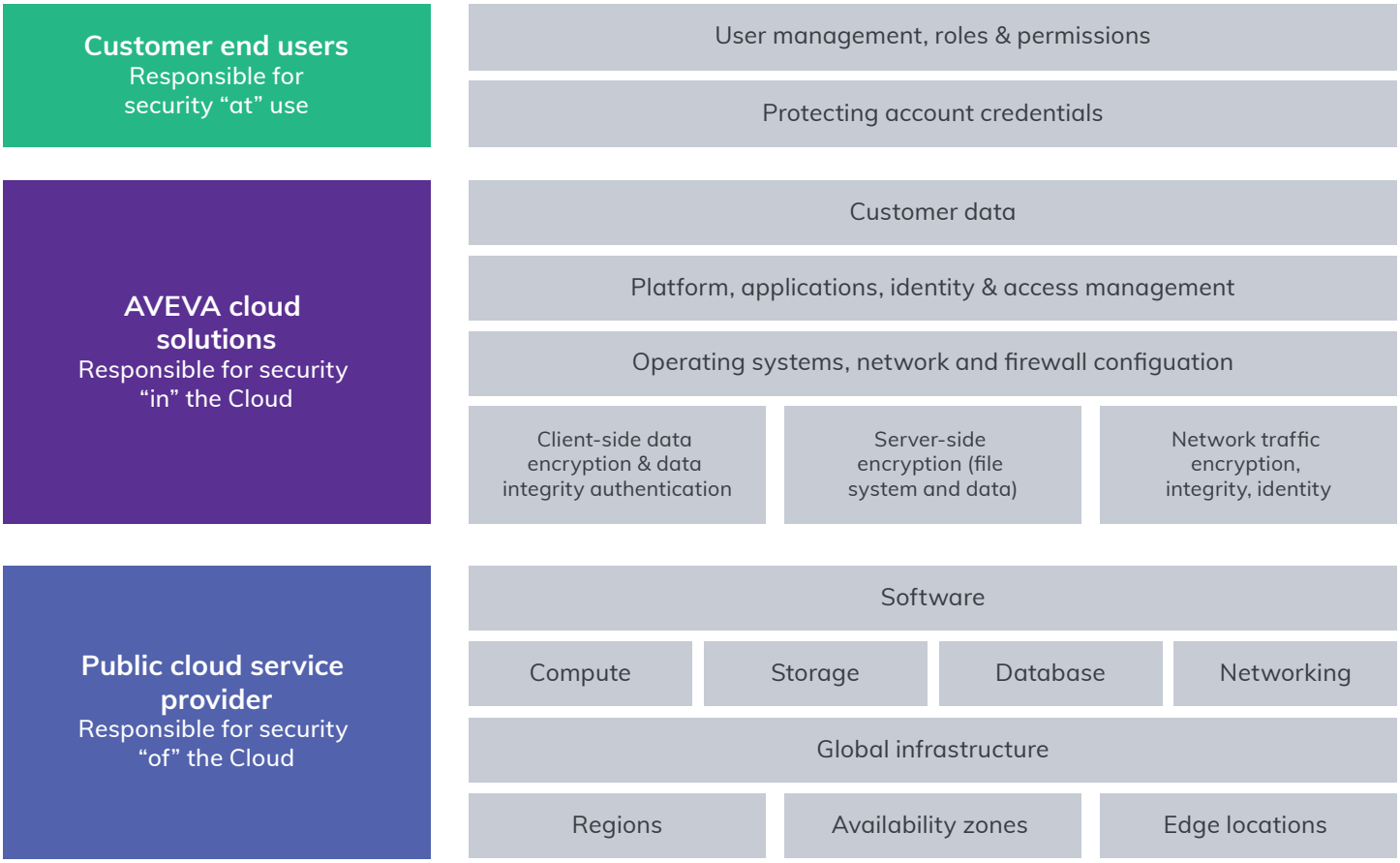


Figure 1: Shared Responsibility model for delivering cloud solutions

Security monitoring and analysis tools are deployed to all environments and are monitored for any anomalies. For example Azure Security Center is used in the Azure environments and AWS Inspector is used for AWS.

Security development lifecycle

The AVEVA Security Development Lifecycle (SDL) is a core element of our Software Development Process (SwDP) framework. Our Quality Management System (QMS) and Software Development Process (SwDP) are regularly evaluated and maintained to incorporate process efficiencies, improved quality and security practices, and better value delivery to our customers.

The SDL process applies to all product offerings and ensures that our applications are developed with security at the core from design and architecture through to implementation, testing and operations.

The SDL is focused on delivering secure software and compliance with industry best practices for designing, developing, and releasing secure software to customers. The following high-level activities occur during the course of all development projects:

Training

- Software developers are required to be trained in SDL practices.

Requirements

- The security requirements are defined and managed in a requirements management system.
- Security risk assessments of requirements are performed.

Design

- Security design requirements are considered for all projects.
- Tools are used to identify and mitigate potential security vulnerabilities.
- Threat models are developed to better understand potential risks.

Implementation

- Static code analysis and compiler options are utilized during projects.
- Unsafe functions are deprecated to reduce risks.
- Code reviews ensure compliance with security practices.

Verification testing

- Tools are utilized to monitor application behavior of any security risks.
- Data validation testing ensures application behavior.
- Tools are used to determine changes in the products surface area.
- Penetration testing is done on a regular basis.

Release

- Security reviews are conducted prior to each software release.

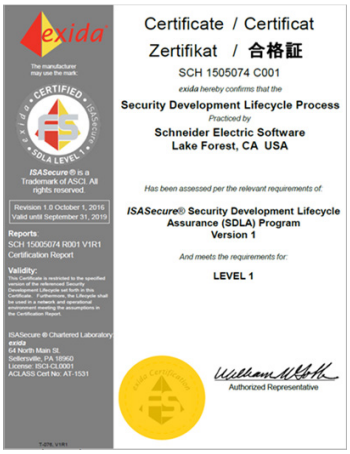
Response

- Incident response plans are followed for any anomalies.

Our SDL process is compliant with the ISA/IEC 62443-4-1 standard for Secure product development lifecycle requirements and has achieved ISASecure SDLA Certification.

DevOps

DevOps is one of the key components in our development of safe, secure and reliable software. This team is responsible for operational control of our cloud environments and follows industry leading best practices to shorten the development/deployment lifecycle. By automating processes between development and IT teams, the DevOps team empowers the AVEVA development teams to provide updates and new features on a frequent basis while ensuring that security best practices are continually followed.



Robust security monitoring tools and practices, such as Azure Security Center and AWS Inspector, are integrated into our cloud environments and are used to ensure that security updates and patches are applied frequently and in a timely manner. Along with proper patching, these tools notify us of any anomalies in our cloud systems, helping us to respond to threats or anomalies quickly and effectively.

We also ensure that only the minimum number of ports are exposed to the Internet that are needed to provide the required functionality and that Web Application Firewalls (WAF) and DDoS protections are in place as added layers of protection.

Our cloud products adhere to strict Service Level Agreements (SLAs) that are detailed in the AVEVA Trust Center: https://trust.aveva.com

We are a member of the Cloud Security Alliance (CSA). The CSA promotes the use of best practices for providing security assurance within cloud computing and provides resources for raising awareness and sharing best practices.

AVEVA has been audited for American Institute of CPAs (AICPA) SOC 2 compliance and can provide reports on request. These reports are intended to meet the needs of a broad range of users that want:

- Detailed information and assurance about the controls at a service organization relevant to security and availability.
- Details about the processing integrity of the systems the service organization uses to process users' data.
- And clarifications with regards the confidentiality and privacy of the information processed by these systems.

Our processes are aligned with ISO/IEC 27001.

Conclusion

AVEVA offers highly scalable, robust and secure cloud solutions by utilizing trusted hosting partners and following industry leading best practices in terms of product development and operations.

References

Microsoft Azure security

- Security fundamentals: docs.microsoft.com/en-us/azure/security/fundamentals/overview
- Azure Trust Center: microsoft.com/en-us/trust-center
- Azure Global Infrastructure: azure.microsoft.com/en-us/global-infrastructure

Amazon AWS security

- AWS Security and Compliance: docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html
- Cloud Security: aws.amazon.com/security
- AWS Global Infrastructure: aws.amazon.com/about-aws/global-infrastructure

Cloud Security Alliance (CSA)

- Overview of the CSA: cloudsecurityalliance.org/about
- CSA Membership list: cloudsecurityalliance.org/membership/current

SOC 2

- AICPA SOC 2 summary: aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

Standards

- IEC 62443-4-1: Security for industrial automation and control systems
- ISO 27001: Information security management.
- ISO 27017: Information security controls for cloud services.
- ISO 27018: Protection of personally identifiable information in public clouds.

AVEVA trust center

AVEVA's Trust Center brings together our system availability, legal policies and security statement for our cloud-based, software-as-a-service (SaaS) offerings. For more information visit: trust.aveva.com

About the Author

Neville van der Merwe works for the AVEVA R&D cybersecurity team and focuses on improving our cybersecurity practices and the security posture of our products. He has over over 30 years of experience architecting and delivering software products in the Industrial Control System space.