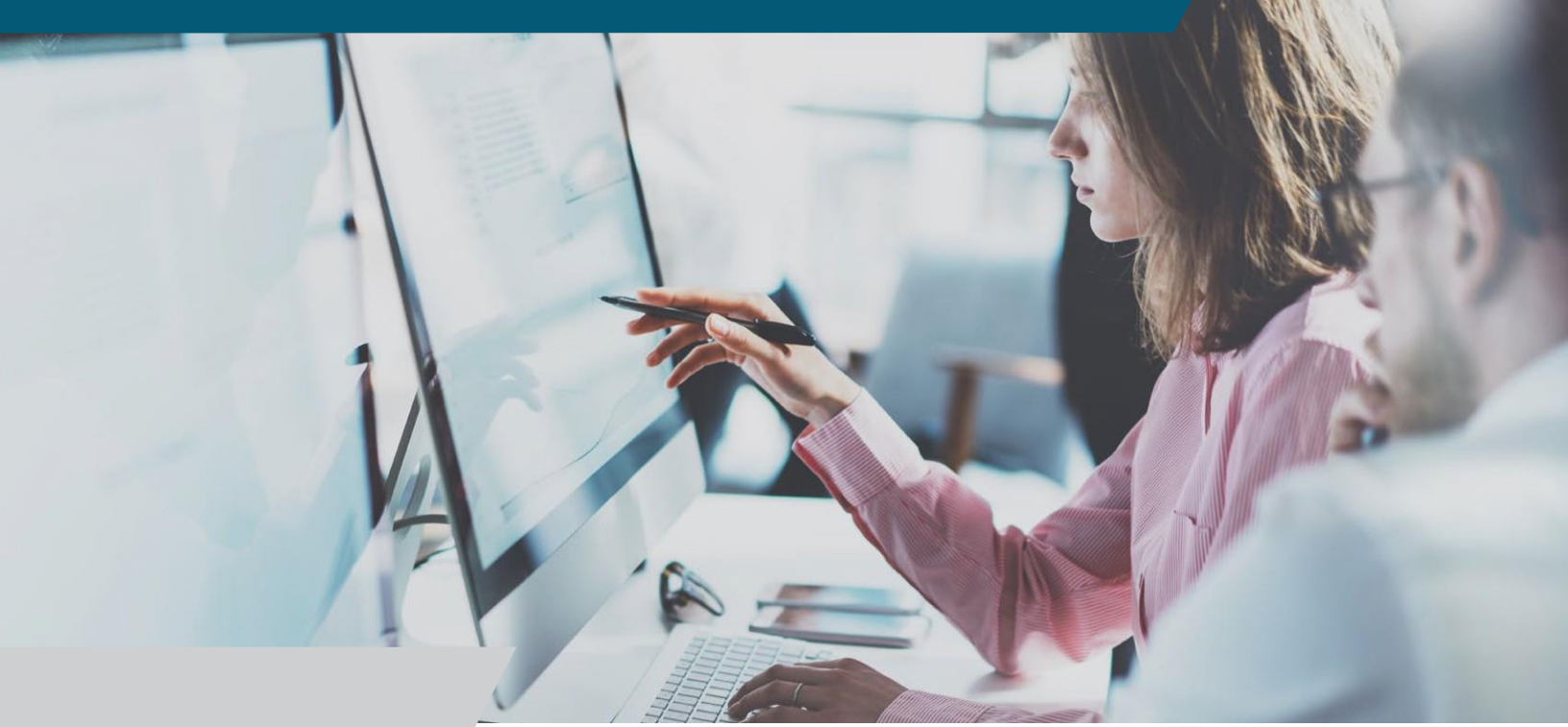
aPriori

aPriori Cloud Security

WHITE PAPER

CONTENTS

aPriori



01. INTRODUCTION

The aPriori cloud solution is a fully managed Software as a Service (SaaS) offering, built on our industry-leading digital manufacturing simulation software platform. It enables easy and secure access to aPriori role-based applications and services through a browser from anywhere and at any time.

aPriori's cloud architecture enables manufacturers to configure and scale deployments to match their enterprise digital manufacturing needs.

All aPriori cloud deployments consist of an aPriori Cloud Foundation (includes application clients, scaled platform services, databases, administrative components, and cloud infrastructure), Manufacturing Process Models, Regional Data Libraries, aPriori named end user licenses and additional modules to meet customer needs.

aPriori maintains a SOC 2 Type II attestation report, validating the suitability of the design and operating effectiveness of controls surrounding the security, availability, and confidentiality of customer data.

This white paper provides an overview of the controls in place relevant to the security of our cloud offering.

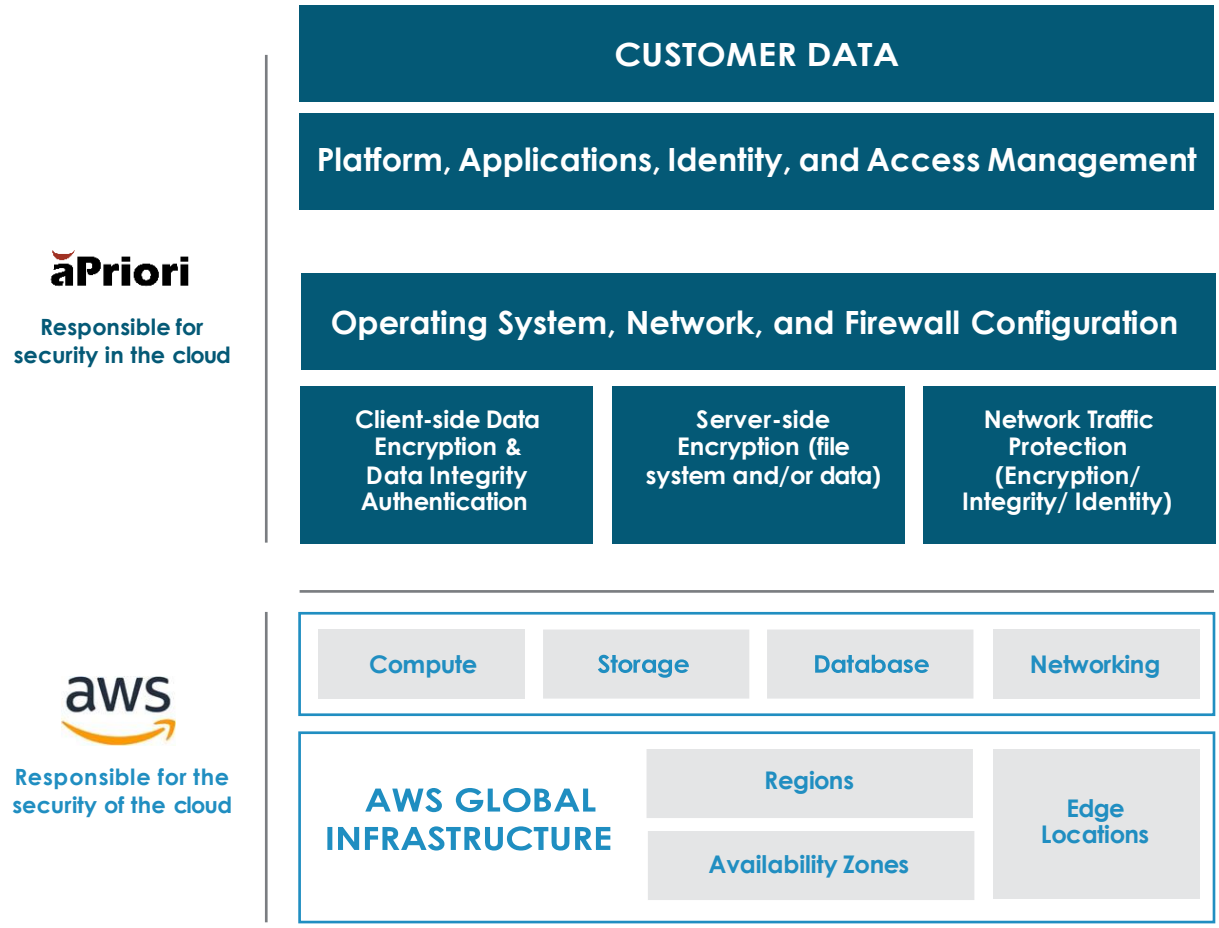
02. SECURITY STANDARDS

aPriori provides a solid foundation to safeguard the aPriori cloud solution using administrative, physical, and technical security controls.

The aPriori cloud solution is built on cloud computing service offerings from AWS and follows industry best practices in Amazon Web Services (AWS) cloud architecture.

aPriori follows the AWS shared responsibility model where AWS is responsible for the "Security of the Cloud" and aPriori is responsible for the "Security in the Cloud."

Throughout this paper, we will reference security capabilities of both aPriori and AWS to provide a comprehensive picture of the controls in place. aPriori is committed to the shared responsibility model and to working with Amazon as both aPriori and Amazon evolve their respective capabilities.



Additional information on the shared responsibility model is available on Amazon's website at: http://aws.amazon.com/compliance/shared-responsibility-model.

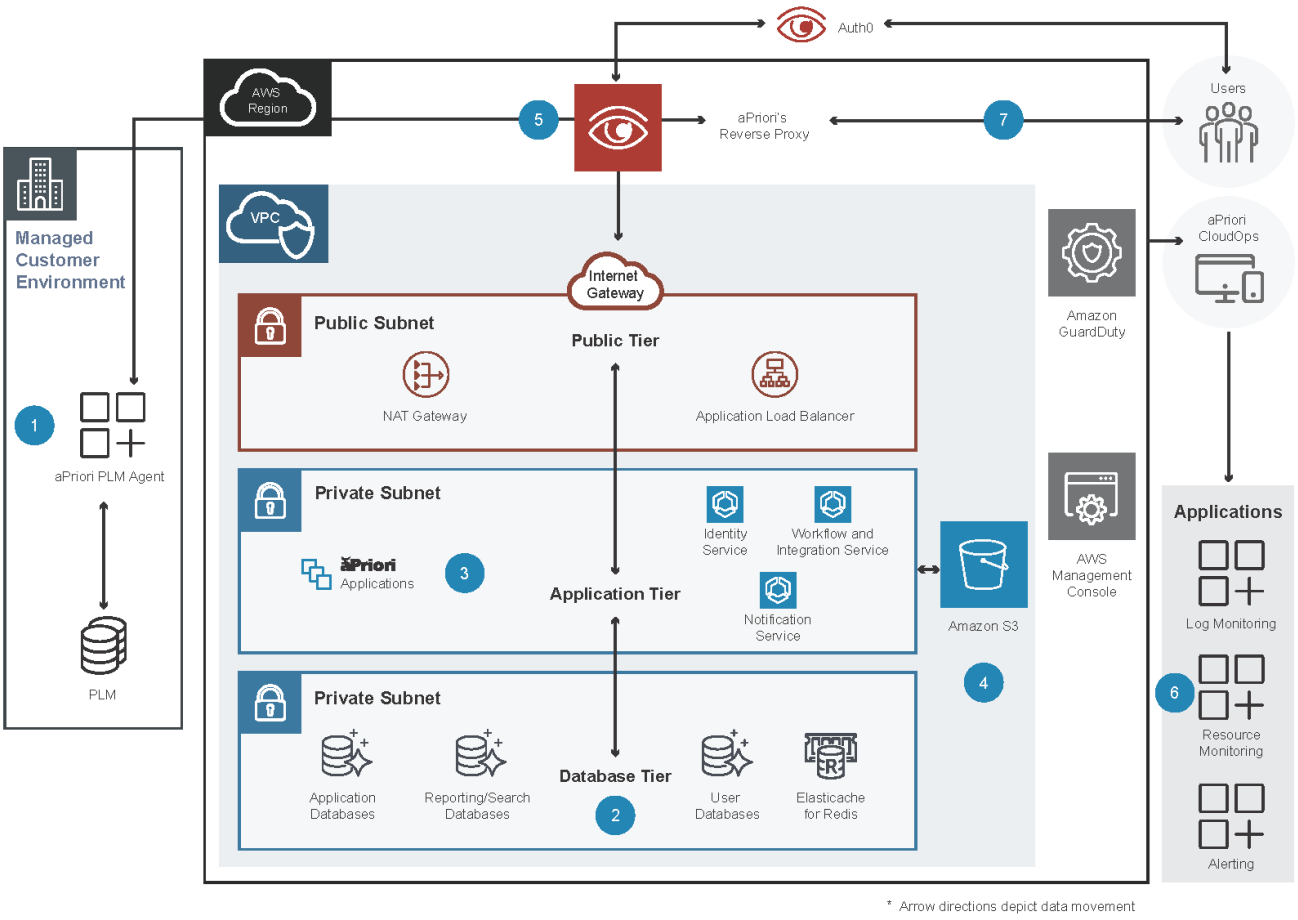
03. THE APRIORI CLOUD SOLUTION ARCHITECTURE

aPriori uses the AWS Infrastructure as a Service (IaaS) offering, which includes compute, network, and storage capabilities. Additionally, AWS offers a variety of managed services that are leveraged to build a world-class application that operates at cloud scale. Using the offerings provided by AWS, aPriori has developed and deploys a scalable, secure, and highly available Software as a Service (SaaS) application for digital manufacturing simulation.

aPriori engineers our applications with security controls, multi-point scalability at every service layer, and system redundancy spanning multiple availability zones. The aPriori cloud solution architecture consists of several layers of components with different security considerations.

All services and databases are deployed across a minimum of two separate availability zones within a given AWS region to provide high availability. Services scale horizontally to ensure customers' demands and growth needs are met. The aPriori cloud solution is monitored to deliver a consistent and reliable service level, which includes performance data capturing and alerting to aPriori teams for any anomalous events.

aPriori and AWS Cloud Security Overview



1. Use the aPriori PLM Agent to schedule CAD file batch processing from on-prem environments. The agent supports write of analysis and reports back to the customer's PLM.

2. Database tier uses Amazon Aurora MySQL as its Reporting & Search database. Amazon Aurora PostgreSQL as its User & Application database. Amazon ElastiCache (Redis) for its in-memory data storage and caching service.

3. Application tier hosts aPriori modules such as aP Design (on ECS) for Cost analysis, aP Analytics (on EC2) for Reporting, aP Connect (on ECS) for Batch Scheduling & CAD ingestion, aP Pro (on Appstream) for advanced design and costing analysis users. This tier also hosts Identity, Notification and Workflow & Integration microservices.

4. The Amazon S3 bucket stores CAD files. Files are processed by aPriori modules with results stored in the database layer and surfaced through application & reporting services.

5. Users securely access aPriori & its modules via a federated SSO login, and aPriori's reverse proxy protects against threats & vulnerabilities.

6. aPriori CloudOps team uses 3P services for Log & Resource monitoring.

7. Use plugins (compatible with all major CAD vendors) to upload CAD files to aPriori.

04. APRIORI SECURITY PROGRAM

Management Commitment

aPriori's senior management team is committed to the security of the company's cloud solution and the protection of customers' data within. Senior management is actively involved and sets the direction of the security initiatives within the company.

Governance, Risk, and Compliance (GRC) Framework

The aPriori Governance, Risk, and Compliance Framework contains a comprehensive set of policies, procedures, and supporting materials to define the fundamental principles to meet our security objectives. The framework defines specific objectives designed to protect the confidentiality, integrity, and availability of company and customer data, and expectations of our personnel.

aPriori security policies and procedures are created and regularly updated using recommendations from a combination of industry standards such as NIST, CIS, and ISO 27001. These standards are used as the foundation for the aPriori security operations and are adapted to meet the unique business requirements and needs of aPriori and aPriori customers.

The GRC Framework demonstrates aPriori's commitment to security by creating documentation to encompass a comprehensive range of information security topics. The framework includes documentation on Information Security, Mobile Devices, HR Security, Information Security Awareness and Training, Asset Management, Acceptable Use, Access Control, Cryptography, Data Classification and Handling, Data Retention, Backups, Physical Security, Vulnerability Management, Network Security, Secure Development, Vendor Management, Incident Response, BC/DR, and Risk Management.

All GRC documents are reviewed annually and updated more frequently as required.

aPriori personnel are required to be familiar with all policies and procedures for general security awareness, with additional technical training and materials for specified roles. aPriori conducts regular security awareness training, phishing tests as well as other security-related communication.

Risk Management

aPriori maintains a risk management program to consistently identify, assess, treat, and monitor risks in the aPriori cloud solution and across the organization. All identified risks are added to the risk register, which is reviewed on a regular basis.

The aPriori cloud solution, supporting infrastructure, as well as all critical assets are subject to full risk assessments at least annually. Other internal and external testing and assessment are performed in accordance with industry standard best practices for SaaS providers, including but not limited to static code scans, dynamic code scans, and penetration testing.

Roles and Responsibilities

aPriori maintains segregation of duties within the aPriori cloud solution. Multiple teams support the solution but maintain distinct roles and responsibilities for the product and services. The following functional groups are organized to address specific security tasks:

1. Engineering: Architects, designs, implements, tests, builds, and releases cloud applications and services.
2. Platform Engineering: Ensures the continuous and secure operation and maintenance of the aPriori cloud solution.
3. Product Management: Ensures customers' requirements are met, and the product is designed to be compliant with relevant global regulations, security standards, and policies.
4. Customer Support: Ensures all issues are attended to promptly and resolved or escalated according to aPriori support policies.
5. Customer Success: Identifies and advocates for the needs of aPriori customers to ensure long-term customer.
6. Security and Compliance: Develops the security strategy and oversees its implementation across the organization. Also provides the operational framework to ensure compliance with legal, regulatory, and contractual obligations.
7. IT: Manages the Identity Management and Access Control organization wide. Supports and operates all enterprise systems, data storage, and services. Manages technology vendors and supply chain. Develops and executes enterprise BC/DR strategies.

05. DATA SECURITY

aPriori is dedicated to customer data confidentiality, integrity, availability, and privacy. A specialized data management team is comprised of trained personnel across the organization with the focus on the appropriate acquisition, handling, and storage of data within aPriori's responsibility and control. aPriori has implemented many administrative, operational, architectural, and technical controls regarding data security including:

- Data and assets are classified and handled in accordance with our data classification and handling policy.
- All data is encrypted at rest, and all traffic outside our private network is encrypted in transit. It is encrypted with the approved cryptographic algorithms, (AES256 and TLS 1.2). Keys are managed and rotated with Amazon Key Management System (KMS).
- Sensitive user data in process, including API access, is protected with identified keys, security tokens, and/or sessions.
- Multi Factor Authentication (MFA) can be enabled on request for non-SAML users managed by the aPriori cloud.
- Access can be configured on request with Federated Single Sign On (SSO). Customers can use their own enterprise identity provider (IdP) with their own user authentication, if the IDP supports the SAML 2.0 standard.
- Only named licensed and authenticated customer users can access customer data. Any access to customer data by aPriori is defined in the license and support agreements between aPriori and the customer.
- Services are protected by web application firewalls, and only specified customer domains and aPriori support are permitted access.
- Customers can configure a retention policy to remove customer-submitted data (i.e. CAD files) to the aPriori cloud solution. The CAD file retention policy has a range from one (1) day (minimum) to 1095 days (maximum).

Physical and Logical Separation

- Storage of customer data is limited to specific geographic regions to meet regulation, privacy, or other compliance requirements.
- aPriori maintains separate development, QA, staging, and production environments. Customer access is configured for production deployments only, while the development, QA, and staging environments are strictly for aPriori development use.
- Customer environments and data are tagged and logically separated. Multi-tenancy services separate the customers' data and access using globally unique customer and user identifiers.

06. APPLICATION SECURITY

aPriori application security starts with software requirements and continues throughout the engineering activities in the full software development life cycle (SDLC). The secure development includes architecture review, design review, implementation, code review, development security operation (DevSecOps), continuous integration and continuous delivery (CI/CD) practices, and secure operations of the SaaS product runtime environments.

Secure coding standards are enforced using static analysis, dependency and vulnerability scanning before code is committed to build pathways. New release versions are held until all scans pass the quality standards defined and managed by teams. This helps aPriori applications run securely and reduces the possibility of successful attacks.

aPriori application security is additionally enhanced with proper identity and access management (IAM) and security controls in the production environment. These include a Web Application Firewall, DDoS protection, as well as Security Incident and Event Management (SIEM) monitoring and alerting.

07. OPERATIONS SECURITY

Operational Procedures

aPriori has a documented library of procedures designed to ensure required procedures are performed in a timely and effective manner. Each operational role is defined in accordance with its set of responsibilities consistent with least privileged access controls. The actions performed by individuals are primarily driven by an internal ticketing system to provide a consistent approach and auditability of the actions performed.

Infrastructure as Code

aPriori uses industry-standard best practices to manage cloud infrastructure as code (IaC). This approach maintains all infrastructure definition and management as source code, allowing the team to fully automate and manage the current state of the cloud infrastructure

through repeatable, monitorable, and auditable processes. The IaC maintains the AWS infrastructure as editable source code.

The aPriori team can automate most AWS configuration changes, which improves customer environment reliability, availability, and serviceability, as well as security. aPriori can quickly propagate the environment configuration changes from one AWS region to another, patch security issues as identified in one customer environment to all applicable environments, and improve security and productivity in engineering.

The AWS environment can be modified consistently, if needed, to deploy a new update from development to production, even if they belong to separate AWS accounts. The ability to perform these functions is tightly managed using best practices around centralized authentication and access control such as strong password policies, session management, multifactor authentication, and more.

AWS Environment Scanning

All aPriori Cloud solution environments in AWS are scanned automatically. The monitoring includes the AWS configuration and usage which enables aPriori to detect, report, and suggest fixes to ensure AWS-suggested best practices are followed.

Protection from Malware, Viruses, and Attacks

Web Application Firewalls (WAF) and AWS Shield are used within the aPriori cloud solution to detect, filter, and block intrusions such as OWASP Top-10 attacks including SQL-Injection, XSS, etc.

Scans are performed daily or in real-time, and alerts are sent to appropriate team members for immediate response.

Cloud servers are primarily transient and replaced regularly. All servers except public-facing HTTP load balancers/proxies run in private networks.

aPriori scans third-party components for known vulnerabilities. Libraries are updated during the regular release process, or with a hotfix when a high severity vulnerability is identified.

Backup

aPriori has documented policies and procedures for backing up customer data within the aPriori cloud solution. All backups are encrypted and undergo regular testing to verify backup integrity and ensure continued protection.

All data at rest is stored in scalable, managed services, that are designed to operate at cloud scale and include fully redundant and highly available configurations. Service failure in a single availability zone will failover to another availability zone automatically. Backups are performed daily via a snapshot capability. Snapshots are stored in a restricted area of Simple Storage Service (S3).

Backup failures are communicated to operations staff via email alert. Daily backup snapshots are automatically expired and deleted after one month (31 days).

Backups of the aPriori cloud solution focus on recovering data on an application-wide basis and meeting our recovery point objective and recovery time objective. Partial or sub-set backup and/or restoration is not supported currently.

08. ACCESS CONTROL, MFA

The aPriori cloud solution access control system is in a dedicated AWS account with a dedicated production Auth0 Tenant. This architecture assures the separation of the accounts or duties with full technical controls. This architecture also enables the organizational controls that are transparent to the customer for user least privileges, as aPriori personnel will not have access to a customer's applications except where access is granted explicitly with the customer's request or approval.

aPriori Administrative Access

Only aPriori personnel, as needed by business requirements, are permitted to access infrastructure within the aPriori cloud solution. Access is generally restricted and only granted by signature sign-off by a duly authorized manager. Each person is assigned access using the least privileges required for the specific work needed to be performed. Access is removed as soon as work has been completed.

Additionally, the privileged user requires multi factor authentication (MFA), and privileged actions are logged and audited.

Employee Access to SaaS Application(s)

aPriori employees, by default, do not have to customer's SaaS applications. If required, access must be requested by the customer through the customer support or customer success team (CSM).

Permissions are granted only for the specific roles or locations within aPriori, aligned with business needs for the functions those individuals perform. Access is automatically revoked and must be requested each time it is needed.

Single Sign On, Role Based Access Control

aPriori recommends customers integrate their own identity provider with aPriori's authentication platform using SAML. Customer users can login once and then access all integrated aPriori services, including the aPriori Help Center (support portal), knowledge base, and other resources.

The aPriori cloud solution uses Auth0 for SSO, which utilizes the SAML 2.0 protocol.

On request, the aPriori cloud also supports federated SSO and the integration between a customer's own SAML Identity Provider (IdP) for authenticating users with Auth0 as the aPriori service provider.

Customer Access to SaaS Application(s)

All requests for additions, deletions, and modifications for customer access are managed through support tickets, which ensures the request originates from an authorized user.

Customer user accounts must use a corporate domain email. The aPriori cloud solution uses an allowlist containing permitted domains for each customer.

The aPriori cloud solution uses a controlled on-boarding process, with the help of the aPriori support team, for secure initiation of customer users. For example, when the customer provides a list of new users with information and credentials, an aPriori cloud administrator creates the user profiles, the default authentication method is user name/password managed by the aPriori IDP.

aP-Cloud sends out an email to the user. The email message contains a link, which enables the user to confirm the registration and the user's email account. In addition, the user is prompted for a self-requested password reset at the first time login.

The customer can optionally enable MFA for some or all users to add additional security to their account.

09. NETWORK SECURITY

Following the shared security model, aPriori has built a secure network to secure the data in the cloud while leveraging AWS to provide protection for security of the cloud. Defense-In-Depth and network segregation with multiple tiers of security controls are implemented for the aPriori cloud solution.

For AWS Regions:

- One or more AWS regions can be independently deployed.
- Network-level security controls are used along with application-level controls to enforce a zero-trust architecture and validation of all inbound requests.

Inside an AWS Region:

- The aPriori cloud solution utilizes an AWS Router, Gateway, firewalls, and GuardDuty to guide normal traffic and block unexpected network traffic.
- The aPriori servers in the cloud are not exposed to the Internet. The aPriori servers and sub-components are deployed in a Private Tier sub-network within a VPC. Only the load balancer (LB) are exposed to the Internet, with controls of defined AWS IAM Security Group configurations. Thus, all servers must either go through the controlled VPN (for aPriori personnel) or LBs (filtered by router, WAF, etc. for customer business) for data to be processed inside the Private Tier. Furthermore, the database servers, as the core asset that hosts the customer data, are in another private subnet dedicated as a Database Tier.
- The gateways between the Public Tier and Private Tier as well as between the Private Tier and Database Tier have been carefully designed to block unknown servers or IP addresses. Similar protections are implemented for both the Public Tier and Private Tier with specific tier security groups.
- VPN access is restricted to permitted aPriori personnel. The permission needs approval and is reviewed annually and when roles change.

10. CRYPTOGRAPHY

aPriori makes extensive use of cryptography with the aPriori cloud solution by hashing, signing, and encrypting the data and access channels. Both symmetric and asymmetric encryption are used with a set of approved ciphers and key lengths.

Transport Layer Security (TLS) 1.2 is used for all data in transit. SSLv2, SSLv3, TLS 1.0, and TLS 1.1 protocols are not supported due to identified weaknesses in the protocols.

aPriori closely monitors security changes in the industry and adjusts its implementation as needed.

The following are the default cryptography settings:

- The Public Key Infrastructure (PKI) key and certificates are 2048 bits.
- HTTPS, SSH, and secure database connections are required to access all data.
- aPriori uses open cryptography algorithms; For example, AES-256 is used for encryption, SHA256 or password-based key derivation function 2 (PBKDF2) is used as the hash function.
- The user password, if not using federated SSO, is stored as a salted hash code in database.

The AWS Key Management Service (KMS) is used by default. The AWS key and other user specific keys are rotated regularly, and the key management policy includes limits before key rotation.

Limits are based on key usage, with rotation on SSL keys consistent with certificate lifetime, and rotation for other uses consistent with content under protection. Key creation, storage, and procedures for handling compromised keys are documented and activities are logged.

10. CHANGE MANAGEMENT

aPriori follows a formal change management process which includes the following areas:

- Policy and procedures that define the process from the change request, review, approval, planning, implementation, documentation, communication, and monitoring.
- Architecture changes and patches use the internal ticketing system to track changes. All planned changes to the production environment are documented, tested, and approved prior to implementation.
- Changes within the software development lifecycle are identified, documented, reviewed, and authorized before release. Before a change is implemented, its validity is confirmed and the impact on other systems is identified and examined with secure by design threat modeling practices. A list and description of software changes are included in the Release Notes for each version.

11. SIEM & MONITORING

Logging, Monitoring, and Alerting

Within the aPriori cloud solution, logging and auditing functions for system security events are configured and enabled on all cloud services, for inter-networking devices, and access control systems.

Logging for intrusion detection is centralized into the Security Incident and Event Management (SIEM) system which monitors, alerts, and reports activities. SIEM logs are prevented from modification by removing write access to the files during data collection and analysis. aPriori utilizes statistical data from the SIEM and AWS Cloud Trail to prioritize prospective security controls.

In accordance with our GRC policy, alerting is enabled for items that meet specific criteria to ensure timely notification and investigation. Monitoring encompasses the aPriori cloud solution as well as critical services running on each service. Service and system checks are performed 24/7. Failures will automatically generate an alert for the appropriate aPriori personnel. aPriori has defined and documented a process covering alert response and service recovery.

Technical Vulnerability Management

aPriori employs regular vulnerability scans of the environment to identify any potential attack vectors. aPriori maintains and enforces a documented system hardening configuration standard. These standards are enforced to ensure that all operating systems are hardened and protected from alteration before being deployed into production.

Server images are based on AWS base images that are updated regularly by Amazon. The servers are generally transient and replaced regularly from these images.

aPriori has defined processes for the monitoring, testing, and deployment of operating systems and application patches. The processes for hot-fixes, security patches, and change management provide additional assurance for cloud delivery technologies.

12. INCIDENT RESPONSE

The aPriori incident response program is aligned with controls as recommended by the National Institute of Standards and Technology (NIST) and includes guidance for preparation, detection and analysis, containment, eradication, recovery, and lessons learned.

Incidents can be reported manually by aPriori employees or customers as well as reported systematically by the SIEM and other automated tools.

Once an incident is reported, it is analyzed by properly trained personnel to determine incident severity, impact, and priority. The incident is escalated to appropriate response teams for containment and eradication. All eradication and recovery steps are performed in a phased approach and prioritized to allow the aPriori cloud solution to be secured quickly. Notifications will be provided throughout the incident response as necessary. Customers are notified within 72 hours if their data was impacted by an incident.

Once an incident has been resolved and the system recovered, a lessons-learned meeting is held to identify root cause and prevent reoccurrence.

aPriori cloud solution security measures including health monitoring, SIEM, asset vulnerability scans, and proactive security patches help stop potential operational issues before they become incidents.

13. VENDOR MANAGEMENT

aPriori maintains a vendor management program which includes policies and procedures for vendor selection, onboarding, termination, and review. All vendors who supply goods or services to aPriori must be evaluated and approved prior to onboarding. The evaluation will include a review of the vendor's security controls and risk profile to determine if they are an acceptable vendor to do business with.

The data sub-processors of the aPriori cloud solution will be required to sign a Data Processing Addendum (DPA), along with Service Agreements that supplement the commitment aPriori makes, with vendor's security, privacy, and compliance commitments in processing customers' data.

A list of our data sub-processors can be found on our website.
https://www.apriori.com/data-subprocessors/

14. COMPLIANCE AND CERTIFICATIONS

aPriori is committed to ongoing compliance with all applicable standards, regulations, laws, ethics, and contractual requirements.

aPriori is constantly working with global services firms and third-party expert consultants to acquire and maintain guidance in various areas of information security, compliance, risk, and privacy.

Since 2019, aPriori has successfully completed the System and Organization Controls 2 (SOC 2) Type II audit for the controls implemented for security, availability, and confidentiality. The report validates the suitability of the design and operating effectiveness implemented with respect to the defined trust criteria. The SOC 2 Type II report is available to customers upon request and under NDA.

aPriori meets the requirements for properly handling personal data as defined by GDPR. aPriori offers our customers a data processing addendum (DPA) under which aPriori commits to process and safeguard personal data in accordance with GDPR, California Consumer Privacy Act (CCPA), California Consumer Privacy Rights Act, and other applicable laws and regulations.

aPriori is committed to complying with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of international data transfers. aPriori has maintained our Privacy Shield certification while continuously enhancing our data privacy program.

For more information about implementing the aPriori cloud solution, please talk with an aPriori representative.

Visit **www.apriori.com**
to learn more.

aPriori

300 Baker Avenue
Concord, MA 01742

Tel: 978.371.2006
Fax: 978.371.2008

www.aPriori.com
info@apriori.com

aPriori provides a unique, end-to-end digital twin solution that empowers manufacturers to unlock and identify new opportunities rapidly for innovation, growth, cost savings, and sustainability. With aPriori, customers achieve a ~600% ROI within three years and payback within six months of adopting our software platform. And companies use our automated manufacturing insights to reduce product cost, improve productivity, and reduce their products' carbon footprint. aPriori also boosts manufacturers' digital thread investments to deliver business value at scale, increase agility, and minimize risk. To learn more about aPriori's cloud and on-premise solutions, visit www.apriori.com.