Avian Cloud

Security Assurance Document

Avian Cloud is a new and innovative Platform-as-a-Service (PaaS) solution designed for Digital Forensics, Incident Response, and eDiscovery. The unique platform enables quick deployment of isolated labs for law enforcement, corporate investigations, and legal teams. It streamlines case initiation and data analysis, offering a secure, rapid and efficient solution for critical use cases.

Contents

Network Security

Avian Cloud employs stringent network security measures to safeguard data and communications:

- **Isolated Virtual Networks**: We implement isolated virtual networks with one isolated tenant per Avian Cloud subscription, ensuring separation and security. See this Microsoft Azure pattern for more information.
- **Default Deny Policy**: Our network follows a strict default deny policy, which restricts Internet communication to explicitly allowed routes, ports, and protocols. All networking policies are documented, and risk assessed annually.

  Currently, access to the internet from within the virtual network is without limitation. We are currently evaluating if and how to restrict this further without limiting relevant investigative tasks.
- **Firewalls**:
  - All virtual machines have internal firewalls in place to prevent lateral movement inside the virtual network.
  - The virtual network is protected by Network Security Groups (NSG) with only access via the Load Balancer, and only on explicitly allowed sockets.
    - This is exempted during provisioning as the centralized deployment engine needs to communicate with the customer tenant endpoints to perform deployment steps. Subsequently, such endpoints are removed before releasing to the customer.
- **Encryption for Data in Transit**: All traffic between endpoints is secured using up-to-date TLS encryption with tenant-specific certificates, guaranteeing the confidentiality of data during transmission.
- **Access Control**: We leverage load balancers and Azure Active Directory (AAD) pre-authentication to limit inbound traffic to actions performed by authenticated users. Pre-authentication utilizes Azure AD authentication to restrict traffic through the load balancer, adding an additional layer of security against unauthorized access

Tenant-wide Security Policies

While Microsoft Azure Security Defaults will be sufficient for most, Avian Cloud optionally empowers clients to enforce custom security policies throughout their isolated tenant, ranging from data access controls to administrative privileges.

Isolated User Registry

Our isolated tenant architecture is built on Azure AD, establishing a secure, separate user registry for each client. This design prevents unauthorized cross-subscription access, ensuring that only users within a specific Azure subscription can access its resources.

Performance Advantage of isolation

The isolated tenant architecture isn’t solely about robust security; it also focuses on optimizing performance. By allocating dedicated resources to each tenant, we eliminate the issue of "noisy neighbors," enabling fine-tuned performance metrics tailored to each client's needs.

Access Control and Authentication

- **Multi-Factor Authentication**: Avian Cloud enhances user account security by leveraging the Multi-Factor Authentication (MFA) capabilities of cloud Identity Provider (IdP) used by the customer organization. We federate user authentication through the IdP, which means that MFA is controlled and managed by the IdP itself and the policies of the customer's organization. This approach ensures the highest level of security for user accounts without the need for custom-built authentication mechanisms.
- **Role-Based Access Control**: Avian Cloud utilizes Role-Based Access Control (RBAC) mechanisms that are seamlessly configured within each customer's Azure Active Directory (Azure AD) tenant. We do not rely on custom-built access controls or manual user assignments. This automated RBAC setup ensures precise control over user permissions within the tenant, aligning with industry best practices for security.

Optional Customer-supplied Encryption Keys and Certificates

For clients who prefer to use their own encryption mechanisms, Avian Cloud provides the option to supply their own encryption keys and certificates.

Layered Data Encryption

- **Azure Platform encryption**: At the foundational level, encryption is handled by the Azure platform, providing baseline security.
- **OS-level encryption**: Additional encryption at the operating system level builds another layer of data protection.
- **Application-level encryption**: Avian Cloud adds a third layer of encryption at the application level, providing the most granular control over data security.
- **Confidential Computing**: Azure's Confidential Computing capabilities ensure that data remains encrypted even during processing.
- **No shared encryption keys or certificates across subscriptions**: We ensure that encryption keys and certificates are not shared between different Azure subscriptions, maintaining a high level of security isolation.

Unique Encryption Keys

Each tenant is assigned unique encryption keys, adding another layer of data protection and enhancing the isolation between different tenants.

Secure Deletion

The layered encryption and customer-specific encryption keys ensure that when subscriptions are terminated then data can never be retrieved again as the link between keys and encrypted data is gone.

Integration and API Security

At Avian Cloud, we prioritize highly isolated systems. To maintain security:

- We limit external integrations to a minimum to minimize potential attack vectors.
- When necessary, all integrations strictly use TLS encryption to secure data transmission.
- Our approach is inside-out, meaning that Avian Cloud does not have any open APIs actively listening for external requests. This approach further reduces the surface area for potential security threats.

This security strategy helps us maintain a highly controlled and secure environment while ensuring data integrity and confidentiality in any integrations that are implemented.

Logging and Audit Trails

Avian Cloud maintains comprehensive logging and audit trails to ensure security and compliance:

- **Log Generation**: Each tenant collects endpoint event logs from endpoints and applications, forwarding them to their dedicated Security Information and Event Management (SIEM) instances. Additionally, Avian Cloud utilizes centralized monitoring through Endpoint Detection and Response (EDR) tools for enhanced security monitoring.
- **Log Storage**: Audit trails comprise a combination of logs from the cloud provider, endpoints, and applications. These logs are securely stored in a dedicated storage area to maintain historical records of security events and compliance-related activities. The subscriber has access to this storage area.
- **Review for Security Events and Compliance**: Logs are regularly reviewed to detect and investigate security events. They also serve compliance purposes by providing a record of activities and ensuring adherence to relevant standards and regulations.

This logging and audit trail approach helps us maintain a proactive stance on security and compliance, enabling timely detection and response to security incidents and ensuring adherence to regulatory requirements.

Data Residency and Jurisdiction

At Avian Cloud, data residency and jurisdiction are determined by our customers. When customers subscribe, they have the flexibility to choose the country where their data resides, provided that a datacenter of the cloud provider is available in that country. As a result:

- Data residency is under the control of the customer, who decides where their data is stored based on their specific requirements.
- Jurisdictional laws applicable to data handling are also governed by the customer's choice, as they act as the data controller.

Avian Cloud enables customers to manage and control these aspects, but the ultimate decision on data location and jurisdiction lies with the customer. Customers may choose to deploy multiple subscriptions in different locations to adhere to data residency restrictions and specific jurisdictional requirements.

Data Privacy

Customers have complete authority over data upload and processing within their tenant. We never initiate data actions without explicit customer instruction. Customers retain the role of data controllers, while Avian

Cloud operates as a processor. Our Terms of Service explicitly mandate that customers only upload and process data for which they hold legal processing authority, ensuring compliance with relevant regulations and laws.

Backup and Disaster Recovery

Our comprehensive backup and disaster recovery strategies are designed to safeguard customer data and minimize downtime in the face of unforeseen events.

- **Backup Policies**: We implement daily backup policies for all storage and endpoints within customer tenants. These backups are retained for eight days to provide a short-term recovery option.
- **Long-Term Retention**: To ensure data resilience over an extended period, we maintain backups for up to five weeks within the same geographic zone. This strategy facilitates a reasonable Recovery Time Objective (RTO) in most scenarios.
- **Geo-Redundancy**: Additionally, we offer the option of geo-redundant backups. This means that data can be backed up to a different geographic zone, further enhancing data availability and disaster recovery preparedness.
- **Annual Testing**: Avian Cloud conducts annual tests of backup policies and RTO procedures to validate their effectiveness and readiness. These tests ensure that data can be restored swiftly and reliably when needed.

Security Patching and Updates

At Avian Cloud, we maintain a proactive approach to keeping our platform secure:

- We perform automatic security updates wherever feasible to ensure that our systems remain up-to-date with the latest patches.
- In cases where updates require reboots or have the potential to disrupt long-running jobs, we coordinate with subscribers to minimize disruption.
- For systems that necessitate manual updates, we work closely with customers to schedule regular service windows for updates to be applied.
- Our Endpoint Detection and Response (EDR) systems actively notify us of vulnerabilities and outdated versions, enabling us to promptly address security concerns.

This approach allows us to maintain a secure and up-to-date platform while ensuring minimal disruption to our subscribers' operations.

Compliance and Standards

Compliance

Avian Cloud operates under a robust Information Security Management System (ISMS) that is compliant with ISO27001 and ISO27701 standards. These internationally recognized standards underscore our commitment to maintaining the highest levels of information security and privacy.

Security Compliance

With ISO27001 compliance and NATO secret vetted staff, Avian Cloud offers a level of security that can be challenging to implement and maintain in an on-prem or general public cloud environment. Additionally,

many organizations require a solution that the internal IT department does not have access to, because of the sensitivity of the matters.

Third-Party Audits and Penetration Testing

Avian Cloud places a strong emphasis on security validation through regular third-party audits and penetration testing. Our practices include:

- **Penetration Testing**: We engage the P3 Group to conduct penetration tests, which encompass assessments of both our centralized provisioning service and deployed tenant environments. These tests are conducted from external and internal perspectives, including breakout tests, to evaluate the effectiveness of our security measures.
- **ISMS Accreditation**: We are actively working towards accrediting our Information Security Management System (ISMS) to align with ISO27001 and ISO27701 standards. This accreditation is planned to be achieved by the end of 2023, further demonstrating our commitment to robust security practices.

Customer Support and Incident Response SLAs

At Avian Cloud, every subscription includes at least standard support with defined Service Level Agreements (SLAs) to ensure timely assistance for our customers.

In the case of severe security incidents, our Incident Response Standard Operating Procedure (IR SOP) is deployed immediately upon detection, prioritizing swift and effective response to mitigate any potential security threats.

Incident Response and Monitoring

Avian Cloud follows an incident response procedure rooted in NIST SP 800-61, Section 3. Our approach to handling security incidents includes:

- **Detection**: We employ Endpoint Detection and Response (EDR) tools that continuously monitor for security incidents. These tools help identify potential threats and vulnerabilities.
- **Reporting**: When a security incident is detected, our procedure dictates that it should be promptly reported to our incident response team. This ensures timely action.
- **Mitigation**: Once reported, our incident response team takes immediate action to mitigate the security incident, following predefined protocols and best practices.

In addition to EDR tools, we maintain a rigorous practice of continuous monitoring for security incidents and vulnerabilities reported by these tools. This proactive approach allows us to swiftly address potential threats, enhancing the security of Avian Cloud.

Security Training and Awareness

Avian Cloud places significant emphasis on security through the following measures:

- **Employee and Supplier Onboarding**: All Avian employees and suppliers undergo comprehensive security onboarding to ensure a strong foundation in our security practices.

- **Quarterly Competence Tests**: We conduct quarterly competence tests to assess and reinforce knowledge, ensuring that our team maintains a high level of security awareness.
- **Ongoing Awareness Workshops**: Regular awareness workshops are held to cover our security policies and procedures in-depth. These sessions promote best practices and provide continuous education on security matters.

These initiatives collectively contribute to our commitment to maintaining a secure environment and promoting security best practices across our organization.

Future Security Enhancements

At Avian, we are committed to ongoing security improvements:

- Our Information Security Management System (ISMS) governs security measures and ensures that we are always evaluating and enhancing security practices.
- We conduct continuous risk assessments, guided by the Plan-Do-Check-Act (PDCA) cycle, which is deeply ingrained in our procedures and company culture.
- Whenever we identify additional proportionate ways to enhance the security of Avian Cloud, we swiftly take action to implement these improvements.
- We ensure that our customers are informed of any significant security changes or enhancements to maintain transparency and trust.

This dedication to continuous improvement in security practices reflects our unwavering commitment to safeguarding Avian Cloud and our customers' data.