maya.ai

Security Controls in Azure Deployment

CONTENTS

1. Security Controls

1.1. Hardware

1.1.1. Virtual Machines

1.2. Networking

1.2.1. Virtua Network / Subnet

1.2.2. Security Groups

1.2.3. Firewall

1.2.4 Jump / Bastion Host

1.2.5. External Endpoints

1.3. Software

1.3.1. maya.ai Platform

1.3.2. Customizations

1.3.3. Deployment Environments

1.3.4. Virus scans on Builds

1.4. Physical Security

1.5. Monitoring and Logging

1.5.1. Monitoring

1.5.2. Logging

2. Identity and Access Management

2.1. Access Management for Azure Cloud

2.1.1. Access Management for Azure Virtual Machines

2.2. Access Management for Crayon employees

3. Data Protection

3.1. Data Segregation

3.2. At-Rest Data Protection

3.3. In-Transit Data Protection

4. Compliance

4.1 Cloud Compliance

4.2 VA and Penetration Testing

Crayon follows the Defense-in-Depth approach in order to address security. This comprehensive strategy, which promotes a security-first culture, spans technology, policies, and procedures. Crayon’s Defense-in-Depth covers Customer Data, Application, Host, Network, Physical, Logging and Monitoring, Policies, Procedures, and Awareness.

1. Security Controls

1.1. Hardware

1.1.1. Virtual Machines

* Virtual Machines (VMs) will be used for multiple purposes in maya.ai including but not limited to hosting applications, API & processing the data.
* All the VMs will be protected by Trend Micro Deep Security, host-based enterprise tool, which protects VMs from Malwares & detect/prevents VMs from vulnerabilities through the virtual patching.

1.2. Networking

All customer specific resources will be hosted on dedicated Crayon Cloud with necessary logical separations. Systems that have highly sensitive information will be isolated logically, especially when client agreements require such isolation. External access to systems will be restricted and accessible only from Crayon Cloud and Authorized Networks (Customer Network & Crayon Office / VPN).

1.2.1. Virtual Network / Subnet

* Virtual networks will be created with enough IP address spaces for flexibility.
* For logical network separation, dedicated subnets will be created for each component (SFTP, Bastion / Jump Host, Data Platform etc.).
* Broad-Range of subnets are avoided.
* Network access controls between subnets will be ensured.

1.2.2. Security Groups

* Network security groups will be segregated to protect against unsolicited traffic into Azure subnets. Strict network security rules will be imposed with the use of 5-tupe approach (source IP, source port, destination IP, destination port, and layer 4 protocol), to allow/deny rules for network traffic.
* Access to application / service ports will be enabled only after proper approvals from stakeholders.

1.2.3. Firewall

* Azure Firewall, cloud-based network security service, will be used to protect Azure Virtual Network resources. It's a fully stateful firewall-as-a-service with built-in high availability and unrestricted cloud scalability to accommodate traffic across network.
* Application and network connectivity policies are centrally managed & logged across subscriptions and virtual networks.
* Azure Firewall is fully integrated with Azure Monitor for logging and analytics.

A screenshot of a cell phone

Description automatically generated

1.2.4. Jump / Bastion Host

* Any customer specific resources will be accessible only from the Jump Host/ Bastion, where-in users connect to Jump Host/ Bastion only through Point-to-Site VPN privately.
* Point-to-Site secure channel will be configured for the users connecting remotely and Point-to-Point secure channel will be configured for the users connecting from Crayon Office Network.
* Dedicated Subnet & Security Group with no access to the Internet will be configured.
* Data stored in client-specific clusters and systems will be accessible only through Jump Host.
* Clipboards & Local Drive mappings will be disabled in the Jump Host to avoid data leakage.

1.2.5. External Endpoints

Crayon understands that any single weakness in one portion of the network can create vulnerabilities that can be exploited to attack or access some other resource elsewhere on the network. Crayon aims to secure every Cloud resource, with network security at its core.

* Internet Facing Endpoints will be restricted with subnet level security groups to allow access only from the Customer authorized IP addresses.
* Azure Web Application Firewall (WAF) on Azure Application Gateway will be used for the endpoints exposed over the internet. Azure WAF provides centralized protection of web applications from common exploits and vulnerabilities based on Top 10 OWASP policies.
* External access to resources will be restricted and accessible only from Crayon Cloud and authorized networks (Customer Network & Crayon Office / VPN)
* Access to public networks from Crayon Data’s systems and networks will only be by approved routes.
* Strict network security policies will be enforced for connecting to Crayon networks from remote systems.
* All connections to the Internet or other internal networks will be secured through suitably configured firewalls & private endpoint connections.

1.3. Software

On Software Engineering Crayon Data practices and follows Secure Development Lifecycle Process which includes Secure Development Environment, System Acceptance Testing Process & Practices.

1.3.1. maya.ai Platform

All components in the maya.ai platform stack that will be installed in the Azure environment are custom built following the Crayon Software Development Lifecycle (SDL) process. All software components will be deployed by following proper change and release management process.

1.3.2. Customizations

All components will be custom developed, based on customer requirements including authentication, UX and frontend interfaces will follow the same SDLC processes followed at Crayon.

1.3.3. Deployment Environments

The solution will have dedicated production, staging & necessary development setup for the complete stack. Production setup will be enabled with failover mechanism for higher availability. Staging setup will be a replica of production and any changes to the production environment will be done only after testing in Staging environment.

## 1.3.4. Virus scans on Builds

Application builds in general are bundled into docker containers to make the dependency management simpler and deployment easier. All the docker container images are scanned in Container Registries as part of CI/CD setup. Any vulnerabilities in the docker images will be notified to DevOps team for reviewing & fixed accordingly. Secured images will be deployed across all the environments.

1.4. Physical Security

The proposed system and application will be hosted and served from Azure data centers. Crayon relies on the best practices and world class physical security controls put in place by Microsoft. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the data center resources. Datacenters managed by Microsoft have extensive layers of protection, access approval at the facility’s perimeter, at the building’s perimeter, inside the building, and on the datacenter floor.

Further information can be accesses at this [link](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security).

1.5. Monitoring and Logging

1.5.1. Monitoring

Monitoring will be enabled for the complete stack with an alerting mechanism for any failures. Detailed monitoring of networking & system components for virtual machines and gateway will be leveraged using Azure Monitor & Insights.

1.5.2. Logging

Logging will be enabled across all layers of the infrastructure. All the logs will be streamed to Azure Log Analytics workspace for diagnosing any ambiguities, with a retention period of a year.

2. Identity and Access Management

Crayon has a dedicated Security Team that is responsible for infrastructure security, application security, security operations, and compliance (ISO 27001). The security team partners with engineering and is involved in all phases of the development process, including security design reviews, code testing, security testing of new features, penetration testing, and secure coding training. All members of the team have advanced technical degrees.

2.1. Access Management for Azure Cloud

* Access to Azure accounts will be managed by IAM users, groups, and roles, based on the principle of least privilege.
* All access requests will be approved by the security team based on business and technical justification provided by the Professional Services team.
* MFA for Azure Portal access will be enabled for all the users with conditional allow from Trusted IPs. Users signing from untrusted IP address are blocked.
* All access requests are managed and available for audit in Jira, software tracking system.
* Additional approvals may be required for specific components based on client requirements.

2.1.1. Access Management for Azure Virtual Machines

Just-in-time access will be enabled to lock down all the VMs at network level by blocking inbound traffic to management ports (like 22 & 3389), which reduces the attack surface by allowing access only upon a specific need. Even admins would need to go through Just-in-time VM request to access any servers through Jump Host.

Below will be the process followed for JIT:

* VMs will be enabled for JIT access with predefined protocols, source Ips & maximum request time of 3 hours.
* JIT request access will be provided to authorized users.
* Upon a user request, based on Azure RBAC, Security Centre will decide whether to grant access. If a request is approved, Security Centre automatically configures the NSGs to allow inbound traffic to defined ports, for the requested amount of time, after which it reverts the NSG rules to its previous state.

2.2. Access Management for Crayon Employees

* Access to all information services and facilities will be controlled through a formal registration through Email / Access Registration form.
* Access for new users or users with changed rights will be processed by the Information Owner / Custodian only post completion of authorization procedures.
* A formal record will be maintained by the Information Owner / Custodian of all persons registered to use the customer infra.
* Periodic (Quarterly) access reconciliations are done to check for accounts that are no longer required.
* Access revocations will be performed as part of employee exit process.

3. Data Protection

3.1. Data Segregation

maya.ai is a single-tenant service, which means deployments will strictly be in a dedicated virtual network offered by the cloud provider.

3.2. At-Rest Data Protection

* Azure Disk Encryption (ADE) will be enabled on OS and Data disks for all virtual machines.
* Azure Disk Encryption (ADE) uses DM-Crypt feature on Linux and Bitlocker feature on Windows, at backend for encryption.
* Additional layer of security will be imposed using Key encryption key (KEK), asymmetric key (RSA 2048) that protects or wraps the encryption secrets, which will be securely stored in Azure Key Vault.
* KEK’s will be rotated on a quarterly basis, with entire process of key creation, management, rotation & retirement handled by Automation runbook.
* Data in storage services will be encrypted using Azure Storage Service Encryption (SSE), which encrypts data before it is stored, and automatically decrypts the data during retrieval.
* Storage Service Encryption (SSE) uses 256-bit Advanced Encryption Standard (AES) encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.
* In addition, Azure data lake will be encrypted with Customer Managed Key (CMK), which will be securely stored in Azure Key Vault.

3.3. In-Transit Data Protection

* Data transfer between Customer Network and Crayon SFTP (if applicable) will happen through Site-to-site VPN established between Customer and Crayon, which uses IPsec/IKE policy with specific cryptographic algorithms and key strengths for transport encryption.
* Point-to-Site VPN will be used to allow individual client computers to access Azure virtual network resources, which uses Secure Socket Tunnelling Protocol (SSTP) at backend.
* Communication to, from and between the virtual machines are encrypted in different ways, RDP sessions to windows machines are encrypted with TLS and SSH sessions to linux machines uses key-pair, asymmetric encryption, for authentication.
* Customer facing endpoints are encrypted with Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway).
* For Azure Data Lake, in addition to encryption at storage layer data is also secured in transit by using HTTPS. HTTPS is the only protocol that is supported for the Data Lake Storage REST interfaces.

4. Compliance

4.1. Cloud Compliance

Crayon will make sure cloud infra components will adhere to following regulatory standards & continuously monitor the same to bridge any gaps.

Azure CIS, SOC TSP, PCI DSS and ISO 27001

Any other customer specific regulatory standards can be considered during engagement.

4.2. VA and Penetration Testing

All virtual machines will be assessed with ASC integrated vulnerability scanner powered by Qualys. Below are the SLA for VA Remediation on account of obtaining the vulnerabilities in regular intervals (Quarterly / Half-yearly).

Periodic Penetration Testing will be conducted and as per client standard requirements.