matrix insights

Technology and Security Overview

Application and Architecture 2
- **Introduction** 2
- **Architecture** 2
- **Application Security** 3
- **Authentication** 3
- **Configuration and Customization** 4
- **Account Management** 5

Security 5
- **Security Policy** 5
- **Security Response Team** 6
- **Physical and Environmental Security** 7
  - Overview 7
  - Fire Detection and Suppression 8
  - Power 8
  - Climate and Temperature 8
  - Management 8
  - Storage Device Decommissioning 9
- **Network Security** 9
  - Firewalls 9
  - DDoS Mitigation 9
  - Spoofing and Sniffing Protections 10
  - Port Scanning 10
- **Data Security** 10

Availability and Redundancy 11
- **Redundancy and Scalability** 11
  - Redundant Infrastructure 11
  - Scalability 11
- **Performance and Availability Monitoring** 12
- **Data Storage and Backup** 13
  - Data Storage 13
  - Database Backups 13
- **Disaster Recovery** 13
  - Multiple Geographic Locations 13
  - Recovery Plan 13

Business Confidential

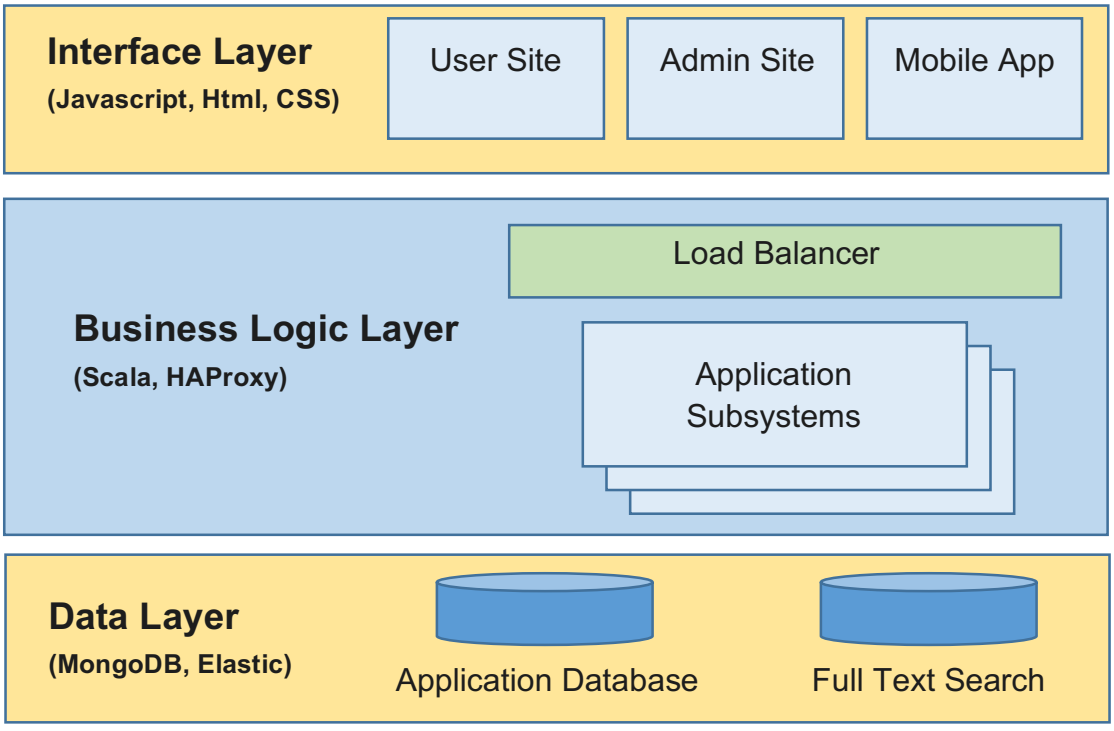
Application and Architecture

Introduction

Matrix Insights offers a wide range of products and services via its Software-as-a-Service (Saas) platform. This document provides details of Matrix Insight's design, development, maintenance, and support practices.

For additional technology or security details, or to answer any questions related to the information in this document, please contact your Matrix Insights account representative to schedule a call with the appropriate Matrix Insights staff.

Architecture



Matrix Insights uses a three-tier application architecture with an interface layer, business logic layer, and data layer.

The interface layer provides interfaces for both users and administrators. The web-based interface utilizes javascript and traditional web technologies to create a single-page application (SPA). The mobile application has separate presentation logic, but utilizes the same business logic layer as the web application. The logic in this layer is limited to data presentation and basic data validation.

The business logic layer provides primary logic controls for the application. It is an object-oriented framework written in Scala and running within a Java Virtual Machine (JVM).

The data layer provides data-persistent services for both primary application data and client-specific data. All data is stored in MongoDB, the application's primary database technology. A subset of the data is also stored in Elastic (Apache Lucene based technology) to facilitate full text searching.

Application Security

Matrix Insights provides data security through a Role-Based-Access-Control (RBAC) security model. The application manages each client's data into separate tenants (organizations). Data visibility is managed through a combination of tenant filtering rules, data visibility rules, and user account privileges ensuring the security and confidentiality of all client data. Access is restricted to authorized users only.

Authentication

There are two primary authentication options for Matrix Insights: Internal authentication and external authentication (single sign-on,

SSO). Custom authentication solutions may also be supported.

Matrix Insights provides a traditional account-based authentication model. Users are required to provide a username and password combination which is associated with their user account. These credentials are stored and maintained within the Matrix Insights application. The system provides robust security options including password management and recovery options.

An external authentication options is made available via SSO utilizing SAML 2.0.

Key SSO capabilities:

- Secured via digital signatures and XML-encryption
- Enables direction connection to existing authentication system or tool
- Does not require the sharing of an individual's credentials

Configuration and Customization

The Matrix Insights application is designed to be highly configurable. Changes to configuration can be managed through the administration site and include:

- Security settings
- Subscription management
- Organization management
- Team/Group management
- Assessment/Content availability
- Messaging and logos
- Other general site preferences

Account Management

The following account management options are available with the application:

- Administration management enables the creation, editing, and deactivation of user accounts within the administrator's organization and all child organizations.
- User management enables configuration of several user settings and preferences including but not limited too: email address, password, communication preferences, and personalization settings.
- Optionally users may also be granted privileges to invite 360 raters or give additional users access to the system.

Security

Security Policy

It is the policy of Matrix Insights to protect its information and assets in accordance with all federal and state statutes and regulations, as well as with effective information security practices and principles.

Matrix Insights specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or causing loss of Matrix Insight's information assets. It also prohibits using information assets to violate any law, commit an intentional breach of confidentiality of privacy, compromise the performance of systems, damage software, physical devices or networks, or otherwise sabotage Company information assets.

Matrix Insights protects its information assets from threats and exploits, whether internal or external, deliberate or accidental. The degree of protection is based on the nature of the resource and its intended use. The Company recognizes that no single office, policy or procedure provides absolute security; therefore, all Company employees and other stakeholders share responsibility to minimize risks and to secure the information assets within their control.

Matrix Insights shall take appropriate action in response to misuse of Company information assets. Any violation of this policy may result in legal action and/or Company disciplinary action under applicable Company and administrative policies and procedures.

Security Response Team

Matrix Insights incident management process has been designed to minimize impact to suspected and actual information security threats through detailed oversight and execution of processes and procedures. The incident management framework is modeled after FEMA/NIMS/ICS procedures 100-400. Matrix Insights has created an Information Security Incident Response Team (ISIRT) with responsibility for managing information security threats.

The ISIRT provides a structured response mechanism for Matrix Insights managerial and technical staff in order to: timely identify potential and realized threats; respond systematically to information security incidents; stabilize impacted environments; and determine root cause and corrective actions while collecting and documenting information consistent with legal requirements and industry standards.

The ISIRT has seven stages of readiness currently defined:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Post-Mortem
- Reporting (throughout the life of the incident)

Physical and Environmental Security

Overview

Matrix Insight's infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3
- Sarbanes-Oxley (SOX)

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

Our infrastructure provider monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, our infrastructure provider's procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Our infrastructure provider uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Network Security

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

DDoS Mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to.

Port Scanning

Our infrastructure checks for port scanning activity. When port scans are detected, they are stopped and access is blocked.

Data Security

- In transit, data is secured by TLS (1.2, 256 bit) for HTTP traffic.
- At rest, data is secured in database servers located behind several layers of firewalls and are inaccessible from the Internet.
- Media containing confidential information is sanitized in accordance with DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization")

Availability and Redundancy

The Matrix Insight application was designed from inception to be a high-availability Software-as-a-Services (SaaS) solution. Availability and performance are key requirements for every SaaS implementation, and infrastructure redundancy and scalability are fundamental in achieving these requirements.

Redundancy and Scalability

Redundant Infrastructure

- The web server/application tier runs on multiple servers in a load balanced group. Failure of a particular server or application instance won't have a catastrophic impact on users. Load is simply rebalanced across the remaining servers and instances.
- All servers have redundant power supplies and network connections to ensure that a failure of one of these components is seamlessly handled and no impact to availability or performance is experienced by users.
- Load balancers, firewalls, and infrastructure monitoring are used to make sure these critical components are available to support user demand, security, and availability requirements.
- Application data and content are housed on highly redundant, mass storage devices that not only ensure high availability, but also high performance.

Scalability

- Both our infrastructure provider and database technology were chosen for their ability to support horizontal and vertical

scaling. This will simplify the process of increasing capacity to meet higher demand and to achieve performance commitments.
- 24x7 monitoring of equipment and application-level transaction performance supports proactive planning, tuning, and expansion initiatives.
- Matrix Insights maintains an exact replica of the production environment for performance testing. All software releases are tested in this environment prior to promotion to production to ensure no degradation in performance is experienced. This environment consists of servers with identical hardware and software configurations to the production environment.

Performance and Availability Monitoring

Monitoring of the application, infrastructure, and Internet connectivity is critical to ensuring that availability and performance commitments are achieved. Matrix Insights uses a variety of tools deployed both internally and externally to monitor the application.

- Within the infrastructure, real-time monitoring is performed to verify application availability and health of various components.
- Hardware-level monitors evaluate CPU, memory utilization, disk space, and I/O.
- Internal monitoring processes are use to verify key system work flows are available and working as expected.
- A 3rd party service is utilized to monitor database responsiveness and backup integrity.
- Every monitor has thresholds established with warning and alert levels which, when not met, result in alert messages being sent to operational support.
- Operational personnel, software development resources, and

management are on-call 24x7 to monitor systems, investigate, and resolve issues.

Data Storage and Backup

Data Storage

Application data and content are housed on highly redundant, mass storage devices that not only ensure high availability, but also high performance.

Database Backups

Matrix Insights uses a best in class database backup service to ensure that every transaction is safely and securely stored. Every change to the database is encrypted and streamed to our database backup service. The service produces full backups every 6 hours and supports point-in-time restorations for the last 24 hours.

Disaster Recovery

Multiple Geographic Locations

Matrix Insights distributes servers over multiple geographic locations to mitigate localized issues that might lead to outages.

Recovery Plan

Matrix Insights has designed, developed, documented, and tested its disaster recovery plan. The plan satisfies the following requirements:

- The recovered applications must satisfy the same performance,

security, and availability service level agreements as the production applications.

- The recovery must include full restoration of data.
- The recovered application must be capable of hosting the application for an indefinite amount of time.