My Workplace Health

Security Overview

OCI (Oracle Cloud Infrastructure)

Version 14 - October 2022

Contents

Document Context

The purpose of this document is to provide an initial overview of our approach to data security in a cloud environment.

An overview of the technical components of My Workplace Health is also provided for background information.

Should there be a need for a more detailed review, then My Workplace Health is more than willing to comply with any IT security audit process.

Figure 1 - Products such as the Emergency Services Health Portal and Check My Vax contribute to My Workplace Health's comprehensive software suite

Who is My Workplace Health?

What is our idea?

- To provide a 'modular' health risk management platform to employers and health providers that delivers a healthier workforce and proves the ROI in employee health.

- To provide technology solutions to support the processes of existing providers in the provision of employment-related health assessments and services.

Figure 2 - The Health Cloud application incorporates many satellite applications for capturing data

Who is My Workplace Health?

What is our solution? *My Workplace Health is a holistic health risk management solution.*

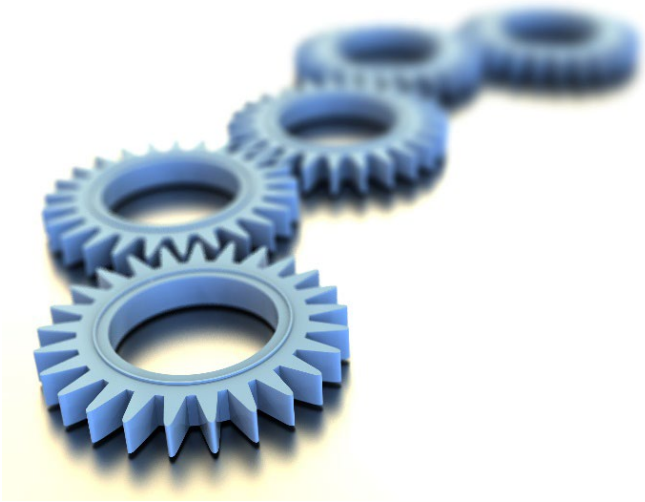
- Managing the complete employee lifecycle, or one to several components including;
  - Vaccination Booking and Management (including COVID 19, Influenza etc.)
  - Pre-Employment Screening
  - Health & Wellbeing Management
  - Critical Incident Management
  - Mental Health Management
  - Injury & Case Management
  - Pharmacy & Inventory Management
  - Provider Management and Invoicing
  - Health Intelligence

Figure 3 - The Emergency Services Health Portal caters to all aspects of health management and tracking

- Enabling the measurement, monitoring & control occupational health risk, in one place
- With unique IP generating health risk profiles (patent) that prompt targeted action
- Easily tailored by the user to automate existing products and services to manage identified health risks
- Delivered via 'the Cloud' - accessible anywhere on any device

Technical Overview

- Health Risk Management Systems HRMS (trading as My Workplace Health software by 2CRisk) is an Independent Software Vendor (ISV)
- 2Crisk is a dedicated, purpose-built cloud-based solution
- Whilst we also deploy on AWS, this document covers our OCI (Oracle Cloud Infrastructure) deployment.
- It is developed and primary hosting is in Australia using Oracle technology
- Instances are established in different geographies to meet local legislative requirements as required
- The architecture of the application and infrastructure is designed to provide secure and controlled access at all levels
- We see this as an essential part of our business model as an ISV providing solutions via the cloud



- The architecture is designed for high availability (>99.98%) & high resilience
- We have been audited by 3rd party organisations such as Hivint, Deloitte's and PWC on behalf of our customers in the past and are happy to support this process

Software Architecture

Hosting

Our solutions are hosted on Oracle Cloud Infrastructures

Data Centre's are in Sydney and Melbourne.

Additional instances are implemented in other geographies as required to meet local privacy requirements

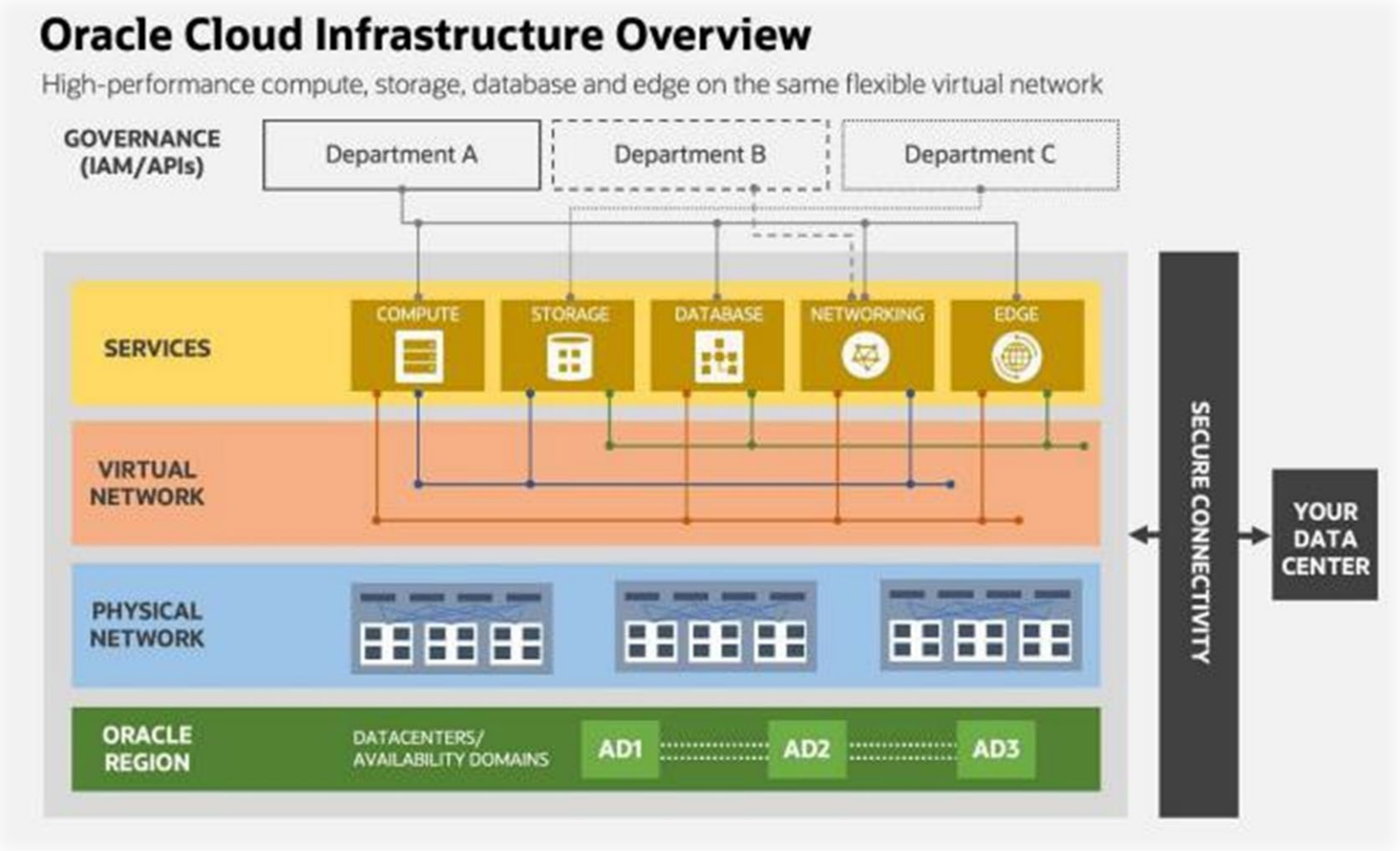
2Crisk Platform

Operating System - Oracle Linux

Database - Oracle Application Development Platform - Oracle Application Express versions 5.1, 18.2 and 20.1

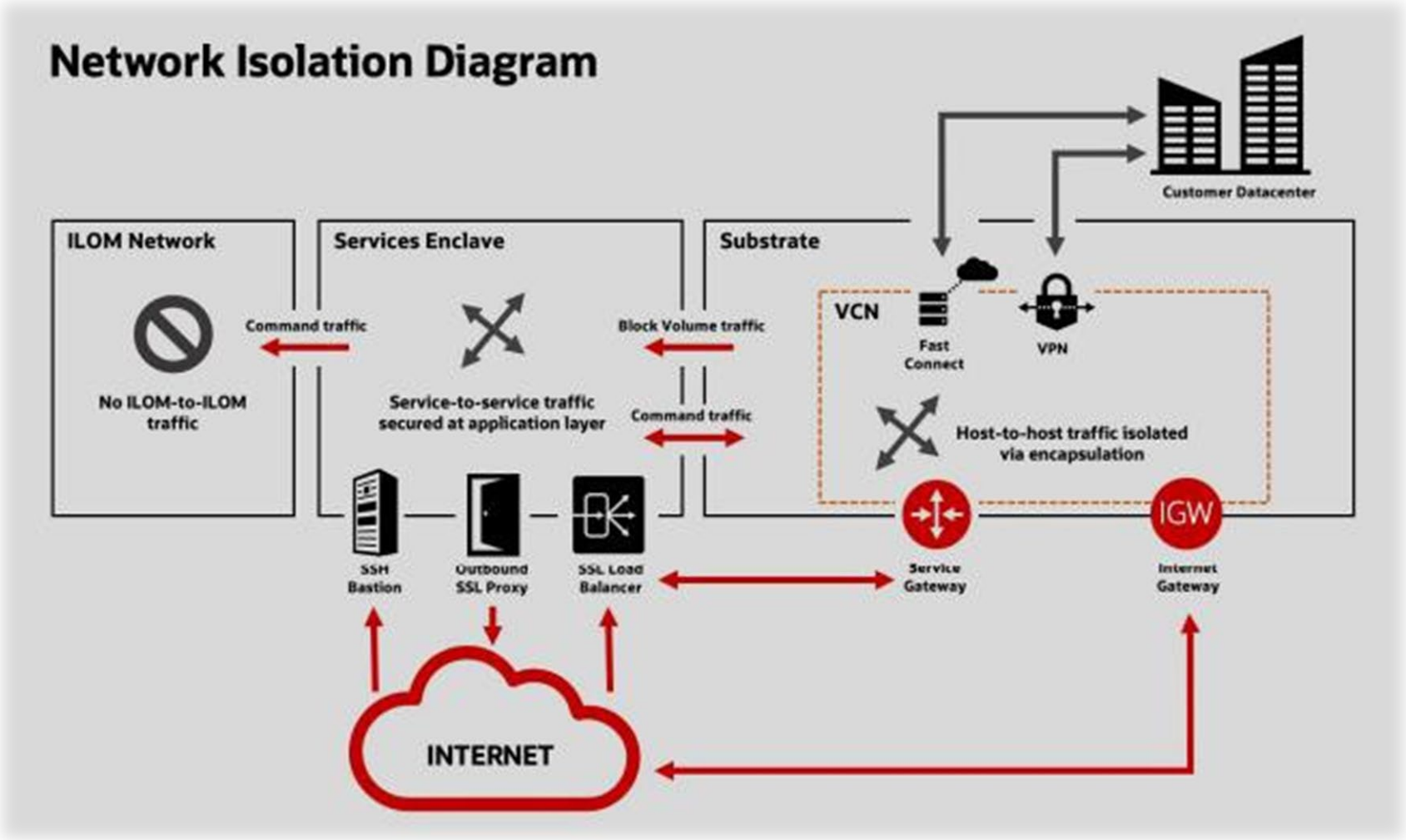
Infrastructure Overview

Figure 4 - Oracle cloud infrastructure overview



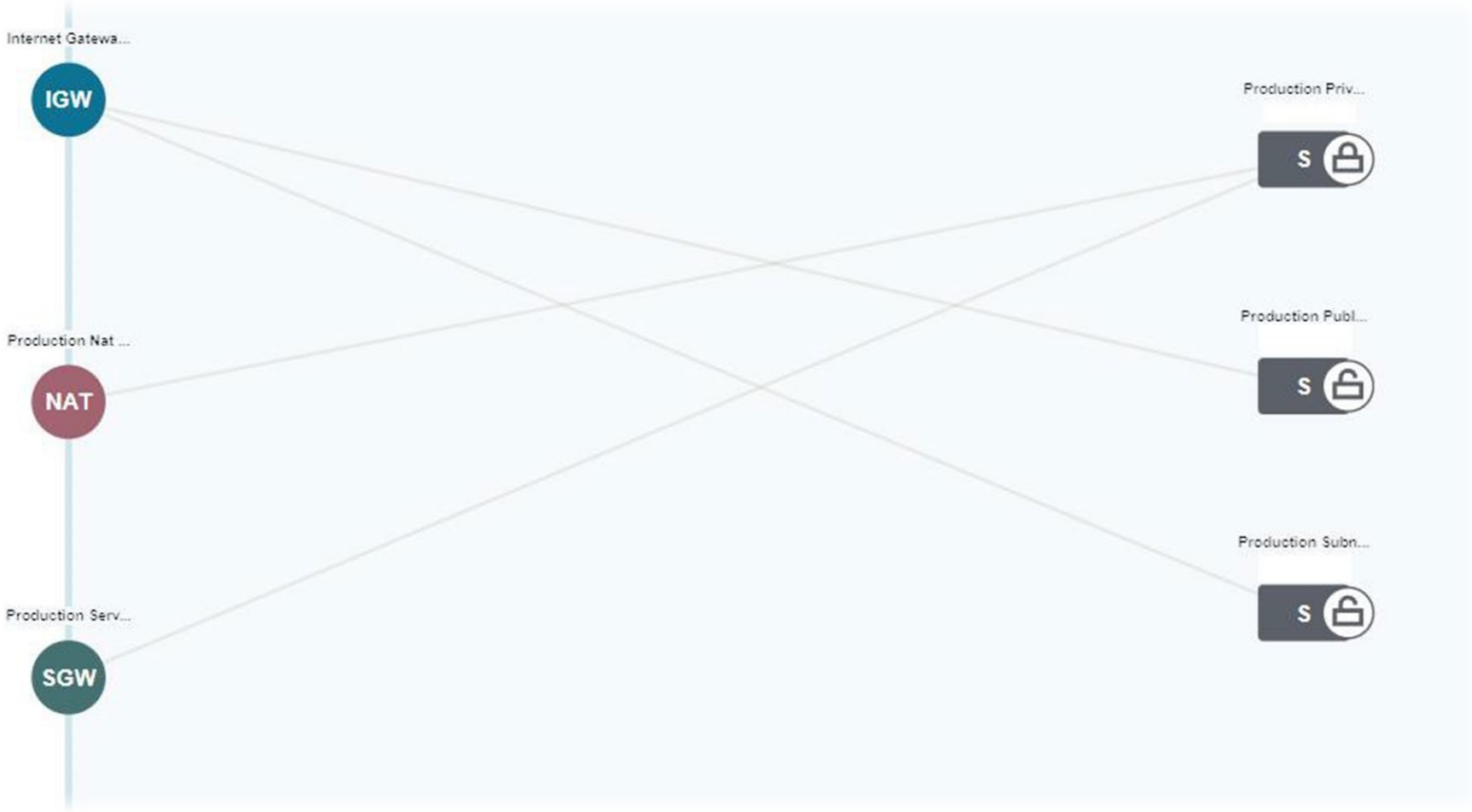
OCI Network Isolation

Figure 5 - OCI network isolation



Internal Network Services

Figure 6 - My Workplace Health internal network services



Privacy & Security - Summary

Availability - > 99.95%

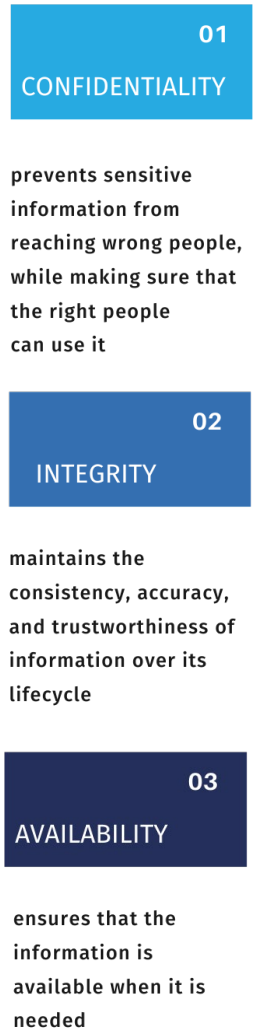
Resilience - Hosting, DRP & BCP

- Instances hosted in Australia on Oracle Cloud Infrastructure
- Incremental back-ups are taken daily
- Full back-ups managed by Autonomous Database Services
- Database can be restored from any back-up, restoration process can begin immediately
- Manual backup operations can also be custom configured

Data Centre Compliance

- OCI complies with and is certified for SOC1, ISO27001, PCI, DSS1
- HIPAA (US)
- ISM (Australia)
- Further information can be found at the OCI Documentation library

Figure 7 - The three pillars of security



External & Internal Vulnerability

- Data encryption in transit
- SSL encryption deployed using TLS
- WAF (Web Application Firewall)
- Protection against Layer 7 DdoS Attacks, Cross-Site Scripting, SQL injection and more
- IDS / IPS (Intrusion Detection & Prevention Systems)
- Penetration testing every 6 months
- Security patches applied monthly or immediately for high level threats

Application Security

- Two Factor authentication (if required)
- Customer defined role based security applied at a user level
- Individual health data can be de-identified
- Full password hardening invoked at user level (SHA3 hashing invoked)

Database Restoration Features

Figure 8 - Databases can be restored from a time stamp

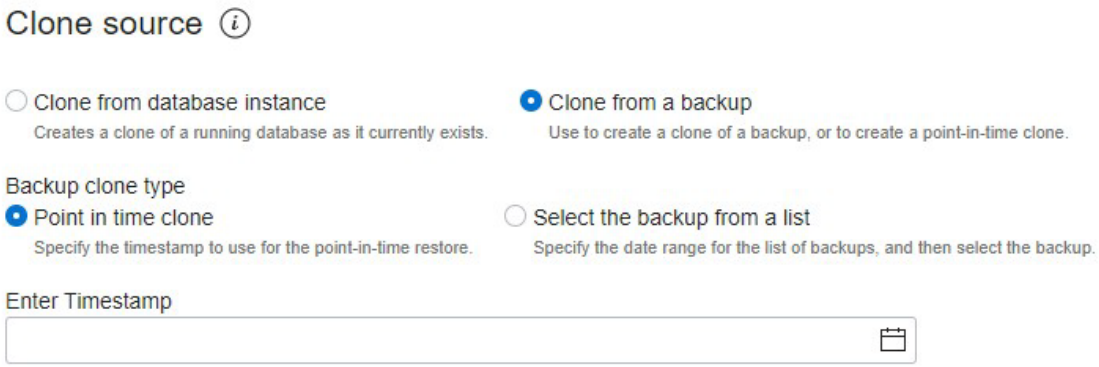
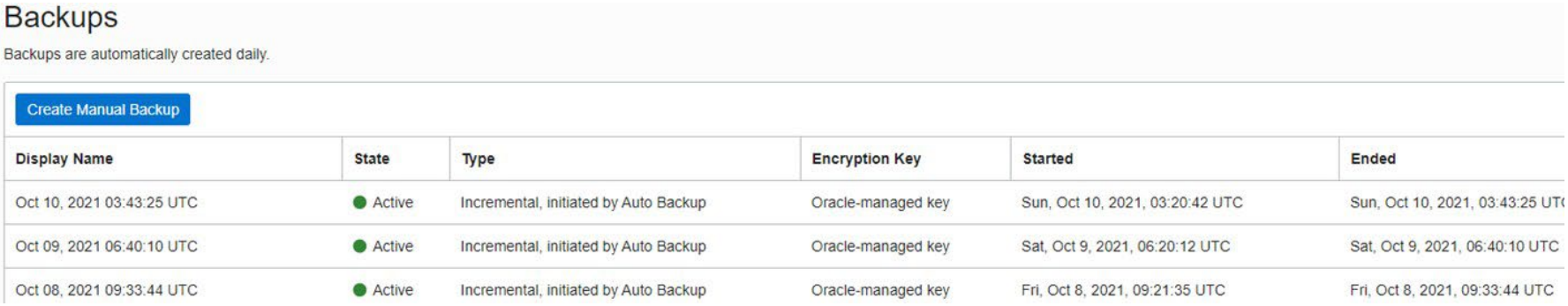
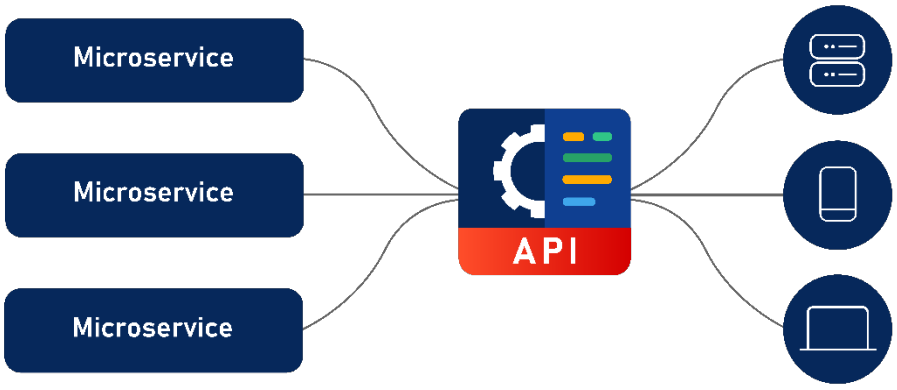


Figure 9 - Databases are backed up automatically



Display Name	State	Type	Encryption Key	Started	Ended
Oct 10, 2021 03:43:25 UTC	Active	Incremental, initiated by Auto Backup	Oracle-managed key	Sun, Oct 10, 2021, 03:20:42 UTC	Sun, Oct 10, 2021, 03:43:25 UTC
Oct 09, 2021 06:40:10 UTC	Active	Incremental, initiated by Auto Backup	Oracle-managed key	Sat, Oct 9, 2021, 06:20:12 UTC	Sat, Oct 9, 2021, 06:40:10 UTC
Oct 08, 2021 09:33:44 UTC	Active	Incremental, initiated by Auto Backup	Oracle-managed key	Fri, Oct 8, 2021, 09:21:35 UTC	Fri, Oct 8, 2021, 09:33:44 UTC

API Capabilities



Existing API Interfaces

- Successfully completed NOI (Notice of Integration) with Services Australia for
- AIR - Australian Immunisation Registry
- Australian Medicines Terminology

We utilize a combination of Oracle API Gateways, which is a fully managed service to intergrade with networks on Oracle Cloud Infrastructure, and Oracle Functions, a platform for deploying serverless computing solutions. API gateways enable customers to publish public or private APIs and process incoming requests. Our. API gateways protect and isolate backend services and meter API calls, whilst our functions ensure separation of API business logic from secure data. Connections to API gateways always use TLS to preserve the15rivacyy and integrity of data.

Privacy & Security - Key Aspects

Section	My Workplace Health
Acceptable Usage	•HRMS employee access to client instance only to investigate reported issues by client or as agreed with client •Sessions terminated after period of activity (current policy setting 60 mins) •All HRMS employees sign IT policy including data privacy & access •Each 2Crisk user has a separate username and password
Access Control	•Full password hardening, hashing (SHA 2) & resetting policies enforced •Compliant physical access controls exist at dedicated 3rd party data centre •Application access & permissions controlled at user level, through customer defined role base security module. •Authentication via SSL security deployed using TLS •Two Factor Authentication •Data can be deidentified and user access can be set to only see deidentified data •Access to Control Panel controlled at user level
Anti-Malware	•Fully compliant anti-virus software and settings at 3rd Party Data Centre
Audit Logging	•All changes are logged at a database level and date time stamped and retained in perpetuity •User accessed audit trails exist in key parts of the application •Time and date are synchronized externally at a database level •All emails and SMS utilizing HL7 requirements

Privacy & Security - Key Aspects

Section	My Workplace Health
Back-Up & Recovery	•Incremental daily back-ups fully managed by Oracle Autonomous Database •Full backups initiated as needed by Autonomous services. •Recovery process is tested on a 6 monthly basis •Recovery can be initialized as a cloned database.
Cryptographic Controls	•Access to the application has full TSL and SSL security and encryption. •EBS Volume Encryption (data at rest inside volume) •Encryption of data in-transit from EC2 instance to EBS storage •FTP (File Transfer Protocol) m3. medium instance, including EBS (Elastic Block Store) and 256bit "gold standard" encryption.
Customers and Members	•Customer access is controlled using identified username and password access as previously described •Two Factor Authentication is available •If member access is required, appropriate controls will be invoked •PDF Reporting-7Zip password protection capability •AES-256bit encryption for 7Zip PDF Files
Electronic Commerce	•N/A - no credit card transactions / payments made with 2CRisk
Evidence Collection	•All changes are audited as previously described
Exchange of Information	•Health data is protected as previously described

Privacy & Security - Key Aspects

Section	My Workplace Health
Physical Security	•Full controlled access and tracking to physical environment is maintained at OCI. Compliant with ISO27001
Roles & Responsibilities	•All appropriate roles & responsibilities are defined and link with HR policies previously described
Human Resources	•All employees sign full contract including confidentiality agreement, IT policy and disciplinary processes •All contractor organisations & individuals sign appropriate NDA agreements
Software Development	•Appropriate coding standards are maintained •Access to source code is controlled with access limited to specific roles •All IDE (Internal Development Environments) utilize VPN access •Thorough testing regimes are maintained prior to release with full test scripts •Issue tracking and resolution process and tools in place
Suppliers and Partners	•Any licensing agreements are formally maintained including fully maintained use of Oracle database

Notifiable Data Breach Scheme

The Notifiable Data Breaches Scheme (NDB) under Part IIIC of the Privacy Act 1988 establishes requirements for entities in responding to data breaches.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 establishes the NDB scheme in Australia from the 22nd February 2018.

2CRisk maintains an eligible data breach statement and includes:

- Identity and contact details of the entity (s 26WK(3)(a))
- Description of the eligible data breach (s26WK(3) (b))
- Kind of information involved (s 26WK(3) (c))
- Recommended steps (s 26WK (3) (d))

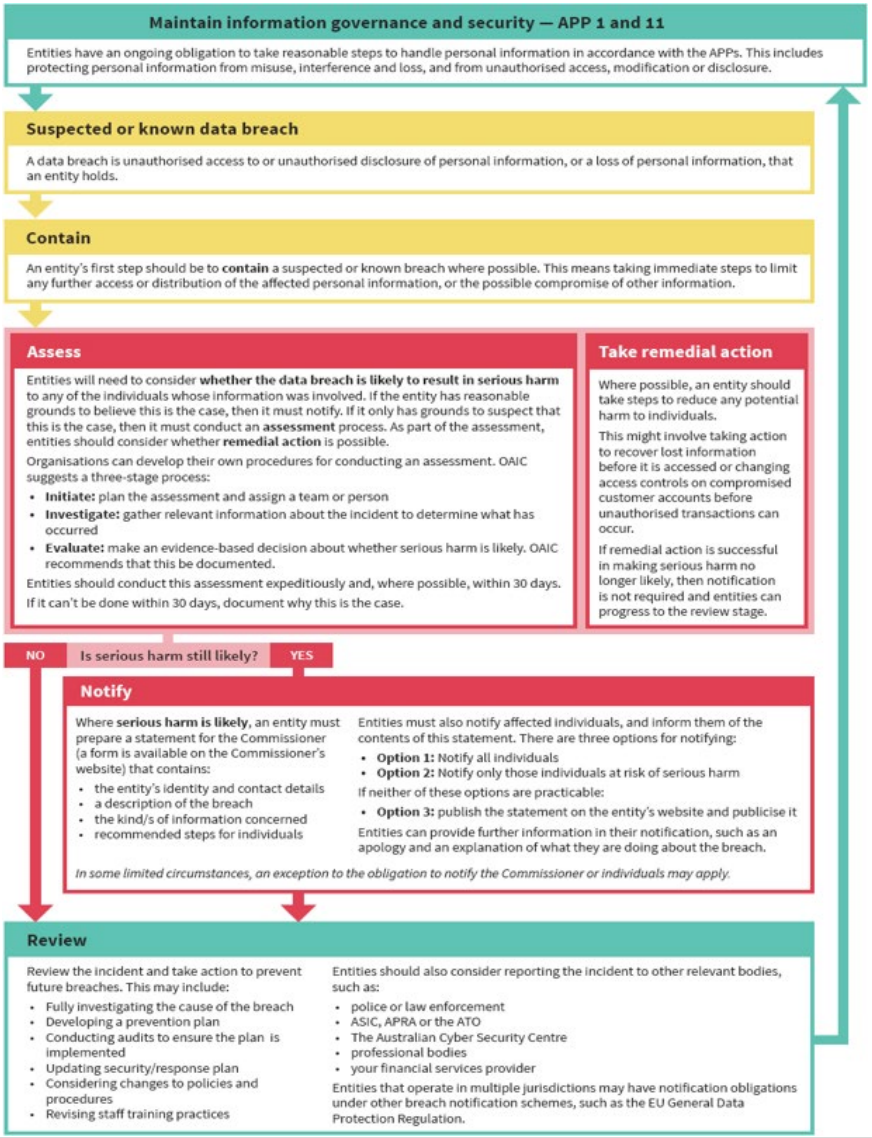
Notifiable Data Breach Scheme

Name	Responsibility
Mark Cassidy	Chief Executive Officer - Privacy/NDB Manager Direct Contact: 0418 893 291, markc@2CRisk.com.au PO BOX 826, Templestowe, VIC, 3105.
Adam Heppenstall	Chief Technical Officer - My Workplace Health
Andrew Douglas	CEO, FCW Lawyers, Company Legal Representative

Organisation	Details
CFC Underwriting	Underwriters for HRMS (2CRisk) Cyber Insurance 85 Gracechurch Street, London, EC3V OAA, UK
Lloyds of London	Policy No: ESG00502679 1 Lime Street, London, EC3M 7HA, UK
Policy: ESG00502679 Start: 00.01 LST 05/02/2018	Health Risk Management Systems Pty Ltd SAAS/ASP Software development, installation and maintenance - Organisational Health and Safety Software.

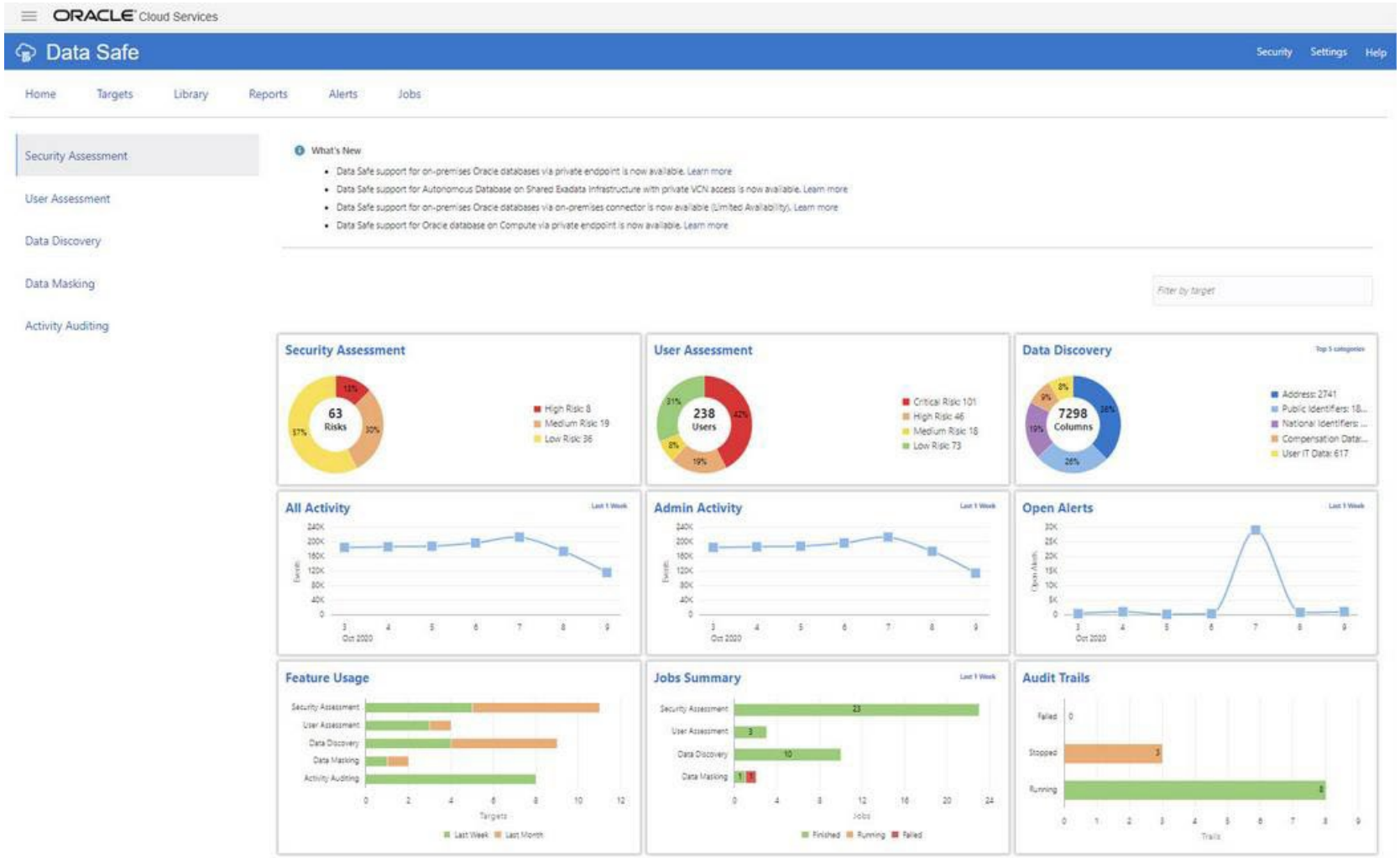
Maintain Information - Process Flow NDS

Figure 10 - Maintain information - process flow NDS



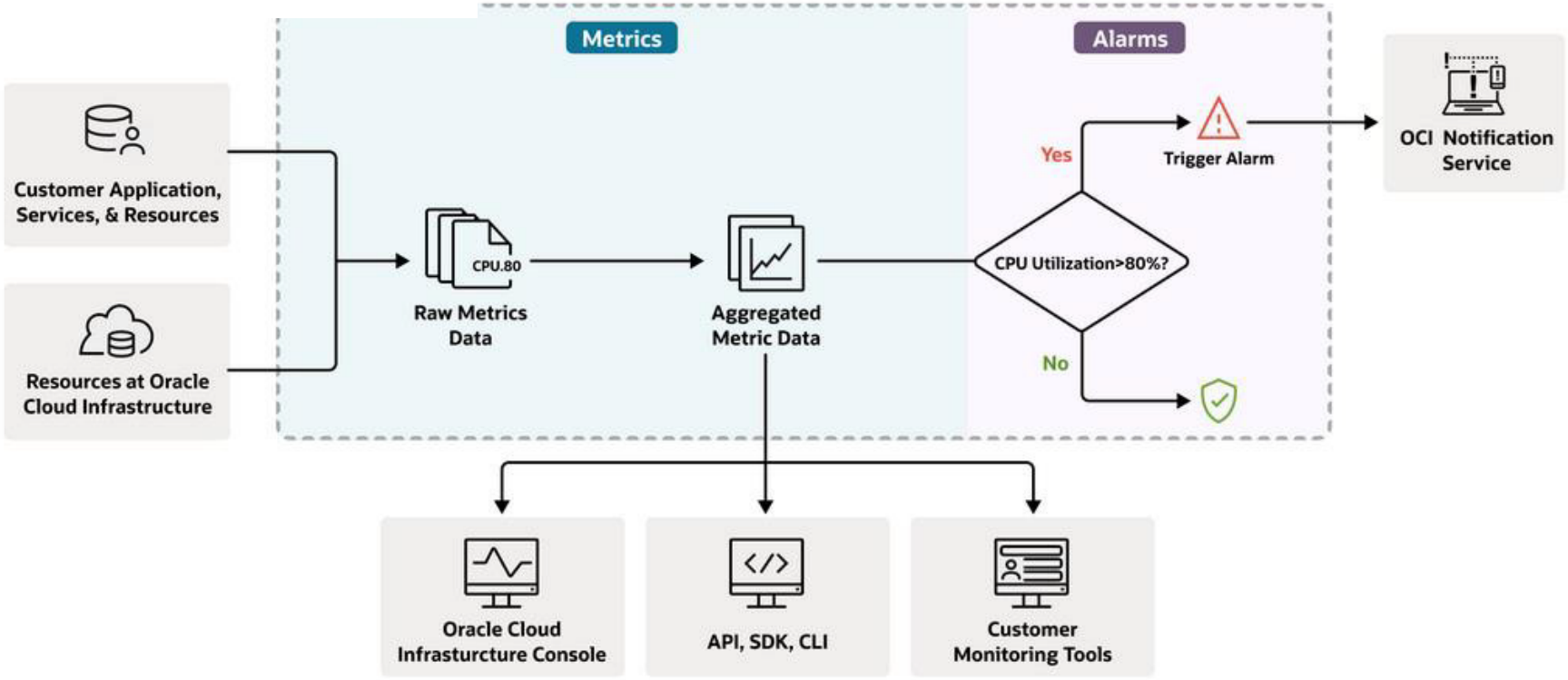
Unified Database Security

Figure 11 - Oracle cloud services provide unified database security



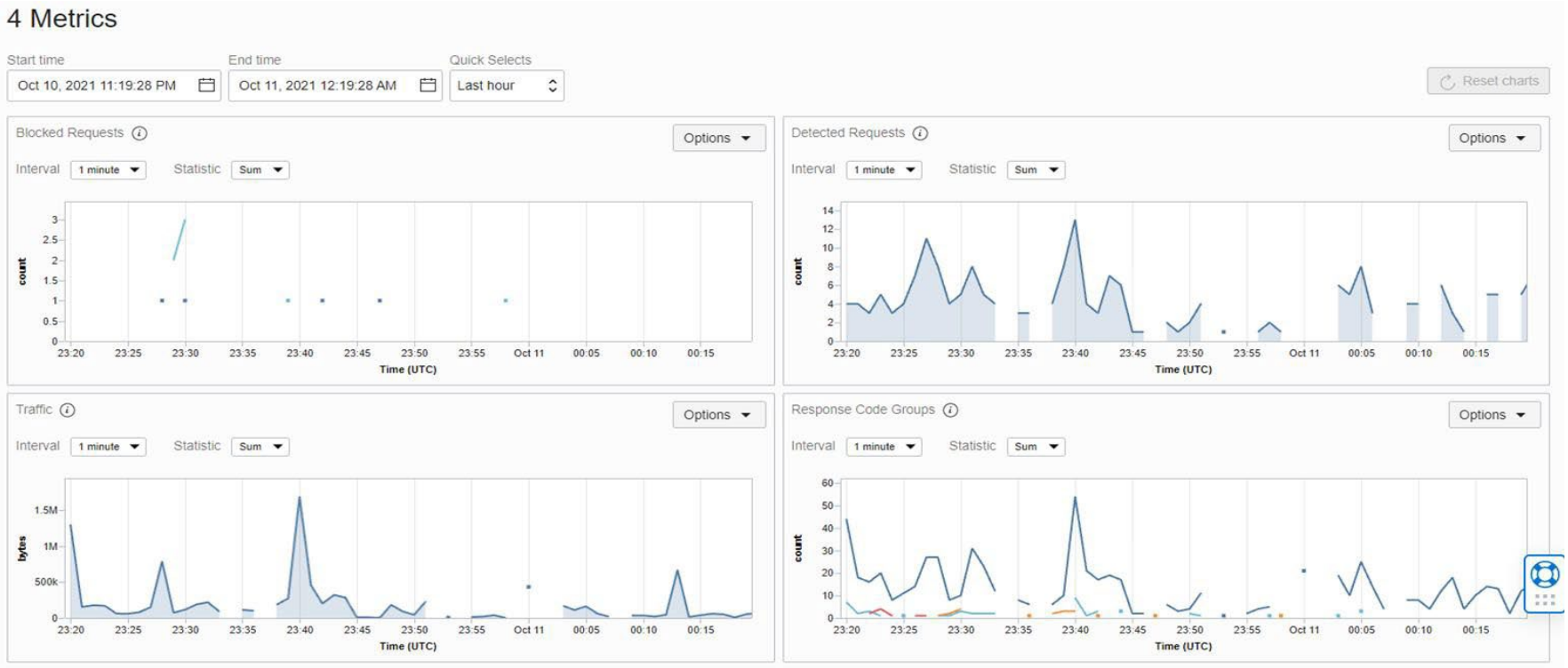
Monitoring & Alerting

Figure 12 - Monitoring and alerting workflow



Threat Notification

- Live monitoring of all request types, including blocked requests, error codes and total traffic.
- Potential attacks logged in real time for auditing.
- Custom alerts and notifications for potential threats.



24/7 Incident Response

- Managing Director and support staff have CFC Critical Incident Response APP loaded onto work mobile devises.
- Notification is made immediately via the APP
- 24/7 Cyber Incident hotline
- CFC response time is 12 minutes from time of notification.
- Providers include:
  - Norton Rose Fulbright
  - Context Security
  - Crowdstrike
  - KPMG
  - Symantec