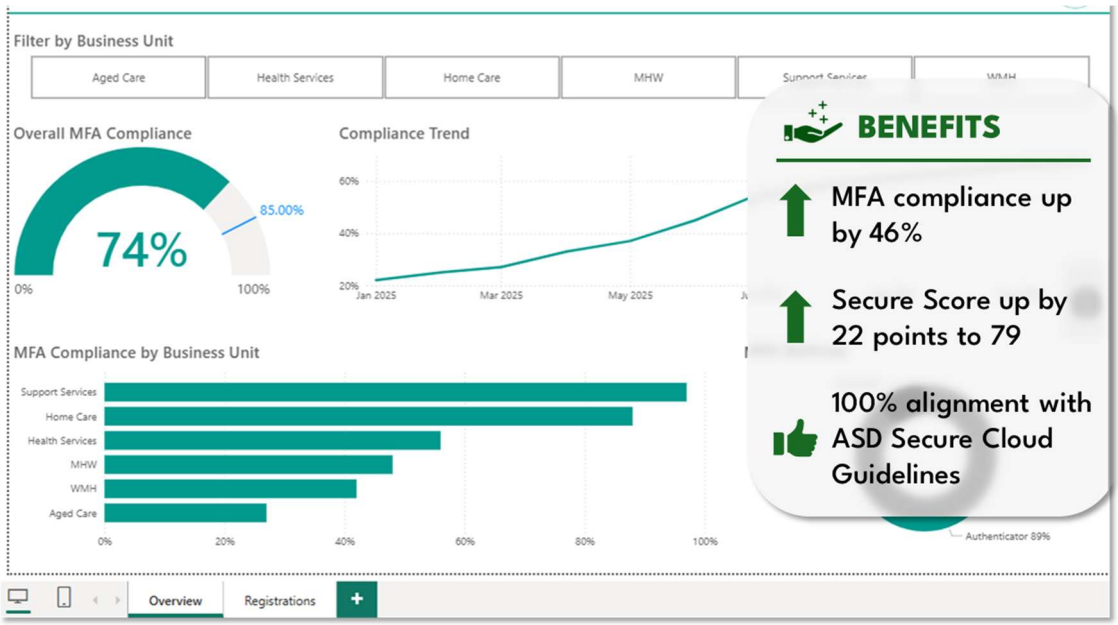
WARREN SPIER

CASE STUDY

Driving Identity Security through Automated MFA Governance Analytics



Solution Overview

Automated identity analytics framework, synthesising Microsoft Entra telemetry with Workday HR data in Power BI, driving organisational MFA compliance from 22% to 68% through granular, data-driven accountability.

My role

In the context of the broader Digital Transformation Program I was leading, I engineered a technical approach to synthesise security telemetry and HR metadata, empowering leadership with the granular insights needed to dismantle a fragmented MFA ecosystem and shift the organisation from a

Background

A healthcare company struggled with a fragmented identity ecosystem and low MFA compliance (22%), leaving sensitive health data vulnerable to attack. Lacking centralised visibility to meet Department of Health mandates, the organisation was unable to identify risk hotspots or hold business units accountable for security adoption.

- **The Risk:** Minimal MFA adoption created an expansive attack surface, leaving sensitive health and corporate data exposed to credential-based attacks.
- **The Cultural Barrier:** There was a prevailing lack of urgency regarding identity security. Without granular data, it was impossible to hold business units accountable or demonstrate the specific areas of risk.

The Solution

Data Engineering:

- Automated Identity Telemetry: Developed a custom ingestion pipeline using the Microsoft Graph API to retrieve live authentication method registrations (Authenticator app, Phone, FIDO2, etc.) from Microsoft Entra.

vulnerable state to a best-practice trajectory.

Skills

- Data Visualisation
- Data Analysis
- API Integration
- Cybersecurity
- Change Management

Tools

- Power BI
- Microsoft Graph API
- Microsoft Entra
- Workday
- Power Query
- DAX

- HCM Synthesis: Performed a complex join with Workday HCM data. This allowed for multi-dimensional modelling across Business Unit, Location, and Employment Type.
- Data Transformation: Inside Power BI, I used Power Query (M) to reconcile the disparate sources, resolving fragmentation issues to create a unified 'single source of truth' identity model.

Data Analysis:

- Drill-Down Logic: Created a hierarchical model allowing stakeholders to move from a 30,000-foot organisational view down to specific departments.
- Trend Forecasting: Utilised time-series analysis to visualise the "MFA Compliance Trend," identifying that while the overall rate was 68%, specific units like "Aged Care" were lagging significantly at 27%, requiring targeted intervention.
- I then developed advanced DAX measures to calculate compliance percentages and apply linear regression, enabling the dashboard to forecast a 'Best Practice' target date of February 2026 based on current adoption velocity.

Visualisation and UX Design:

- Strategic Layout: Designed the dashboard using a "Summary-to-Detail" approach. High-level KPIs (Actual vs. Target) are positioned at the top, followed by a Business Unit Compliance bar chart to drive internal accountability.
- Method Composition: Integrated a distribution analysis of MFA methods (Authenticator vs. Phone vs. Passkey) to encourage the shift toward more secure, "Phishing-Resistant" methods.

Results

- **Risk Reduction:** Successfully transitioned from a high-exposure state (22% compliance) to a robust 68% and climbing, significantly hardening the identity perimeter.
- **Cultural Shift:** The automated, transparent reporting created a "gamification" effect among Business Unit leaders. By seeing their specific compliance scores compared to peers (e.g., Support Services at 97% vs others), a culture of accountability and security awareness was established.
- **Operational Excellence:** Automated a previously manual process, enabling the Security team to focus on ongoing change management and user support rather than data collection.