User Requirements Document

for

Data and Authentication Monitoring Platform (DAMP)

[1. Introduction 1](#_Toc151582875)

[2. Scope 2](#_Toc151582876)

[3. Requirements 3](#_Toc151582877)

[2.1. Functional 3](#_Toc151582880)

[2.2. Non-Functional 3](#_Toc151582881)

[4. Conclusion 4](#_Toc151582882)

# Introduction

The Data and Authentication platform has multiple distributed systems that need to be proactively monitored. These systems host critical services utilising multiple technologies and running variety of applications which generate stats, metrics, and logs.

# Scope

The document sets out the requirements that need to be met by the monitoring system for proactive detection and effective raising of critical alerts to the operational team.

# Requirements



# Functional

The monitoring system shall:

1. Be operational and available 24/7.
2. Monitor services hosted both on-premises(virtual or otherwise) and in hybrid clouds.
3. Collect metrics and logs for Operating System and services/applications.
4. Secure personal data that flows through the system.
5. Handle Unix based tech stack running applications and infrastructure built with Ruby and Java based applications.

# Non-Functional

The system should be:

1. Scalable.
2. Cost effective.
3. Self-diagnose and ensure operational support team are aware of any issues.

# Conclusion

The requirements set out in this document are the minimum to implement a robust monitoring system that is operational and available 24/7. This is a living document that will evolve over time to accommodate changing requirements and latest changes in processes and tools as the system matures.