

## Introducing Naimuri

**Naimuri specialises in creating bespoke data intelligence solutions.**



Working exclusively in partnership with UK government and law enforcement agencies, we build software, cloud and data analytics products and services that deliver transformative mission impact and help make the UK a safer place.

Our work is enabled by deep commitments to innovation, Agile ways of working, strategic partnerships with leading Technology companies (e.g. Elastic, AWS, Neo4j and Microsoft) and a network of 200+ academic contacts that ensures we leverage the latest academic research.

Our success is founded on our customer-centricity, a proven track record in delivery and successfully integrating diverse data sources and digital systems, and the diversity, creativity and expertise of our people.

Founded in 2015, Naimuri was acquired by QinetiQ (a world leader in defence, security and critical national infrastructure) in 2020, and now employs over 150 specialists in software development, cloud infrastructure, business change and analysis, and data science and analytics.

## Agile and Naimuri

**Naimuri means 'no overburden' in Japanese, an ethos that inspires and informs the lean, Agile approach we apply to everything we do.**

Naimuri was born of the need for Agile, and our deep appreciation of how Agile methodologies simultaneously simplify, support and expedite project delivery, communications and forecasting.

Our success in applying Agile is founded on our understanding that true agility doesn't just relate to how software development teams work: Developing and delivering in an Agile way also increases product quality, delivery speed and customer satisfaction rates, and effectively empowers our customers to make informed choices and retain control over their decision-making processes.

**Nai – muri**

**No**

overburden  
excessiveness  
unreasonableness  
impossible  
beyond one's power

## Secure By Design

Having designed, developed and supported multiple systems and applications across UK Government, security is always our first consideration.

We hold CyberEssentials and ISO27001 certification, and our 'Secure by Design' ethos is underpinned and evidenced by annual accreditation, auditing and certification by HMG-recognised bodies.

Our approach to system architecture draws heavily from national and international best practices (e.g. NCSC & GSG Secure by Design and MoD SbD and CISA SbD) - We engage with security and accreditor stakeholders at the outset of every project, to ensure secure design and controls are considered and applied as early as possible.

## The Data Intelligence Lifecycle

Naimuri's Data Intelligence Lifecycle captures key themes applicable to the creation of effective data intelligence solutions, to which our extensive in-house capabilities are aligned.

**Collection and Processing** - Developing secure platforms and automating collection and enrichment of data.

**Storage and Search** - Architecting scalable, secure storage, with embedded access controls and governance.

**Analysis and Insights** - Reducing the burden of analysis by automating alerts and notifications, and quickly placing insights at users' fingertips.

**Reporting & Dissemination** - Enabling collaborative, unified reporting and secure dissemination, and reducing cognitive load through timely alerts and signposting.

**Planning, Decision-making, Action and Feedback** - Providing mission impact to Data Intelligence teams through intuitive, effective tooling.

**Artificial Intelligence (AI) and Machine Learning (ML)** - All capabilities are enhanced by our expertise in leveraging AI and ML to add maximum value.



## Key Capabilities - Data

**Naimuri's extensive Data capability is highly experienced in handling and modelling vast amounts of data quickly and securely, and enabling organisations to maximise value and intelligence from data.**

Leveraging our proprietary data analytics platform, and employing best practice in Data Engineering, ML Engineering, MLOps and ML Assurance, our capabilities include:

**Data Engineering, Analytics and Visualisation** - Our bespoke software enables users to easily and efficiently interrogate their data. Creating meaningful, information-rich visualisations also assists us in conveying deep and complex relationships to our customers in innovative and intuitive ways.

**LLMs** - We design, build, deploy and monitor LLM-based solutions for secure Government applications, including implementing cutting-edge model architectures using techniques such as fine-tuning and RAG.

**Knowledge Graphs** - We are experts in creating structured graph databases from both structured and unstructured data sources, using the latest advancements in knowledge graph databases and algorithms. We use graph algorithms and Graph Neural Networks (GNNs) to gain insight from graph databases, including developing extensive and scalable knowledge graphs, and networks of transactions or people.

**Data Governance** - We provide tools to help manage and ensure the integrity, security and compliance of data stored in cloud environments, incorporating features such as data access control, lineage tracking, auditing, and security.

**AI Assurance** - Providing third-party AI Assurance for Government customers and their vendors enables risk-quantification of AI solutions prior to deployment of best practices for automation and increased accessibility to MLOps. Our expertise in a range of sub-disciplines includes computer vision, language models, uncertainty quantification, research tasks and automation).

**Data Synthesis** - We are experts in creating artificial data capable of effectively emulating statistical correlations, distributions and patterns present in live data, on occasions when such sources are unavailable, or where security dictates.

**Deepfake Detection** - Applying SME experience and built capabilities in deep-fake image detection, to help combat the rise of AI-generated deepfakes.

## Key Capabilities - Analysis, Change & Design

**Our Analysis, Change and Design team focuses on ensuring customers' users remain central in all design and development decisions, so that products can be quickly adapted and iterated to meet their changing needs.**

We ensure User-Centred Design (UCD) informs a holistic approach to product delivery by building, maintaining and safeguarding cultures that prioritise people, interactions and accessibility.

UCD at Naimuri focuses on understanding users, tasks and environments - Our User Researchers and User Experience Designers are highly experienced in working with users to quickly identify and understand challenges they face, and rapidly and iteratively create effective and efficient solutions.

We also understand that successful UCD approaches must carefully consider how teams are built, empowered and adapt to solve problems directly when using both Agile and more traditional waterfall development and delivery methodologies.

In our experience, UCD is most effective when embedded at the heart of an Agile 'DevSecOps' approach to product development and delivery.

Founded on the principles of iterative development, effectively adapting to change, and delivering value early, Agile DevSecOps ensures user feedback informs and improves each iteration of a product's development.

We take pride in delivering tangible benefits to our customers within days and weeks (rather than months) using a proven suite of Accelerated Capabilities which help deliver mission impact at pace.

These capabilities include **Accelerated Discoveries**, which provide fast and Agile approaches to requirement gathering and design commencement that effectively supports development.

Our technology experts collaborate with users to identify, understand, document and prioritise key business requirements before beginning the design and prototyping process.

Participants receive clear requirement sets, insightful prototypes, and outputs that support outline business cases.

## Key Capabilities - DevSecOps & Software Development

Naimuri are pioneers in DevSecOps, having built and deployed multiple secure hybrid cloud infrastructures for collecting, storing, processing, retrieving and analysing data across multiple agencies, audiences and geographic locations.

Delivering projects under a variety of Agile methodologies (e.g. Kanban, SCRUM, SAgFe), we use lean DevSecOps practices to build CI/CD pipelines that incorporate frequent code check-ins with merge requests, release versioning, and test automation.

Our DevSecOps Engineers use GitLab CI to implement CI/CD systems, following industry best practices for: assurance, coverage, security and testing; and Terraform for Infrastructure as Code (IaC), to ensure we consistently version system changes.

Critical Infrastructure testing is used to ensure that what is designed translates to what is deployed, providing confidence to our customers.

Naimuri are AWS, Microsoft and Elastic partners, and our experience and expertise enables our solutions to remain 'cloud agnostic' and guided by customers' needs.

## Key Technical Proficiencies

**Full stack development:** Java; Spring; Typescript; React; Node.js; Go; Python; HTML; RESTful; GraphQL; SQL/NoSQL; NiFi.

**Cloud Native / Agnotics:** Azure; AWS; GCP; Terraform; Cloudformation; Kubernetes; IaC.

**Rapid prototyping:** Figma; Balsamic; Gemini AI.

**Test automation:** Cypress; Cucumber; Gherkin; K6; Gitlab CI/CD.

**Database design:** Elasticsearch; MongoDB; Oracle; Neo4j; Postgres.

**CI/CD:** Github; Gitlab; ArgoCD.

## Key Capabilities - Platforms

**Leveraging access to the latest tools, techniques and insights through our strategic partnerships with AWS and Microsoft, Naimuri has built multiple services operating on public cloud infrastructure, delivered within the control gateways defined by Digital, Data and Technology (DDaT).**

Designs are validated against NCSC cloud principles, such as: Least-privilege access; encryption of data in transit and rest; understanding of responsibility models (e.g. AWS Shared Responsibility Framework); authenticated and authorised systems; limited perimeter attack surfaces.

Secure cloud deployment models are default on Naimuri projects: Automated CI/CD tooling and reusable patterns enable our teams to remain secure whilst delivering at pace, with development systems secured through: use of centralised authentication; limited access to code repositories; specific IAM roles for pipelines; limit perimeter attack surface through the use of VPNs and zero-trust architecture; and internal use of DevSecOps tooling.

Naimuri's **ENDAN** and **ANZENNA** platforms provide landing zones for secure cloud development and production environments using AWS and Azure respectively, and enable highly secure environments whilst preserving code portability and eliminating vendor lock-in, and rapid mobilisation of new projects whilst minimising dependency on Platforms Engineers.

Naimuri's exclusive cloud infrastructure testing approach provides:

**Cloud security:** Ensuring our customers' highly sensitive systems and data are secure on a public cloud infrastructure.

**Containerisation:** For greater portability, security and efficiency of our customers' applications.

**Serverless Technologies:** Enabling our customers to lower running costs and reduce attack surfaces.

**Cloud Infrastructure Testing:** Managing the demands of working in the cloud.

**CI/CD Expertise:** Experienced Operators of Gitlab as our primary CI/CD tooling.

## Support Services

**Naimuri is highly experienced in providing sustained application and environment support and management (including hybrid support and development models), and is trusted to deliver support services to several Threat to Life operational systems.**

We have extensive experience and knowledge of working with organisations to manage resilience and risk, including: Event Monitoring; IT Operations Centre and Service Desk teams; and setting up and configuring alerts to facilitate high system availability.

This ensures issues, or potential issues, are rapidly identified and alerted so triage and resolution can commence as quickly as possible (and, potentially, before the issue becomes service or user impacting).

Naimuri's tested approach to Business As Usual sustained service support is to deploy a Site Reliability Engineering (SRE) team, whose deep understanding of the application (i.e. the code, how it runs, is configured, and scales) enables them to proactively monitor and support operational systems, and is a key skill.

Our support service operates to the following principles:

- Enabling knowledge transfer processes that ensure support tasks are understood within short timeframes.
- Embedding support alongside existing Naimuri development teams reduces risk and ensures consistency of knowledge, development, configuration management and deployment practices.
- Working closely and integrating with customer teams and all other stakeholders to ensure smooth running of the system, from first- to third-line support.
- Working with Agility within defined ITIL processes, procedures and best practice, to remain secure by design (i.e. complying with all applicable security standards and industry best practice) whilst demonstrating a commitment to continuous improvement.