Zero Trust Architecture & Strategy + Advisory

Service description details

Zero Trust Architecture & Strategy + Advisory

Methods is an NCSC Assured Cyber Consultancy, facilitating the development of frameworks, policies and technologies to ensure that the right users (part of the IT ecosystem within an enterprise) have the appropriate access to resources as part of a Zero Trust Architecture, providing enhanced security posture and resilience to threats.

What is the Service

Methods is an NCSC Assured Cyber Consultancy who has been assured to the highest standards as defined by National Cyber Security Centre (NCSC) and professional bodies such as UK Cyber Security Council. With a proven track record of delivering cyber security consultancy expertise, we pride ourselves on working closely with our clients - often augmenting in-house capability.

A Cyber Security Essentials Plus certified company, the services provided by the Cyber Portfolio align with ISO/IEC 20700 family of information security management standards, ensuring work is appropriately scoped, planned and delivered to the highest standards.

Methods provide a holistic approach to Cloud Platform Security with work undertaken by industry qualified Cyber security experts, many holding CCP Lead Practitioner else qualified to Chartered status, able to offer approved guidance and support to both public and private sector clients, covering the entirety of the Security organisation.

Methods manage engagements in accordance with industry best practice standards and frameworks and meet NCSC requirements for certified professional cyber services companies. Methods provide services for Critical National Infrastructure (CNI) customers across Government and the wider public and private sector. Engaging and working closely with our clients to ensure the services we provide have been correctly scoped, planned and delivered securely, with our customers interests and needs at the forefront of our thinking.

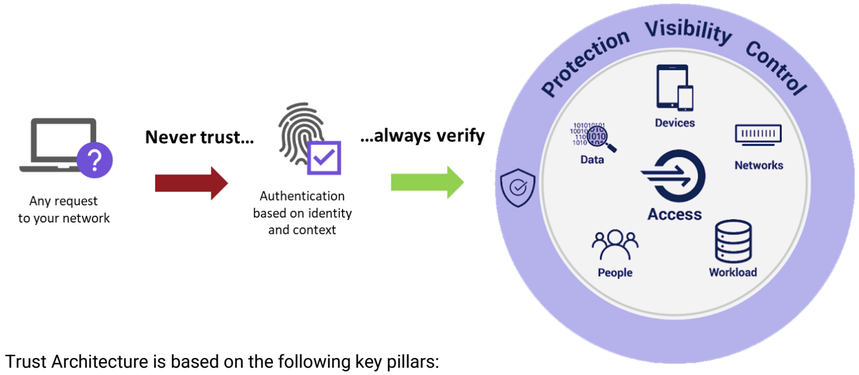
Methods is a leading provider of Zero Trust Architecture services, with a proven track record of delivering successful projects for clients across various sectors. Helping to design, implement and manage a zero-trust architecture that suits specific needs and goals, using the best-in-class tools and technologies, that assumes no trust for any entity, whether internal or external, and which requires continuous verification of identity and permissions. Providing ongoing support and guidance, ensuring that Zero Trust Architecture is always up to date and effective, based on the principle of ""never trust, always verify"" and challenges the traditional perimeter-based security model that relies on firewalls and VPNs.

Methods understand the Zero Trust Architecture, operates on the principle of “never trust, always verify”, which is quickly rising as the one of the most favoured cyber security strategies, to prevent security breaches. Recognising that organisations have different security postures and may be challenged to find skilled and experienced professionals, to develop and implement a zero-trust strategy.

Some of the challenges we have overcome:

- Zero trust requires a cultural shift and a mindset change for both service providers and customers, who need to adopt a more proactive and collaborative approach to security.
- Zero trust demands a high level of technical expertise and resources to design, implement, and maintain a complex and distributed security architecture.
- Zero trust involves a trade-off between security and user experience, as it may introduce more friction and inconvenience for legitimate users who need to comply with multiple verification steps.

Zero Trust Architecture cyber security model assumes no trust for any entity, whether internal or external, and verifies every request and transaction before granting access. Focusing on protecting the data and the applications with the organisation ecosystem, regardless of where they are located or accessed from.



Zero Trust Architecture is based on the following key pillars:

- Identity and Access Management: Ensuring that only authorised entities (people or services) can access (applications or data), using strong authentication and encryption methods.
- Micro-segmentation: Dividing the network into smaller and trusted zones and applying granular policies to each zone, limiting the lateral movement and blast radius.
- Data protection: Encrypting the data at rest and in transit and applying data loss prevention and classification tools to prevent unauthorised access or leakage.
- Continuous monitoring and response: Collecting and analysing data from various sources, such as logs, sensors, and endpoints, to facilitate the reactive and proactive, detection and response to anomalies and threats in real time.
- Security orchestration and automation: Using tools and processes to integrate and streamline the security operations, reducing the complexity and the human error.

Zero Trust Architecture offers several business benefits, such as:

- Enhanced Security Posture
- Decreased Cyber Risk
- Improved Regulatory Compliance
- Increased Performance and Productivity
- Lowering Total Cost of Ownership

Zero Trust Architecture provides a holistic cyber security strategy that encompasses cloud/multi-cloud, internal and external user endpoints, on-prem and hybrid systems, including IT, OT and IoT. As a result, our strategy is applying the following key steps, as part of the secure security posture:

1. Performing a discovery of the organisation's security posture
2. Planning the implementation of Zero Trust Architecture
3. Defining Trust Boundaries and which resource will adopt the Zero Trust principles.
4. Establish policies for access control and integration with other security technologies and systems.

Contact details

bidteam@methods.co.uk

020 7240 1121

www.methods.co.uk

Service description details

5. Network Segmentation using micro-segmentation and network security controls.
6. Maturing Endpoint Security and Data Protection
7. Continuous Monitoring, Analytics and machine learning
8. User Education and Awareness
9. Regular Testing and Evaluation
10. Governance and Compliance, to regulatory requirements
11. Culture of continuous improvement and innovation

Our methodology and approach are agile, which is designed to integrate seamlessly into the organisation, complementing and innovating the current working practices. Whether the organisation is looking for ad-hoc support, or a long-term partner, our team of professional, verified and approved by NCSC Cyber Security and UK Cyber Security Council, our experts, with the ability to help identify and implement best and most viable solutions. Aligned with NIST, NCSC, OWASP, and MOD Secure by Design & DEFSTAN 05-138 for dynamic security solutions.

We assume all connectivity and access is hostile and denied by default and only permitted by explicit configuration, operating a "zero-trust and defence in depth model". Security will be enforced in the pipeline (static code, dependency and vulnerability analysis) and in depth of architecture (logical segregation – low & high trust zones), zero trust, monitored and active protections.

One of our core tenets is collaboration, which lays out how our team works with the client. We adopt the principles of openness and knowledge transfer to empower the people and build impressive, sustainable governance around complex multi-cloud solutions. We work closely with key stakeholders and programme teams to devise a bespoke solution that meets the demands of the business processes, strategic business objectives and regulatory requirements. Our consultants have a strong background in both public and private sectors and will quickly adapt to the environment, providing specialist expertise to design innovative and risk-based solutions that meet your specific business needs and outcomes.

We at Methods, provide pragmatic and proportionate risk-based guidance as trusted consultants covering compliance, architecture and design assurance; system accreditation across MOD DefCon standards. Our experienced consultants have proficiency working on a variety of Government projects with different divisions including critical national infrastructure (CNI), defence, policing, justice, education, healthcare, border control, central government, local authorities and government digital services.

In line with HMG requirements, Methods is certified to Cyber Essentials Plus, ISO/IEC 27001, ISO 27017 and ISO 9001 standards, so we can provide customers with robust, consistent assurance in our quality processes and the protection of our systems and customer-related data. We adopt certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above. Methods has a large pool of SC and DV cleared UK personnel and has experience of designing, building and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET and ABOVE SECRET classifications.

What it can do for you

Methods is an NCSC Certified consultancy dedicated to guiding our clients in understanding their supply chains better, assessing risks, and seizing opportunities. We work to ensure that end products are available when and where needed by addressing vulnerabilities and enhancing compliance across intricate global supply chains.

Additionally, it can empower you to proactively identify opportunities for improvement within your supply chain, driving efficiency and agility. Ultimately, it can ensure that your organisation is well-prepared to withstand disruptions and thrive in dynamic environments.

Our services include:

- Comprehensive risk assessment services tailored to your supply chain, identifying vulnerabilities and providing actionable strategies to mitigate risks. Focuses include single points of failure to geopolitical complexities.
- Assist you in fostering clear communication, collaboration, and contingency planning with your suppliers.
- Empower your team with the knowledge and skills to manage supply chain risks.
- Workshops and training programmes designed to build internal capabilities and enhance resilience within your organisation.
- Comprehensive suite of services, you can fortify your supply chain against disruptions and navigate uncertainties with confidence.
- Proactive risk management and opportunity identification within the supply chain.
- Identifying structural weaknesses, geographic risks, and areas lacking visibility.
- Optimising multi-tiered supply chains and coordinating timely responses to events.
- Enhancing organisational understanding of risk profiles and accountability.
- Implementing secure and robust assurance arrangements to safeguard operations.

Service Features

1. Defining protect surface
2. Mapping the transaction flows
3. Building a Zero Trust architecture
4. Creating a Zero Trust Policy
5. Monitoring and maintaining the network
6. Network Defence in depth
7. User management - Single sign on, federation
8. Ensuring "Need to know" and "least-privilege" principles are adopted
9. Realtime detection and automation response
10. Separation of duties and separation of privileges

Service Benefits

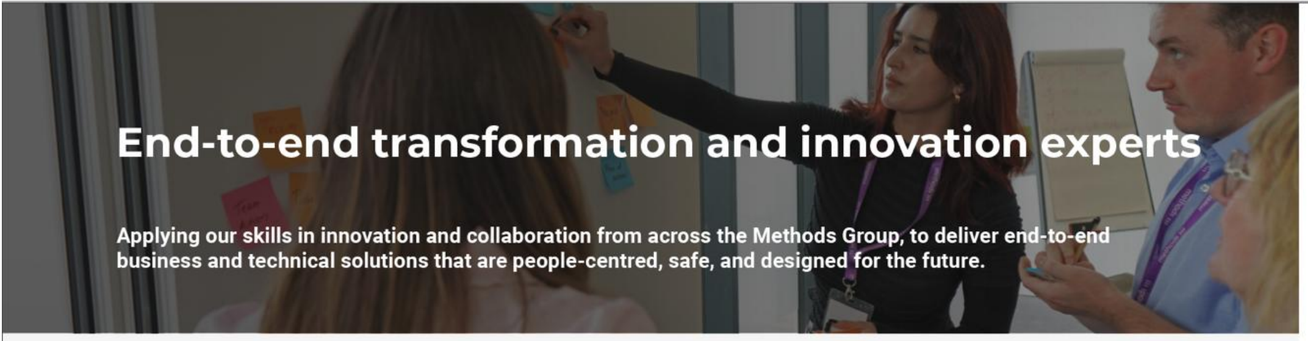
1. Enhanced security by granting access on a need-to-know basis
2. Minimising the attack surface and blast radius
3. Improved visibility and control – providing granular view of network
4. Reduced risk of insider threats
5. Data Protection, access only granted to those that need it
6. Adaptability to modern environments, supports remote working and BYOD
7. Improved regulatory compliance, potential penalties, maintaining positive brand reputation
8. Turning IT and Security into a business enabler
9. Increased confidence in the organisation's commitment to security/data protection
10. Enhanced organisational agility and adaptability to changing business environments

Contact details

bidteam@methods.co.uk

020 7240 1121

www.methods.co.uk



End-to-end transformation and innovation experts

Applying our skills in innovation and collaboration from across the Methods Group, to deliver end-to-end business and technical solutions that are people-centred, safe, and designed for the future.

Methods provide collaborative and innovative solutions to help Central Government adapt to the changing landscape and deliver better outcomes for citizens.

With a focus on driving interoperability and innovation in UK Central Government, we have helped multiple organisations in the sector modernise their IT architecture, systems, strategy, and operating models to improve organisational resilience and service delivery.

Methods deliver wide-ranging services and thought leadership to support delivery including:

Onboarding and offboarding process

1. **Understand Requirements**

It is essential that we work with you to understand the requirement so that we provide the right resources with directly relevant experience at an appropriate level of seniority

2. **Protect Team Availability**

Having the right team on board from the start and maintaining continuity throughout the project ensures timely delivery of desired outputs

3. **Work Synergistically and Innovatively**

Drawing from our past experiences, we can frequently recommend optimal delivery methods and/or alternative solutions which will deliver benefits (or cost-savings) over time

4. **Service Scope**

Ensuring that the scope of the service to be delivered is properly quantified involves agreeing on logistics (e.g., deliverables, timelines, quality criteria, etc.) and understanding your constraints, sensitivities, and key drivers to match your expectations accurately

5. **Review/Agree Engagement**

After initial discussions and planning, you'll review and amend a draft Statement of Work(s)/Services to ensure mutual agreement and alignment of objectives before starting the assignment. We may iterate the Statement of Work(s) with you to finalise the requirements

Ordering and Invoicing

Once we have agreed a Statement of Work(s) we will sign the appropriate agreement and complete a Call Off contract with an attached Statement of Work(s), and submission of a Purchase Order. We will then set up a mutually acceptable start date and commence work.

Payment terms are 30 days or less as may be agreed.

Please note - we are unable to accept Government Procurement Card (GPC) payments.

Customer Responsibilities

For any given requirement, we will identify any dependencies on the customer (e.g. access to key stakeholders, facilities, documentation, etc.) and agree these at the start of the work.

Making a difference

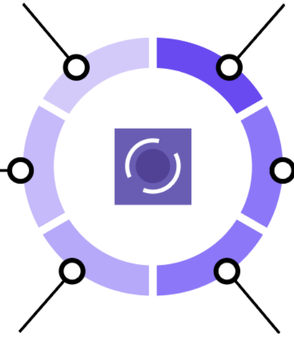
The work we do each day is focused on delivering a positive difference for the public sector for the benefit of society as a whole.

Environment

We use the 'recycle, reuse, repair, refuse' approach to waste reduction to minimise landfill waste, support climate initiatives, and enhance biodiversity, creating a sustainable environment for our colleagues and community

Volunteering

We continue to support charitable causes that align with and support our values including our charity partner and VCSE initiatives



Investment in Talent

We cultivate young talent through our GRAVITATE programme, championing vibrant apprenticeship and graduate schemes while aiding tech career exploration for individuals aged 14-24

Diversifying our Supply Chains

We diversify our local supply chains, promoting small business enterprise and engaging local people, SME, and micro-business suppliers

Staff Wellbeing

We support colleague wellbeing through clear career pathways, strengthened PDPs, and our continued commitment to the Armed Forces Covenant, including achieving Gold Employer Status. Moreover, we continue to support our colleagues holistically, considering them as complete individuals at every career stage with Methods

Safeguarding Services

We continue to provide insightful thought leadership on leveraging modern technology to secure our public services for future generations. This involves speaking at industry events, educating youth on tech career paths, and offering pro-bono advice to senior policymakers

Customer stories

Cloud Hosting & Service Modernisation
Modernised digital services using secure cloud hosting, streamlined legacy workflows, and improved data insights. Delivered faster decisions, reduced manual effort, and a more transparent, **user-friendly experience** for internal teams and external users.

Cloud-Based ITSM Consolidation
Unified multiple service desks onto a cloud-based ITSM platform, standardising processes and automating workflows. Improved incident, change, and problem management, **boosting** overall **service reliability, efficiency, and organisational visibility**.

Large-Scale Cloud Migration (100+ Apps / 120TB)
Delivered cloud migration of **100+ legacy applications** and **120TB of** data with **100% availability**. Strengthened compliance, improved transparency, and significantly enhanced operational resilience across critical digital services.

Azure Migration & Modern Workplace Enablement
Migrated data centres to Azure and deployed modern workplace cloud services, delivering secure, scalable infrastructure. Achieved improved user experience, strengthened security posture, and **£1m savings** - all with zero service disruption.

Cloud ITSM Migration (ServiceNow SaaS)
Successfully migrated from a legacy ITSM tool to a modern, cloud-based ServiceNow platform. Delivered scalable, robust service operations, strengthened governance, and enabled faster, more consistent digital service delivery across the organisation.

Cloud-Native Data Pipelines (Azure Integration)
Built automated Azure Data Factory pipelines into a Lakehouse architecture, using Bronze/Silver/Gold layers and Delta with CI/CD. Delivered secure daily refreshes, improved data quality, lower manual effort, and more efficient reporting.