REPLY

MICROSOFT ZERO TRUST IMPLEMENTATION

Service Definition
G-Cloud 15

REPLY
38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
infouk@reply.com

www.reply.com

TABLE of CONTENTS

SERVICE DEFINITION 1

TABLE OF CONTENTS 2

SERVICE DESCRIPTION 3

ONBOARDING 5

- OFFBOARDING 5

SECURITY 6

- PERSONNEL SECURITY 6
- INFORMATION SECURITY 6
- PHYSICAL SECURITY 6

ABOUT REPLY 10

SERVICE DESCRIPTION

Modern data platforms are at the heart of digital transformation, enabling businesses to harness the power of big data and analytics for quality decision-making.

Our services, leveraging Microsoft Azure, include strategy, planning, development, testing, training, and support, help clients create scalable, secure, and efficient data solutions that enhance analytics, reporting, and business intelligence capabilities, empowering organizations to unlock valuable insights and optimize operations.

Service Features

- **Comprehensive Strategy and Planning:** Tailored approach to adopting Zero Trust, aligning with business objectives and security requirements.
- **Implementation Services:** Expert deployment of Zero Trust principles, including secure identity verification and access control.
- **Microsoft Entra ID Integration:** Utilise Microsoft's identity and access management service for secure authentication and authorisation.
- **Microsoft Intune Deployment:** Implement device management solutions to ensure secure access from any device.
- **Microsoft Defender Integration:** Utilise advanced threat protection across identities, devices, applications, and networks.
- **Continuous Support and Optimization:** Ongoing support to adapt and optimize the Zero Trust architecture as threats evolve.

Service Benefits

- **Enhanced Security Posture:** Significantly reduce the risk of breaches by verifying every access request, regardless of origin.
- **Identity and Access Management:** Strengthen control over user access with sophisticated IAM tools, enhancing organizational security.
- **Seamless User Experience:** Provide secure access without compromising the user experience, leveraging single sign-on and multi-factor authentication.
- **Device Security:** Ensure only secure, compliant devices can access your network, protecting against compromised endpoints.
- **Network Security:** Secure network layers with encryption, segmentation, and threat detection to prevent unauthorized access.
- **Adaptability and Scalability:** Future-proof your security architecture with a framework that adapts to evolving threats and grows with your organization.

Service Offerings

We understand that each organisation's journey towards implementing a Zero Trust architecture is unique, with specific needs and timelines that vary widely. In recognition of this diversity, we have designed our service offerings to be both comprehensive and modular. This flexibility ensures that our clients can engage with us in a manner that best suits their immediate needs, strategic objectives, and budgetary considerations.

Our service offerings are not only integral components of a holistic Zero Trust implementation journey but are also crafted to stand alone as independent services. This design allows you to tailor your engagement with us, selecting the services that align with their current stage in your cybersecurity maturity model, or to address specific gaps in your existing security posture.

- **Planning -** Ideal for organizations at the outset of their Zero Trust journey or reevaluating their security strategies. It offers a standalone consultation and strategy formulation service that lays down a robust foundation for Zero Trust adoption. The Planning phase is a critical initial step in establishing a Zero Trust architecture within an organisation. Our service involves a comprehensive assessment of the

current security posture, identifying potential vulnerabilities, and understanding the unique business and technological context of the organization. A tailored Zero Trust strategy is then developed, aligning with the organization's business objectives, security requirements, and IT infrastructure. The planning process also includes defining clear milestones, deliverables, and a roadmap that guides the transition towards a Zero Trust environment. This process ensures that the Zero Trust implementation is strategic, aligned with the organisation's goals, and designed for the specific challenges and opportunities it faces. It involves stakeholder engagement, workshops, and the utilisation of best practices and benchmarks from Microsoft technologies to ensure a robust foundation for the subsequent phases of Zero Trust implementation.

- **Setup and Migration -** Perfect for organisations ready to embark on or progress their Zero Trust implementation. This service is designed to deploy the necessary technologies and migrate systems and processes securely, even if the initial planning was done in-house or with another partner. The service involves the practical aspects of establishing a Zero Trust framework within the organisation's IT environment. It includes the deployment and configuration of necessary Microsoft technologies such as Azure Active Directory (AAD), Microsoft Entra ID, Microsoft Intune, and Microsoft Defender, among others. The setup process is carefully planned to minimise disruption to existing operations, with a focus on identity and access management (IAM) systems, securing endpoints, and implementing network segmentation and encryption. This process ensures that all elements of the organisation's infrastructure are aligned with Zero Trust principles, from identity verification and device security to data protection and network access. The process is designed to be seamless, ensuring that existing systems and data are securely transitioned to the new Zero Trust framework with integrity and minimal operational impact.
- **Training -** Acknowledging the critical role of human elements in cybersecurity, our training programs can be procured independently to elevate the security awareness and technical acumen of your workforce, irrespective of where you are in your Zero Trust implementation. Our Zero Trust training service is designed to empower the organisation's workforce with the knowledge and skills required to effectively utilise and maintain the new security framework. This includes educating IT staff on the technical aspects of the deployed Microsoft technologies, ensuring they can manage, troubleshoot, and optimise the Zero Trust architecture effectively. Additionally, broader organisational training is provided to ensure all employees understand their role in maintaining security, including awareness of phishing attempts, the importance of multi-factor authentication, and best practices for secure remote access. Customised training programs can be developed, ranging from in-depth technical workshops for IT professionals to accessible sessions for general staff, ensuring a high level of organizational readiness and resilience against security threats.
- **Ongoing Support -** Ongoing Support ensures that the organization continues to benefit from a robust Zero Trust security posture over time. This service offering encompasses continuous monitoring of the security environment, regular updates and optimizations to the security measures in place, and rapid response to any emerging threats. The support provided includes technical assistance, security incident management, and regular health checks to ensure the Zero Trust architecture remains effective against evolving security challenges.

ONBOARDING

New clients are onboarded through a structured, collaborative process that ensures a smooth transition. Initially, a kick off meeting is conducted to understand the client's objectives, current infrastructure, and specific security challenges. Following this, a detailed assessment of the client's IT environment is performed to identify vulnerabilities and areas for improvement. Customized planning sessions are then organized to outline the Zero Trust implementation roadmap, tailored to the client's unique needs. Training sessions for both IT staff and general employees are scheduled early to facilitate a seamless adoption process. Throughout the onboarding, continuous communication is maintained to address any concerns and adjust plans as necessary. This process is designed to establish a strong foundation for the Zero Trust architecture, ensuring the client is well-prepared to leverage the full benefits of the service from day one.

Offboarding

Securing exit and offboarding a client, or transitioning to another supplier, is conducted with a structured, secure process that protects all parties' interests and data integrity. The process begins with a notification period as agreed upon in the service contract, allowing ample time for a planned exit. A detailed exit strategy is then executed, encompassing data export, transfer, and secure erasure protocols. This strategy ensures the client's data is handed over securely and efficiently, with all necessary support provided during the transition to a new supplier if required. Throughout the exit process, we conduct rigorous security checks to prevent data breaches or leaks. Finally, a debriefing session is held to review the exit process, gather feedback, and confirm the completion of all contractual obligations. This systematic approach ensures a secure, transparent, and respectful transition, maintaining professionalism and integrity until the final stages of the service engagement.

SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels.

Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains.

Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.

TRAINING & KNOWLEDGE TRANSFER

This service includes structured enablement designed to build client capability through joint delivery rather than standalone training activities. We recognise that confidence and long-term value are achieved when client developers actively participate in the migration process and understand the patterns applied.

We enable client developers by working alongside them throughout the four-week engagement. Delivery is collaborative, with development, testing, and validation activities performed transparently to support learning through practical involvement.

Knowledge transfer is provided through:

- Paired working between our consultants and client developers.
- Walkthroughs of migrated integrations, test suites, and Azure Integration Services configurations.
- Explanation of prompt-driven GitHub Copilot usage and reusable prompt patterns.
- Documentation of migration patterns, assumptions, and operational considerations.

Formal classroom-based training is not included as part of this service. Following completion of the engagement, we can continue working with you to support further delivery, extended enablement, or targeted training activities as part of follow-on services.

This approach ensures that client developers leave the engagement with practical experience, validated patterns, and the confidence to progress with broader integration migration initiatives.

CUSTOMER RESPONSIBILITIES

To ensure successful delivery of our data services, several key inputs from the customer are essential. Firstly, a clear understanding of the customer’s business goals, current IT infrastructure, and specific data needs is crucial for tailoring our services effectively. Access to relevant technical documentation and systems is also required to assess the existing environment and design an appropriate data strategy. Active engagement and collaboration from the customer's IT team are vital, both for sharing insights during the planning phase and for effective knowledge transfer throughout the project. Lastly, timely feedback on deliverables and open communication regarding any changes in requirements or challenges faced are imperative for agile project management and ensuring the project remains aligned with the customer's objectives. These inputs are foundational to a successful partnership and the delivery of a solution that fully meets the customer's needs.

ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations