Cloud Orchestrated Re-Useable Environments (CORE)

Service Definition Document

Cloud Orchestrated Re-Useable Environments (CORE)

1 WHAT THE SERVICE IS

Leidos Cloud Orchestrated Re-usable Environments (CORE) is a secure, modular and integrated product that provides automated infrastructure and services. It delivers capability for Continuous Development / Continuous Integration (CICD), performance monitoring and service management, protective monitoring, Security Incident and Event Management (SIEM) and systems management (patching). Our product is created specifically for public sector customers and is optimised to support environments up to OFFICIAL classification (including SENSITIVE handling caveat).

We can rapidly deploy Leidos CORE to any cloud (hyperscale, hybrid, multi-cloud, hybrid or private cloud) giving the customer a development, test and production workload management capability with integrated monitoring and security in short timescales. This allows you to concentrate and accelerate development, hosting and evolutions of the applications that support your business and deliver value to your customers.

Why use Leidos CORE

Leidos CORE is built to be vendor-agnostic and support multi-cloud deployments / use-cases. This means we can deliver the product's capabilities using components tailored to the needs and requirements of each customer, their preferences, in house staff skill levels and take advantage of any existing software licensing agreements in place.

The modular nature of Leidos CORE allows deployment of only the features required for your specific project. All deployed modules are integrated with:

- Identity and Access Management (IAM/IDAM).
- Appropriate roles and responsibilities (RBAC).
- Secret and key management.
- Logging.

The product is flexible such that individual products (CI/CD pipeline components, service management integrations, AV products, etc.) can be changed to suit your requirements. The product and its components are fully managed, supported and updated by Leidos throughout its lifecycle.

We have distilled our experience in the creation (and ongoing development and evolution) of this product to automate as much as possible. Product enhancements based on customer request can be delivered quickly and iteratively. Overall, our development and management of the product across our customer base is efficient – cost reduction is achieved through short CORE implementation timescales and the practical elimination of human error.

Our Approach

Leidos CORE is built on the following principles:

- Secure by Design and in Delivery – ensuring a robust security posture with extensive hardening, comprehensive privilege access, key and secrets management capabilities, and a pattern-based architecture to support secure Public Sector, National Security and Defence deployments, hosting services and data classified at OFFICIAL (with SENSITIVE handling caveat). Compliant with NCSC security principles;
- Segregation of roles and responsibilities – enforcing need to know, segregating duties, and minimising risk to operational platforms and your data;
- Abstraction and modularisation – maximising the separation between components, ensuring defined boundaries between application, platform and infrastructure layers and supporting the exchange of products to deliver the solution required;
- Infrastructure as code (IaC) – defining logical infrastructure configuration through code rather than manual configuration, ensuring consistency, accuracy and replicability;
- Automation and Orchestration – using automated processes to build and configure the OS and application stack over the infrastructure, reducing the potential for human error, maximising repeatability. Minimising impact through change by improving build and deployment time and quality, with the aim being secure, immutable services where practical;
- Automated testing – assuring deployment quality through extensive rapid testing built in to the engineering lifecycle;
- Smart Monitoring – using protective monitoring capabilities with tooling capable of identifying security and operational issues which minimises direct human access and exposure to assets and limits human risk whilst maximising the value of monitoring and auditing;
- Vendor-agnostic – can be implemented on any public cloud platform, multiple cloud platforms or in a hybrid deployment spanning legacy on premises systems, providing a secure and flexible cloud base on to which we can migrate systems. The integrated toolchain provided by Leidos CORE is also modular, allowing any component to be exchanged for an alternative if required

These principles make Leidos CORE a flexible and secure product to provide you with the services you need in your cloud platform to allow your organisation to concentrate on delivering business value rather than monitoring, managing and updating your platform and tooling.

Leidos CORE Components

Figure 1 shows Leidos CORE's key components:

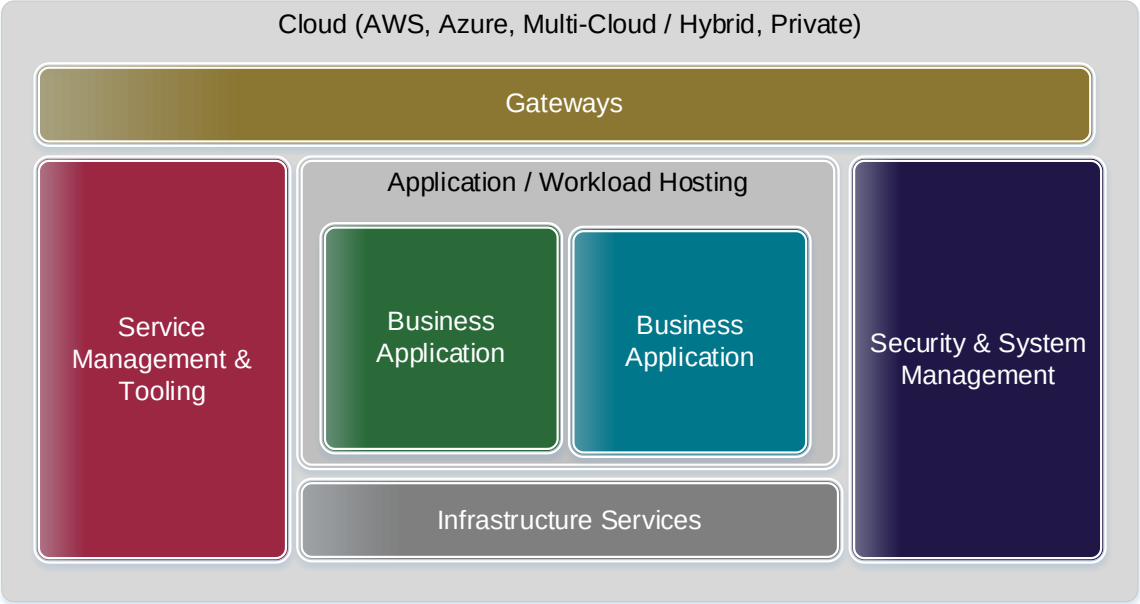

Figure 1 - Leidos Core Components

- **Infrastructure Services** – The key infrastructure building blocks are primarily services natively provided by the underlying infrastructure or cloud platform, including all compute, storage, networking, backup, encryption, key management, monitoring and operating systems. In hyperscale cloud deployments, these elements are provided by the Cloud Service Provider (CSP) but are configured, managed and automated by Leidos CORE. In private cloud environments, these are provided by a hypervisor, but managed and automated in the same way by Leidos CORE as for hyperscale cloud;
- **Gateways** – Secure common gateways to all networks, including PSN networks and the Internet. No traffic reaches the applications or the other components without traversing a secure gateway. In hyperscale cloud, these are provided by the CSP, but configured and managed as part of Leidos CORE. In private cloud deployments, these are designed using (virtual) networks and security appliances
- **Security & System Management** – Security and management capabilities for the applications, cloud platform, and supporting services, including network monitoring, Public Key Infrastructure (PKI), anti-virus, anti-malware, Security Incident and Event Management (SIEM), Identity and Access Management (IAM, IDAM), and vulnerability scanning;
- **Service Management & Tooling** – All service management tooling required to monitor and manage your cloud platform and broader services and all the tooling that will support engineering and development activities, including automation and orchestration of the platform and applications;
- **Application Hosting** – All applications are hosted within an appropriate security domain which are segregated by in private networks (VPC, VNets). All traffic between these are monitored and strictly controlled and pass through gateways and proxies deployed within the private networks.

Immediate Continuous Delivery Capability

Continuous delivery is supported by Leidos CORE's integrated toolchain which provides you with an out-of-the-box development, test and deployment tool stack, including the industry standard deployment, provisioning tools of your choice. This means your software developers can start developing as soon as the product is deployed with the ability to deploy new environments as required without having to worry about the underlying platform.
Critically, the entire solution is modular, allowing any tool to be exchanged for another equivalent tool (cloud native/third party) to enable deployments where the customer assumes responsibility for platform management or where there is a shared responsibility for platform management between your team and Leidos.

SecDevOps

To yield best customer benefit from Leidos CORE, Leidos engineers use our Agile SecDevOps methodology (Figure 2) which provides a standard set of integrated tools, methods, playbooks and guidelines. It encourages a collaborative, continuous learning culture where ideas, processes, and capabilities are shared and leveraged. Collectively, these support consistent, repeatable, automated delivery, enabling increased focus on innovation and customer mission and reducing time spent on technology issues. It also means that enhancements and new feature requests can be delivered quickly and iteratively so they become available to you in a timely manner to support your business activities

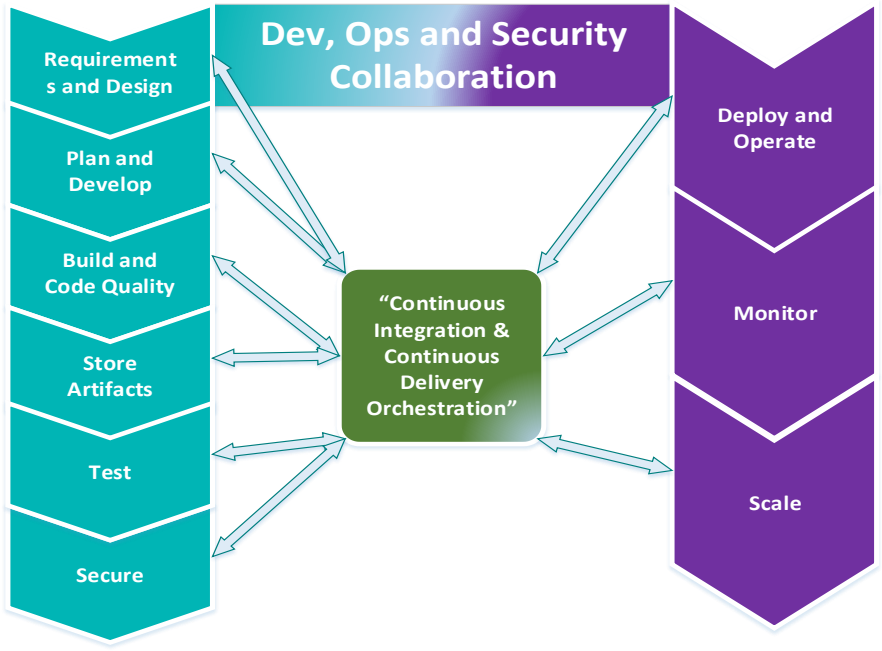

Figure 2: Agile SecDevOps Methodology

Our SecDevOps approach provides the following benefits:

- Increased efficiency, speed of delivery, product evolution and accuracy resulting from reuse of artefacts and software assets;
- Continuous integration/continuous delivery of secure software solution in an agile, iterative fashion;
- Integration of the Leidos EngineeringEdge® common Agile processes and best practices ensuring delivery of quality code;
- Fully automated deployments with consistent, repeatable results, including immutable infrastructure and blue-green deployments using IaC.
- Leidos has established cross-functional, security-cleared teams with vast experience and mixed expertise, designed to maximise use of Leidos CORE assets and SecDevOps processes and tools. This allows us to

deploy integrated and experienced teams quickly to projects or work packages, knowing that they are trained and competent in the required technologies, toolsets and ways of working.

Features and Benefits

The features and benefits of Leidos CORE as show in the table below:

Features	Benefits
Vendor agnostic, multi-cloud technology	Flexibility - Customers can use any public cloud provider, build solutions that span multiple providers and existing on premises facilities. Any element of the integrated toolchain can be changed if required
Reusable components minimise new development, reducing delivery time	Cost and Time optimised deployments - Reduced timescales, costs and risks through use of already tested and proven assets and validated patterns
Comprehensive automation via IaC, automated deployment and automated testing	Assured security, through greater availability and repeatable assured services such as system patching. Customer benefits from being able to deploy new environment for testing as required.
Secure by design with all development accomplished using the proven Leidos SecDevOps methodology and tools	Leidos CORE will always be secure and aligned to required accreditation and new enhancements will be made available quickly for the customer's benefit
FinOps Integration - Experience based resource optimisation.	Ongoing focus on waste reduction, costs control and optimisation of your estate ensures value for money throughout
Industrialised service support and management processes and procedures	Reduced Mean Time to Repair (MTTR) in the event of issues
Repeatable processes include: Automated OS & application updates, patching and certificate renewals, with updates tested centrally before deployment to customer test environments.	You don't need to spend time doing any of these tasks, Leidos CORE manages this for you.

Engagement Process

Leidos CORE can be delivered as part of a larger cloud migration exercise or as a standalone product. As part of a cloud migration (Figure 3) if deemed optimal, the deployment of Leidos CORE occurs within the "Build" Phase as shown in Figure 3. In order to deploy Leidos CORE effectively, we must first understand your organisation, vision, mission, objectives and strategy. This is achieved in the "Strategise" phase. This is followed by a detailed discovery of your current estate and analysis of the best approach to cloud migration based on all the information gathered.

Our methods are based on the industry-standard cloud adoption frameworks from AWS and Microsoft (for Azure) and are done in Agile fashion over a defined number of sprints and categorise workloads to be migrated using the 6Rs (rehost, replatform, repurchase, refactor, retain, retire).

Prior to deploying Leidos CORE, we define the target architecture, operating model and security plan. In many cases, customers choose to have Leidos manage their migrated environment. Our industrialised support and management processes cover all aspects of a fully managed service and are aligned to ITIL framework and industry best practices with clearly defined metrics and measurements (KPI, SLAs). These are aligned to and support your business requirements.

Leidos can also work in a shared support model as required based on your specific needs. In such scenarios, we will review your organisation's readiness to support and operate your cloud environment if required, including skills gaps assessments and create training and development plans.

2 ANY ONBOARDING AND OFFBOARDING SUPPORT YOU PROVIDE

Where relevant, Leidos will adopt a consultative approach with customers to define and validate their requirements in order to determine how best to engage with the services. The onboarding and offboarding process is dependent on the specific requirements of the solution, and the delivery methodology agreed upon.

3 PRICING

Please refer to the associated Pricing Document relevant to this Service.

4 TERMS AND CONDITIONS

Please refer to the associated Terms and Conditions Document relevant for our Service Offerings

5 FURTHER INFORMATION

Please send your requirement to publicsector@uk.leidos.com. Alternatively, if you wish to discuss your requirements in more detail, please send us the following information and we will be happy to contact you:

1. Your organisation name
2. The name of this service
3. Your name and contact details
4. A brief description of your business situation
5. Your preferred timescales for starting the work.

ABOUT LEIDOS

Leidos is a leading partner to the UK government and the Scottish government as well as having key client partners in transportation and energy. Leidos employs 1300 people across the UK supporting technology and business process transformation programmes for clients such as the Home Office, the Ministry of Defence, the Metropolitan Police Service and NATS.

The success of this work in the UK and beyond shows that we are a trusted partner in the region and that our people can deliver innovative solutions to solve the most challenging problems.

LEVERAGING OUR CORE CAPABILITIES

Our technical core capabilities define the areas in which technical excellence is critical, not only for our business, but in the work we do daily to help customers achieve the important missions on the frontlines of their industry. Explore our core capabilities here.

INCLUSION AND DIVERSITY IN LEIDOS UNITED KINGDOM

Leidos is committed to creating a diverse and inclusive workplace, where every colleague has the opportunity to contribute, share their unique ideas and talents, and be supported in their career. Explore Inclusion and Diversity in the UK here.

SOCIAL VALUE

We're committed to supporting sustainability initiatives, tackling workforce inequality and STEM education by enriching the communities to our operations. Learn more about Social Value in the UK here.