Building a Cloud Blueprint

Security. Visibility. Speed.

March 2020

servian_

Table of Contents

1. Overview

1.1 Introduction

Servian designs, delivers and manages innovative data and analytics, AI/machine learning, digital, customer engagement and cloud solutions that help clients sustain competitive advantage.

It has a diverse enterprise and corporate customer base that includes over 200 clients across government, finance, telecommunications, utility, insurance, construction, airline and retail sectors.

Founded in 2008 and headquartered in Sydney, Servian has offices across Australia and New Zealand, as well as London and Bangalore. It has over 500 consultants, making it the largest pure play IT consultancy in Australia.

Servian is platform agnostic and can implement technology solutions across any data, digital and cloud environment (including Google, Amazon and Microsoft).

1.2 Objective

The objective of this document is to outline Servian's opinionated approach on how to provide a safe and secure heterogeneous cloud operating model.

Servian believe a mature cloud operating model can deliver effective cost and agility backed by a safe and secure posture.

2. Cloud Operating Model - Key Concepts

2.1 Cloud - Drivers and Concerns

A lot of focus on initial cloud payloads involved digital teams with systems of engagement being moved to cloud resources to help improve agility. Whichever use case was first for enterprises, the requirements to scale out on public cloud or move to a hybrid/multi-cloud ecosystem is a challenge for many organisations.

The drivers for moving to a public cloud or moving to a hybrid/multi-cloud ecosystem can include:

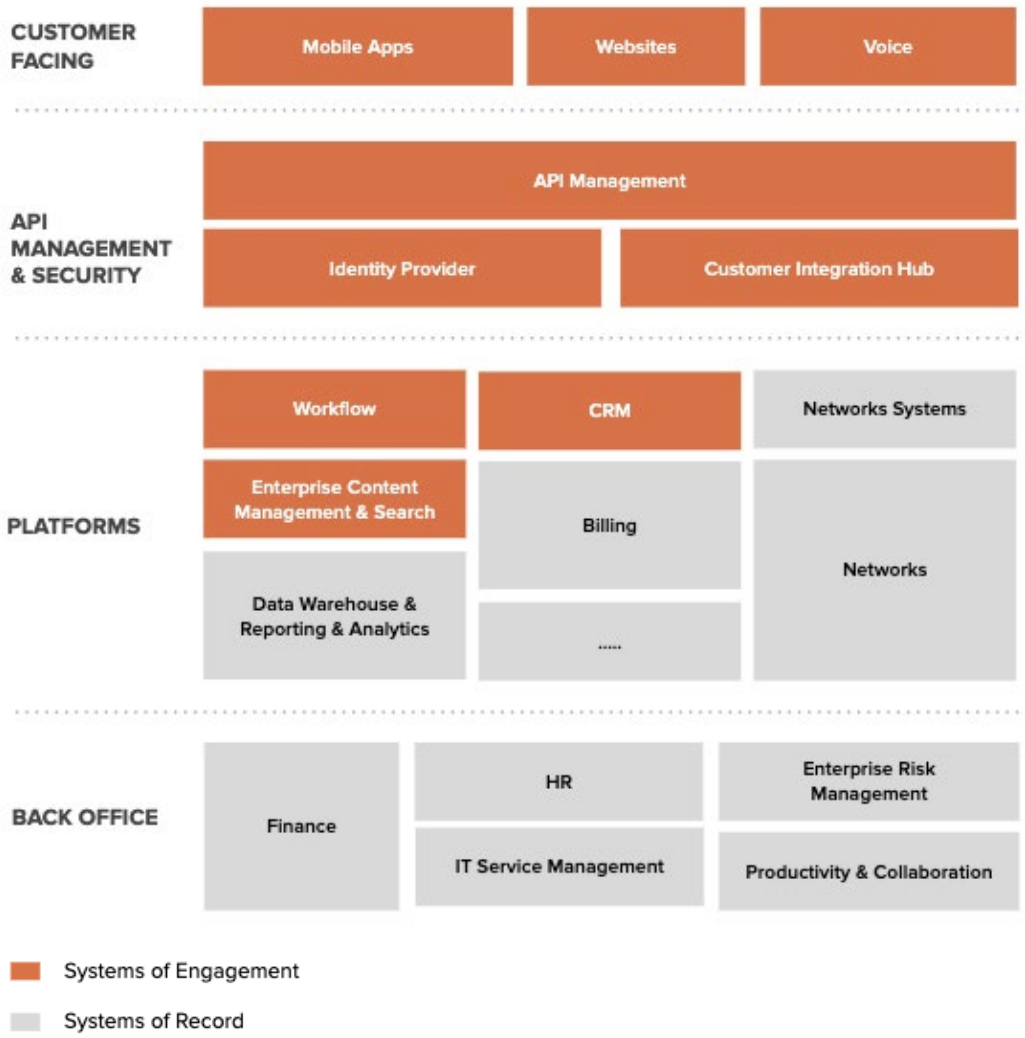
- Increasing agility requirements
- Costs; such as data centre exit or avoiding large CAPEX for large systems such as Big Data infrastructure
- Requirements to leverage new technologies, e.g. machine learning
- Multi-cloud to avoid vendor lock in and mitigate risk, offering improved DR & BCP options

The following articulates some of the shifts required to be able to leverage cloud technologies at scale.

FROM	TO
Hierarchical controls framework based on physical data centre access	Hybrid-cloud, policy oriented access and deployment
Many applications, with Single Sign On	IAM & Secrets management for users, service accounts, public key/encryption
Policy & architecture documents	Infrastructure and policy as code
Micro segmented network with secure perimeter	Secure perimeter + Defense in Depth + Service Mesh
Manual Service Transition, Blended CI/CD, fragmented logging, fragmented access management alerts, user events	Continuous Delivery & SRE influenced DevSecOps

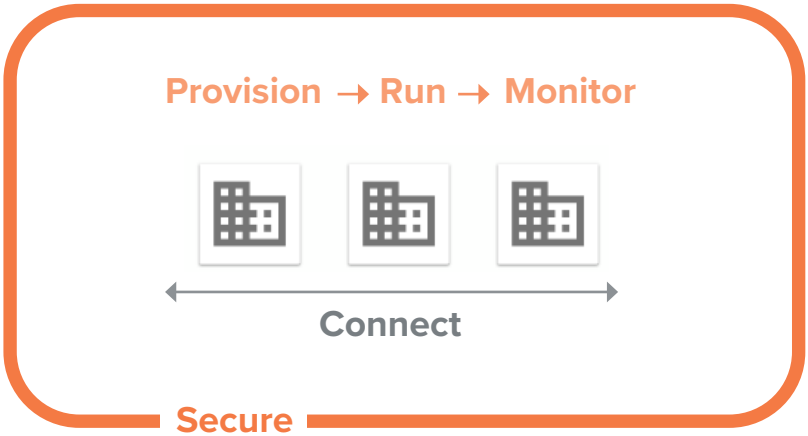
2.2 Cloud Application Lifecycle

One of the keys to success in a cloud operating environment is the ability to support the application lifecycle without impeding agility. Many organisations struggle to take digital capabilities which have delivered systems of engagement and scale the patterns across the rest of the enterprise.



At Servian we believe that in order to achieve operating cloud successfully at scale,security and connectivity need to be baked into the building blocks which underpin the application lifecycle.

- **Provision:** Provisioning, running and changing infrastructure
- **Run:** Developing and operating applications
- **Monitor:** Monitoring for risk, governance and security exceptions
- **Connect:** Networking between hosted cloud capabilities and the networking between services
- **Secure:** Perimeter security and defense in depth



Looking at each of the above areas in each cloud environment adds significant complexity.

Servian recommends clear decisions are made for where tooling can be chosen by project teams, and where mandatory tooling must be utilised. This should be expressly determined per environment (multi-cloud/on-prem) and with a view for which components should be centrally cloud agnostic, and which make use of specific services that are unique.

	RIGID	DYNAMIC			
Process	On premise	Private Cloud	AWS	Azure	GCP
Provision	vCenter	vCenter	Cloud Formation	Resource Manager	Cloud Deployment Manager
Run	vSphere	vSphere	EKS | ECS | Lambdas	AKS | ACS | Azure Functions	Compute Engine | GKE | Cloud Functions
Monitor	3rd Party	3rd Party	CloudWatch	Azure Monitor	Stackdriver Forseti
Connect	Hardware	Hardware	CloudMap | AppMesh	Proprietary	Proprietary | Istio
Secure	Identity: LDAP/AD	Identity: LDAP/AD	Identity: AWS IAM	Identity: Azure AD	Identity: GCP IAM

2.3 Shared Responsibility Model

Cloud requires the customer, platform and related system integrators to create a viable secure operating model with different accountabilities across the technical stack.

- Cloud providers are responsible for securing the infrastructure; public or private
- Cloud consumers are responsible for securing their data and applications
- Servian can work with cloud providers and other vendors to help you with a principled approach that can include templates, frameworks, products & solutions

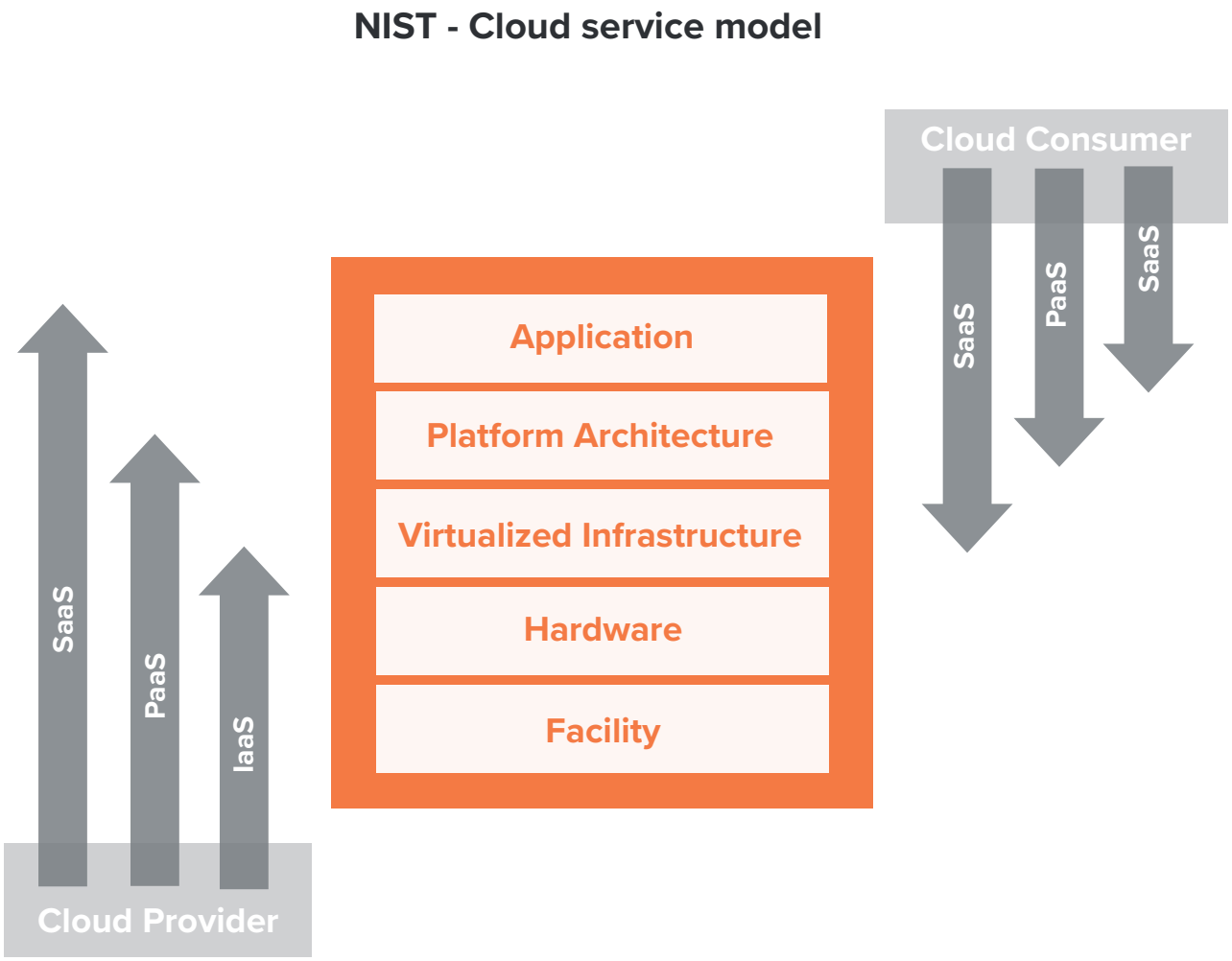


Figure 1: Differences in Scope and Control among Cloud Models

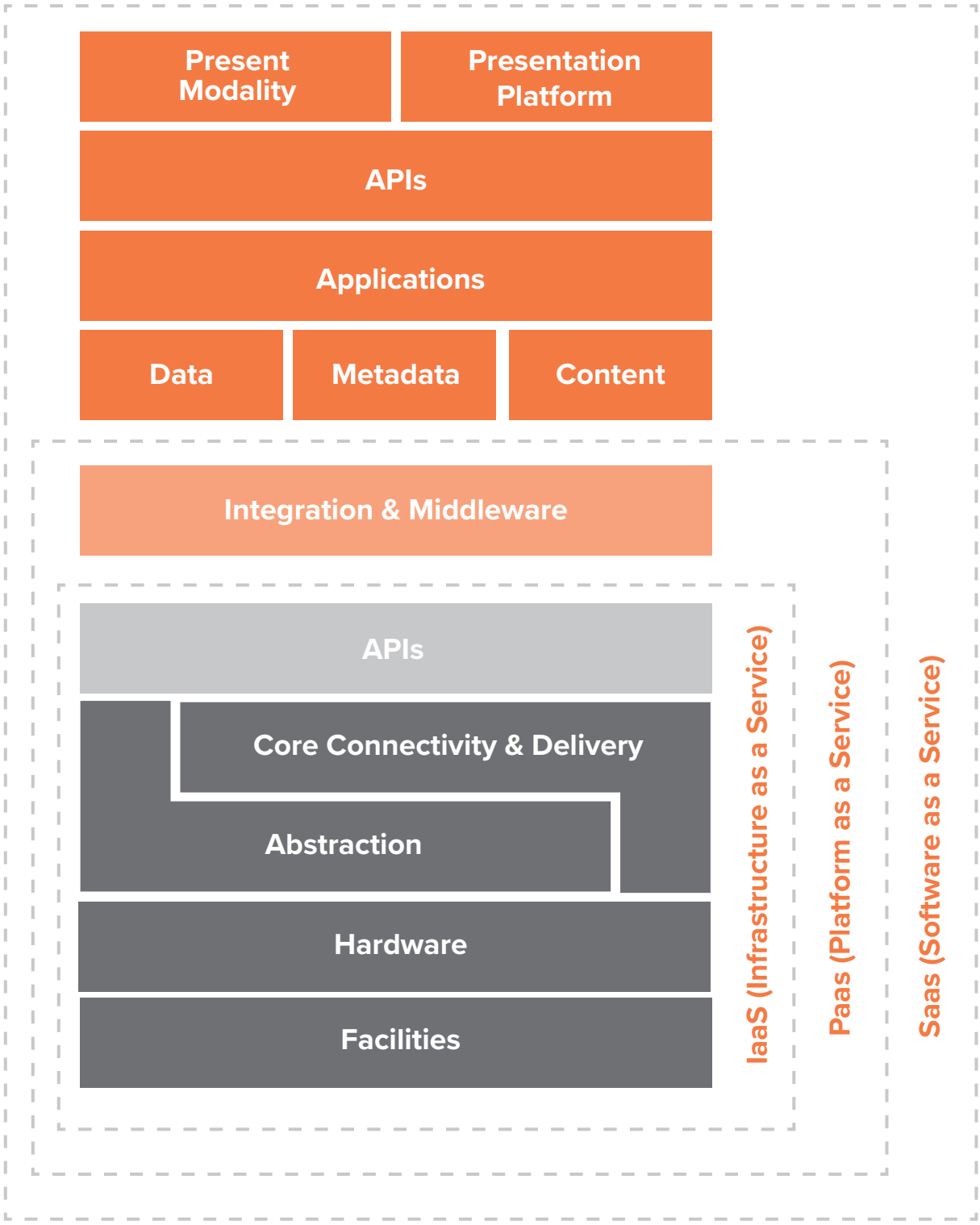


Figure 2: Cloud Security Alliance Shared Responsibility Model
(https://cloudsecurityalliance.org/artifacts/security-guidance-v4/)

The above diagrams make clear the separation of responsibilities and express the clear understanding that the more IaaS utilised in the organisation, the greater the need for security to be more clearly managed.

2.4 Bi-Modal Operations Modes - Innovation and Operation

Our experience helping organisations manage private and public cloud platforms has uncovered two main modes of operation; Innovate and Operate. These align with classifying Systems of Engagement and Systems of Record.

Innovate activities are typically oriented for agility and speed to market whilst Operate activities are focused on business critical services.

We believe that support requirements differ significantly in both modes. By assessing our client's environments based on these criteria, we can ensure that the support plan and resources assigned are designed to fit requirements at all stages of the life cycle.

INNOVATE MODE	MAXIMISED FOR CHANGE
• Regular changes and releases • Lean documentation • High incident frequency • Moderate change governance processes • Discovery usage pattern • Low business risk	Innovate time is designed to provide services in emerging, frequently changing or problematic environments. Our plans include a blend of support services for incidents and standard service requests, as well as delivery services on hand to action more complex changes and to provide expert guidance to help increase stability over time. Much more than traditional support, these plans can help to design, shape and build the solution whilst performing a seamless transition to operations.
OPERATE MODE	**RELIABLE OPERATIONS**
• Infrequent change • Comprehensive documentation • Low incident frequency • Operational usage pattern • Large user base • High business risk	Operate time is designed to fulfil support requirements in well established environments where the key priority is operational availability. We apply ITIL v3 processes that prioritise: • Managing business risk and service disruption or failure • Establishing cost-effective systems for managing demand for your services • Supporting business change whilst maintaining a stable service environment

2.5 Cloud Operating Model - Secure

When designing a Cloud enablement program in regards to an implementation of a Cloud Platform, there are a range of areas of responsibility, in addition to ongoing processes to consider. Security in a cloud operating model is as detailed.

The following table highlights the key considerations.

Category	Description	Policy, Process, and Tool considerations
Identity Access Management	• User lifecycle • Application access and authorisation- RBAC • Identity management	Having a single source of truth of user authentication eases operational and security complexities. Tools such as Google Cloud Directory Sync allows synchronisation of existing directories to GCP.
Application Security	• Scanning and Testing • API Security • Application & Endpoint patching • Compromise prevention • Device Management	Application security should be inline with internet facing standards. Servian development standards include using cloud vendor security recommendations, OWASP recommendations and ISO27001
Security Operations	• Threat Prevention • Detection • Incident Response • Logging	Security Operations should have processes inline with internet facing standards. As the footprint grows, so should the resourcing to support the capability. Sensitive data has specific implications for logging. When support tickets are raised, for example with Google Cloud, support may request access to resources. Access to resources are made visible via 'Access Transparency logs'
Data Security	• Encryption at rest • Encryption in transit • Sensitive data • Preventing exit/loss	Data classification is a key dependency As an example CIA (Confidentiality, Integrity, Availability) ratings can be used to assess criticality from C1 to C4. Key management is a key concern for many organisations. An investment in a Secret Management and Key infrastructure software is recommended for consideration. Prevention of data loss is a key design consideration for data platforms which requires process and technical design focus.

Network security	• Defining / enforcing perimeter • Segmentation • Managing remote access • DoS defense	Any cloud platform should contain multiple security zones. Public Internet facing vs internal facing zones as an example, which can be supported by cloud provider network configuration.
Infrastructure	• Cloud Infra. (Layers up to and inc OS) • Network • • Patch policy, VM imaging policy • Configuration Management and VM lifecycle	Cloud infrastructure can be managed as code within a CI/CD process which may help tighten spend and risk processes. Typically these include • There are fixed patching policies • Controlled, hardened OS images • Infrastructure policy tools such as Hashicorp Sentinel are considered.
Governance, Risk Compliance	• Understanding risk • Defining and enforcing policy • Demonstrating compliance • Backup, Logging, Reviews, Audit, Policy register	User audit capabilities may include capabilities such as Sailpoint Identity governance or equivalents. Security Policy audit tools such as Forseti or Prisma should be considered. Logging & Telemetry should be used for application, infrastructure and audit activity, with long-term data archived.

There are a number of security frameworks available which can help shape the design of a detailed blueprint and secure cloud operating model. These include:

- Outcomes Framework - NIST
- Threat Detection Model - Mitre Att&ck Framework
- CIS Benchmarks - AWS, GCP, Azure, Kubernetes

All of an organisation needs to build and maintain systems with a primary goal of platform development and operations, to include the integration of these frameworks to ensure defense in depth throughout the organisation.

2.6 Cloud Operating Model - Connect

Networking in a heterogenous cloud model can be implemented in a very similar way to traditional segmented networks which are built in static data centers.

However, this misses the opportunity to leverage new approaches which follow patterns long established by technology giants, who have simplified their networking with service to service mappings and API gateways. They have done this in order to be able to deliver security and agility at scale.

FROM	TO
Perimeter Defence	Perimeter Defence
Segmented Network Zones	Micro Segments defined in Infrastructure as Code with Service to Service mappings for Cloud native services
North/South traffic secured by firewalls	North/South traffic enabled by API Gateways which provide access to internal and external developers
East/West Traffic secured by firewalls	East/West traffic secured by mTLS and configured via Service Mesh capabilities which leverage policy configuration to provide service to service security, traffic routing plus logging visibility and observability

2.7 Cloud Operating Model - Provision | Run | Monitor

Ultimately technology organisations are evaluated on their ability to provide agility for delivering change, operational stability and cost effectiveness with a secure posture.

This requires the development and deployment, or migration to cloud infrastructure, to optimise costs and take advantage of the ability to squeeze more compute from private or public data centers, while leveraging the ability to adjust demand for compute and storage at short notice.

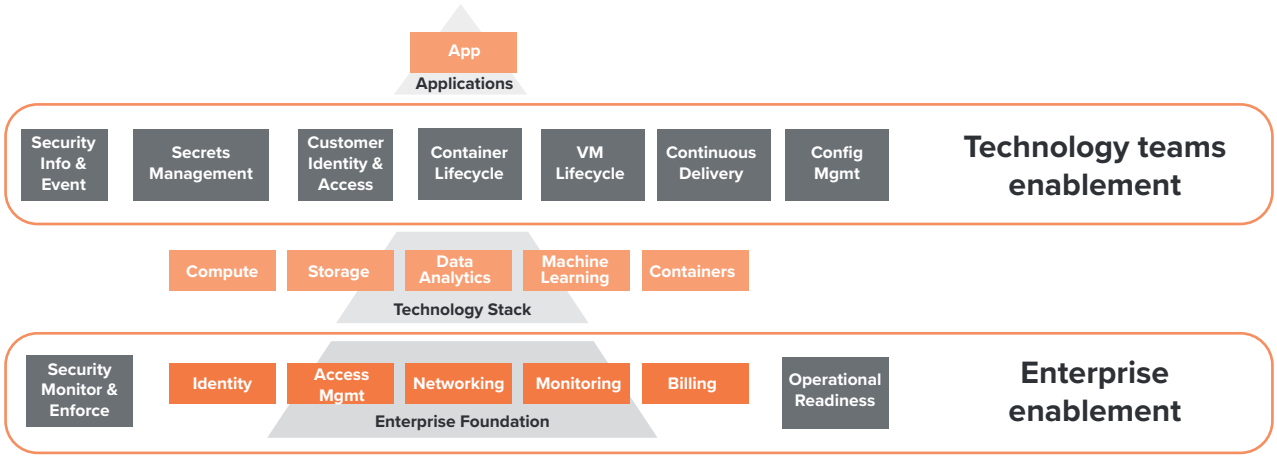
Servian's experience with on-premise and cloud has identified 2 broad patterns of application architecture which should provide a focus for applying new cloud capabilities. These are:

- Traditional 2 or 3 Tier applications;
  - Application Server VMs, inc. Linux or Windows
  - RDBMS - Relational Databases, inc. Oracle, MS SQL Server, Postgres etc
- Cloud Native;
  - Containers
  - NOSQL & Big Data data stores

2.8 Key Capabilities

In order to enable teams to meet expectations for a secure, cost-effective cloud operating model, specific capabilities are needed to mature the ways of work within enterprise teams.
The recommended capabilities are outlined below.

All can be developed in a cloud agnostic manner, which can be rolled out across both on-premise and public cloud infrastructure.



Security Info & Events	Security Info & Event management (SIEM) - aggregate logs, event signals to be able to take action and or respond effectively to events
Secrets Management	Effectively manage and automatically rotate application passwords and encryption keys to meet risk requirements without impairing agility
Customer Identity & Access	Customer Identity & Access Management (CIAM) - provide seamless but secure customer authentication and authorisation
Container Lifecycle	Update container builds and deploy effectively across clusters to meet risk & security requirements. Provide a repository of secure, CIS hardened containers
VM Lifecycle	Update VM builds of SOE/Golden images and deploy effectively to meet risk & security requirements such as CIS and internal standards
Continuous Delivery	Enable stage gates to rapidly accept and deploy applications, building scale to increase throughput of approved change into production
Configuration Management	Manage and deploy parameters throughout the dev and ops lifecycle. Key enabler for Continuous Delivery, high performance microservices at scale and Infrastructure as Code.

3. Building a Blueprint

3.1 Principles of Constructing a Blueprint

The following are principles to consider when building a blueprint for an organisation:

- Leveraging Infrastructure as Code to underpin deployment processes and limit configuration drift
- Baking in security to development and deployment processes through the use of;
  - Artifact scanning
  - Environment scanning
  - Logging and alerting
- Pipelining Continuous Delivery to enable a level of composable consistency to deployments
- Enabling agility by having a fast lane process for pre-approved patterns

3.2 People, Process, Technology Considerations

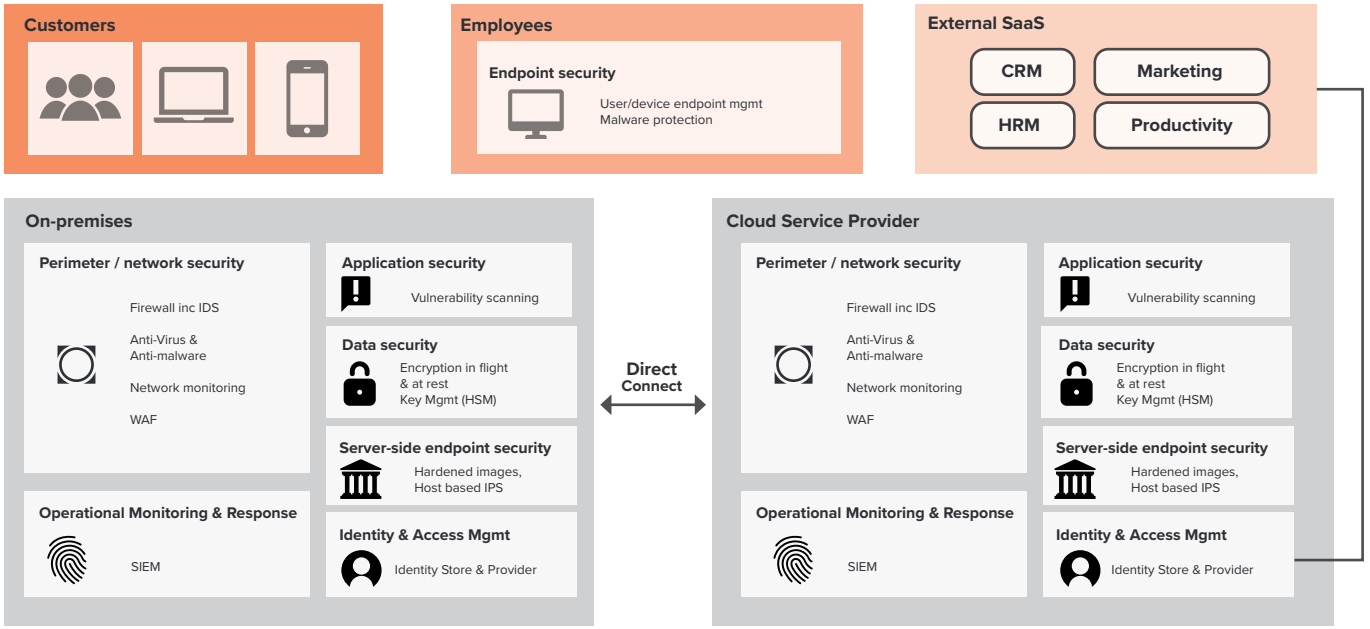
Each cloud provider has their own capabilities and commercial model. How does an organisation evolve its operating model to be able to benefit from this variation, while also delivering a level of coherence and consistency across their service offerings? There are a number of concerns:

1. **People -** what are the skills needed to operate a heterogeneous cloud environment? What training and documentation is needed to empower?
2. **Process -** how are central technology roles able to become enablers of self service speed and cost effectiveness?
3. **Technology -** what technology is needed to stand up and then run successfully in a heterogeneous cloud environment? How does an organisation unlock the value cloud providers are offering while maintaining their security posture?

3.3 Generic Cloud Security Blueprint

Servian's Cloud Security Blueprint highlights that all the same disciplines are required in a cloud world, however there are differences in the application of each discipline in public cloud, in addition to the tooling and other differences across each public cloud.

This highlights that where possible, common tooling which cuts across public clouds and on premises assets, will have the advantage of enabling security, networking, operations and development teams to work in a consistent manner.


Customers
Employees
Endpoint security
User/device endpoint mgmt
Malware protection
External SaaS
CRM
Marketing
HRM
Productivity
On-premises
Perimeter / network security
Firewall inc IDS
Anti-Virus &
Anti-malware
Network monitoring
WAF
Application security
Vulnerability scanning
Data security
Encryption in flight
& at rest
Key Mgmt (HSM)
Server-side endpoint security
Hardened images,
Host based IPS
Identity & Access Mgmt
Identity Store & Provider
Operational Monitoring & Response
SIEM
Direct
Connect
Cloud Service Provider
Perimeter / network security
Firewall inc IDS
Anti-Virus &
Anti-malware
Network monitoring
WAF
Application security
Vulnerability scanning
Data security
Encryption in flight
& at rest
Key Mgmt (HSM)
Server-side endpoint security
Hardened images,
Host based IPS
Identity & Access Mgmt
Identity Store & Provider
Operational Monitoring & Response
SIEM

4. Example Roadmap

4.1 Example Roadmap

The following is an example roadmap based on the sequencing that Servian has observed across multiple industries which grows an organisation's cloud maturity.

4.2 Example Roadmap

Initial Project

- Manual configuration
- Small number of users
- Config can be adapted

  into future Enterprise enabled setup

Enterprise Enablement

- Infrastructure as Code approach
- Setup of Org Identity, User identity and Access Management, Networks, Billing, governance controls & reporting
- Security Monitoring & enforcement

Capability Enablement

- Secrets Management
- Container lifecycle
- VW lifecycle
- DevSecOps / SIEM Data Platform
- Continuous Delivery
- Configuration Management
- Multi-Cloud setup

Applications On Ramp

- Cloud native development
- Development of data pipelines, AI APIs
- On prem to Cloud migration
- Hybrid cloud ops

5. Tooling

	RIGID	DYNAMIC				SERVIAN	
Process	On premise	Private Cloud	AWS	Azure	GCP	Recom-mend	We also work with
Provision	vCenter	vCenter	Cloud Formation	Resource Manager	Cloud Deployment Manager	Terraform	All cloud specific tools
Run	vSphere	vSphere	EKS | ECS | Lambdas	AKS | ACS | Azure Functions	Compute Engine | GKE | Cloud Functions	Cloud Na-tive Func-tions | Kubernetes	Nomad
Monitor	3rd Party	3rd Party	Cloud-Watch	Azure Monitor	Stackdriver Forseti	Use cloud native. Aggregate to Elastic	Splunk, DataDog....
Connect	Hardware	Hardware	CloudMap | AppMesh	Proprietary	Proprietary | Istio	Istio | Consul	
Secure	Identity: LDAP/AD	Identity: LDAP/AD	Identity: AWS IAM	Identity: Azure AD	Identity: GCP IAM Scanner: Forseti Container: Binary Au-thorisation	Federated AD Se-crets:Vault Container: Aquasec Aggregate: Redlock	Tenable Nessus ArcSight

It is extremely important to identify which areas should be cloud agnostic, using centralised tooling etc. (ie. Monitoring, Provisioning), and which should take advantage of cloud-specific tools (Run, PaaS, SaaS).

6. About Servian

Mission

The Servian mission is to become the number one Australasian professional services company in the technology space. We are focused on enabling our clients to build competitive advantage and maximise ROI on their technology investment by:

- Providing thought leadership and innovation to deliver practical and best practice advice and solutions that address many of the key business challenges faced by our clients
- Allocating experienced, quality consultants who work collaboratively with our clients to meet outcomes and exceed business expectations.
- Transforming our clients information landscapes with new technology driven interactions that help them build trust both internally and externally
- Driving a cloud first mindset that builds collaboration across our clients' entire ecosystems to help them build best in class products and services

We are committed to providing excellence first, with delivery quality being a key metric in achieving the desired customer satisfaction optimum results, delivering efficiencies, cost-effectiveness and performance enhancement over the life of the client relationship.

History

Servian is a Professional Services organisation which provides IT advisory, consulting and managed services to clients seeking to use their data better to drive business performance. Founded in 2008, we have grown to become the largest pure play participant in the Australian Information management consulting market with 600+ consultants across ten main offices.

At Servian we have a diverse Tier 1 customer base and have worked with over 200 clients across government, finance and banking, telco, utility, insurance, construction, airline and retail sectors. We are highly referenceable among our clients; known for both our technology thought leadership and the quality of our delivery, we operate within the $12B Australian IT services industry.

We are uniquely platform agnostic and can implement technology solutions across any data, digital and cloud environment (including Google, Amazon and Microsoft).

Call us today see how we can work for you

We are experienced in delivering solutions across many industries such as banking, retail, telecommunications, insurance and utilities. Our clients include many of Australia's leading Tier 1 companies as our valued customers.

sydney
Level 46, 264 George Street
Sydney NSW 2000
t +61 2 9376 0700

melbourne
Level 20, Tower 5, 727 Collins Street
Docklands VIC 3008
t +61 3 9081 3700

brisbane
Level 3, 200 Mary Street
Brisbane QLD 4000
t +61 7 3193 3200

adelaide
Level 1, 5 Peel Street
Adelaide SA 5000
t +61 414 458 763

canberra
Suite 2, 6 Napier Close
Deakin ACT 2600
t +61 457 345 536

hobart
Level 2, 162 Macquarie St
Hobart, TAS 7000
t +61 402 658 878

auckland
Level 22, Crombie Lockwood Tower,
191 Queen Street,
Auckland NZ 1010
t +64 9 918 0580

wellington
Level 1, 139 The Terrace
Wellington 6011
t +64 4 499 6988

london
Uncommon, 34-37 Liverpool Street,
London, EC2M 7PP
t +44 (0)20 8092 5231

bengaluru
Level 2, Plot 23, 8th Main Road
Jayanagar 3rd Block
Bengaluru, India 560 011
t +91 80 4370 4670

servian.com