NETWORKING HEALTHCARE INNOVATION:

Creating a Foundation for Securing User Data and Workloads across the Cloud

epsilon
a kt company

SUMMARY

1.

THE HEALTHCARE CLOUD MARKET OVERVIEW

The COVID-19 pandemic rapidly accelerated digital transformation on a global scale. For healthcare organisations, the sharp rise in healthcare demand has created an urgency to focus on innovation efforts. According to a recent survey by McKinsey of more than 100 healthcare leaders, 90% agreed that the pandemic will fundamentally change the way they do business, requiring new products, services, processes, and business models.

Healthcare is an industry that is closely monitored and regulated by governments. Over the last decade, the protection and handling of customer data has been specifically regulated in many countries across the globe. This has significant impact on how healthcare organisations transform and adapt to new demand, making it complicated to drive change and innovation, particularly with regards to data.

Whilst the focus is on the protection of customer data and information at rest, most industry regulations also specify how sensitive data in motion needs to be handled. Common regulations like GDPR, HIPAA and SOC 2 have varying requirements for managing the transfer and movement of data traffic.

Therefore, how healthcare companies manage and secure their networks is as critical as any other form of security. Without complying to these regulations, enterprises face barriers to innovation in healthcare.

The cloud is fundamental to innovation, but can pose challenges in terms of data protection without the right security measures. Enterprises in the healthcare sector need to find a simple yet powerful cloud model to enhance operations, comply with regulations and keep up in a changing market with new innovation.

THE HEALTHCARE CLOUD MARKET BY THE NUMBERS

- The market for healthcare cloud computing is expected to grow from **$28.1 billion** in **2020** to **$64.7 billion** by **2025** (MARKETSANDMARKETS).

- **93%** of healthcare organisations globally have already adopted or are in the process of adopting a digital transformation strategy, with **78%** using cloud computing in operations (BDO).

- In a **2021** survey, **64%** of respondents named data loss/leakage as their biggest cloud security concern (STATISTA).

2.

THE SECURITY GUIDELINES APPLICABLE TO HEALTHCARE SERVICE PROVIDERS

Generally, the following are the key areas of security driving regulatory impact on networking:

- **Access to the network** – If you have access to a network, you have access to data – so managing who has access is critical. This means effective management of users and other system access.

- **Data-in-motion security** – When data is in transit or moving between systems, sites and even countries, it must be made as secure as possible.

- **Auditability** – Many regulators stipulate that any activity and change must be reviewable, trackable and open to audit. Keeping a consistent and linked path showing all networking changes is critical.

There are a whole range of guidelines to help defend healthcare networks and their data. When using cloud services, these guidelines and the issues driving them are vital for enterprises to follow.

IMPORTANT REGULATIONS:

- ✓ **The Health Insurance Portability and Accountability Act (HIPAA)** – US federal law that sets a national standard to protect medical records and other personal health information. The rule defines "protected health information" as health information that identifies an individual and is maintained or exchanged electronically (e-PHI) or in hard copy.

- ✓ **The General Data Protection Regulation (GDPR)** – Defines strict processes that businesses must follow when collecting and storing personal data of EU citizens (this still includes the UK). Data can only be stored with the specific consent of the user and only for the purpose stipulated.

IMPORTANT STANDARDS:

- ✓ **SOC 2** – SOC 2 compliance is part of the American Institute of CPAs' Service Organization Control reporting platform. Its intent is to ensure the safety and privacy of customers' data. It outlines five trust service principles of security, availability, processing integrity, confidentiality, and privacy of customer data as a framework for safeguarding data.

- ✓ **The Network and Information Systems (NIS2) Directive** – The EU-wide law on cybersecurity, NIS2, helps achieve a higher and more even level of security of network and information systems across the EU. It sets a range of network and information security requirements which apply to operators of essential services (OESs) and digital service providers (DSPs).

- ✓ **ISO 27001** – The internationally recognised specification for an Information Security Management System (ISMS). It is one of the most popular standards for information security. ISO 27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series. The basic goal of ISO 27001 is to protect three aspects of information:

  - **CONFIDENTIALITY:** only the authorised persons have the right to access information.
  - **INTEGRITY:** only the authorised persons can change the information.
  - **AVAILABILITY:** the information must be accessible to authorised persons whenever it is needed.

ADDITIONAL UK SUPPORTING GUIDELINES

In the UK, the legal frameworks covering how patient data must be looked after and processed are the Data Protection Act (DPA) 2018, which brought the EU GDPR into law, and the Common Law Duty of Confidentiality (CLDC).

The Data Security and Protection (DSP) Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Professional bodies such as the General Medical Council and Health and Care Professionals Council also set out standards which their members must meet (aimed at local providers but applicable to all).

3.

THE CLOUD & NETWORKING CHALLENGES

There are a number of challenges related to networking and security created by the adoption of both single and hybrid cloud architectures:

NETWORK & SECURITY COMPLEXITY:

- Single or multi-cloud
- Connecting to the cloud
- Consistency across clouds

SKILLS GAP:

- Different native constructs
- Lack of automation
- Clouds are application-focused

EXPLOSION OF CLOUD CONNECTIVITY OPTIONS:

- Connectivity to the cloud
- Networking in the cloud
- Encryption
- SD-WAN

OBSERVABILITY & TROUBLESHOOTING:

- Non-existent from cloud providers
- Multi-cloud visibility
- Flying blind

Healthcare enterprises face a unique set of challenges on top of the overarching challenges of the cloud:

TRANSPORT – When your data is in motion, it must be protected, whether it's the transfer mechanism, encryption in motion or simply access to the data whilst in transit.

AUDITABLE – All facets of data protection must be auditable, including the network, its access and its transport data.

ENCRYPTION – All data must be encrypted whether at rest or in motion.

AVAILABILITY & PROCESSING – Systems and data should be available at all times, and flexible enough to deal with incidents quickly and efficiently.

SECURITY – The defense of the data, systems, infrastructure and network must be defended with up-to-date security technologies and processes.

ACCESS – Only those permitted to access certain types of data, system and/or infrastructure should be able to, and access should be easily maintainable.

4.

COMMON ISSUES WITH CLOUD SERVICE PROVIDERS

CSPs do not deliver enterprise-class networking and security. Enterprises need more than basic networking and security, whilst a lack of common standards across clouds causes cost, time and resource issues.

IT and network teams are faced with more complexity when managing applications and workloads in the cloud, yet CSPs do not overcome these challenges or meet the needs of their enterprise customers.

NEEDS NOT SERVED:

1. Networking to, within and between cloud and other environments
2. Utilisation of enterprise grade networking
3. Monitoring and operational control

PROBLEMS NOT SOLVED:

1. Lack of visibility caused by no real-time network data and analytics
2. Limited troubleshooting tools - Packet Capture, Ping, Traceroute
3. Lack of control for high availability, encryption at scale, traffic engineering and correctness
4. No support for multi-cloud network architecture
5. Lack of multi-cloud Infra-as-Code-Automation, repeatable POD-like design and common security policies
6. Complexity and skill gaps caused by differing multi-cloud environments and constant cloud change

REALITY OF CLOUD NATIVE TOOLS *VS* STANDARDS & OBLIGATIONS

REALITY OF CLOUD NATIVE TOOLS	HIPAA STANDARDS OBLIGATIONS
• **Complexity in security** and firewall-insertion	**Access control.** A covered entity must implement technical policies and procedures that allow only authorised persons to access electronic protected health information.
• **No audit trails** for networking elements • **No centralised auditability**	**Audit controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
• **Lacks encryption** of data-in-motion • **No consolidated encryption** models across multiple environments	**Transmission security.** A covered entity must implement technical security measures that guard against unauthorised access to e-PHI that is being transmitted over an electronic network.

REALITY OF CLOUD NATIVE TOOLS	SOC 2 GUIDELINES
• **Complexity in security** and firewall-insertion • **Inconsistent security** tools • **No singular user management** function • **Lacks encryption** of data-in-motion • **No consolidated encryption** models across multiple environments • **No audit trails** for networking elements • **No centralised auditability**	**Security**. Protect information and systems from unauthorised access. This may be through IT security infrastructure such as firewalls and other measures to keep data safe from unauthorised access. **Processing**. Systems perform functions free from error, delay, omission, and unauthorised or inadvertent manipulation. **Confidentiality**. Protect data that should be restricted to a specified set of persons or organisations. **Privacy**. Safeguard personally identifiable information from unauthorised access.

REALITY OF CLOUD NATIVE TOOLS	SOC 2 GUIDELINES
• **No visibility** – no real-time network utilisation and packet statistics • **No cross-account traffic engineering** or network correctness • **No multi-cloud network architecture** • **Limited troubleshooting**	**Audit controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

REALITY OF CLOUD NATIVE TOOLS	GDPR REGULATIONS
• **Complexity in security** and firewall-insertion • **Inconsistent security** tools • **No singular user management** function • **Lacks encryption** of data-in-motion • **No consolidated encryption** models across multiple environments • **No visibility** – no real-time network utilisation and packet statistics • **No cross-account traffic engineering** or network correctness • **No multi-cloud network architecture** • **Limited troubleshooting**	**Processing and storing personal data + protection by design.** Maintain security of data when it is at rest or in motion performed with a consistent access/role-based management capability and high-performance encryption. Implement role-based control of network and application access. Reduce vulnerability with common security protocols which are consistent and easy to deploy and manage. Provide visibility and control over how data is transported, removing it from sightless and control-less exposure via public internet.
• **No audit trails** for networking elements • **No centralised** auditability	**Records of processing.** Create and maintain a record of all processing when it comes to network access and security with auditable change and control.
• **No visibility** – no real-time network utilisation and packet statistics	**Report data breaches within 72 hours.** Have a common control layer that can quickly identify where an issue is or isn't, pertaining to access and transport of customer data in readiness for 'fix and report'.

REALITY OF CLOUD NATIVE TOOLS

- **Complexity in security** and firewall-insertion
- **Inconsistent security** tools
- **No singular user management** function
- **Lacks encryption** of data-in-motion
- **No consolidated encryption** models across multiple environments
- **No visibility** – no real-time network utilisation and packet statistics
- **No cross-account traffic engineering** or network correctness
- **No multi-cloud network architecture** for ease of and consistency of other cloud and environment deployments
- **Limited troubleshooting**
- **No audit trails** for networking elements
- **No centralised auditability**
- **No visibility** – no real-time network utilisation and packet statistics

ISO 270001 STANDARDS OBLIGATIONS

- **A.9. Access control.** Limit access to information and information assets according to real business needs for both physical and logical access.
- **A.10. Cryptography.** Proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.
- **A.12. Operations security.** Ensure that IT systems are secure / protected against data loss and have the means to record events and generate evidence, verification of vulnerabilities and make precautions to prevent audit activities from affecting operations.
- **A.13. Communications security.** Protect the network infrastructure and services, and the information that travels through them.
- **A.14. System acquisition, development and maintenance.** Ensure that information security is taken into account when purchasing new information systems or upgrading the existing ones.
- **A.16. Information security incident management.** Ensure the proper communication and handling of security events and incidents, so that they can be resolved in a timely manner, preserve evidence and learn from incidents to prevent their recurrence.

A.17. Information security aspects of business continuity management. Ensure the continuity of information security management during disruptions and availability of information systems.

5.

MOVING TO ENTERPRISE-CLASS CLOUD NETWORKING

As healthcare moves to the cloud, more than basic networking and security is required.

Epsilon makes it simple to achieve compliance to guidelines and regulations:

AUDITABILITY

- Stored logs record all aspects of change management functions for review
- Incident review availability and compliant for reporting

ACCESS CONTROL

- 'Use' and 'Function' group assignment across entire IT estate with single controller, and share responsibility issue mitigation
- Common security domain enablement reducing open doors and mistakes

AVAILABILITY

- Instantly identify root cause and deal with incidents
- Fix with troubleshoot tools and create new common instances in DR environments instantly

NETWORK COMPLIANCE

- Enable multi-cloud segmentation connectivity
- Deploy connectivity to and from the VPC/VNET level within the cloud
- Remove public internet from transport path

END-TO-END ENCRYPTION

- Full and high-performance encryption (up to 75 Gbps) over Epsilon's global private network

MONITORING & OPERATIONAL VISIBILITY

- Advance visibility and operations via controller and CoPilot for real-time management
- Ability to see data-in-motion across private network

We provide **networking tools** for today's cloud environment that are available as your own:

NETWORK TRANSPORT – Dedicated path networking over a private MPLS network that you control:

- Full configurable via software-defined networking (SDN) and Network as a Service (NaaS) model
- Visible performance metrics
- Clouds, data centres and Internet Exchanges

NETWORK CONTROL – Configurable end to end set up, control and routing and policy functions for directing and protecting your traffic:

- Fully configurable portal(s)
- Across public and private networks
- Visible and configurable performance metrics and policies

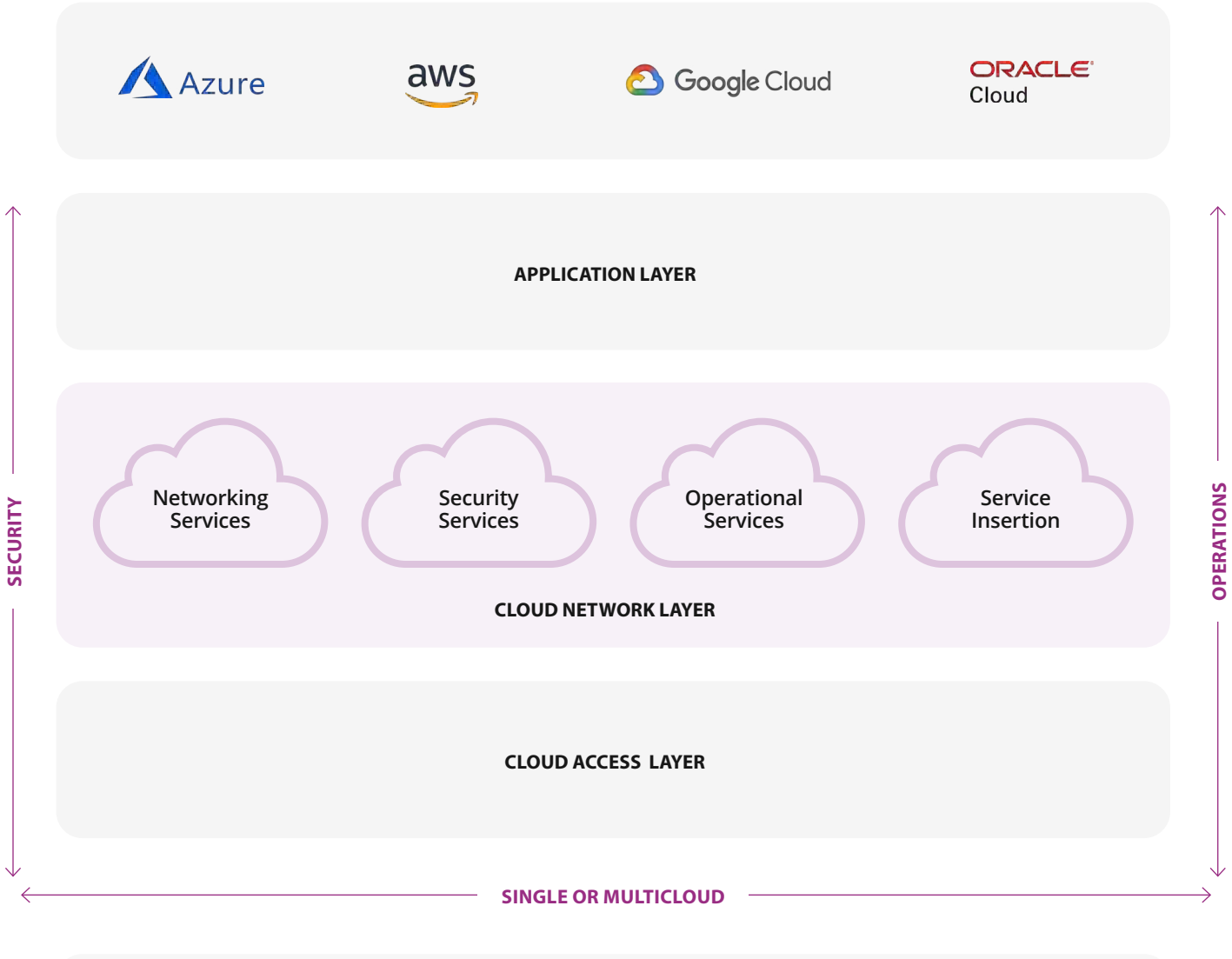
6.
EPSILON CLOUD NETWORKING

Epsilon's Cloud Networking service is a fully managed end-to-end multi-cloud network that incorporates on-prem and VPN user deployments with private network transport and a BYO security capability.

It allows you to directly control native cloud networking constructs to maintain cloud simplicity, with the automation, operational visibility and control needed for today's cloud-orientated IT environment.

The Cloud Networking service uses Epsilon's private network as underlay and the Aviatrix cloud network platform as overlay to create an enterprise-class network inside and between public clouds, up to the VPC/VNET level. It allows customers to consume security services, such as FQDN filtering and service insertion of next-gen firewalls, to meet their security and compliance requirements.

> MULTI-CLOUD NETWORK ARCHITECTURE



> IMPROVE OVERALL BUSINESS KPIS

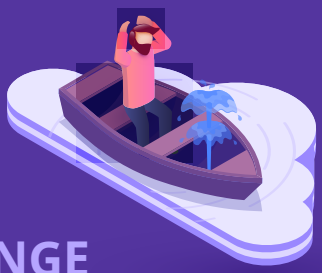
We enable you to increase efficiency by reducing CAPEX and OPEX:

- Improved productivity of engineering and operations teams – 14x build/deployment (32 hours without, 2 hours with) and 7x tactical ops (8 hours without, 1 hour with)
- Simplified networking and security in the cloud
- Hassle-free configuration and network onboarding
- Overcome skillset gap in public cloud

7.

USE CASE – OPERATIONAL IMPROVEMENTS IN HEALTHCARE

A healthcare organisation in the UK was seeking a way to **improve its cloud and networking functions with higher operational efficiency**. It needed to keep up in a changing market and future-proof its cloud strategy.



CHALLENGE

The organisation was facing continually repeating processes for function such as migrations, inter-networking and lack of copy functions. There were continual cycles of differing delivery needs for client services in different clouds.

This lack of consistency caused difficulties within the network architecture, with simple networking tasks using different approaches and set up steps. On top of this, there was a lack of team resources for across the board, multi-cloud tasks and experience.

It was facing inefficiencies in the 'build' and 'operate' areas of networking, particularly related to the cloud.

The combination of these challenges led to:

- Cloud provider networking inefficiency
- Lost business and revenue opportunities
- Added infrastructure costs

SOLUTION

The organisation selected Epsilon Cloud Networking to set up networking on cloud platforms in a much more familiar and consistent way across all platforms. It can now set up, automate, and support application environments, data stores, and other business infrastructure requirements across Microsoft Azure, Amazon Web Services and Google Cloud Services, with access to advanced networking and security tools that enterprises expect.

The organisation can take advantage of IT efficiencies to save costs and respond to business opportunities and emergencies much more quickly.

RESULTS

- ✓ Increased margin on new business (average of **$2.4 million** over three years)
- ✓ Faster delivery time to market (from **months to weeks**)
- ✓ Increased Network Engineer efficiency by **70%**
- ✓ Infrastructure cost saving (average of **$85,000** per annum)

8.

CLOUD NETWORKING BENEFITS

REDUCED TIME & EFFORT

- **Visibility** – Save time by working by exception, and not to rule
- **Commonality** – A common deployment model that is repeatable across all environments
- **Inclusive** – Ability to manage each device and VPN user profile with access privileges in common domain saves time and effort
- **Speed** – Deploying new instances becomes fast and simple and can result in faster cash to book situations

INCREASED PERFORMANCE

- **Scale** – Larger encryption tunnels support security of data-in-motion at scale
- **Distribution** – High-performance encryption distributes processing across multiple cores for load balancing and volume
- **Edge** – Router functions within the cloud remove trombone routing requirements
- **Private** – Using private networks reduces performance inhibiting issues of the public internet

IMPROVED UPTIME

- **Visibility** – Seeing issues enables working by exception and not to rule, saving time and effort
- **Proactive** – Immediately identifying and addressing potential fault or potential trouble points avoids downtime

IMPROVED EFFICIENCY

- **Incorporation** – Utilisation and incorporation of existing functions such as security and SD-WAN services
- **Inclusive** – Can utilise native tools such as core network and security to reduce existing cost model

REDUCED SKILLS GAP ISSUES

- **Commonality** – A common, 'repeatable across all environments' deployment model reduces the need for multiple cloud and other skills

TIGHTER SECURITY

- **Function** – Additional security functions enabled particularly within the cloud networking environment
- **Commonality** – A common domain for all-inclusive security, whilst also allowing BYO security
- **Private** – Reduces dependance on open and vulnerable public networks
- **Audit** – Complete audit trails provide compliancy and backward views for analysis and improvement

These benefits enable healthcare professionals to:

- Strengthen the protection of patient data as it moves in transit
- Strengthen access policy to key IT software and infrastructure
- Ensure more efficient management of the IT component
- Provide a common visibility capability for management and control
- Troubleshoot problems faster
- Reduce the potential for mistakes and errors to create security and compliancy holes
- Ensure the auditability of key network elements
- Synchronise security across all elements including cloud into a common view and domain

9.

THE FUTURE OF HEALTHCARE

For healthcare organisations, it is vital that they not only adopt cloud technology, but also understand how to leverage it to accelerate transformation into the future. Complexity is only set to increase in the healthcare sector, as new innovations and developments require new regulations and security guidelines.

Innovative technology is becoming increasingly accessible for all healthcare organisations, and is constantly evolving to meet changing demands in the industry. Compliance and data management are needed to innovate and expand the use of cloud-based applications and services, so these need to be a priority for all kinds of healthcare professionals.

With an innovative and comprehensive cloud networking solution, healthcare enterprises can seize the digital opportunity of today, to meet the needs of patients tomorrow.

info@epsilontel.com
www.epsilontel.com

epsilon
a kt company