**Enterprise Network Architecture**

Enterprise network architecture refers to the physical, virtual or logical connectivity of an organization’s specific business setup and layout of business network design vital for running the business-critical assets. It provides support to various tasks, such as internet calls and general communications systems, data storage systems, data analysis and management systems and more upcoming marketing business related IT inventions in that keep coming up in the IT world.

**Sample cases from businesses that have developed a successful Enterprise Network Architecture**

1. **Safaricom Limited (PLC)**

Safaricom is the leading provider of converged communication solutions in Kenya. In addition to providing a broad range of first-class products and services for Telephony, Broadband Internet and Financial services, Safaricom seeks to uplift the welfare of Kenyans through value-added services and support for community projects.

**Advantages**

* More focus for IT staff to work on specific projects and innovations
* Promotes more innovation for each department
* Gives a stronger technology infrastructure at the core technology
* Guides where services should be directed to
1. **Hewlett Packard Enterprise**

HPE-Aruba consistently ranks at the top of the enterprise networking solutions space and is known for its focus on unified networks. Aruba delivers SDN to scale along with an end-to-end interface. It offers zero-touch provisioning and end-to-end orchestration within a single pane of glass. It handles automated policy enforcement for the user, device, and app in both wired and wireless networking.

The platform also supports a high level of programmability through Python scripting and APIs, and a variety of cloud-based solutions designed to streamline IT operations and boost performance in SD-WANs. Users rank the company high for user experience, re-configurability and cybersecurity.

Aruba recently acquired Silver Peak Systems, a leader in the SD-WAN space. The platform unifies SD-WAN, firewall, segmentation, routing, WAN optimization, and more with advanced orchestration and automated lifecycle management, self-learning capabilities through machine learning, and more.

**Advantages**

* Automated security: HPE’s networking portfolio eliminates inconsistent policies and keeps all security information safe while pushing policies to the entire organization.
* Efficient network operations: The enterprise networking tools streamline analysis and identify vulnerabilities quickly for onboarding and configuration and enables segmentation for remote work, office connections, and the internet of things (IoT).
* Network Visibility: HPE Aruba has a singular source to monitor data for infrastructure with any sized business. It allows the business to have alerts, performance, and client data flow.
1. **Dell Technologies**

Dell Technologies offers a robust and highly-rated portfolio of enterprise solutions. The company offers a wide array of products and solutions for enterprise networks, including Ethernet switches, wireless gear, smart fabric management software, services for automated fabric management, network operating systems, and various products and tools that facilitate SDN.

Dell Technologies also focuses on maximizing connectivity at the edge with cloud integration: integrated hardware and software solutions for SD-WAN and clouds. This enables autonomous fabric deployment, expansion, and lifecycle management for software-defined infrastructures.

The company aims to “meet the demands of modern workloads and virtualization environments while greatly simplifying deployments and management” through a single pane of glass.

**Advantages**

* Automation saves time: Tasks done by automation are praised for the time and money that is saved using Dell’s networking services.
* Helpful backups: When Dell Technologies backup customer data, they feel secure and protected.
* Support helpful: The customer support Dell provides is helpful and knowledgeable on how to fix errors through different parts of the network.
1. **Extreme Networks**

Extreme Networks offers switching, routing, analytics, security, and other management solutions. The Extreme Networks product line is defined by Extreme Cloud IQ, a platform that automates end-to-end, edge-to-data-center network operations through the use of AI and machine learning. It is designed to scale to more than 10,000 managed devices per wireless appliance and includes comparative analytics and ML-driven scorecards.

Extreme Management Center provides on-premises network management in a variety of networking environments. In the realm of unified communications, Extreme Campus Controller delivers wired and wireless orchestration for campus and IoT networks.

**Advantages**

* Faster deployment: Some networking tools take time to deploy, and Extreme Networks has a positive reputation for their deployment.
* Reliability: After a business installs the tools, they do the work and do not require supervision.
* Easy to manage: Customers say that all of the data is in one place for the tech and business to manage their systems.
1. **Manage IT Africa**

It is an African technology company that focuses on IT infrastructure, managed services, system integration, enterprise solutions and SAP, server and network management, mobile device management and IT modernisation.

**Advantages**

* Reduces risk and exposure
* Decreases total cost of service ownership
* Reduces redundancy of effort and services
* More reuse of current methods and system components

**Industry Level Business Requirements for Enterprise Network Architecture**

****

* **Business architecture:** documentation that outlines the company's most important business processes;
* **Information architecture:** identifies where important blocks of information, such as a customer record, are kept and how one typically accesses them;
* **Application system architecture:** a map of the relationships of software applications to one another; and
* **The infrastructure technology architecture:** a blueprint for the gamut of hardware, storage systems, and networks. The business architecture is the most critical, but also the most difficult to implement, according to industry practitioners.

**Characteristics of Architecture Principles**

* Architecture principles define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise. They reflect a level of consensus among the various elements of the enterprise, and form the basis for making future IT decisions.
* Each architecture principle should be clearly related back to the business objectives and key architecture drivers.

**Components of Architecture Principles**

It is useful to have a standard way of defining principles. In addition to a definition statement, each principle should have associated rationale and implications statements, both to promote understanding and acceptance of the principles themselves, and to support the use of the principles in explaining and justifying why specific decisions are made.

**Ways of keeping Information Secure**

It is important to keep information secure so as to reduce the risk of data breaches and cyber-attacks in IT systems. It is necessary to apply security controls to prevent unauthorized access to sensitive information. It is mandatory to prevent disruption of services, e.g., denial-of-service attacks. Protect all the IT systems and networks from exploitation by outsiders. Some of the measure to be undertaken include:

 **1. Back up your data**

You should back up your data regularly. If you’re using an external storage device, keep it somewhere other than your main workplace – encrypt it, and lock it away if possible. That way, if there’s a break-in, fire or flood, you’ll minimise the risk of losing all your data.

Check your back-up. You don’t want to find out it’s not worked when you need it most. Make sure your back-up isn’t connected to your live data source, so that any malicious activity doesn’t reach it.

**2. Use strong passwords and multi-factor authentication**

Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored. They must be difficult to guess. The National Cyber Security Centre (NCSC) recommends using three random words.

Where possible, you should consider using multi-factor authentication. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message.

**3. Suspicious emails**

You and your staff need to know how to spot suspicious emails. Look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated. A phishing email could appear to come from a source you recognise. If you’re not sure, speak to the sender. NCSC provide useful training materials to help you and your staff recognise suspicious emails.

**4. Install anti-virus and malware protection**

Make sure the devices you and your employees use at home, or when you’re working away, are secure. Anti-virus software can help protect your device against malware sent through a phishing attack. Ensure that the anti-virus is up-to-date.

**5. Protect your device when it’s unattended**

Lock your screen when you’re temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer, put it in a secure place, out of sight.

**6. Make sure your Wi-Fi connection is secure**

Using public Wi-Fi, or an insecure connection, could put personal data at risk. You should make sure you always use a secure connection when connecting to the internet. If you’re using a public network, consider using a secure Virtual Private Network (VPN).

**7. Limit access to those who need it**

Different workers may need to use different types of information. Put access controls in place to make sure people can only see the information they need. For example, payroll or HR may need to see workers’ personal information, but your sales staff won’t.

If someone leaves your company, or if they’re absent for a long period of time, suspend their access to your systems.

**Testing and Analyzing Business Cases**

* 1. It helped us to understand our customer's business goals and constraints which is a critical aspect of network design. Armed with a thorough analysis of our customer's business objectives, we are able to propose a network design that will meet our customer's approval.
	2. It made it possible to learn something about the client's market, suppliers, products, services, and competitive advantages. With the knowledge of our customer's business and its external relations, we can position technologies and products to help strengthen the customer's status in the customer's own industry.
	3. We were able to minimized the equipment required to test large-scale networks and identified gaps in network readiness and validated and refined device configurations.
	4. It helped certify new hardware, operating systems, and software features to enhance the operations of the company and i8mprove the client and customer base.