p +61 1300 113 112
e info@hyperscalers.com



# Ridgeback Network Defence

Introduction

Hyperscalers with Ridgeback Network Defence


Monday, 30 January 2023

# 1 INTRODUCTION

Ridgeback is an active network threat detection, monitoring and response platform. Modern malware, ransomware, and spyware mostly spread through communication platform like emails, where firewalls are not enough to safeguard your network. Traditional, signature-based end-point security solutions are unable to keep up with the daily emergence of more and more malware. Here is where Ridgeback defence comes into play: a unique, contemporary defence to identify and stop lateral attacks within your network. It is an effective real-time network defence system that runs at the core of your network and safeguards your data.

Ridgeback significantly raises the time and labour cost of attack for the attacker without requiring continual upgrades, giving the company back control.

Ridgeback is plug-and-play, doesn't require extensive configuration or impose any infrastructure burden, starts working immediately after activation, needs little to no supervision, and won't interfere with or burden your live network.

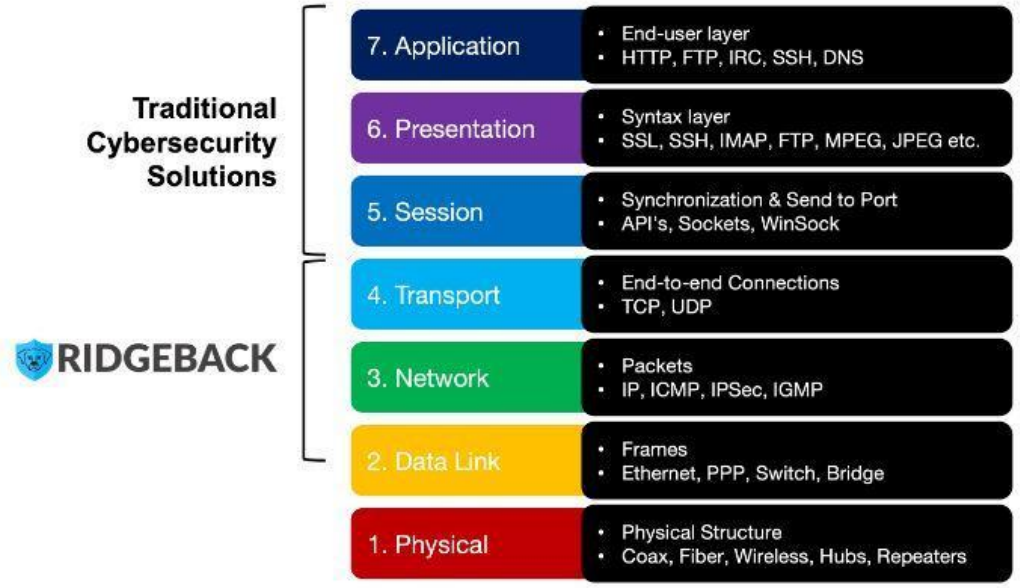


*Figure 1 Ridgeback location on network*

While competing solutions function at higher levels requiring ubiquitous agents, using enormous amounts of resources, and producing several false positives, Ridgeback operates at OSI Layers 2, 3, and 4 and interrupts assaults in real-time by man-in-the-middle automation that engages, disables, and evicts attackers at the start of the exploit.

## Infrastructure

S5K | D43K-1U – 1U as a Highly Available two node Proxmox 7.2-11 cluster:

- 2x AMD EPYC 7313 16-Core Processor
- 16x DDR4 3200Mhz 32GB Register Samsung M393A4K40DB3-CWE
- 1x Dual port 10GbE Mellanox Technologies MT27800 Family [ConnectX-5]
- 2x OS SSD WD_Green_M.2_2280 240GB
- 1x Data SSD 2.5" U.2 NVMe SSD Samsung PM9A3 3.84TB NVMe PCIe MZQL23T8HCLS-00A07

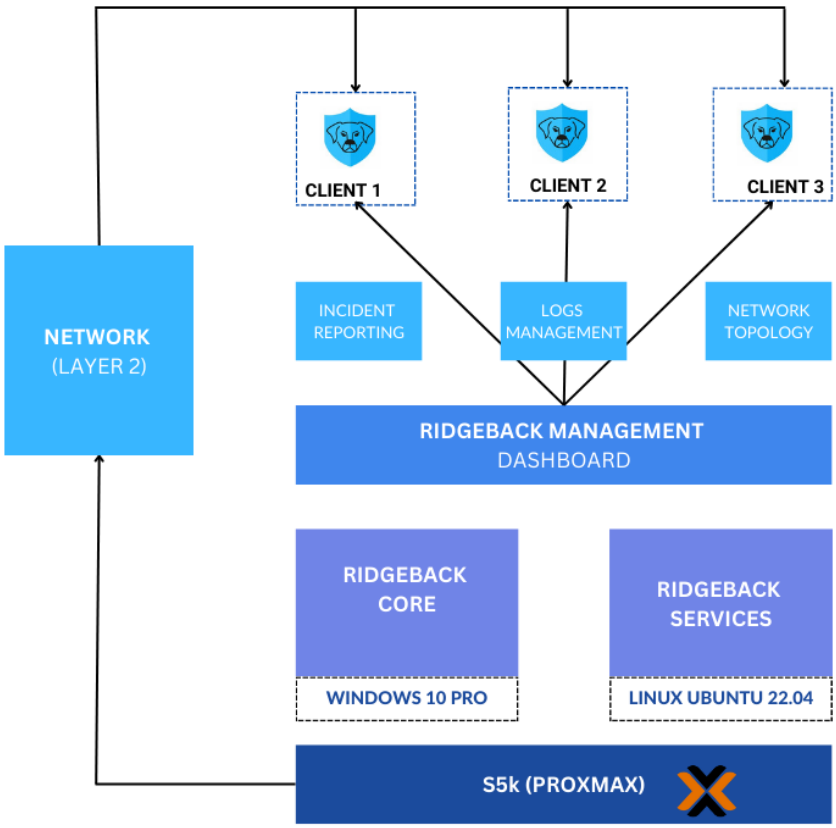


*Figure 2 Ridgeback Network Defence Architecture Design*

## Ridgeback Business Use-cases

Ridgeback can be setup in any network, from small companies to large organizations, due to its strict network Defence features. Due to Ridgeback's design, any industry like insurance, education as well as government services can use this easy and cost--effective solution to safeguard your network from various threats.

***Banking and financial services cybersecurity.***

Compliance with regulations necessitates complete, in-depth visibility into system operations. Ridgeback offers insights on weaknesses and productivity issues, particularly when branch office locations are involved across different network segments.

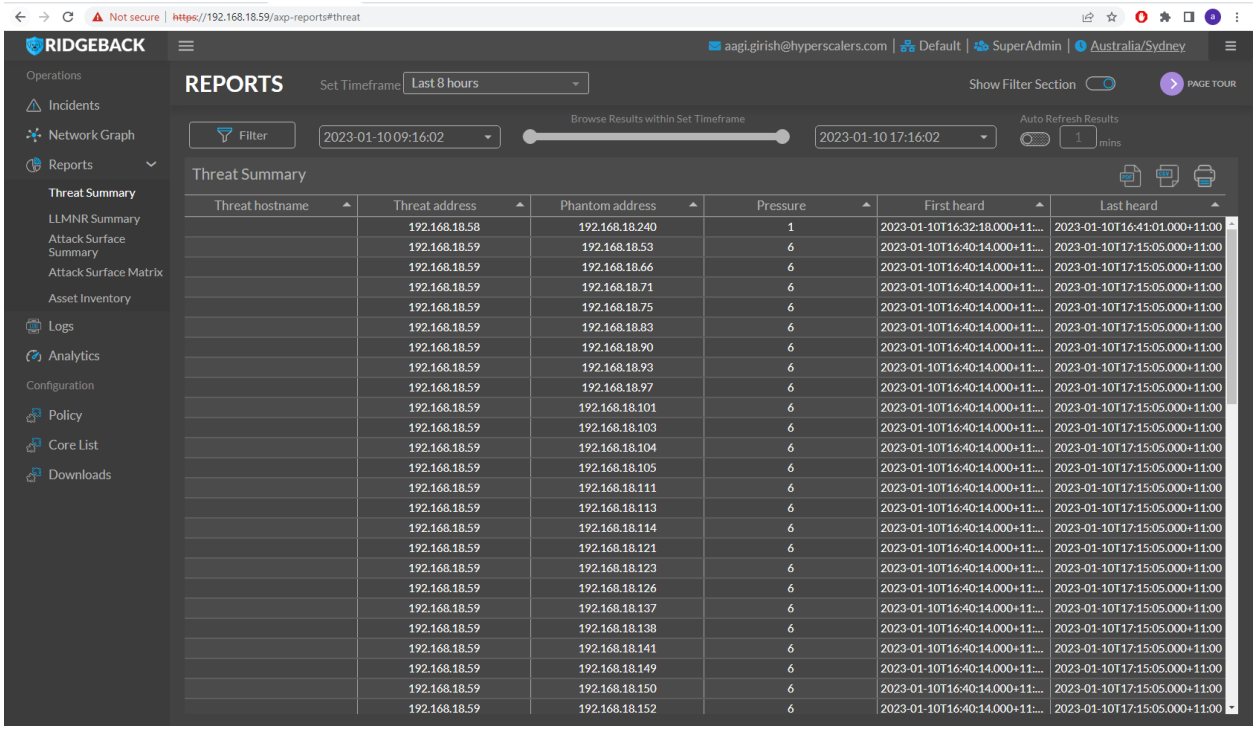


*Figure 3 Ridgeback reports*

***The Private Equity Life Cycle Management.***

Catastrophic cyber-attacks on a portfolio can now more than ever decimate a private equity owner's financial return. Ridgeback provides ownership life-cycle services, starting with pre-closing due diligence and ending with a smooth departure.

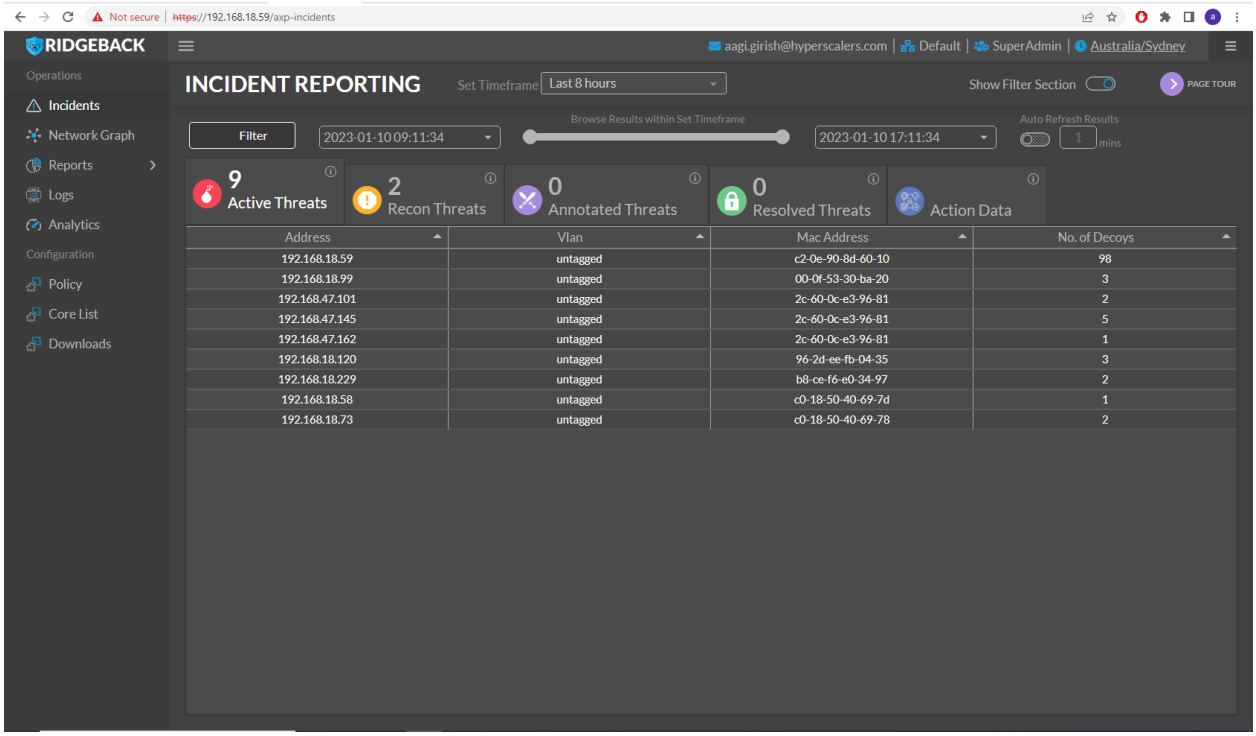


*Figure 4 Ridgeback threat incidents*

***Managed Services and Managed Security Services.***

Ridgeback satisfies situational awareness and security requirements across a wide and diverse client base for an IT services provider thanks to multi-tenancy and an architecture for deployment that is unmatched in its simplicity.

***Cyber security for public utilities***

As you may have seen in the news, foreign governments as well as ransomware-seeking criminals attack public utilities to interfere with the functioning of our nation. Ridgeback should be utilised to secure the networks of all public utilities since they are all too crucial.

***Network Defence in the Manufacturing Sector***

OT-heavy workplaces are managed by manufacturers. Ridgeback operates at layer 2, enclosing all networked endpoints within its security perimeter regardless of their hardware, operating systems, or status as managed or unmanaged devices.

***Healthcare and cybersecurity***

Healthcare and cybersecurity Ridgeback incorporates each networked endpoint, regardless of the kind, inside its security envelope, so you do not have to worry about patient information or the safety of lifesaving IoT healthcare equipment.

## Features and benefits of Ridgeback:

***Network Protection:***

When a hacker tries to get into our systems, Ridgeback defends our systems with the security measures that turns it into a defensive mode immediately for intruders by deploying an automated layers of protection to access any network assets. In simple terms, when an intruder tries to access from a compromised node, Ridgeback can automatically recognize it and raise the alarm on the system dashboard and can isolate the offending node.

***Lateral movement Prevention:***

Ridgeback enhances security by providing helpful remediation tools that stop security risks' damaging lateral movement. When an attacker gains access to your system, they seek to further enter your network to do more damage. This is known as lateral movement. By limiting the harm done by intruders, the programme rapidly neutralises these security concerns, ensuring the safety and security of your network.

***Continuous visibility:***

The solution offers total visibility by constantly keeping an eye on your whole network and all the data/information it contains. Your network-connected laptops, mobile devices, and tablets are all regularly scanned for and evaluated for security vulnerabilities by Ridgeback. It makes sure that only people with permission may access your information.

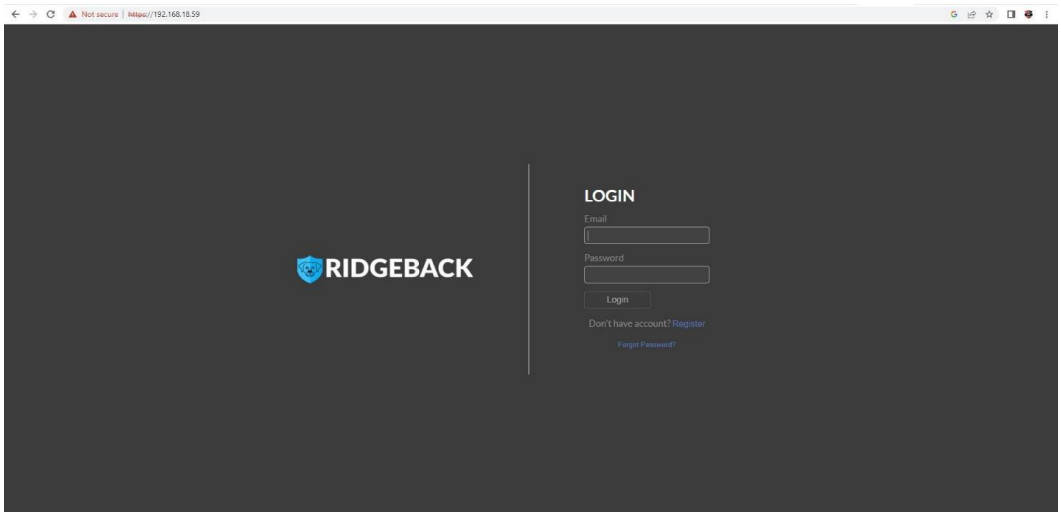


*Figure 5 Ridgeback dashboard*

***Policy Enforcement:***

Ridgeback makes sure that your security policy is strictly followed. Every action on your network is constantly checked against your custom policies, which ensures that all your rules are consistently followed.

***Integration:***

The programme has useful integrations, such as support for SEIM (security information and event management), so it may be easily included into your current security framework.

***User friendly:***

Ridgeback's cloud-hosted design allows quick and easy setup. Once it is operating, the system is basically autonomous and doesn't need much supervision.

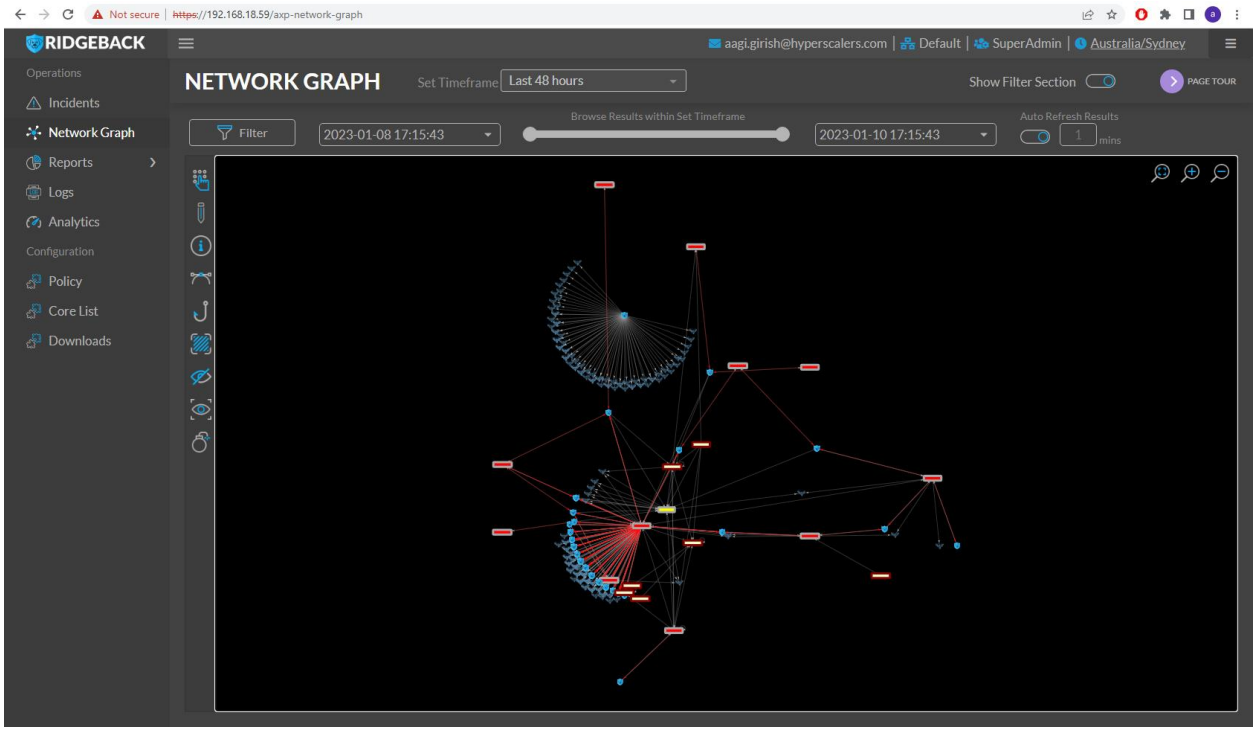


*Figure 6 Ridgeback Network Graph*

# Why Hyperscalers

Hyperscalers [1] is the world's first open supply chain Original Equipment Manufacturer- OEM, solving Information Technology challenges through standardization of best practices and hyperscale inspired practices and efficiencies. Hyperscalers offers choice across two open hardware architectures:

- Hyperscale - high efficiency open compute equipment as used by macro service providers.
- Tier 1 Original – conventional equipment as per established Tier 1 OEM suppliers.

Each architecture is complete with network, compute, storage, and converged GP GPU infrastructure elements, and is open / free from vendor lock-in.

Hyperscalers' appliance solutions are complete with hardware, software and pre-built (customisable) configurations. These were all pre-engineered using an in-house IP Appliance Design Process and validated in partnership with associated major software manufacturers. Many can be "test-driven" using Hyperscalers Lab as a Service (LaaS). Hyperscalers appliance solutions are ideally suited to IaaS PaaS and SaaS providers looking to implement their services from anywhere.

To access the Hyperscalers Lab as a Service (LaaS) portal, navigate to https://www.hyperscale2.com which is a repository of enterprise appliances that can be used to test drive the use cases before deploying on a mass scale.

Ridgeback cyber Defence can be accessed from https://ridgeback.hyperscale2.com/ (Please request for the credentials to info@hyperscalers.com and we can assist you.)

# Digital IP Appliance Design Process

Hyperscalers has developed a Digital- IP-Appliance Design Process and associated Appliance Optimizer Utility which can enable the productization of IT-appliances for Digital-IP owners needing to hyperscale their services very quickly, reliably and at a fraction of traditional costs.

### *Appliance Optimizer Utility AOU*

The Appliance Optimizer Utility (AOU) automates the discovery of appliance bottlenecks by pinging all layers in the proposed solution stack. A live dashboard unifies all key performance characteristics to provide a head-to-head performance assessment between all data-path layers in the appliance, as well as a comparison between holistic appliances.

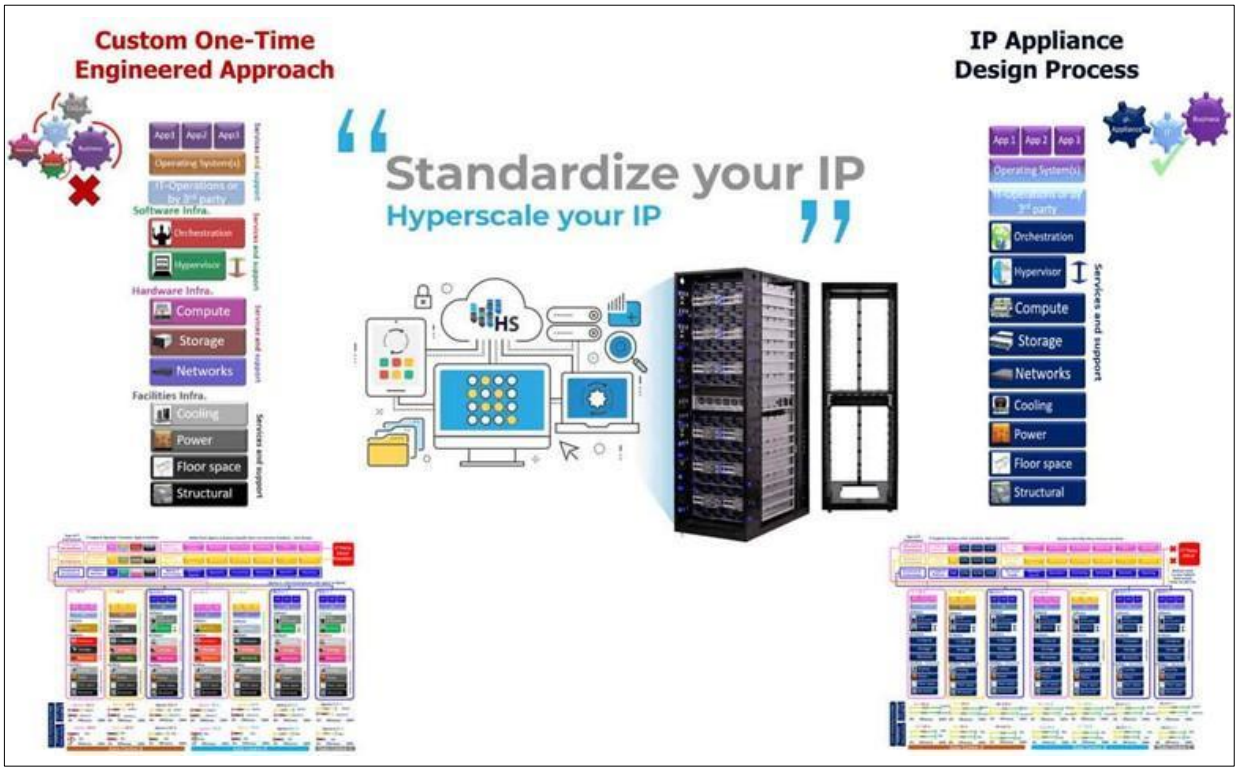


*Figure 7 Digital IP-Appliance Design Process*

# Building Blocks:

[S5K | D43K-1U Ultimate 1U Server for AMD EPYC Milan 3rd Gen Processors]

Native design for AMD EPYC™ 7003 Processors, ready for PCIe 4.0 eco-system deployment. Up to 128-core within 1U form factor, optimized for HPC workloads. With 4 AMD xGMI-2 between dual EPYC™ processors up to 16GT/sec of CPU interconnect speed. Up to 5 PCIe expansion slots in a 1U chassis. Flexible I/O options with a variety of SAS mezzanine and OCP mezzanine option for diverse configurations. Flexible storage configurations, tailored for diversified software defined workloads. NUMA balanced PCIe topology for NVMe drives.

[S5X 2.5" | D53X-1U Ultimate 1U Server for Intel Xeon 3rd Gen Processors]

The S5X 2.5" (D53X-1U) based on PCIe Gen 4.0 and Intel's 3rd Generation Processor Family (Ice-lake) offers: Two (2) CPU Sockets for up to 80 cores using Intel® Xeon® Platinum 8380 Processor 40cores each. 32 Memory slots for up to 8TB DIMM or Up to 12TB DIMM+DCPM (PMEM 200 series). 12 Front Storage drive bays 2.5" hot-plug U.2 NVMe or SATA/SAS. Five (5) x PCIe 4.0 expansions slots for Network Interface Cards NIC. Two (2) M.2 onboard storage. Three (3) accelerators like NVIDIA T4 GPU.

## S5Z | T43Z-2U The Power of Hyper Convergence

The S5Z | T43Z-2U based on PCIe Gen 4.0 and Intel's 3rd Generation Processor Family (Ice-lake) is a high performance, multi node server offering eight (8) CPU in 2RU as part of four (4) independent nodes. Each node offers two (2) CPU Sockets for up to 80 cores using Intel® Xeon® Platinum 8380 Processor 40cores each, 16 Memory slots for up to 4TB DIMM or up to 6TB DIMM+DCPM (PMEM 200 series), four (4) 2.5" U.2 NVMe front storage drive bays with two (2) M.2 NVMe for OS or caching, and three (3) x PCIe 4.0 expansions slots for Network Interface Cards NIC or accelerators like GPU.

# Terminologies:

***Network layer:***

In the context of computer networking, the network layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing logical addressing and routing services. The network layer is responsible for routing data packets between devices on a network. It does this by assigning a unique address to each device on the network, and then using this address to determine the best path for the data to take from its source to its destination.

***Containers:***

A container is a lightweight, standalone, and executable package that includes everything an application needs to run, including the application code, system tools, libraries, and runtime. Containers are often used in conjunction with container orchestration tools, which are used to manage and deploy large numbers of containers across a network. Container orchestration tools allow users to define and automate the deployment, scaling, and management of containerized applications, making it easier to manage complex distributed applications.

***Lateral Movement:***

Lateral movement refers to the process an intruder uses to expand their control from one network resource to many within an organization's network. It is often used by attackers to gain access to additional systems and data once they have compromised a single device or system. Lateral movement is a common technique used by attackers to gain a foothold in an organization's network and to escalate their privileges. It is often used in conjunction with other tactics, such as phishing attacks or malware, to gain initial access to a network, and then to move laterally within the network to gain access to sensitive data or systems or disrupt operations where they are most critical.

# 2 REFERENCES

1. Ridgeback Network Defence, I. (no date) *Ridgeback - 2023 reviews, pricing, features, Ridgeback - 2023 Reviews, Pricing, Features*. Available at: https://www3.technologyevaluation.com/solutions/54883/ridgeback (Accessed: January 30, 2023).
2. *Solving it's complexity* (no date) *Solving IT's Complexity*. Available at: https://www.hyperscalers.com/ (Accessed: January 30, 2023).
3. *We stop lateral movement* (no date) *Ridgeback Network Defence*. Available at: https://www.ridgebacknet.com/ (Accessed: January 30, 2023).