ESG Technical Review

The Business Value of Containerized NetBackup Data Protection Deployments with the Veritas Flex Appliance

Date: March 2019 **Author:** Vinny Choinski, Senior Validation Analyst; and Christophe Bertrand, Senior Analyst

Abstract

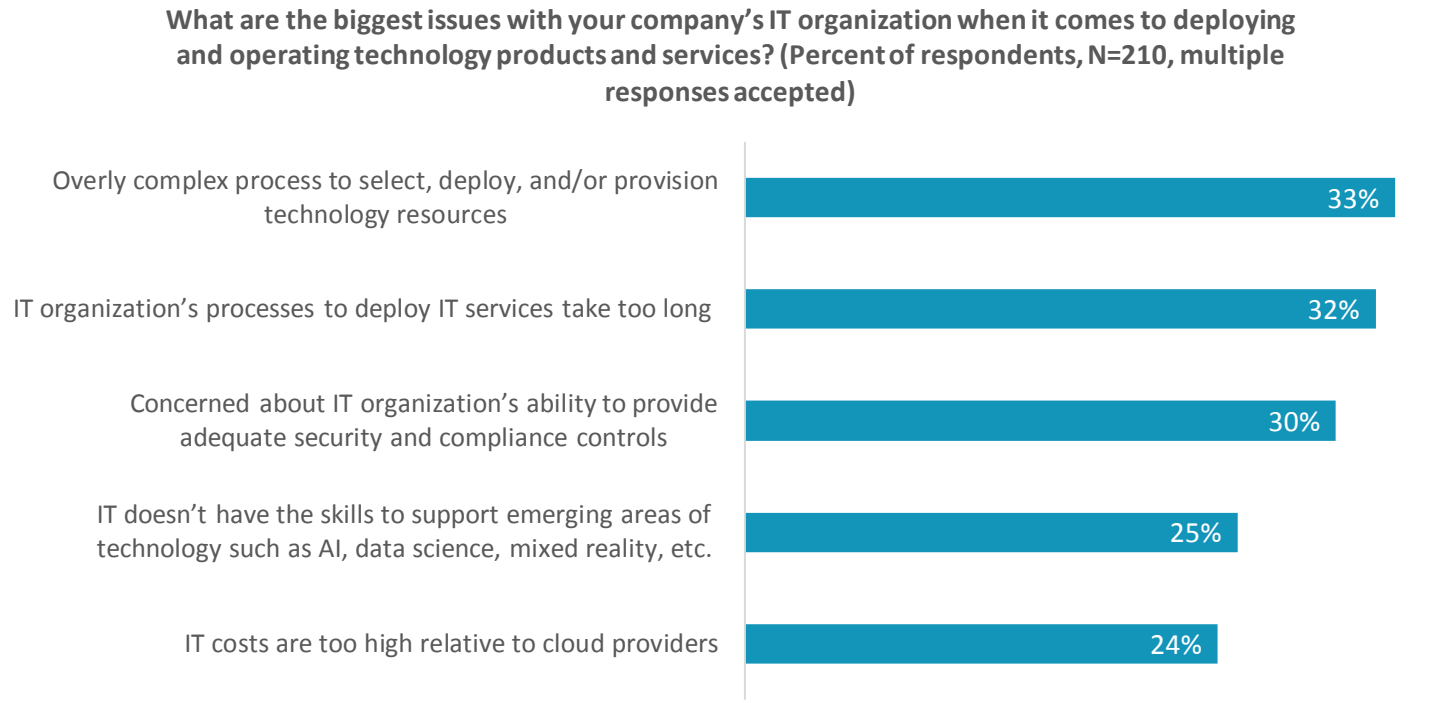
This ESG Technical Review documents hands-on validation of the Veritas Flex 5340 NetBackup Appliance with a focus on how Flex and microservice containers can be used to simplify infrastructure, reduce costs, and consolidate NetBackup resources into a single, scalable infrastructure for organizations and managed service providers.

The Challenges

Today, as applications become more intelligent and infrastructure transforms, the data center is going through widespread systems and resource consolidation initiatives. In today's agile business environment, time to market, efficiency, consolidation, and reducing complexity have all become core business and IT drivers. Data protection is one such area where organizations worldwide are looking for consolidation, a hybrid pathway to cloud resources, and the ability to address growing security, data separation, and privacy concerns all while still controlling costs and complexity.

In fact, ESG research indicates that organizations have growing concerns about the ability to deploy technology within the IT organization (see Figure 1). Thirty-three percent of business managers surveyed by ESG are concerned about the complex process to select, deploy, and provision technology resources. Additional cited concerns include time to deploy workloads and security.[1]

Figure 1. Top Five Issues with IT Organization Deploying and Operating Technology Products and Services



Source: Enterprise Strategy Group

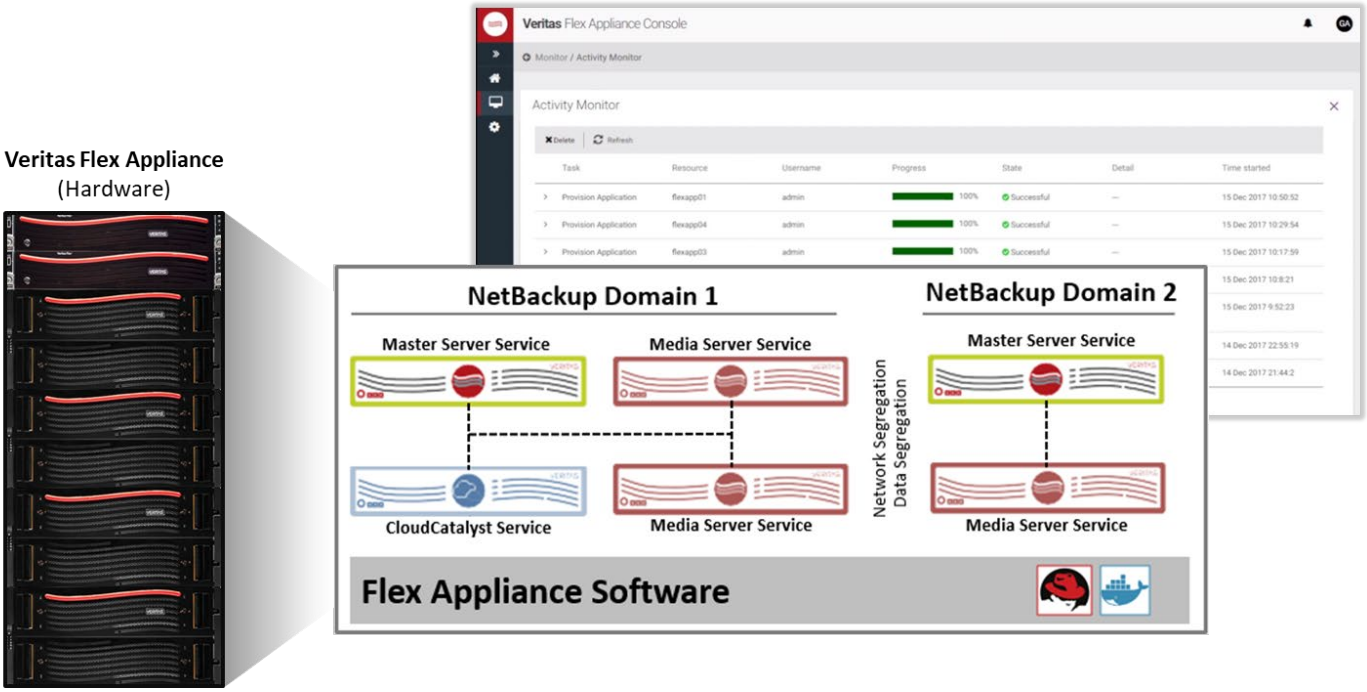
[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.

This ESG Technical Review was commissioned by Veritas and is distributed under license from ESG.
© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Solution: Veritas Flex 5340 NetBackup Appliance

To meet differing requirements from multiple business and functional units, IT organizations must often support multiple deployments of servers for backup, data reduction, and cloud tiering. As shown in Figure 2, the Veritas Flex 5340 appliance simplifies IT by consolidating multiple data protection application deployments into a single, integrated solution. The Flex Appliance utilizes microservice containers to create a menu of NetBackup services including master server services, media server services and NetBackup CloudCatalyst services. With this architecture, data protection deployments are created by simply choosing the appropriate containerized NetBackup services from the menu and configuring them to meet the needs of a data protection user. Data protection deployments can now be provided as an on-demand service with the Flex Appliance.

Figure 2. Solution Overview



Source: Enterprise Strategy Group

Key features include:

Docker containers: Containers allow a user to create isolated NetBackup data protection deployments as a service by configuring containerized Master Server services, Media Server services, and Cloud Catalyst services under one domain. Containers are also used to isolate the Red Hat operating system, which is used by all the NetBackup services, allowing for less disruptive OS-level updates.

Scalability: Flex 5340 is a modular architecture that scales from one to four shelves and from 120 TB to 1.92 PB with high availability replication to a second node with the same configuration.

Consolidation: Veritas customers now have a single platform to consolidate all their NetBackup and data protection resources into a single scalable, resilient system, while maintaining the ability to enforce data separation through isolated containers. Existing physical and virtual servers can be consolidated.

Multitenancy: The Flex 5340 is a multitenant design, allowing an organization or managed service provider to dedicated resources, application access, and management for departments, geographies, or customers.

A single user interface: Allocating resources is quick and easy through a single interface. Organizations can deploy NetBackup in any needed configuration in a matter of minutes.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

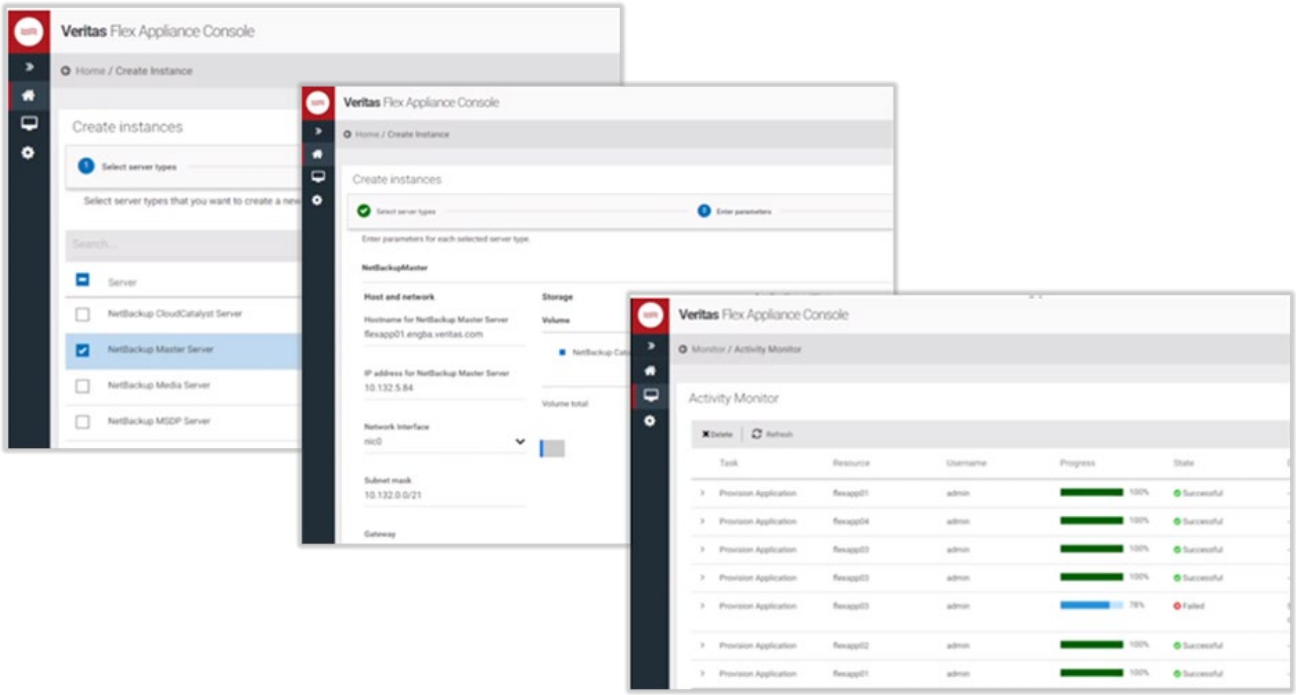
ESG Validated

The Flex 5340's ideal scenario is to consolidate multiple data protection deployments into a single, scalable environment to reduce the costs and the complexity of running and managing many siloed hardware deployments. To validate this, ESG conducted a review of the platform's architecture, performed a series of test deployments, and looked at some of the underlying software components such as the use of microservice containers. Testing was done on the Flex 5340 appliance from our corporate office in Milford, MA leveraging a remote Veritas demo environment.

Veritas Flex Ease of Use

ESG testing began with an exploration of how easy it is to deploy resources through the Flex 5340 user interface. Some of the test parameters included storage allocation, setting up domains, configuring containerized NetBackup services, and deploying a NetBackup Master Server service, then a NetBackup Media Server service and a Cloud Catalyst service. The testing started with a single deployment of each service in a domain and then expanded to multiple services in each domain. As shown in Figure 3, ESG ran a variety of deployment scenarios to validate the ease of use and simplicity of the user interface. From a single view, we were able to select the type of NetBackup service to deploy. The options included the Cloud Catalyst service, Master Server service, Media Server service, or MSDP server service. As shown in Figure 3, we chose to configure a Master Server service since in most cases this would be the first server a customer would deploy. Next, we were presented with the Master Server service configuration options. For networking, this included hostname, IP address, network interface, subnet mask, and gateway. We were able to allocate storage form a global pool in GB or TB increments. We finished the deployment by adding the NetBackup license keys.

Figure 3. Intuitive User Interface



Source: Enterprise Strategy Group

Once we applied our settings, the Master Server service was configured and displayed in the Activity Monitor. From the monitor page, an administrator can view the system topology, alert information, and CPU utilization for each server node. Each new NetBackup deployment we configured appeared in the Activity Monitor. The user interface doesn't show it, but each service is being deployed into a new container within the domain we selected. Multiple domains can be configured

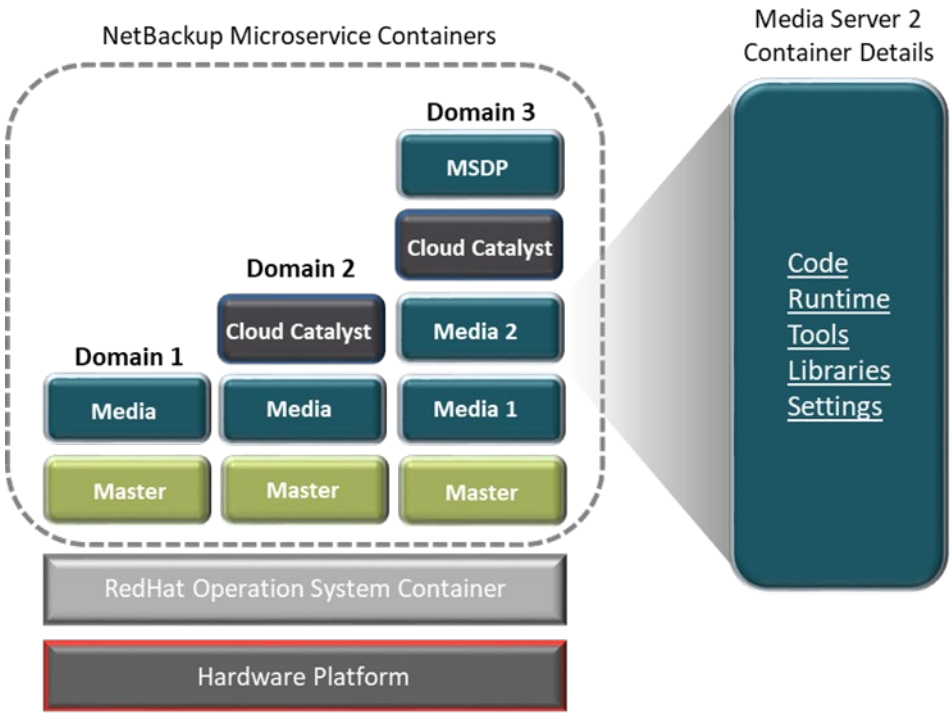
© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

and managed through the same user interface. We observed building a complex environment with multiple domains, with each running multiple NetBackup applications, all within separate containers with no conflicts.

Containers

The Flex 5340 uses containers to separate NetBackup applications running on the same operating system and physical hardware. In our testing, we configured containers within domains to run the NetBackup applications. The right side of Figure 4 shows that each container hosts a set of processes that include the application code base, runtime, tools, libraries, and settings for the application. This creates a standalone software runtime environment and dependencies combined into a single package. For example, when deploying a NetBackup Media Server service, the code base is deployed along with all its dependencies into a single, isolated container.

Figure 4. Microservice Container Design



Source: Enterprise Strategy Group

The left side of Figure 4 shows an expanded view of the container design. As shown, the hardware, software, and application layers are separate and distinct from one another. This design allows an IT administrator to isolate functions for code upgrades, security patches, and the movement of containers when required. The software layer, which is running Linux Red Hat, is in its own container and provides the OS for all the running containers, regardless of the domain. By isolating the operating system, IT administrators can deal with operating system-level upgrades without affecting applications. This dramatically reduces downtime on the system compared with a typical upgrade.

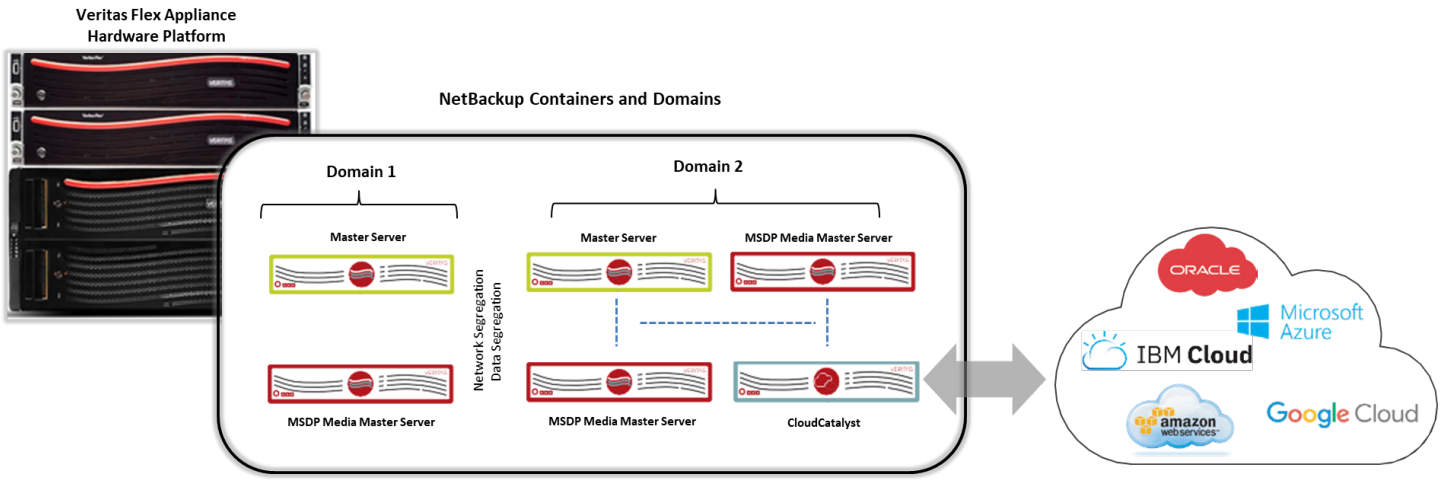
The application layer is where an IT administrator can dynamically configure containers for each NetBackup deployment. As shown in Figure 4, there is flexibility in the configuration for each domain. Domains may be created for departments, geographical regions, or customers, in the case of a service provider. Within the domain, the administrator adds each of the needed Veritas NetBackup applications. For example, the organization may want to start backing up to the cloud, which is done by adding a Cloud Catalyst service to the configuration and pointing it to the public or private cloud destination. This modular design increases operational reliability, including the ability to move a container from one location/environment to another.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Scalability

ESG began its review of the Flex Appliance for scalability by understanding the attributes of its architecture and design. The Flex Appliance architecture is designed for scale in capacity and on-demand applications service delivery. Data protection services built from the containerized NetBackup services are completely isolated from one another—eliminating inter-services interference. Data and network connectivity are segregated to each deployed containerized service. With a single Flex Appliance, deployments can scale in capacity and multiple data protection services can be deployed. The capability to add workloads on a single appliance adds a new dimension to scalability. In the Flex system, you can add domains and, within each domain, add multiple NetBackup server services. The base system has a minimum configuration of 120 TB, which can then scale to a maximum of 1.92 PB in a single rack design. Organizations can configure a maximum of four storage shelfs with two size options: 264 TB or 528 TB. There are also ten 10GB ethernet ports and an additional four 1GB ethernet ports reserved for system management. For high availability (HA), the primary node can be replicated to a second node.

Figure 5. Scalability Overview



Source: Enterprise Strategy Group

Why This Matters

The Flex Appliance offers the ability to consolidate and scale in a compact data center footprint. All NetBackup and data protection resources can be delivered on the Flex Appliance, with each running separately in containers while sharing a common management interface and storage resources. This eliminates separate data protection servers, applications, and storage and brings them into a simple, easy to manage system that can scale.

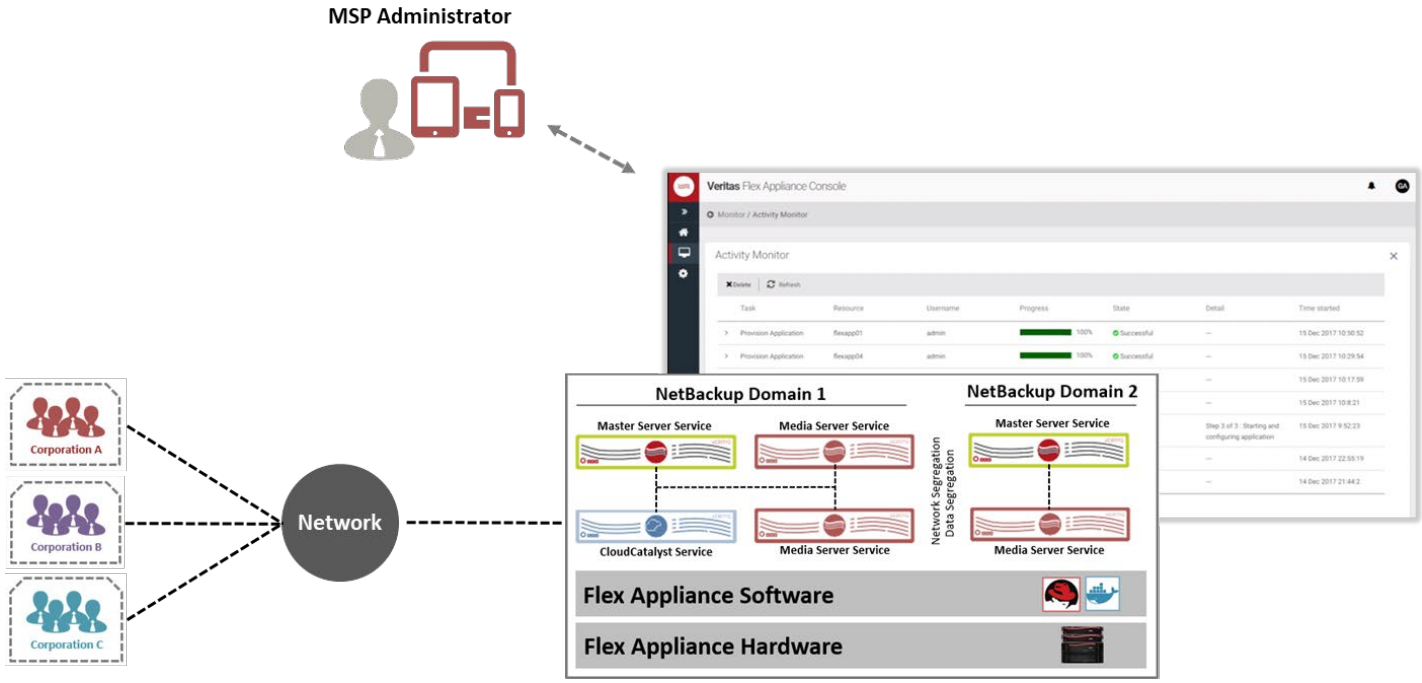
Multitenancy

The Flex is designed as a multitenant solution, allowing the delivery of NetBackup as a service. Each tenant is set up under a separate domain with dedicated, tenant-specific NetBackup services deployed. Multitenancy allows for the isolation and

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

protection of customer dedicated resources. ESG evaluated the Veritas Flex 5340 from the view of a service provider to determine if it is a viable solution for offering managed data protection services. Each entity is treated as a customer with data separation and designated access controls.

Figure 6. Multitenancy Overview



Source: Enterprise Strategy Group

The following key attributes make the Flex a solid solution for service delivery:

- **Scalability** – Storage is scalable to almost 2 PB, providing the ability to grow and scale up as needed. At the application layer, containers allow for the fast deployment of applications on demand.
- **Upgradeability** – Non-disruptive upgrades are critical for service delivery. Each container is upgraded separately with no disruption to other customers. OS patches are made with a separate, isolated OS container.
- **Data separation** – Containers create separation of workloads, applications, and storage between each customer, providing security and data separation.
- **Monitoring** – A single application monitoring screen allows a service provider to monitor all of the customers on Flex from one screen.

Why This Matters

The delivery of applications as a service on a single, multitenant system is becoming a core requirement for both IT organizations and managed service providers. With the Flex Appliance and its multitenant features, IT can simplify the separation of backup data by business units, subsidiaries, or geographies in compliance with corporate governance and data privacy laws. IT and DevOps are evolving into the service provider model for more organization and the Flex is designed to meet these requirements head on.

© 2019 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

IT budgets and staffing levels aren't increasing, but the workloads are. Having the right amount of scalability and flexibility to ensure your organization's IT system can meet changing business requirements is a constant balancing act. Protection of the organization's information is a critical part of IT systems, and over time, technology and methodology sprawl as organizations grow. This creates a challenge for IT administrators to deliver the SLA for data protection that is demanded by the organization. Cybersecurity concerns and data privacy issues both put more pressure on IT to be sure that data protection is at the highest levels of efficiency.

Veritas is not new to the data protection world and has long been a pioneer in the market. The Flex is a new step in its journey to merge the network to the cloud and offer a higher level of simplicity and control to data protection with a hyperconverged solution. The Flex combines storage hardware, the operating system, and containers to deliver a powerful, scalable solution to consolidate all data protection into one easily managed system while still allowing for the separation of workloads by domains. Veritas saw some challenges in the data center with disparate data protection systems acting as silos and created a solution that brings them all into a single system. Some of the key features we found include:

- Containers
    - Containers for each deployment of a NetBackup application.
    - An OS container to deliver a single OS to all of the NetBackup containerized server services and manage the OS layer separately from the hardware and software layers.
- Management
    - Intuitive central management user interface with on-demand deployments and active monitoring capabilities.
- Scalability
    - Scalable storage infrastructure up to 1.92 PB with four storage shelves and a small data center footprint of a single rack design.
    - Application-level scalability with the ability to add domains and data protection services as needed in minutes.
    - True High Availability design that replicates from one node to two nodes and all of the applications.

Enterprise professionals have depended on NetBackup for many years to manage their global deployments with unified data protection. With the addition of the Flex Appliance, consolidating all data protection resources into an easily managed system just got easier than ever before.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.