Data Center Consolidation for Modern Mission-Critical Applications

Allow no Sacrifices in Performance, Reliability, or Security

By: Stephen Guarrieri

White Paper

Executive Summary

Organizations consolidate data centers for many reasons including cutting costs by increasing server density, simplifying infrastructure, increasing network performance, and leveraging the increased power of commodity-priced hardware and software.

Today, most data center consolidation solutions include off-the-shelf virtualization from a number of vendors, which, according to industry research, can cut costs between 20 and 50%[i]. However, similar research shows that most organizations have only virtualized 65%[ii] of their data center applications. Why? Primarily, they lack the confidence in the security, performance, and reliability of commodity virtualization. This lack of confidence is forcing organizations to choose between competing IT pressures such as security, performance, scalability, and cost – but the truth is – enterprises should not have to choose. Today, organizations looking to move modern mission-critical systems to consolidated data centers or secure cloud environments now have another option - *Forward!* by Unisys™.

With *Forward!* organizations no longer have to choose between sacrificing modern mission-critical reliability and performance with cost-containment. *Forward!* meets the predictable performance and security of a purely physical server environment yet allows customers to provision and maintain modern mission-critical applications with confidence.

The Evolution of Modern Mission-Critical Data

Today's modern mission-critical IT application systems are accessed by a wide variety of devices including PCs, laptops, smart phones, tablets, embedded systems, and more. Users demand 24/7 availability of modern mission-critical applications with a high level of stability. Applications must provide consistent performance, yet retain the mainframe-class capability of protecting valuable data in the face of increasingly sophisticated cyber-attacks or potential system failures.

In addition, companies are facing increasing IT budgetary pressures to drive down costs and increase agility within the data center. CIOs and senior management continue to seek not only an effective and cost-efficient way to reduce the number of physical servers in the data center, but also maximize all the resources they already have in place. But they must maintain the integrity, performance, and security of its most critical applications by allocating them the dedicated resources they need to retain operational efficiency.

While many of today's technologies, such as virtualization, are helping organizations reduce server sprawl by increasing server density and deploying virtualized storage, these technologies have not been able to deliver satisfactory isolation of critical applications without removing critical functionality like virtual machine mobility and high availability. These commodity technologies, due to their tiered architectures and reliance on generic hypervisors, cannot deliver the predictable performance required by modern mission-critical applications.

General Consolidation Challenges: From the Data Center to Applications

One of the many challenges facing organizations today in the data center consolidation is finding a cost-effective way to move Physical Environments and migrate their modern mission-critical workloads without the risks typically involved in common virtualized infrastructures. With data center consolidation, IT organizations face two challenges: the architectural complexities of migration from a data center point of view; and safely and securely migrate applications to Linux/Windows to more cost-effective x86-based systems. These challenges include the following:

- Effectively and efficiently deliver the same level of performance and enhanced security of existing Physical configurations on an Intel platform with dedicated resources
- Create cost savings by reducing the data center footprint
- Redeploy major applications, such as SAP, yet maintain the performance and reliability of these applications they enjoyed in on physical Linux and Windows
- Maintain 24/7 availability
- Avoid unplanned downtime with a robust and reliable x86 solution
- Make certain that systems can be easily upgraded with little or no requirements for planned downtime
- Provide increased capacity on short notice, without disruption to existing operations
- Ensure systems are capable of supporting different environments and database models in a secure environment

[i] Gartner. "Data Center Conference." 2012

[ii] Aberdeen Group. "Analyst Insight" 2013
http://www.stratus.com/~/media/Stratus/Files/Library/AnalystReports/Role-of-Fault-Tolerant-Servers-in-Protecting-Virtualized-Applications.pdf

Primary Obstacles to Using Common x86 Virtualization for Critical Applications

A number of technological and business continuity and performance issues make migration to x86 and virtualization of modern mission-critical data centers an unattractive option for many top-tier enterprises. When enterprises rely on processing trillions of dollars of data on its reliable yet expensive physical or legacy environments and RISC-based systems, it is no wonder that data center consolidation stalls at just over 50% adoption rates in most cases[iii]. Fears of the potential unreliability and security vulnerabilities of x86 virtualization are not unfounded. The difference between 99.5% and 99.99% uptime can translate into an exponential loss of 4.5 times in lost productivity and operations, which translates into millions of dollars for many enterprise. For example, nearly 70%[iv] percent of all SAP production systems still run on dedicated, physical servers for many of the following reasons.

Disadvantages of Multi-Instance Virtualization Resource Sharing

In common x86 virtualization implementations, a single physical server emulates multiple, virtual instances of servers and virtualized storage allocations for each server. While this certainly increases efficiency and more fully utilizes all the resources of a given x86 server, there are a number of performance disadvantages to this implementation. The underlying hypervisor allocates resources across all instances dynamically, and as a result, may not fully prioritize any given instance over another—the process is purely resource-demand driven. As a result, a modern mission-critical application—or multiple critical applications under one hypervisor—many cause under or over provisioning of instances strictly on load balancing or other resource demands. That does not bode well for performance-dependent applications, which may need real-time, dedicated resources 24/7 to accommodate fluctuating peaks in computing, storage access, or even network bandwidth. The result is a decrease in critical application performance— which is not acceptable to modern mission-critical operations and may put corporate SLAs at risk.

The Vulnerability of a Common Hypervisor Layer

Because all VM instances are controlled and monitored by one underlying hypervisor layer, any disruption of the hypervisor affects the performance, or even the operation, of all the VM instances under its control. As a result, any critical applications running on a VM under the common hypervisor layer are at risk. If the hypervisor goes down, all instances go with it.

Insecure Partitioning

Shared I/O, memory and execution space can introduce vulnerabilities into a common virtualization environment. Documented evidence of virus and worm propagation in common virtual machine environments show that only hardened and complete isolation of VM instances can keep critical applications safe from either intentional or unintentional system disruptions[v].

Reduced performance and Increased Complexity in Multi-Tiered Operations

Because I/O within and across most common vitalization solutions require a multi-tiered architecture, performance within and between VM instances is adversely affected in many cases, particularly during burst modes of disk access or data transfers. Therefore, many common virtualization implementations must introduce load balancing hardware and/or software to maintain peak performance. This also necessitates an increase in management, maintenance, and vigilant configuration. Even with load balancing in place, performance is not guaranteed. As a result, corporate SLAs are in jeopardy. For example, if an automated SAN replication operation is performed, it will consume a burst of bandwidth and storage I/O; meanwhile, payroll may find its operational performance severely degraded, missing deadlines and compromising its network SLA guarantees.

Enterprises require the following if they are to move critical applications off silo-based, individual servers, mainframes, and RISC-based systems to a reliable x86-based VM:

- Isolate critical applications in hardened partitions
- Provision dedicated (not shared) resources for guaranteed application performance
- Deliver high-speed connectivity without the overhead of multi-tiered architectures and/or load balancing
- Provide high reliability and flexibility

The *Forward!* by Unisys Data Center Solution Overview

With *Forward!* all of the above, and more, is possible as this unique computing platform was specifically designed for today's demanding environments. *Forward!* is a revolutionary, high-speed fabric computing platform designed to support an organization's critical applications along with the capability of consolidating Windows® and Linux® environments on the

[iii] Gartner. "Data Center Conference." 2012.

[iv] Abeerdeen Group Study. "The case for virtualizing SAP."

[v] SYSRET 64-bit operating system privilege escalation vulnerability on Intel CPU hardware. CERT Vulnerabilities database, Department of Homeland Security.

same platform. *Forward!* also leverages Unisys-developed hard partitions using Intel Xeon® Technology to deploy highly secure Windows and Linux workloads. Unisys created *Forward!* to provide organizations the same virtualization for dedicated resources (CPU, memory, I/O) on an Intel platform for applications that companies typically reserve for its mainframes In other words, the *Forward!* by Unisys architecture is the next-generation of the renowned Unisys modern mission-critical mainframe computing platform, which provides predictable performance and unmatched security, but using an affordable and flexible x86 platform. The *Forward!* fabric-based architecture also adds high bandwidth and low latency to x86 systems.

Forward! Modern Mission-Critical x86 Solutions

Forward! allows enterprises to break modern mission-critical applications out of their costly, silo-based environments without sacrificing the security, reliability, or performance they demand from the applications that are the backbone and lifeblood of their enterprises. With *Forward!* by Unisys enterprises can finally realize the following:

- Migrate modern mission-critical applications to virtualized environments with predictable performance
- Eliminate silos and their proprietary hardware and management systems
- Actually increase the speed and performance of modern mission-critical applications
- Leverage existing in-house x86 and virtualization expertise
- Add a more flexible and agile environment for critical applications to meet future business needs

Forward! Hardened Partitions

Forward! Secure Partitioning (s-Par®) firmware, allows a system to be divided into a number of partitions, each of which is securely separated from the others, and each with its own dedicated resources. For example, a critical application might be stabilized on a number of dedicated servers, but consolidating that application into a typical commodity virtualized environment could lead to unpredictable performance due to resource sharing. This could lead to the application becoming unstable after the consolidation process. However, with *Forward!* because the resources are not shared, predictable performance is the result. The same benefit also applies to deploying new applications; as both the predictable performance provided by *Forward!* secure partitions, as well as the stability and security provided by the way that *Forward!* systems are delivered, also reduces risk.

On installation, *Forward!* loads the s-Par firmware using files pre-loaded at Unisys's secured manufacturing facility on local disk LUNs. The management software allows customers to create dedicated resource containers and load Unisys-certified gold operating system templates. Customers are assured that the OS template is hardened, secure, and ready for deployment into the partition. Customers can choose from Windows, Red Hat, or customer-provided operating systems to load into the hardened partition. *Forward!* currently supports 192 simultaneous high-performance, hardened partitions per fabric.

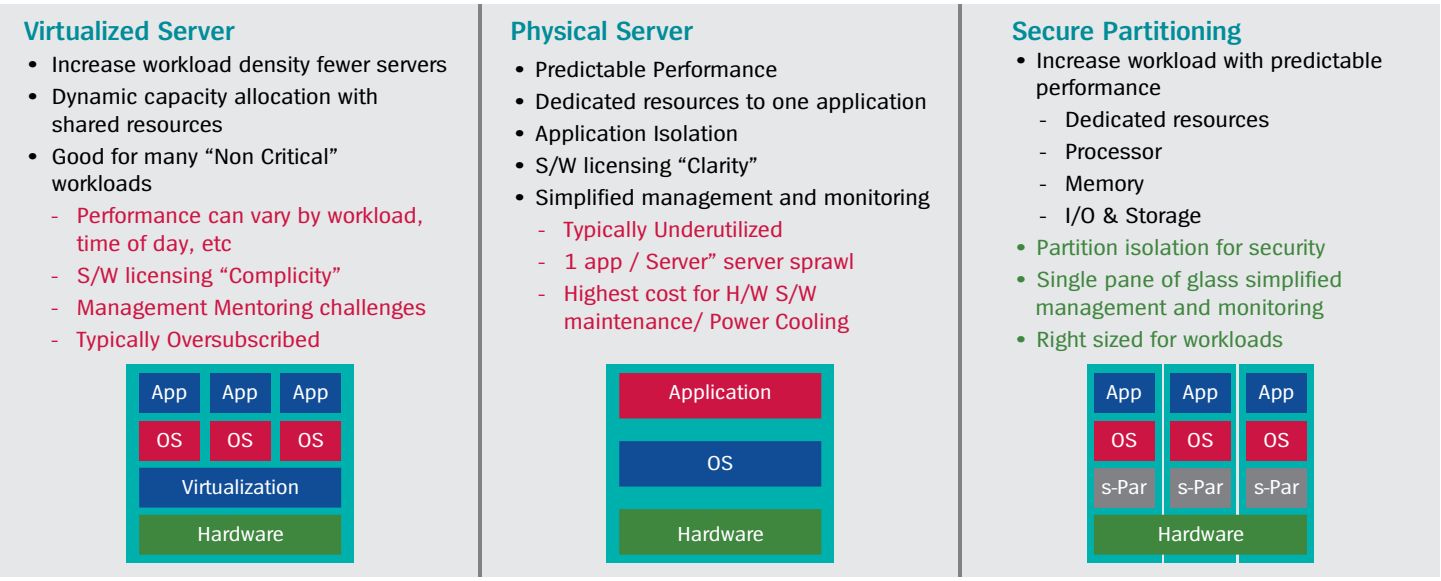

Figure 1. Benefits of s-Par over common virtualized or physical servers.

Forward!-based rack servers can be configured with the following number of internal drives; each of these drives may be configured at a customer selectable RAID level including 0, 1, 5, 6, 10, 50, 60:

- Single socket, 8 drives
- Two socket, 16 drives
- Four socket 24 drives

In its latest release, *Forward!* also integrates with leading third-party storage systems from NetApp® and EMC®, will offer Solid State Disks, and FIPS compliant self-encrypting disks in addition to a number of hard disk drives. More vendor drives and storage devices are continually being certified.

Besides security, s-Par with its dedicated allocation of CPU, memory, and storage delivers the following benefits for modern mission-critical applications:

- Predictable performance
- Higher workload density
- Maximized performance
- Maximized flexibility
- Reduce cost overhead compared to standard virtualization

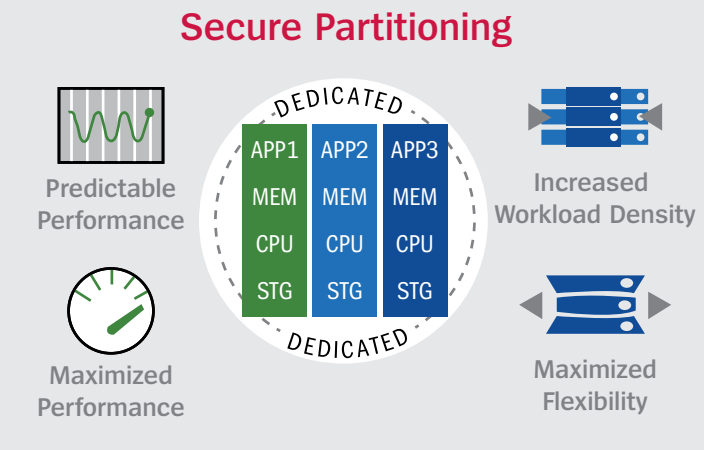

Figure 2. IT benefits of secure partitioning.

Fabric-Based Performance and Reliability

Forward! uses a fabric-based rather than tiered architecture for greater performance within and between *Forward!* partitions by using a high-speed network backplane that supports InfiniBand and Gigabit Ethernet. The Interconnect between *Forward!* partitions is a combination of hardware, software, and firmware, which interlinks the platforms and partitions within it and hides the underlying connection technology from the applications and operating systems. This not only boosts performance but also creates a more secure environment. The *Forward!* fabric also offers full redundancy—if one I/O channel goes down, a configured failover channel immediately picks up traffic with no disruption to applications.

The *Forward!* fabric natively supports 56GB FDR, as well as a broad selection of commodity, industry-leading NICs and HBAs in dual/quad configurations from quad 1GB to dual 100GB capacities. This high-speed backplane fabric eliminates the need for multiple network switches while also providing higher performance, particularly for applications that require dedicated I/O.

Interconnection and integration with common VMs and network servers outside the *Forward!* fabric are also supported, giving enterprises the ability to finally integrate its entire enterprise securely.

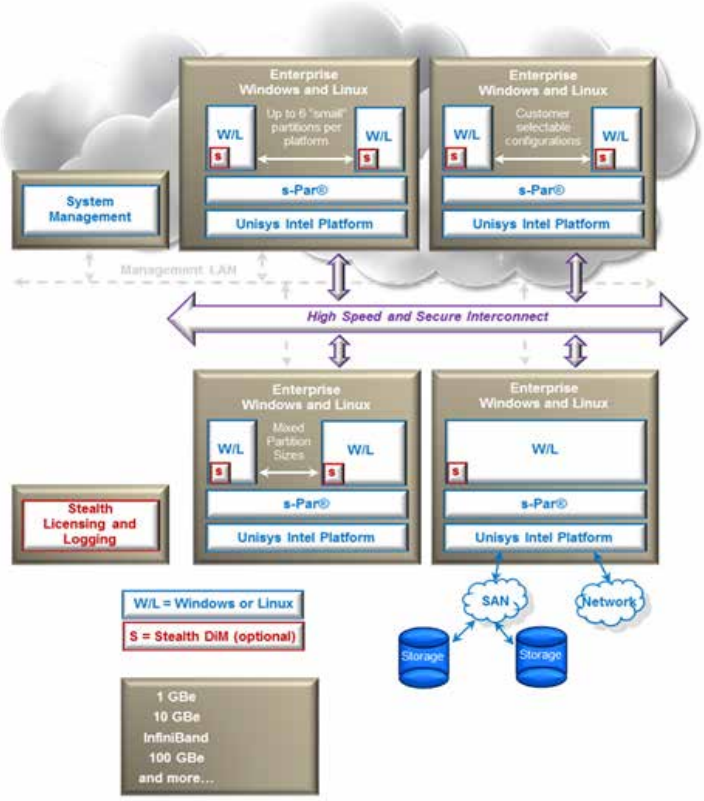

Figure 3. The *Forward!* Architecture.

(Click Image to Enlarge)

Easier Management

Forward! delivers flexible partitioning, provisioning, automation and resource management through its Integrated *Forward!* Fabric Manager (FFM) and optional Choreographer™ and software. In addition, *Forward!* by Unisys provides easy integration with existing enterprise system management systems such as Tivoli®, HP OpenView®, and many others. *Forward!* Fabric Manager allows administrators to monitor and configure Ethernet and InfiniBand I/O interfaces, while Choreographer automates disaster recovery, business continuity, and cloud-based operations in one application.

Figure 4. *Forward!* Fabric Manager features.

Added Security with Unisys Stealth

Forward! also can incorporate optional Unisys Stealth™ technology. Stealth groups partitions and platforms together with user endpoints into secure groups called Communities of Interest (COIs); groups of people who share information only with each other while denying access to users outside their COI. This feature makes data communication endpoints undetectable on a network, which makes them less vulnerable to attack Because organizations need to access many physically separated networks for security, regulatory, or compliance requirements, Stealth was designed to eliminate the need for rigid, physical networks by offering flexible software-defined networks and virtualized COIs. Stealth deploys a three-layered approach to security: cloaking, encryption, and isolation.

Cloaking

IP addresses of any endpoint are cloaked from outside the COI, which makes them less vulnerable to attacks.

Encryption

Stealth applies AES 256-bit encryption to all data in motion, both within the *Forward!* fabric interconnect, and out into the entire network. This highest form of encryption available delivers the most secure transfer of data within and beyond the corporate environment.

Isolation

With data center consolidation, especially for modern mission-critical applications, the predictability and security characteristics of *Forward!* allows applications, which may have been running on dedicated hardware, to be safely moved into the *Forward!* fabric without any effects on their behavior, even if the applications are deployed on a number of separate servers. And combined with Stealth, data centers can securely segment data centers and protect data and systems by cloaking strategic assets.

Non-Disruptive Migration

With *Forward!* enterprises can migrate applications with confidence. Secure replication and configuration of existing applications and data is performed non-disruptively. Administrators can then thoroughly test the replicated application within each partition to make certain it is performing as expected, in real time. Once the migration and testing is complete, the optimized and *Forward!* migrated partition and its application(s) can easily be brought online.

Proven, Predictable Performance

Applications that rely on low-latency, high bandwidth infrastructures will find *Forward!* surpasses the performance of common virtual environments. In a recent independent test conducted by ESG, test analysts found the following:

- The *Forward!* by Unisys s-Par was 21% to 38% faster than the industry-standard hypervisor (faster response times)
- *Forward!* delivered up to 62% more overall performance than an industry standard hypervisor (more IOPS)
- S-Par performance scaled in a near-linear fashion compared to the industry-standard hypervisor, especially at high levels of concurrent activity[vii]

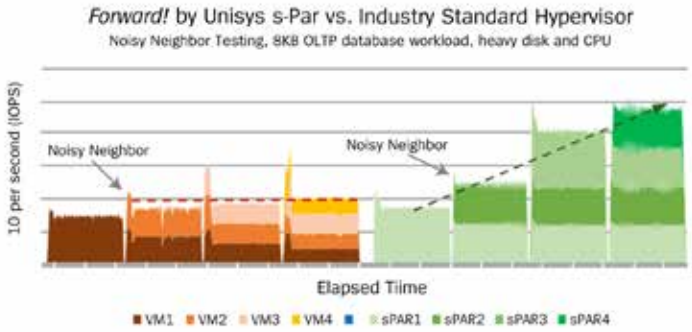

Figure 5. Affect of "noisy neighbor" partition on system performance

(Click Image to Enlarge)

Read the entire report:
http://outreach.unisys.com/Forward_ESGStudy

According to the report, "*Forward!* by Unisys with NetApp Storage performed up to 38 % faster, and up to 62% more scale, minimizing the impact of [high-resource neighbor partitions] (43% more IOPS), and transparently created a high-speed internal InfiniBand network with extremely low latency and high bandwidth (as low as 32 microseconds; up to 4.8 GB/sec)."[viii]

Forward Facing, Fully Certified

Unisys is committed to providing the very best in performance, security, and reliability to modern mission-critical enterprise computing. From its s-Par hardened partitions to certified storage and operating systems, Unisys rigorously tests every component before certifying it for use on the *Forward!* platform.

As a company, Unisys is committed to a heterogeneous, open network framework to allow the secure integration of the widest possible applications, devices, and network technologies—without sacrificing performance, reliability or security. Enterprise customers can deploy *Forward!* confidently, knowing that Unisys third-party partners deliver products and services that meet or exceed the customers' own rigorous standards.

Conclusion

With *Forward!* enterprises now have the modern mission critical data center consolidation solution. *Forward!* drives down costs, increases agility in their data centers, and reduces the number of physical servers. In addition, IT organizations can maximize the efficiency of remaining resources, and ensure that all of the applications being used have dedicated resources.

With *Forward!* organizations no longer have to choose between modern mission-critical security, performance, scalability, and cost. *Forward!* can match or surpass the predictable performance and security of a physical environment yet confidently deliver modern mission-critical applications in a high-performance, consolidated data center.

About Unisys

Unisys is a global leader in designing, delivering and managing modern mission critical IT hardware, software and services. Market-leading organizations choose Unisys to solve their critical IT challenges and transform their businesses.

Clients rely on Unisys to provide high-end servers with unmatched security and reliability, increase efficiency and utilization of their datacenters, modernize their applications, protect their assets and information and achieve effective IT globalization. We have domain expertise in and proven solutions for the financial services, public sector, transportation, communications, life sciences and retail.

For More Information

More information on *Forward!* by Unisys is available at:
www.unisys.com/forward

vii. ESG Lab Preview. "Unisys *Forward!* with NetApp Storage." 2014.
viii. ESG Lab Preview. "Unisys *Forward!* with NetApp Storage." 2014. Page 4.

For more information visit www.unisys.com

© 2014 Unisys Corporation. All rights reserved.

Unisys, the Unisys logo, s-Par, Choreographer, and *Forward!* by Unisys and the *Forward!* by Unisys logo are registered trademarks or trademarks of Unisys Corporation. All other brands and products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders

Printed in the United States of America 06/14 14-0294