WHITE PAPER

Mission-Critical Virtualization Security for Today's Workloads

Sponsored by: IBM

Gary Chen
September 2013

IDC OPINION

Today's modern datacenter is a virtualized world, with the majority of workloads virtualized and evolving to a cloud architecture. The benefits of virtualization and cloud are numerous:

- Consolidation that provides hardware, power, cooling, and real estate savings
- Wide availability of virtualization-based infrastructure services such as high availability and disaster recovery to virtual machines (VMs)
- Flexibility for hardware upgrades and planned/unplanned maintenance
- Fast provisioning and self-service
- Accelerated time to market and development of new applications and services

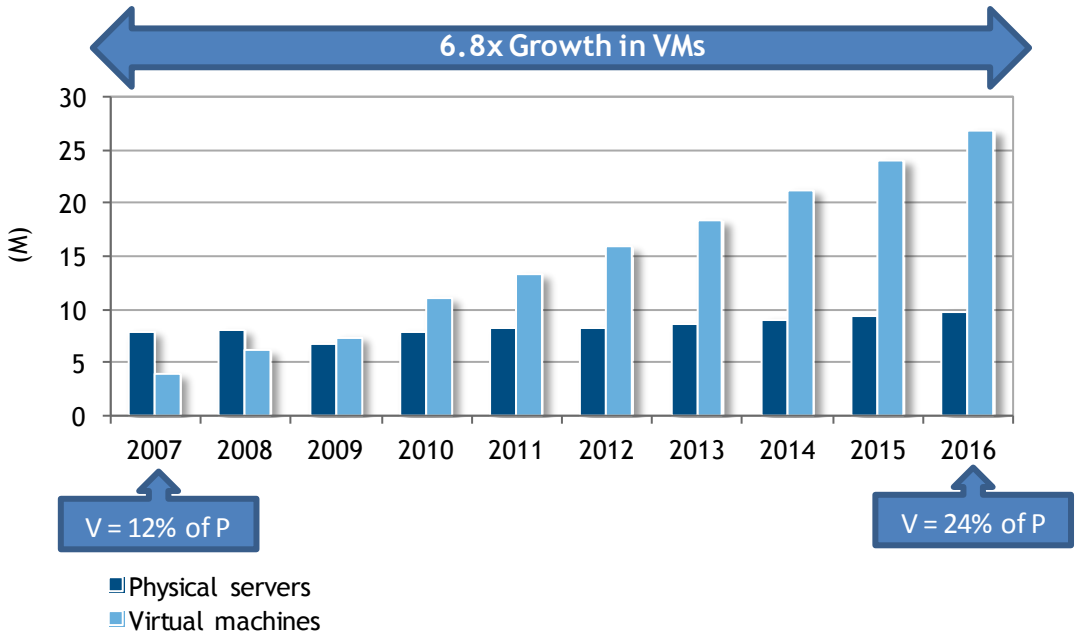
As virtualization has already become mainstream and the standard for new servers, much of the focus today is on the "last mile," the push to virtualize the remaining workloads, which tend to be the mission-critical, tier 1 applications. Many of these workloads run on non-x86 server architectures, requiring the virtualization discussion to extend beyond x86 when addressing these applications. Non-x86 systems also have mature virtualization solutions, with different architectures and capabilities often targeted to the workload profiles they tend to host. The Power architecture profile is interesting in that it is highly virtualized (80–90% by IBM estimates), and a large majority of those applications are tier 1 applications. Integrating these systems into the larger datacenter virtualization strategy brings these systems into the fold of the modern datacenter to be able to leverage private, public, or hybrid clouds. Yet many are concerned with the security risks of virtualization and consolidating these different and sometimes disparate workloads onto the same physical host. Security continues to be a major inhibitor to virtualization of tier 1 applications. However, if customers can successfully manage the security risks, the modernization and virtualization of these systems can bring tremendous benefits.

SITUATION OVERVIEW

Server virtualization has had an incredible trajectory over the past decade, offering dramatic cost savings initially through consolidation and then progressing into agility benefits. Today, virtual servers are deployed 2:1 compared with physical servers. As Figure 1 demonstrates, virtualization is the new default in today's datacenter, and the number of VMs is predicted to rise dramatically over the next few years.

FIGURE 1

Worldwide Virtualization Shipment Forecast



Source: IDC's Server Virtualization Multiclient Study, 2012

While various forms of server virtualization have existed for many decades, it was the rise of x86-based hypervisors emulating an isolated, full x86 hardware server that really caught on in the mainstream. Critical features such as being able to live migrate a running VM cemented the technology as a mainstay of datacenters. The cost savings from consolidation were obvious and easily proven, and new management features brought unprecedented agility to datacenters. Virtualization of workloads started with less critical test/dev and progressed to production as customers gained confidence in the technology. The challenge today is to virtualize mission-critical applications.

Many mission-critical applications run on non-x86 architectures such as Power. x86 is a general-purpose architecture that serves a wide range of computing use cases, whereas Power tends to focus on mission-critical enterprise workloads. Power is prevalent in tier 1 applications, regulated industries, and environments that have strict security and compliance requirements.

While the consolidation and agility benefits of server virtualization are undeniable, virtualizing mission-critical environments, which Power Systems typically do, increases the focus on several security considerations. Consolidating forces multiple logical servers to coexist on the same physical server. These could be from different business units or multiple tenants in a more shared infrastructure. Any breakdown in isolation would be disastrous. Customers need to protect themselves from several threat scenarios:

- Customers need to ensure that if one VM becomes compromised, it can't compromise or affect another VM in any way. The virtualization layer must enforce the separation and isolation of VMs to prevent data theft or a malware infection spreading from one VM to another VM or in any manner influencing the execution of another VM.
- The hypervisor itself must be protected, preventing any compromise of the code or the hijacking of its execution. The hypervisor essentially sees and controls everything, so losing control of the hypervisor would be to lose the keys to the kingdom. An attacker with control of the hypervisor would have full access to all the data and code execution of all the VMs on the server.
- Beyond the hypervisor and VMs, the management console and framework must also be protected as an attack vector. Flaws or unauthorized access to these control paths may also place data and applications at risk.
- All hypervisors that provide live VM migration move the memory content of a running VM across the network in order to relocate the VM on a different physical host. Live VM migration has become an expected and essential feature of virtualization. However, the VM memory contents traversing the network may contain sensitive information such as passwords, customer data, and financial information.
- Ultimately, what customers want in these mission-critical Power environments is to reap the benefits of virtualization but have the security and isolation level over and above that of a physical server.

IBM PowerVM Virtualization

IBM has had virtualization capabilities in various forms since the 1960s and on Power since 2001 with the POWER4 processor. Taking into account Power's customers and use cases, IBM focused much of PowerVM's development on security for mission-critical environments. Several PowerVM security features are important to understand when considering the security level of a virtualized Power environment:

- The hypervisor virtualizes and manages server resources and thus has the most critical role in enforcing separation and isolation. The PowerVM hypervisor is firmware based and runs in a privileged CPU state. This privileged level cannot be accessed or attained by the guest VMs. The PowerVM hypervisor is also cryptographically hashed and signed by IBM. The Power hardware enforces that only IBM's hypervisor firmware can be installed and loaded and that this code is not altered in any way – for example, by malicious code or a third party.
- Power also virtualizes the Trusted Platform Module (TPM). Guest operating systems (OSs) such as AIX can utilize the vTPM to verify the integrity of the operating system, ensuring that only trusted OS code is booted and that only known trusted operating system code is executed after the boot process is completed.
- Power's management framework extends the concept of trusted code to applications as well, allowing only signed and uncompromised application code to run.

- Power can protect all VM live migration data with strong encryption as the VM's memory is moved over the network. When a PowerSC security profile is applied to the Power Virtual I/O Server, the system realizes the customer is operating in a secure environment and automatically encrypts all VM migration data.

The PowerVM hypervisor has established a track record of secure code with no reported vulnerabilities, according to the public Common Vulnerabilities and Exposures (CVE) database. In addition, PowerVM has attained an EAL4+ security assurance certification.

PowerVM uses several techniques within the hypervisor to implement secure isolation:

- Processor isolation
  - PowerVM Micro-Partition isolation is provided by the hypervisor via the privilege state of hardware registers.
  - The PowerVM hypervisor operates at the highest privilege level, which cannot be attained or accessed by guest VMs.
  - The context switch between running VMs is completely controlled by the PowerVM hypervisor. It ensures that no residual data of the vacating VM is left behind. All cache lines from other VMs are inaccessible, and registers are cleared before dispatching a different VM.
- Memory isolation
  - The hypervisor controls access to real memory. The guest OS accesses what appears to be real memory but is actually real-virtual memory. The guest OS is assigned a memory range that is set by the administrator and enforced by the hypervisor. If a guest OS attempts to access memory beyond its size range, it will receive an exception error from the hypervisor I/O isolation.
- I/O isolation
  - Power Systems allow for devices to be directly attached to a guest OS or virtualized. If the virtual administrator assigns a device directly to a VM, the hypervisor ensures that only that VM can issue requests to the device.
  - PowerVM virtualizes devices through the Virtual I/O Server (VIOS). The virtual administrator defines which devices can be shared in the virtual environment, and the VIOS and hypervisor enforce strict separation of all I/O paths.
  - Network traffic is segregated by VLAN tags and MAC addresses. The VLAN tags are assigned by the virtual administrator and enforced by the hypervisor. The guest OS cannot send network packets with an arbitrary VLAN ID; the hypervisor will always enforce the configured VLAN ID. The MAC address is uniquely assigned and enforced by the hypervisor as well.
  - Since the hypervisor controls memory, I/O control falls within the same safeguards as other controlled resources.
- Trusted execution
  - Provides cryptographic signature-based system verification of the operating system and applications using a "known good" model of distribution and validation

- Two modes of integrity checking
  - System: Comparison of current system with stored database
  - Runtime: Validation of binary at execution time
- Configurable policies
  - Monitor all executions and loads of files, loads of kernel extensions, and shared libraries in signature database
  - Disable trusted file opens for write

IBM PowerSC Security Management

The PowerVM management framework is also essential to consider, beyond the hardening of the hypervisor and OS code itself. Security of the management framework is one aspect, but management tools are essential to give administrators information on the security status of systems and enforce policies. PowerVM features role-based access control (RBAC), where an administrator can be confined to read-only mode or be given access to only a specific set of VMs, with no visibility into any other VMs. One of the key security solutions used in conjunction with virtualization on Power Systems is PowerSC, which consists of an extension to PowerVM and a management console specifically designed to enhance security and compliance for AIX and Linux guest environments. PowerSC has several important features to manage security levels and monitors and alerts in real time:

- **Compliance Automation.** Applying security settings on multiple systems to comply with regulations can be time consuming and error prone. PowerSC provides prebuilt profiles for PCI, HIPAA, SOX, and U.S. DoD STIG. These profiles automate configuration, monitoring, and auditing. They are IBM's recommended settings to simplify a company's adherence to and reporting of regulatory compliance policies. These profiles can be easily customized to meet the specific needs of customer environments.
- **Trusted Boot.** Trusted Boot provides a vTPM for each VM to ensure that it boots only trusted code. PowerSC works with PowerVM to monitor and store the results of the boot process and allow admins to monitor and verify that the system status is trusted.
- **Trusted Logging.** Security compliance requires strict control over logs for auditing. PowerSC centralizes all VM logs for easier manageability. Admins cannot tamper with the logs, and logs persist even if a VM is deleted.
- **Trusted Firewall.** Trusted Firewall ensures that each VM has the appropriate network isolation settings. PowerSC implements a firewall within the hypervisor that is monitored and controlled by administrators. Beyond security, a hypervisor-based firewall improves network performance by not having to route traffic out to an external firewall and back again in the case of VM-to-VM communication on the same physical server.
- **Trusted Surveyor.** Infrastructure must often be segregated on the network to meet compliance requirements. PowerSC simplifies this task by monitoring the network segregation of each VM, comparing it with logical network maps and policies and alerting administrators if configurations are out of policy.
- **Trusted Network Connect and Patch Management.** Patching becomes a problem at scale, and virtualization complicates this problem by creating a large number of logical servers. PowerSC automatically detects noncompliant VMs upon boot and notifies administrators.

A single vendor for the entire system has its benefits. For example, support is simplified, with only a single vendor responsible. IBM believes that by designing, testing, and certifying the entire stack of hardware, hypervisor, OS, and management together, it is able to offer an extremely high level of security for a virtualized Power environment that is equivalent to or better than the security provided by physical systems.

FUTURE OUTLOOK

IBM continues to invest in and grow the Power platform, with several interesting announcements about its future:

- **OpenPOWER Consortium.** IBM is opening up much of the Power technology (processor specifications, firmware, software), allowing third parties to license this technology and expand on and collaboratively enhance the Power ecosystem.
- **Expanded Linux support.** In addition to AIX, IBM is committing to further enhancing support for Linux as a guest operating system, bringing more PowerVM and PowerSC features to Linux.
- **KVM support.** The KVM hypervisor will be supported on Power in the future, giving customers another choice for a hypervisor on Power. While a discussion between the differences between KVM and PowerVM is beyond the scope of this paper, having more choice is certainly not a bad thing, and it allows standardization on KVM across multiple architectures.
- **OpenStack support.** OpenStack is an open source cloud platform that is drawing a lot of interest from the industry. IBM is a major backer of and contributor to the project and is developing support for Power Systems and PowerVM in OpenStack. Power Virtualization Center (PowerVC) is a new product that allows users to deploy and manage PowerVM in OpenStack environments.

CHALLENGES/OPPORTUNITIES

Challenges

- **Virtualization fragmentation and silos.** Ideally, customers would like to manage all VMs under a single umbrella, regardless of architecture or hypervisor. In reality, most virtualization is managed in fairly separate silos, even within just x86. Bringing in additional virtualization platforms can be a challenge, especially for platforms such as Power, which are typically a minority in the datacenter.
- **Trust and education.** Many issues, including performance and security, make customers uncomfortable when virtualizing mission-critical applications. IBM has made considerable investments in addressing these issues with products such as PowerVM and PowerSC, but customers must invest time in a deep technical discussion so that they can understand the products and contrast them against other virtualization architectures. Education and experience with virtualizing critical apps over time will lead to an understanding of the security architecture and confidence in the system, but the process can be slow.
- **Differentiation.** x86 servers have been growing in share, and they are also much of the focus of trends such as virtualization and cloud. Power and non-x86 systems also have their own virtualization technologies and cloud initiatives, but many customers often are not aware of them and of the differences between the implementations, which can be very significant in terms of performance, management, and security.

Opportunities

- **Virtualization of mission-critical apps.** As customers progress in virtualizing workloads, many have reached the point where the majority of their applications are virtualized. Power Systems tend to have a high rate of virtualization, and the workload profile includes a large mix of tier 1 applications. PowerVM virtualization was designed with this profile in mind, providing unique security capabilities for sensitive applications. The benefits of virtualization are well known by customers. The technology has been a huge success in organizations, and customers are seeking to spread this benefit to as many of their workloads as possible. Many of these mission-critical applications are on non-x86 platforms such as Power, leading to an expanding opportunity for secure virtualization on the Power platform.
- **Bringing mission-critical apps to the cloud.** Cloud is a big shift for the IT industry, and as customers seek to gain the benefits of cloud, they must first virtualize and assess workloads. Private clouds offer the idea of abstracting across vast pools of infrastructure, and customers wish to eventually connect these to public clouds. By the numbers, x86 servers make up the vast majority of servers, but a disproportionate number of critical workloads run on non-x86 servers. Mission-critical apps are a big part of the cloud decision, and if they are to be included in the modern datacenter, they will need to be virtualized in order to be included in cloud. Solutions such as PowerVM offer virtualization benefits and a tie-in to cloud without having to do a difficult application migration.
- **Openness.** IBM is pursuing many open initiatives around Power, including the OpenPOWER Consortium, enhanced Linux support, OpenStack, and KVM. Openness will help drive an increase in ecosystem support, collaborative industry development, and customer interest. Many of these projects, such as OpenStack, have a lot of momentum behind them, and adding Power support will help Power stay relevant and benefit from these trends.

CONCLUSION

The PowerVM virtualization platform implements multiple unique technologies to allow secure virtualization of workloads. Customers seeking to virtualize sensitive and critical applications must consider many things in detail. They must inspect the architecture of the entire solution stack, including hardware, hypervisor, guest OS, applications, and management. The inner workings of the hypervisor and how it isolates virtual CPU, memory, and I/O must be considered because approaches vary greatly. The architecture of the system must also be considered in the framework of management. Having a secure virtualization platform is of little value with no way to implement, monitor, and verify the security level.

As customers begin the journey to the virtualized, "cloudified," modern datacenter, they must bring these initiatives to all workloads and systems, including tier 1, mission-critical applications on non-x86 platforms. IBM has developed and prioritized security technologies in PowerVM that can help customers minimize the risk and reap the benefits of virtualizing these demanding applications.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1000 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For more than 48 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com