

WHITE PAPER

Server Security, Patching and Virtualization



Introduction

Virtualization is not a new concept in the world of information technology. The roots of modern day virtualization can be traced back to computer science research from the 1950s. Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments.

One of the many benefits of virtualization is the ability to consolidate the workload of multiple underutilized servers into fewer physical machines. The “virtual machines” can then be consolidated and spread across one or more physical machines, as resources permit. Servers in this context are much like files in a file system that can be easily transferred from one location to another. This kind of deployment flexibility means that servers can be instantly deployed or reallocated to accommodate demand without the need for additional investment in hardware.

For decades, virtualization was commonly found in mainframe computing environments. Then, in 1998 a company called VMware introduced virtualization technology to the Intel x86 platform, which allowed the simultaneous creation and execution of multiple, virtual x86 computers on a single server. Virtualization has become ubiquitous thanks in part to the efforts of VMware. According to VMware at the time of the writing of this paper, more than 4 million users and 20,000 corporate customers of all types and sizes use VMware software, including 99 of the Fortune 100 companies.

The benefits of virtualization combined with its ubiquity have led to widespread adoption. As companies have discovered new and increasingly more creative uses for server virtualization, they have also encountered some challenges. One of the biggest challenges mirrors a problem in the physical server world: security patching. Combating the threat of software vulnerabilities in the virtual world requires a unique approach. This paper describes in greater detail the benefits and challenges of server virtualization, and offers insight into how Blue Lane customers are utilizing the PatchPoint® System to combat the threat of software vulnerabilities.

Benefits of Server Virtualization

- Physical servers with a single operating system frequently operate well below capacity. By dividing the physical resources of the server among multiple operating systems (virtual machines), the workload can be optimized. This enables administrators to get more performance out of their server infrastructure without having to make any additional investment in hardware. Server consolidation can lead to several additional benefits, including:
 - Reducing the amount of square footage, rack space, power and cooling requirements in the datacenter
 - Reducing administrative costs by simplifying tasks such as server backup, ghosting and provisioning
 - Reducing required investment in physical hardware
- Virtual machines can run multiple operating systems simultaneously. A variety of different versions and different systems can be ready on hot standby. Some systems, such as legacy, may prove difficult or impossible to run on newer (real)

hardware so the virtual machine is a convenient way to extend the life of those legacy applications. For example, virtualization could encapsulate Windows NT systems that otherwise could not be upgraded to newer hardware that does not provide support for Windows NT.

- Virtual machines can provide an isolated sandbox for running applications, which creates opportunities for test and development that would otherwise be cost prohibitive for many organizations to duplicate in the physical world.

Challenges of Server Virtualization

The primary challenge in managing a virtual server environment is that change and configuration management issues become magnified. Many companies struggle to keep up with security patches in their physical server infrastructure. Because virtual machines can be created so easily and quickly, deployed instantly, and shuffled around the infrastructure like files, managing change become incredibly complex.

Consider a software development organization. Software developers are typically heavy users of virtualization because of efficiencies of scale afforded by a virtual environment. In a typical test and development environment, engineers may require hundreds of different iterations of servers to determine whether or not all versions of software and hardware combinations work with the new software product. The iterations of servers will often include outdated versions of software as well as unpatched applications and operating systems, which mimic the distribution in the real world. Because these servers exist in a known vulnerable state, they can be easily compromised if not segregated from the rest of the network.

In the datacenter, virtual servers are frequently added to existing pools of servers as additional resources are required. To achieve the greatest amount of efficiency, administrators will standardize on a single “gold standard” build of a particular, pre-configured server and then bring up new instances of that server to fulfill demand. The problem in this scenario is that gold standard builds are created at a given point in time and do not change. Unfortunately, new security vulnerabilities are announced and new patches that address those vulnerabilities are released on an ongoing basis, making it impossible for organizations to maintain their standard. Once the gold standard build is patched, administrators must either re-provision all the servers or patch all existing servers in production.

Another challenge to managing a virtual server environment is simply to know what servers exist. In the physical world, this problem is more manageable because a physical server requires a significant amount of effort to be physically deployed on the network. Physical hardware must be configured, physical space must be obtained, physical network and cabling connections must be made. In the virtual server world that administrative overhead disappears and, as a result, servers tend to “flow” into and out of the network with much less friction. A virtual server that existed on the network one moment may be turned off and replaced by a completely different virtual server the next. Hundreds of servers may suddenly appear as if from nowhere and although they do not require the addition of physical hardware or the administrative overhead of a physical server, they present all of the same security challenges as their physical world counterparts.

While virtualization can reduce hardware and maintenance expenses, it is normal to see some increased security burdens, especially when it comes to keeping enterprise software and databases up-to-date with the vendor's latest vulnerability patches.

Extending Virtualization to the Security Patch

For years the answer to addressing security vulnerabilities in the operating systems, applications and databases on virtual servers was to resort to the same methodology utilized in the physical world:

1. First find the servers (which, as discussed above, can be much more difficult in the virtual world)
2. Determine vulnerabilities
3. Establish a baseline of acceptable risk
4. Install patches (which may be impractical if the servers are purposely in an unpatched state for a specific reason, e.g. testing and development)
5. Reboot (if required)

The difficulty in this approach in the virtual world mimics the difficulty of this approach in the physical world. This is especially true when the applications are difficult or impossible to patch:

- The server/application is part of a larger, more complex system where any change to one component could dramatically alter the functionality of the whole system
- The application itself is complex and special skills are required in order to deploy a patch
- A third-party application vendor must first test, validate, and then approve any patching of underlying operating systems
- The change management process is extremely rigid or the maintenance windows of the organization are extremely tight
- The system is required to run 24x7 and cannot be rebooted
- The application is part of an embedded system
- The software vendor has declared "end of life" for the product and will release no more security updates

The optimal way to solve the security patch problem for virtual servers is to extend the paradigm of virtualization to the security patch itself. In other words, having the ability to instantly tap a readily available pool of servers without the administrative overhead found in the physical world would ideally be complemented by the ability to instantly tap an available pool of security patches that could be deployed without the risk or maintenance overhead of their physical counterparts.

The PatchPoint System: An Inline Patch Proxy

Blue Lane Technologies developed PatchPoint, the world's first inline patch proxy, to solve the specific problems associated with server patching. PatchPoint is an appliance that sits in the network as close as possible to the servers it protects. It is an inline device but not a perimeter security solution. Rather, it provides a complement to existing technologies such as firewall and network intrusion prevention. PatchPoint provides instant patch protection for servers without requiring any patches to be physically installed on the servers hosting business applications.

PatchPoint relies on sophisticated application proxies to properly interpret server-bound traffic. Each application supported by PatchPoint (e.g. Microsoft Exchange®, Oracle® DBMS, etc.) must be accompanied by an appropriate proxy. PatchPoint uses these proxies to "listen" to client-server transactions and to deterministically establish when the conditions exist for a particular patch to be applied.

In the same way that Blue Lane develops an application proxy for each application, an inline patch is developed for every applicable vendor patch on that platform. The inline patch, when applied to the network traffic, performs the same corrective action inline that the software patch would do on the server. The result is that PatchPoint is able to perform an "application correction", which means to deterministically fix to server-bound traffic without having to heuristically determine whether or not traffic contains malicious content, eliminating the risk of false positives.

The PatchPoint inline patch proxy is entirely architected around the functionality of the original software patch and how that patch would operate within the context of the overall software application. By porting that logic to the network however, PatchPoint is able to secure servers without incurring any of the inherent risk involved in the physical deployment of the patch. And because the inline patch proxy deals with software vulnerabilities at the root cause, rather than focusing on specific exploit traffic patterns or behavior, PatchPoint can fix the vulnerability instantly and permanently, no matter how many exploit variants may emerge in the future.

By porting the functionality of the software security patch to an aggregation point in the network, PatchPoint can provide instant patch protection to any number of servers, whether they are physical or virtual. PatchPoint also provides a discovery feature which enables administrators to monitor and adapt to dynamic changes in the datacenter, like a rapid introduction of new, unpatched virtual servers. Because PatchPoint operates via the network, no software or configuration changes are required of the actual servers and no servers must be rebooted to achieve complete patch protection. These capabilities are especially important in environments (e.g. test and development) where companies must have a variety of unpatched versions of operating systems and applications in place.

Summary

The benefits of virtualization far outweigh the challenges, and the rapid rate of adoption of platforms like VMware proves this to be true. Still, challenges remain. Security patching of servers currently plagues the virtual world much as it does the physical, but presents a slightly unique set of problems. The solution to maintaining these virtual environments is to apply the same concept of virtualization to the security patch. PatchPoint is the world's first inline patch proxy capable of replicating the function of the software security patch on the network wire, not on the server. As such, PatchPoint is capable of creating a completely trusted domain in which virtual machines can be protected regardless of their state.

About Blue Lane Technologies

Blue Lane provides the only inline patch proxy systems for enterprise servers that checks for the same conditions and applies the same corrective action as the software vendor security patch to fix application-specific vulnerabilities at the root cause. Solving the dilemma of "patch now or patch later," PatchPoint instantly secures critical applications and preserves the uptime of the business while eliminating the cost and risks associated with unscheduled patching. Founded in 2002, Blue Lane is headquartered in Cupertino, California. For more information, contact the company at www.bluelane.com.



Blue Lane
10450 Bubb Road
Cupertino, CA 95014

www.bluelane.com
info@bluelane.com
408-200-5200