

Securing virtualization in real-world environments



Contents

- 2 Introduction
- 3 Virtualization: Enjoy the ride, but don't forget to buckle up
- 5 Security implications of virtualization
- 7 Securing virtualization
- 8 Virtualization security solutions from IBM
- 11 Summary
- 12 For more information

Introduction

IT organizations are under increasing pressure to deliver more functionality faster and with smaller budgets. Increasing costs attributed to power and cooling of servers, coupled with the headache of managing an expanding number of servers, makes this a serious challenge requiring new advancements within the data center.

At the heart of many data center transformations is virtualization. Through its ability to consolidate workloads and reduce the amount of time and energy IT spends purchasing, installing and maintaining racks of servers, virtualization allows the organization to satisfy its goals with fewer physical resources and reduced operational costs. Early adopters of virtualization are also attaining additional returns on their investment through simplified systems management, automation and optimized server utilization. In short, both the expectations and benefits are very real.

However, the key to successful virtualization is providing benefits like energy efficiency and performance without compromising security. Organizations typically struggle to stay ahead of today's threats while also addressing various regulatory-based compliance standards. Adding new technologies such as virtualization exacerbates this problem, making it essential for organizations to identify and address the new security gaps that are introduced by virtualized environments.

For example, in a physical server environment, if someone compromises the security of one server, most organizations have the security tools in place to address and contain that breach. But in a virtual server environment, where a single physical server can be running multiple applications from different resources, a breach of one virtual server can potentially be a breach across a multitude of virtualized servers. And traditional security tools can't help, because they weren't designed to address virtualization. It's only a matter of time before a tremendous security breach associated with server virtualization makes headlines.

Given the potential for catastrophe, organizations must act now. The first step is to take the time to understand how to properly integrate, deploy and manage security in virtualized environments. Without a baseline plan or a real understanding of virtualization and security, IT groups may decide to disable many of the advanced features of virtualization for fear of unintended consequences, or even worse, they might introduce more risk into the process.

This white paper examines many of the security concerns associated with virtualization and helps you understand and prioritize these risks, as well as describing the IBM security solutions that can help you secure virtual environments and position your organization to reap the full rewards of this exciting technology.

Virtualization: Enjoy the ride, but don't forget to buckle up

Virtualization has tremendous appeal for a variety of reasons. Most notably, organizations are successfully reducing capital and operating expenses through server consolidation. By breaking down silos of physical resources, organizations can simplify data center management and reduce server sprawl.

While reducing data center costs has become the primary success metric for organizations, investments in server virtualization also come with greater expectations. Organizations have additional goals of increased availability, automation and flexibility that are possible only with virtualization. Realizing these goals is a critical step towards greater levels of service management through virtualization, including advanced IT service delivery and strong business alignment. It also helps break the lock between IT resources and business services—freeing you to exploit highly optimized systems and networks to further improve efficiency.

However, in addition to providing these benefits, virtualization significantly impacts security. As data centers evolve into shared and dynamic infrastructures, security concerns increase. The industry has already expressed anxiety over physical-to-virtual migrations, security of the virtualization management stack, and visibility into the virtual network. As virtual data centers become more complex, additional concerns around workload isolation, multi-tenancy, mobility, virtual machine sprawl and trust relationships are gaining visibility. Negatively impacting the overall security posture and increasing risk are never the intentions of IT groups deploying virtualization, but that potential readily exists.

Concerns over risk have the potential to limit the benefits an organization will realize from virtualization. For example, many companies have seen no change in the number of resources needed to manage virtual environments (see Figure 1). This is likely the result of organizations not enabling automation capabilities such as dynamic resource allocation and mobility. Additionally, adopters of virtualization may not be changing—and ultimately improving—the efficiency of server provisioning processes for fear of introducing risk or of moving out of compliance with security policies. Until these organizations enable more advanced virtualization features, they will not realize the enhanced manageability and availability benefits that virtualization brings.

The security challenges of virtualization

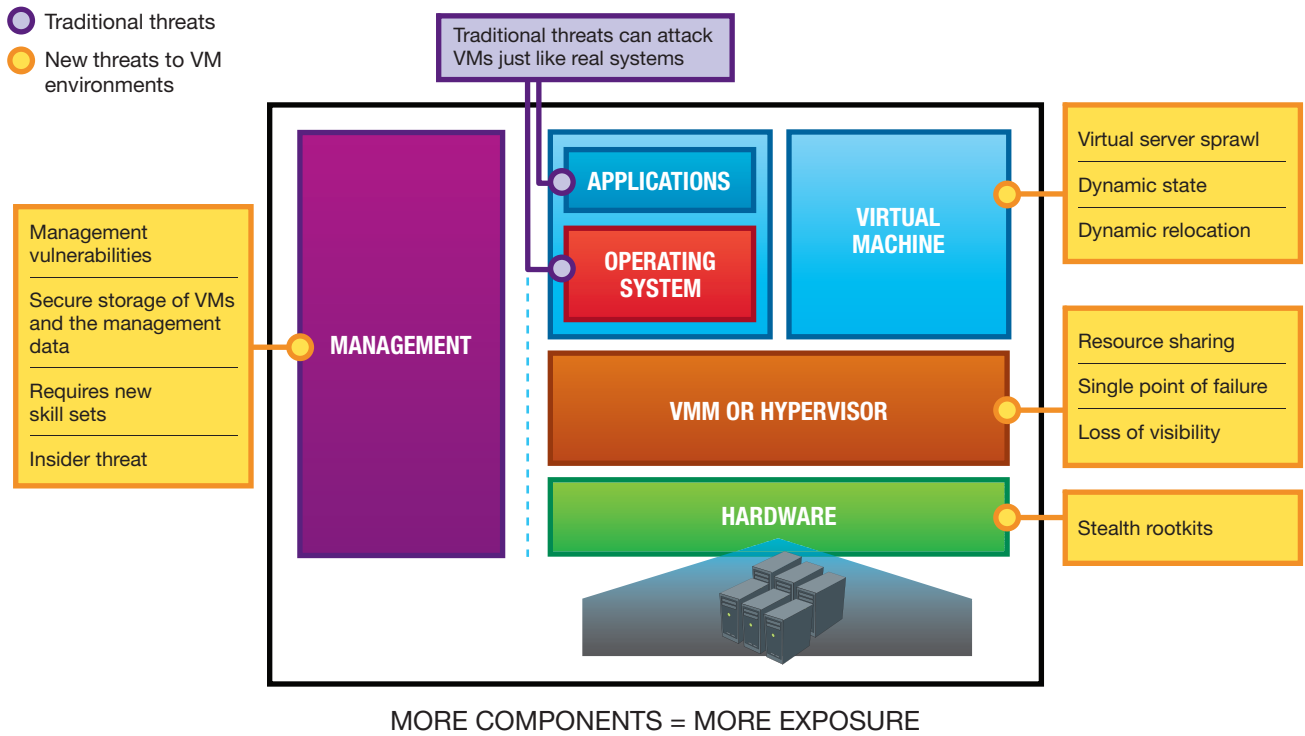


Figure 1: The unique security challenges of virtualized infrastructures generate new risks for IT organizations, and the risk increases with the number of components involved.

On the other hand, many early adopters have rushed to take advantage of these technologies, often without fully understanding the security concerns. For example, server consolidation increases overall efficiency, but also complicates matters by introducing a new architecture with various technical and organizational complexities. Both IT and security professionals must adapt as consolidation forces change.

As network and server administration begin to converge, physical security devices and other security tools become less effective. Even the most basic features of virtualization greatly impact the day-to-day security responsibilities and processes used to achieve and maintain compliance.

Perhaps a lesson can be learned from the automobile industry in that safety and security increase with maturity. The first modern automobiles were available in the late 19th century, but seat belts were not offered as standard equipment until 1958. Clearly, technological advances allowing cars to travel much farther and faster outpaced advances in safety. Likewise, new virtualization capabilities are currently being introduced at a pace that challenges risk mitigation solutions. While mature virtualization platforms have strengthened their inherent security capabilities over time, new virtualization products with widespread appeal and poorly understood security capabilities are now on the highway.

In response, organizations must buckle up. They should understand the new security risks that are introduced in virtualized environments, and then evaluate new security solutions specifically designed to address these new virtualization security challenges. Yes, virtualization introduces new concerns, but it also provides an opportunity to extend defense-in-depth to new and unique areas of integration. As we optimize security

controls, strengthen the platform and increase awareness of potential security implications, organizations will be able to realize more benefits without adding new risk.

Before we examine the solutions offered for virtualization security, let's take an in-depth look at the major concerns.

Security implications of virtualization

Some characteristics and attributes of virtualization have inadvertent yet influential consequences on information security. Physical servers and other computer resources are heavily shared, barriers between virtual machines are logical, and workloads can move around the data center—en route to new servers or geographic locations in real time.

Understandably, people, processes and technology must adapt. To do so, we must fully understand the new risks and security challenges unique to this technology. The following sections describe several major security concerns of virtualized environments.

Isolation

In order to safely consolidate servers and allow a single physical server to host multiple virtual machines, virtualization uses logical isolation to provide the illusion of physical independence. No longer able to verify that machines are separated by network cables and other physical objects, we rely on the hypervisor and other software-based components to provide these assurances. This becomes increasingly important when workloads from users of different trust levels share the same hardware. In order to properly contain information, administrators must pay special attention to configuration settings that affect virtual machines and network isolation, as well as continuously monitor the entire infrastructure for changes that could result in leakage of sensitive data.

Server lifecycle and change control

Patch management and change control windows are vital to keeping operations running smoothly and safely. This is done by applying important security fixes in a timely manner. In fact, this is so important that many IT organizations have built an exact science around server maintenance. Without question, a great amount of time and money are invested annually to maintain servers in the data center. Virtualization adds to this complexity by changing the rules of the game. Servers are no longer constantly running; virtual machines can be stopped, started, paused and even rolled back to a previous state. The speed at which machines are configured and deployed also dramatically increases. What used to take hours now takes seconds or minutes. The result is a highly dynamic environment where machines can be quickly introduced into the data center with little oversight, and security flaws can be absent or reintroduced based on virtual machine state. Security professionals must fully understand what virtual machines are being deployed, which are currently running, when they were last patched and who owns them.

Virtual machine mobility

Mobility, in the language of virtualization, refers to the ability of a virtual machine to automatically relocate itself and its resources to an alternate location. This capability, while highly desirable, can also create problems. In a traditional data center, physical server 'A' might be located on Row 5, Rack 8, Slot 3. In the hybrid data center, virtual machine 'B' is not as easily locatable. As part of a resource pool, server 'B' could be spread across multiple physical resources. If configured for mobility, the virtual machine could relocate to another physical server, either automatically as part of a disaster preparedness plan or in response to a performance threshold.

The mobile aspect of virtual machines means flexibility, time and cost savings for the data center, but it also introduces security concerns similar to laptop and large-scale dynamic host

configuration protocol (DHCP) environments. Static policies and other security mechanisms designed for traditional servers and networks may become easily confused. The ability of security products to operate intelligently across multiple physical and virtual environments, as well as to be more infrastructure-aware through integration of platform and management APIs, will allow administrators to enforce control over the mobility of virtual machines within various security zones.

Virtual network security

Networks and servers are no longer two separate, distinct layers of the data center. Virtualization allows for the creation of sophisticated network environments, completely virtualized within the confines of the server itself. These virtual networks facilitate communications for virtual machines within the server and share many of the same features used by physical switches and other traditional networking gear. A physical port in the data center that used to represent a single server now represents tens or hundreds of virtual servers and drastically affects how we secure data center networks. Network traffic between virtual machines within the same physical server does not exit the machine and is not inspected by traditional network security appliances located on the physical network. These blind spots, especially between virtual machines of varying trust levels, must be properly protected with additional layers of defense running within the virtual infrastructure.

Separation of operational duties

Separation of duties and the policy of least privilege are important security principles used to limit the capabilities of IT administrators as they manage resources and perform routine tasks. Server management is usually handled by the server administrator, and network management by the network administrator—while security professionals work with both teams and handle their own specific tasks. Virtualization has

changed the natural boundaries and lines of demarcation that built these divisions. Both server and network tasks can be managed from a single virtualization management console, which introduces new operational challenges that must be overcome. Organizations must clearly define proper identity and access management policies, allowing administrations and security professionals to properly maintain and secure the virtual environment without granting excessive authority to those who do not require it.

Additional layers of software

As virtualization is introduced into the data center, so are additional lines of code that make up the software needed to implement it—from the management consoles that control virtual machines to the hypervisors that provide the foundation for the technology itself. As such, new vulnerabilities related to virtualization software can be introduced, with some attributed to the popularity, accessibility and relative immaturity of x86 virtualization. In addition, there is a heightened sensitivity from vendors to analyze and disclose vulnerabilities. Many disclosures can be attributed to third-party code that is packaged with the virtualization software stack, and vendors are taking measures to reduce the footprint of their software and dependency on uncontrolled code. However, it goes without saying that fault-free code is largely unattainable, especially as vendors integrate complex features into their platforms. Organizations should treat virtualization as they would any critical application and apply proper defenses to stay ahead of these threats.

Securing virtualization

IBM believes that a foundation in security is the basis from which organizations can reap the most benefit from virtualization. If many of today's virtualization security challenges simply mirror yesterday's challenges, logically, we should be able to use

the same security technology. The reason we cannot is due to a fundamental shift in the way organizations plan, deploy and manage virtualization platforms. This shift requires, in some instances, a simple adaptation, and in others, a completely new way of operating.

For example, it is true that some of the threats exposed by virtualization can be mitigated or reduced by using existing people, processes and technology. Traditional network and host security products for example, can be used to protect the network, desktops and servers. Given a small adaptation, host intrusion prevention systems (HIPS) can also be installed on each virtual machine. However, what cannot be effectively protected by traditional processes and technologies is the virtual fabric composed of the hypervisor, management stack, inter-VM traffic and virtual switch. While people, processes and technology are recyclable, they also need to evolve to the new architecture and concepts exposed by virtualization.

Change control and patching procedures are good examples. The patching procedures for virtual machines certainly need to adapt to fluctuating running states and dormancy. Furthermore, how do organizations use virtualization management suites to reclaim the separation of duties lost when network and host administration merge onto the virtualization platform?

Deploying access control and applying the policy of least privilege to the management console, administrative roles and virtual images are certainly not unique concepts; however, slowing the growth of virtual networks and preventing virtual server sprawl is. Administrators must also adapt to the concept of shared resources and ensuring a fair distribution of RAM, CPU, storage and bandwidth.

All of these practices are used in today's networks—in some form—to mitigate risk. Since even virtual networks are really hybrid networks, these traditional solutions are still absolute necessities in the fight for security. However, organizations should keep in mind that organizational security is only as good as the sum of its parts. Defense-in-depth must be extended from physical to virtual environments. In today's era of reduced cost and complexity, the value of a single suite of centrally managed security products that protects both physical and virtual networks and hosts is critical to achieving organizational security and maximum return on investment.

Virtualization security solutions from IBM

Most organizations are running hybrid infrastructures with varying percentages of physical and virtual hosts, applications and devices. While many are rushing headlong into virtualization, others are testing in laboratories or waiting until the value of their servers and appliances have amortized. Regardless, the stark reality of virtualization is that there is an adoption period. Current investments in security will not be thrown away but will be recycled and reused. Without question, organizations will look to cannibalize their existing investment in security in order to effectively extend their investment.

It is critical to understand that the true value of security is not in point products that address virtualization only, but in solutions that extend security to the new risks exposed by virtualizing production servers. Organizations interested in reducing cost and complexity while achieving enterprise-grade security must pay close attention to how solutions will fill the coverage gaps introduced by virtualization.

IBM is focused on providing best-of-breed, end-to-end security solutions for key control points—network, endpoint and server. IBM provides a range of virtualization security products, services, and leading-edge expertise to help organizations maintain security while realizing the promise of virtualization.

Virtualization security products

IBM's virtualization security product offerings fall into three areas within the virtualization spectrum: Virtual environment ready, virtual appliances and virtual infrastructure protection.

Virtual environment ready solutions utilize IBM security offerings to protect virtual environments. With these solutions, IBM can protect virtual environments with proven technologies that incorporate recommended policies from the IBM X-Force™ team, which is one of the oldest and best-known commercial security research groups in the world. Certified by the International Computer Security Association (ICSA), and developed according to National Security Services (NSS) libraries for cross-platform security development, these solutions have the ability to block threats and provide seamless integration with no interruption of your workflows.

Virtual appliances such as IBM Security Network Intrusion Prevention System help reduce operational expenses while increasing flexibility for your security infrastructure by allowing the reuse of assets you already own. These solutions can easily migrate from older technologies without changing hardware, and they provide a foundation for future expansion. The same policies of the physical appliance can be reused, and there can be numerous virtual appliances running on every virtualization server.

Virtual infrastructure protection solutions include IBM Security Virtual Server Protection for VMware, an integrated threat mitigation solution designed to allow organizations to fully exploit the benefits of server virtualization while protecting critical virtualized assets (see Figure 2). It provides the same intrusion prevention capabilities of other network IPS solutions, but with the advantage of being integrated into the hypervisor through the VMsafe interface made available by VMware—which means you need to install only one instance for each virtualization server in order to protect the entire virtualized infrastructure.

IBM Security Virtual Server Protection for VMware

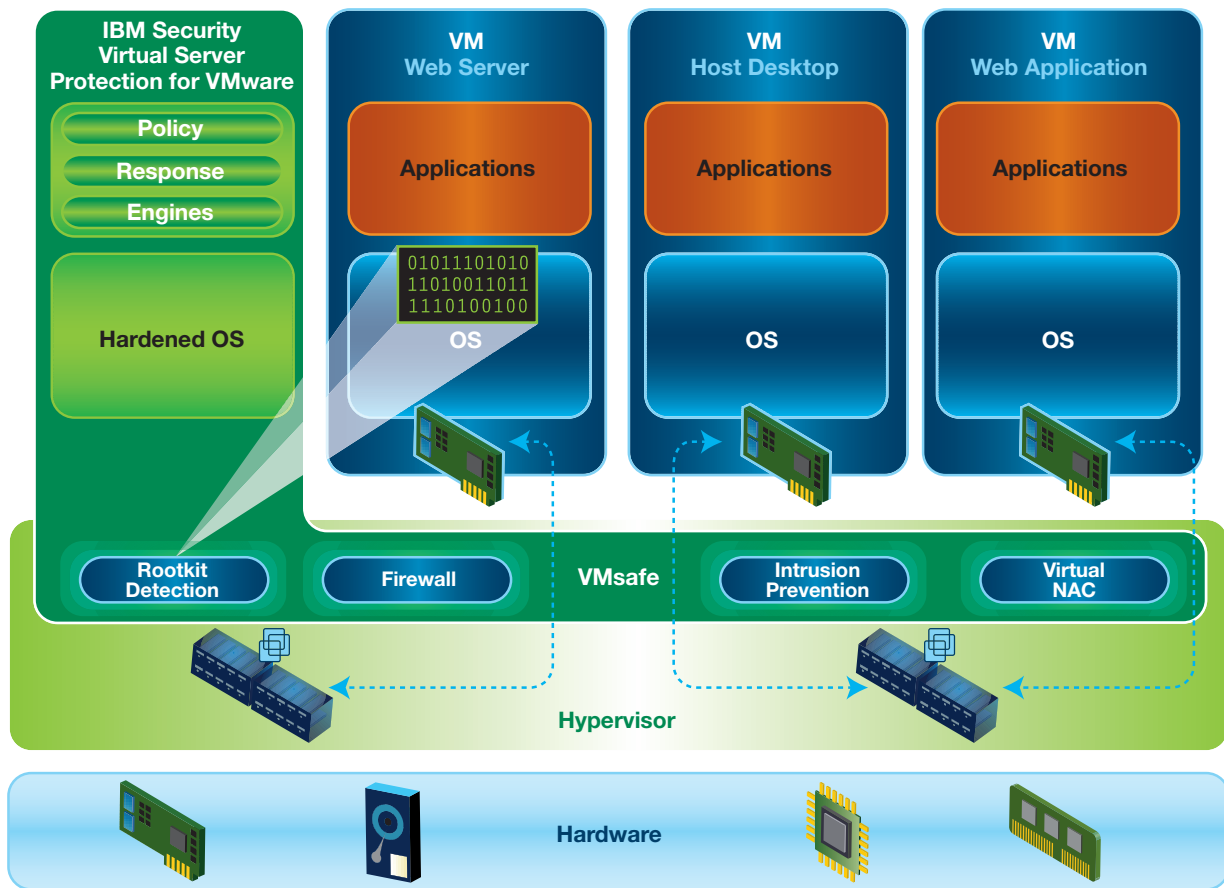


Figure 2: IBM Security Virtual Server Protection for VMware helps organizations operate more securely and cost-effectively by delivering integrated and optimized security capabilities for virtual data centers.

IBM Security Virtual Server Protection for VMware automatically protects virtual machines as they come online or move across the data center, and it monitors traffic between virtualized servers with a holistic view of the virtual network. In addition to delivering IPS capabilities, the solution enables the security team to search for malware by looking for rootkit activity in virtualized systems and to configure firewall rules and network access control (NAC) rules.

IBM Security SiteProtector™ System is integrated into Virtual Server Protection for VMware, providing a simple, cost-effective way to manage security solutions for physical and virtualized systems across the entire IT environment. Security SiteProtector System provides a central management point to control security policy, analysis, alerting and reporting.

Security management solutions

IBM provides a wide range of security management offerings, from managed services to plug-and-play solutions:

- IBM Managed Security Services offers the option to outsource the deployment and management of your security products, thus reducing the cost and complexity of training and maintaining in-house staff. IBM Managed Security Services also offers an innovative and simple way to secure the virtual infrastructure by choosing to have IBM manage your security operations from one of eight IBM operation centers around the world. Called the IBM Virtual-Security Operations Center (Virtual-SOC), this service is designed to ensure that all physical and virtual security solutions are active and updated with the latest patches and software updates, including security intelligence provided by the IBM X-Force research and development team.

- IBM Security SiteProtector System offers the industry's largest portfolio of centrally managed security products and is supported on VMware ESX. Designed for simplicity and flexibility, Security SiteProtector System can provide centralized configuration, management, analysis and reporting for select IBM security products.
- IBM virtualized infrastructure security provides virtual environment awareness and forms a transparent plug-and-play threat protection solution to address security concerns associated with virtual machine sprawl, lack of virtual network visibility, and mobility. Through integration with virtualization platforms, IBM provides consolidated network-level intrusion prevention and auditing of the virtual environment, reducing the need for network traffic analysis in the guest operating system. Through this approach, organizations can limit the security footprint per guest OS, thereby eliminating redundant resource consumption and reducing security management complexity.

Solutions backed by IBM X-Force

IBM security excellence is driven by the world-renowned X-Force team, which provides the foundation for IBM's preemptive approach to Internet security. This leading group of security experts researches and evaluates vulnerabilities and security issues, develops assessment and countermeasure technology for IBM security products, and educates the public about emerging Internet threats.

The X-Force team delivers security intelligence that customers can use to improve the security of their networks and data. Regardless of whether the product is a physical 1U appliance or a piece of software installed on a virtual machine, the same security intelligence and threat content developed by the X-Force team is installed on that IBM security device and helps manage the threat mitigation process.

In addition to providing security content updates to IBM security products, the X-Force team also provides the IBM X-Force Threat Analysis Service (XFTAS). The XFTAS delivers customized information about a wide array of threats that could affect your network through detailed analysis of global threat conditions.

Summary

Without a doubt, virtualization has changed—and is changing—how organizations run, manage and store applications and data. New, complex technologies are rapidly increasing the potential for more gaps in protection.

Virtualization security need not mean scrapping current security investments in IPS technology, firewalls or multifunction devices. Networks will always have some amount of physical hardware, and virtual security will always be limited by a finite amount of resources. But you do need to plan now and consider how to best protect your physical and virtual resources.

IBM continues to develop solutions that not only help protect capital investments and confidential data, but also make it easy to track, monitor, automate and manage your critical infrastructure resources, including those in the virtualization stack.

For more information

To learn how IBM can help you enable secure virtualization, contact your IBM representative or IBM Business Partner, or visit ibm.com/tivoli/security. To learn more about IBM virtualization solutions, visit ibm.com/services/us/iss/html/virtualization-security-solutions.html



© Copyright IBM Corporation 2011

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
January 2011
All Rights Reserved

IBM, the IBM logo, ibm.com and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information provided in this document is distributed “as is” without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Please Recycle