

Rewriting the rules of patch management

IBM Tivoli Endpoint Manager shifts the patching paradigm



Contents

- 2 Introduction
- 3 The patch management conundrum
- 4 Changing the patch management paradigm
- 9 Why it works
- 10 Continuous compliance
- 11 How customers are using it
- 12 A comprehensive portfolio of compliance and security solutions
- 13 Conclusion
- 13 For more information
- 13 About Tivoli software from IBM

Introduction

Malware attacks are in a race against time to exploit vulnerable computer systems before software vendors publish patches and their customers can apply them. When malware wins the race, organizations lose productivity and risk loss of sensitive data, potential litigation and regulatory fines. The sheer enormity of the problem is alarming—the ongoing battle between hackers and software companies costs the U.S. economy an estimated \$266 billion annually, according to the Cyber Secure Institute, a Washington, D.C.-based advocacy group.¹

To combat this threat, more and more software vendors are issuing more and more patches in attempts to keep pace with the frenzy of malware exploits. Unfortunately, most organizations are not equipped to handle this onslaught of patches in a time- and cost-effective manner. Because of organizational processes, it takes most IT departments weeks or even months to deploy patches throughout the environment. According to some estimates, it can take organizations as long as four months to achieve a 90 to 95 percent patch compliance rate. By then, countless additional patches have been issued, meaning that organizations are perpetually at high risk and out of compliance—and the situation only gets worse over time.

Patch management has always been an uphill climb because of the massive complexity involved. Despite the risks, some organizations are reluctant to patch because of the time and labor required, plus the potential of disrupting business operations. In an organization with a heterogeneous hardware and software environment, staying on top of the multitude of patches—and issuing them in a timely manner—can overextend IT staff and budgets. What is needed is a rapidly deployable, cost-effective, policy-based patch management solution that:

- Works for all endpoints in organizations of all sizes, including the very largest.
- Supports multiple vendors, operating systems, applications and platforms.
- Works over low-speed connections and supports devices that roam outside of the organizational network.
- Minimizes the demand on IT staff.
- Operates in real time, deploying patches organization-wide in hours.

IBM Tivoli® Endpoint Manager, built on BigFix® technology, combines the separate pieces of the patch management puzzle into an intelligent, simplified solution that streamlines and optimizes the process of researching, assessing, remediating, confirming, enforcing and reporting on patches.

The patch management conundrum

Patch management seems straightforward and yet is one of the most complex and critical challenges an organization faces. The nuances of effective patch management run much deeper than simply having a system administrator push out patches or relying on vendor-supplied patch mechanisms, hoping that they will be successfully applied but never knowing for sure. The patch management conundrum raises questions that many organizations may find difficult—if not impossible—to answer. For example:

- How should an organization deploy critical “out-of-band” patches that arrive urgently and off the routine patch schedule?
- How can system administrators keep track of patches in an environment with hundreds or hundreds of thousands of endpoints running a variety of operating systems and applications?
- How are system administrators supposed to monitor the status of roaming laptops and other mobile devices?
- How long will the patching process take from start to finish, and how will system administrators confirm (and prove) that every endpoint in their infrastructure has been properly patched—and stays that way?
- How can system administrators quickly test patches before deploying them and roll them back if they cause problems?
- How can patches be deployed without interfering with end-user experience and productivity?

While surveys show that patch management is one of the most important security priorities for organizations, these questions indicate just how many barriers organizations face when implementing effective patch management practices. Between a lack of visibility and personnel, potential business impact, network bandwidth limitations, lack of manageability, long remediation times, scalability issues, and coverage for different platforms, third-party applications and roaming endpoints, the hurdles are many.

Fortunately, these hurdles are surmountable. Tivoli Endpoint Manager removes these obstacles with a comprehensive solution that is purpose-built for highly distributed, heterogeneous environments. With this solution, organizations can finally see, change, enforce, and report on patch compliance status in real time, on a global scale, through a single console.



With Tivoli Endpoint Manager, patch management becomes a fully unified, closed-loop process that helps enhance security and save money.

Changing the patch management paradigm

While there is no single, official patch management best practice, the general approach involves a closed-loop process with six basic steps: research, assess, remediate, confirm, enforce, and report. Historically, many of these steps were implemented via separate, non-integrated technologies, making it virtually impossible to create a closed-loop, real-time patch management process. Tivoli Endpoint Manager provides all of these steps as part of a unified, fully integrated process that can help enhance security and save money, time, and resources.

Here is a before-and-after look at how this solution changes the rules for patch management.

Step 1: Research

Before: The first step in the patch management process involves discovering which patches are available. This includes researching patch availability through vendor email messages, application pop-up notifications, websites, blogs, and a variety of other sources. This process must be repeated weekly—or even daily—for hundreds of patches, across scores of operating system, application and anti-malware vendors. One alternative—relying on default vendor auto-updates—may lead to mistakes that can have negative consequences, because automating acceptance of patches without testing them can put organizations at huge risk, there is no enterprise control over timing or reporting, and relying on users to apply updates is risky and unreliable.

A better approach is to have a patch management vendor provide a consolidated stream of the most common patches so that the organization only needs to evaluate each load of patches as they come in, test them for compatibility with the organizational environment, and then deploy them via highly granular policies targeted to specific machine profiles, because it allows specific patches to be applied only to the endpoints that need them. The problem with this approach is that if not automated, it requires significant time and resources that organizations may not have.

After: IBM acquires, tests, packages and distributes patches from operating system, anti-malware and common third-party application vendors directly to customers, removing considerable patch management research overhead. When a supported vendor releases a new patch, IBM receives the patch, conducts preliminary analysis and creates patch policies, called IBM Fixlet® messages, which wrap the update with policy information such as patch dependencies, applicable systems, and severity level. Fixlets are then automatically sent to Tivoli Endpoint Manager customer servers. The solution also provides a process wherein customers can configure the product to download patches directly from vendor sites or store the patch content locally; customers may also create their own custom Fixlets using a wizard-driven interface. This process works for virtually any update, including internal application patches.

Step 2: Assess

Before: For each identified patch, the IT organization must determine the applicability and criticality of the update, identifying which endpoints need patching across the organization. In the case of security updates, this critical data translates directly into risk, as business risk increases with the number of unpatched endpoints. Many organizations do not have access to the complete, current asset and configuration data set required to quantify the scope and impact of patches across the organization. There are tools that can help acquire this data, but many require days or weeks to collect and collate this information by scanning every endpoint on the network—and many roaming endpoints are rarely connected to the network—a process which can take days to complete. This information must be immediately available to system administrators at the time of patch release since many patches are time critical, and the process of risk assessment and patch prioritization must take place as quickly as possible.

After: With Tivoli Endpoint Manager, a single intelligent software agent is installed on all managed endpoints to continuously monitor and report endpoint state, including patch levels, to a management server. The agent also compares endpoint compliance against defined policies, such as mandatory patch levels and standard configurations. This information is especially critical during emergency patch scenarios when a vendor releases a highly critical, out-of-band patch, and organizations must rapidly quantify the overall magnitude and risk from the related exploit(s). In one example, a customer using Tivoli Endpoint Manager installed agents on 5,100 endpoints and discovered that over 1,500 (30 percent) of their endpoints were missing at least one critical patch. Taken as a whole, endpoints across the institution were missing 20,033 “critical” patches—an average of 13 patches per endpoint. Once the total number of patches is mapped to the endpoints that need them, and the business criticality is defined, the IT organization can proceed to the remediation step.

Step 3: Remediate

Before: After a patch is assessed and a determination is made to distribute it across the organization, it must be packaged and tested to ensure that it will not conflict with other patches and third-party software installed on the target endpoints. Patch prerequisites and dependencies, such as minimum service pack levels, must also be determined. This is usually accomplished by applying and testing the update on a select number of endpoints before a general release—a process that can take days or weeks to complete using manual tools. Once testing indicates that the patch is probably safe for organization-wide deployment, it is applied to affected endpoints, typically in batches, further extending the patch window. Long remediation times are primarily due to the inability to rely on patch quality, and secondarily due to unreliable distribution mechanisms, both of which result in low first-pass patch rates. Most organizations are therefore forced to proceed slowly in case a patch causes an unforeseen problem, as well as to ensure that network links are not overwhelmed by the patch distribution process. As a result, remediation is often difficult to accomplish quickly and effectively on an organizational scale.

Another major problem is that many patch management tools only work for Microsoft® Windows® due to dependencies on Microsoft tools like Windows Server Update Services (WSUS). Many tools also require deep platform expertise and highly trained personnel to operate them. Many of these tools do not work until endpoints are connected to a high-speed corporate network, leaving roaming laptops and other mobile endpoints out of the update cycle for long periods. Many do not provide the fine-grained, policy-based controls that operators need to effectively deploy patches to all affected endpoints in the organization. Controls such as patch installation time windows, whether or not a user must be present, reboot options, the method of distribution (including bandwidth and CPU throttles), system type, and user notification options must be available inputs into the automated update processes.

After: When IBM publishes new patch Fixlets via Tivoli Endpoint Manager, organizations can determine the scope of the update by creating a report in minutes that shows which endpoints need the update. The patch Fixlets include distribution instructions, including OS, version, and prerequisite requirements, eliminating the need for IT to “package” and thoroughly test the patch. Operators can then spend a few minutes determining when the patch should go out, what notification to display to end users (if any), whether or not to allow users to delay a patch implementation and for how long, and whether to force (or delay) reboots. Within minutes, the endpoint agent receives the new policy and immediately evaluates the endpoint to determine if the patch is applicable, and if so, it downloads and applies the patch, reporting back success or failure within minutes. This approach, combined with Tivoli Endpoint Manager’s relay structure and ability to reach Internet-connected devices, significantly reduces network load and improves first-pass success rates to 95+ percent.

The solution also provides a highly secure mechanism that employs cryptographic identities, ensuring that only authorized administrators can create and distribute policies. Moreover, since no Active Directory dependencies exist, Tivoli Endpoint Manager administrators do not need to be Active Directory domain administrators. The solution stores audit information that tracks who ordered which policies to be applied to which endpoints, and does not require specific operating system expertise for operators that initiate the remediation process. Any Tivoli Endpoint Manager operator with a few hours of basic training can safely and rapidly patch Windows, Linux®, UNIX®, and Mac operating systems with no domain-specific knowledge or expertise.

Step 4: Confirm

Before: After patches are scheduled to be applied, successful installation must be confirmed so that IT knows when the patch cycle is complete, and to support compliance reporting requirements. This data should be communicated back to a central reporting system that updates personnel on the process, including exceptions, in real time. However, many patch management technologies do not effectively perform this process, requiring weeks to re-scan all endpoints and even longer to correct exceptions. This lag time introduces significant uncertainty around the organization's overall business risk and compliance posture.

Many products do not provide confirmation that patches are applied—or if they do, it can take days or even weeks to obtain an organization-wide report. Even worse, some tools incorrectly report that patches are applied when in fact the files were downloaded but the patch was not actually applied. With this amount of delay and uncertainty, some endpoints are often left exposed, leaving a significant window of vulnerability.

After: Once a patch is deployed, the Tivoli Endpoint Manager agent automatically and continuously reassesses the endpoint status to confirm successful installation, immediately updating the management server in real time (or in the case of roaming devices, at the earliest opportunity). This step is critical in supporting compliance requirements, which require definitive proof of continuous patch installation. With this solution, operators can watch the patch deployment process in real time via a centralized management console, receiving confirmation of patch installation within minutes of initiating the patch process. Closing the loop on patch deployment enables organizations to ensure patch compliance in a way that is smarter, faster and much more reliable.

Step 5: Enforce

Before: After the initial application, many updates do not always “stick.” Users intentionally or accidentally uninstall patches, new applications or patches may corrupt existing updates, malware may deliberately remove patches, or problems created by the update may necessitate a rollback. Patch management technologies must continuously monitor machines to ensure compliance with update policies, providing rapid, policy-based rollback capabilities in the event of a major patch problem. If a patch is removed contrary to security policy, it must be immediately reinstalled, and if a patch creates a major problem after application, organizations must also be able to issue a rapid mass rollback. Without the proper tools, this step becomes next to impossible.

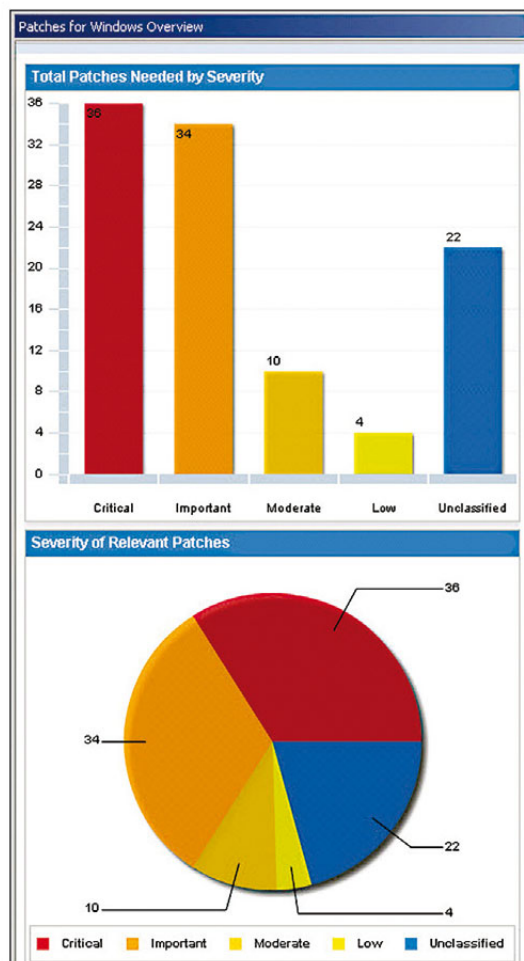
After: The Tivoli Endpoint Manager intelligent agent continuously enforces patch policy compliance, ensuring that endpoints remain updated. If a patch is uninstalled for any reason, the policy can specify that the agent should automatically reapply it to the endpoint as needed. In the event of problems with a patch, Tivoli Endpoint Manager administrators can quickly and easily issue a rollback to endpoints—either en masse or to a select few. Through the same centralized console, endpoint compliance status is reported in real time, allowing IT administrators to easily monitor the state of all managed endpoints in the organization.

Administrators enjoy full control of their endpoints, allowing them to handle many times the quantity of work of other products that require significant manual intervention and introduce significant time lags into the reporting process.

Step 6: Report

Before: Reporting is a critical component of the patch management process. Compliance and corporate policies require highly detailed, up-to-date dashboards and reports that indicate the organization’s risk position and patch management status for a variety of consumers, including compliance auditors, executives, management and even end users. Without an overall solution, there is no clear-cut way to report on patch status organization-wide.

After: Tivoli Endpoint Manager’s integrated web reporting capabilities allow end users, administrators, executives, management and others to view up-to-the-minute dashboards and reports that indicate which patches were deployed, when they were deployed, who deployed them, and to which endpoints. Special “click through” dashboards show patch management progress in real time.



Dashboard reports in Tivoli Endpoint Manager show patch management progress in real time.

Why it works

Traditional patch management approaches utilizing manual processes and cumbersome scan- and poll-based mechanisms are no longer fast or cost-effective enough to meet business and regulatory requirements, leaving organizations with unacceptably high risk and costs. Many organizations that try to utilize “free” or low-cost vendor tools such as Windows Server Update Services (WSUS) quickly realize that these solutions are not enterprise-class. They are limited to a single vendor, do not provide organizational control over what patches go where and when, are disruptive to the end user, and offer poor reporting that does not reflect real-time status. WSUS is a perfect example of a point product used to accomplish just one step in the patch management process outlined above, yet it is used because it is viewed as “free.”

Microsoft has introduced regular patch release cycles, known as “Patch Tuesdays,” which have unfortunately also spawned “Hack Wednesdays,” during which cyber criminals are provided golden opportunities to exploit un-patched endpoints without having to work to uncover new vulnerabilities. Endpoints not immediately patched become a window of opportunity for criminals—and a window of organizational risk. Moreover, organizations need to manage updates for a wide variety of vendor products and hardware form factors—not just Windows.

Tivoli Endpoint Manager leads the market in terms of breadth of coverage, speed, automation and cost-effectiveness, providing comprehensive operating system and third-party application patches. The solution, which includes deploying a single multi-purpose, lightweight intelligent agent to all endpoints, supports a wide variety of device types ranging from servers to desktop PCs, “roaming” Internet-connected laptops, and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks.

A single management server can support up to 250,000 endpoints, regardless of their location, connection type and speed or status, and additional servers can provide virtually unlimited scalability. Policy-based controls provide IT administrators with fine-grained, highly automated patch management capabilities, and comprehensive reports support compliance requirements. Policy compliance is continuously assessed and enforced by the intelligent agent, regardless of endpoint connectivity to the network. Other products are back-end heavy, requiring massive amounts of hardware and personnel to support deployments—in many cases, dozens, scores or even hundreds of servers, multiple agents per endpoint, and an army of operators—to support the same environment that Tivoli Endpoint Manager handles with one management server, one endpoint agent, and as little as 1/20th of the personnel.

Another key aspect of the architecture is support for endpoints that are on and off the corporate network. Roaming devices like laptops, for example, can receive patches via any Internet connection such as Wi-Fi or even dialup. The patch management process is virtually transparent to the user, and IBM Fixlet messages control the total amount of bandwidth and CPU consumed by the endpoint agent, which is location- and connection-aware to optimize network usage.

Continuous compliance

Many organizations need to establish, document and prove compliance with patch management processes in order to comply with governmental regulations, service level agreements (SLAs) and corporate policies. Regulations such as Sarbanes-Oxley, PCI DSS and HIPAA/HITECH require that a regular, fully documented patch management process be in place, and proof of continuous compliance is necessary in order to pass audits. Unfortunately, many organizations spend an enormous amount of time and resources on patch management, yet still cannot meet compliance requirements. The ability of Tivoli Endpoint Manager to enforce policies and quickly report on compliance can help improve an organization’s audit readiness and pass rates.

How customers are using it

Organizations are meeting the challenges of patch management head-on using Tivoli Endpoint Manager. For customers, the results have included faster deployment, better compliance, reduced IT costs and shorter management cycles.

Challenge: Deploying patch management in days or weeks—not months or years

- Albany County, NY, consolidated a number of patch and configuration management tools in just two days.
- O'Charley's Restaurants deployed patches to over 350 restaurants in just four days.
- SunTrust Banks implemented a solution to 50,000 endpoints spread across nearly 1,800 locations in three months with just two people.
- International Islamic University Malaysia completed a full deployment on 7,000 fixed and mobile computers across seven bandwidth-constrained university campuses in just six weeks.

Challenge: Achieving compliance with SLAs, corporate policies and regulations

- Purolator achieved 100 percent compliance with a 24-hour SLA from their managed service provider.
- SunTrust Banks achieved 98.5 percent patch compliance across 50,000 endpoints.
- Concord Hospital increased patch compliance from 40 to 60 percent, to 93 percent.

- Entergy IT, which must comply with SLAs that require patch deployment across more than 22,000 endpoints within a 10-day window of release, has deployed over 4.9 million patches across the enterprise since 2004—and has not missed a single SLA during this time.

Challenge: Reducing IT costs

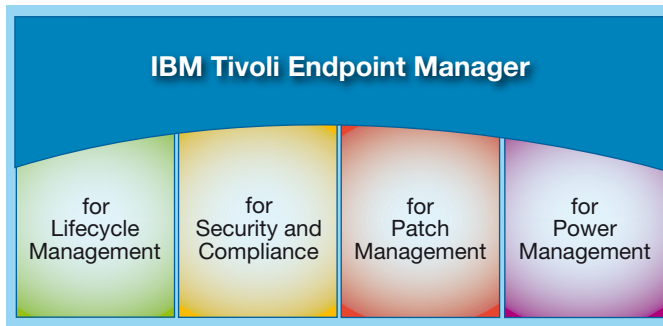
- BGC Partners eliminated expensive travel to remote service branch offices across six continents, saving tens of thousands of dollars.
- Tax Tech reduced patch management full-time equivalents (FTEs) by 20 to one.
- Stena Lines achieved a 12:1 labor savings ratio by reducing administrative overhead time for patch processes from 240 hours to 20 hours.
- Western Federal Credit Union reported a 50 percent reduction in labor costs through automation and unified patch management.

Challenge: Reducing patch management cycles

- Concord Hospital decreased patch cycles from weeks to just 15 minutes.
- SunTrust Banks reduced patch cycles from two to three weeks to two to three days.
- Tax Tech fully automated overnight patch distribution to 1,000+ locations connected via VPN.
- Entergy's desktop and server management group installed 70,000 patches across the enterprise in 24 hours.
- Kronos distributes software updates, policies, and patches to all eligible endpoints within 15 minutes across the globe.

A comprehensive portfolio of endpoint management and security solutions

IBM offers patch management capabilities through a stand-alone product—IBM Tivoli Endpoint Manager for Patch Management—or as an integral part of two larger endpoint management solutions—IBM Tivoli Endpoint Manager for Lifecycle Management and IBM Tivoli Endpoint Manager for Security and Compliance. The Tivoli Endpoint Manager family all operates from the same console, management server and endpoint agent, enabling organizations to consolidate tools, reduce the number of endpoint agents, and lower management costs.



IBM Tivoli Endpoint Manager is a family of products that all operate from the same console, management server and intelligent endpoint agent.

Tivoli Endpoint Manager is part of a comprehensive IBM security portfolio, helping organizations address security challenges for users and identities, data and information, applications and processes, networks, servers and endpoints, and physical infrastructures. By enhancing real-time visibility and control, and improving endpoint security and management, the IBM portfolio supports today's ever-expanding, smarter data centers to facilitate the instrumented, interconnected and intelligent IT operations of a smarter planet.

Tivoli Endpoint Manager technology provides:

- **A single intelligent agent**—Tivoli Endpoint Manager utilizes an industry-leading approach that places a single intelligent agent on each endpoint. This agent performs multiple functions including continuous self-assessment and policy enforcement—yet it has minimal impact on system performance, using less than two percent of the endpoint CPU on average. The agent initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations or other information to the endpoint when necessary to comply with a relevant policy. As a result of the agent's intelligence and speed, the central management server always knows the compliance and change status of endpoints, enabling rapid and up-to-date compliance reporting.

- **Instant answers**—Whether it's finding out how many instances of Adobe® Acrobat are installed or validating which laptops are impacted by a manufacturer recall, Tivoli Endpoint Manager provides answers within minutes—across the organization. Thanks to the intelligent agent, there is no need to wait for lengthy scans to complete, a centralized server to churn on the details, or thousands of SQL queries to finish running before dashboards and reports are generated. Each agent evaluates the relevance of the question, analyzes the information, reports back, and even takes action based on the analyses if desired.
- **Coverage for roaming endpoints**—The corporate-owned laptop has moved well beyond the confines of a corporate office. Users are connecting from home, hotels, airports, and even airplanes. Always staying a step ahead, Tivoli Endpoint Manager provides the unique ability to manage endpoints in real time—even for roaming devices.

Conclusion

Tivoli Endpoint Manager addresses key challenges that many organizations currently face, providing a centralized, organization-wide server, desktop and mobile device patch management solution that automates and alleviates much of the patch testing process from IT. Tivoli Endpoint Manager deploys in days, and a single management server supports up to 250,000 endpoints, drastically increasing patch success rates, improving regulatory compliance and reducing expenditures.

In a world where seconds matter, Tivoli Endpoint Manager can be the difference between a successful patch management strategy and one that leaves the organization at risk.

For more information

To learn more about IBM Tivoli Endpoint Manager, contact your IBM sales representative or IBM Business Partner, or visit: ibm.com/tivoli/endpoint

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: ibm.com/financing



© Copyright IBM Corporation 2011

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

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

IBM, the IBM logo, ibm.com, BigFix and Tivoli 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

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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.

¹ <http://cybersecureinstitute.org>



Please Recycle