

IBM Tivoli Endpoint Manager: Control for retail environments

Enhancing compliance and reducing costs, even for locations without onsite IT support



Highlights

- Manage endpoints across widely distributed environments
 - Enhance compliance with PCI security standards
 - Gain centralized control for diverse operating systems and devices, including POS devices
 - Manage roaming endpoints that are intermittently connected via the Internet
-

The distributed nature of the retail industry is a boon to customers and an opportunity for sales. But it can be a headache for IT. Rare is the retail organization that can put IT staff at each of its locations. So how can a company manage what may be hundreds of thousands of computing devices—everything from servers to point-of-sale (POS) terminals, self-service kiosks, desktop computers and roaming laptops—in worldwide locations?

How can it implement changes across the network? See the results of those changes in real time? Discover devices connected and not connected to the network? Protect against data leaks, security breaches and access by rogue devices?

How especially can the retail organization ensure compliance with Payment Card Industry Data Security Standards (PCI DSS)? How can it configure each device for regulations covering areas such as security, vulnerability management, patch management and endpoint protection?

This is how two companies did it.

When the number of business units requiring PCI DSS assessments nearly tripled, IT administrators at one major retailer faced weeks of manual, labor-intensive procedures to collect and correlate compliance findings. By implementing a new endpoint management solution, they were able to automate system updates and improve audit procedures dramatically.



When another retailer received high numbers of false positive alarms from its monitoring software, it needed to know whether the reports reflected unauthorized changes or not. By implementing a new endpoint management solution, they were able to deliver accountability for server and POS changes and reduce false positives by 80 percent.

Each of these companies implemented IBM® Tivoli® Endpoint Manager, built on BigFix® technology. This solution's centralized and automated capabilities for distributed endpoint management provide visibility and control to support compliant, secure and responsive retail environments.

Supporting an increasingly complex retail ecosystem

In a world where systems and information are more instrumented, integrated and intelligent than ever before, customer expectations, retail opportunities and supply-chain complexities have reached new heights. Customers know more about products and pricing for a company's offerings—and for its competitors. The retail organization gathers more information on customer behavior and market trends. And supply chains have more links across a longer reach.

Supporting this wide-ranging ecosystem are thousands of computing devices that have to be maintained. They have to work together fast and seamlessly to provide the consistent customer experience and effective business operations necessary for success.

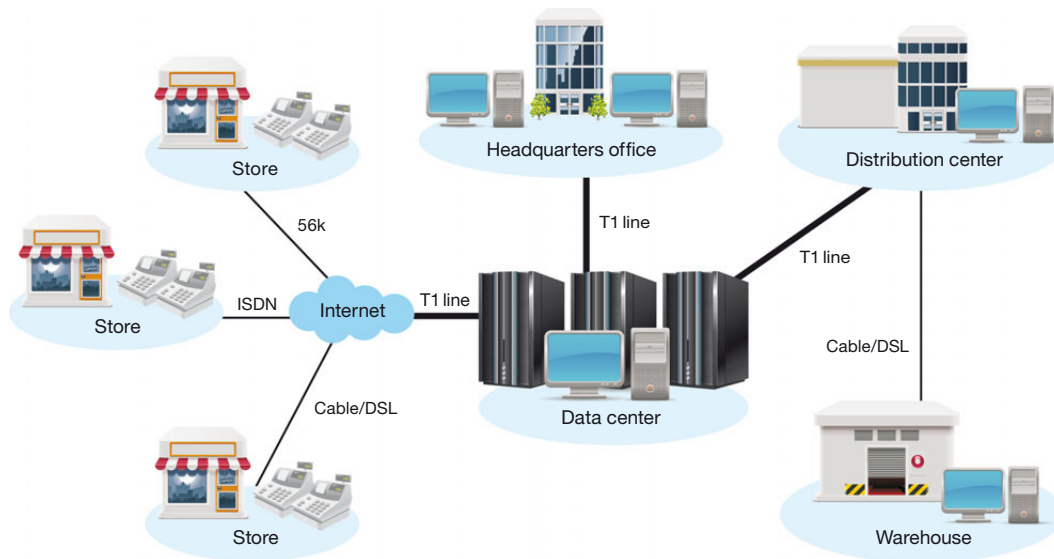
A national retailer, for example, mothballs large numbers of computers and POS terminals when they are not needed in the off season. During the times of year when sales accelerate, the company must quickly bring those systems back into service. It has to locate and inventory its equipment. And it likely will have to do some catching up as quickly as possible—installing new software versions, applying patches and updates, and otherwise bringing each machine up to the current state of corporate technology and compliance to ensure that they are secure and ready to transact business.

Retail environments face unique challenges

Retail environments face distinct challenges to achieving effective, efficient endpoint management. These challenges include:

- **Heterogeneous infrastructures and a wide variety of devices.** Retail endpoints often include servers and desktops as well as POS terminals, embedded PCs in cash registers, kiosks, and wireless/mobile inventory tracking devices. They often run a variety of operating systems, including Microsoft® Windows, Linux®, Unix® and Mac.
- **Requirements for “always up” availability.** Store-based devices operate as front-end data collection nodes that feed information back to headquarters, distribution centers and suppliers. These are mission-critical devices—in many cases, business cannot be transacted without them. High availability for the supply-chain infrastructure is essential, so operations tasks need to be completed and validated quickly and transparently.
- **Ever-increasing compliance requirements.** While PCI DSS is the most common retail compliance standard, retailers must increasingly contend with Sarbanes-Oxley, the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA) and other requirements. Typical compliance activities often are reactive—triggered by an upcoming audit rather than conducted continuously, forcing organizations to get systems into compliance within difficult time frames.
- **Cost and efficiency pressures.** Retail competitiveness often revolves around being the low-cost supplier of a good or service. Spending on IT is often a low priority for management, who feel pressure to deliver cost savings. Yet manual, labor-intensive IT processes both increase the cost and decrease the efficiency of endpoint management.
- **Poor visibility into systems.** In a distributed environment, it's hard to know what is installed on each endpoint, whether new software has been delivered and installed correctly, and which endpoints need which patches. Poor visibility makes it difficult to manage compliance. It exposes the organization to technology and business risks including spending on software that may be unauthorized or unnecessary.

IBM Tivoli Endpoint Manager for retail environments



- **Slow implementation and response times.** When retail networks stretch across a region, a country or the globe, infrastructures can struggle to keep up. Many run over low-bandwidth, high-latency networks. As a result, system and security management tasks such as software distribution can take up a high percentage of available bandwidth, slowing network performance, end-user productivity and the ability to transact business.

Managing the wide diversity of POS devices

Particularly in bricks-and-mortar businesses, retail infrastructures are widely distributed with only a few computers in each location. Tivoli Endpoint Manager meets this and related challenges with a centralized management solution that performs

multiple tasks across multiple platforms and devices. Its unified console and easy-to-use graphical user interface provide visibility to keep track of all endpoints, show exactly what is running on each, and support using this information to optimize budgeting and security decisions for upgrades, change control, and other asset-related initiatives and expenses.

With the ability to support up to 250,000 endpoints from a single management server, regardless of their network connectivity, Tivoli Endpoint Manager is an ideal platform for asset management, software inventory and distribution, vulnerability assessment, automated malware defense, compliance and policy enforcement, power conservation and patch management—without compromising network performance or end-user productivity.

In environments where POS systems dominate, Tivoli Endpoint Manager meets the enormous challenges posed by a vast quantity and diversity of these devices. Endpoint management must overcome circumstances unique to retail such as random reboots by untrained staff, extremely low bandwidth, unreliable connections including modem and satellite links, and separate download and control channels.

Management systems must accommodate unique retail opportunities such as “tax holidays,” which require setting tax tables in POS devices to zero for a day and then returning to the normal rate. The retail organization needs tools such as Tivoli Endpoint Manager that can audit and enforce change on a large scale.

Overcoming PCI DSS compliance challenges

When an environment mixes large numbers of specialized technologies such as cash registers, POS terminals, kiosks and hand-held inventory tracking devices with large numbers of users not trained for systems administration, compliance can become an issue. Users’ interaction with devices can be a distraction from their main jobs—running a store or a restaurant and serving customers—that creates the potential for disrupting or violating IT administration and maintenance. In these cases, the need for centralized management becomes more acute than ever.

And the results of noncompliance can be significant. Customers are likely to avoid patronizing stores or restaurants where they think their personal data won’t be protected. Within the PCI community, credit card companies issue fines or suspend card privileges for merchants who don’t meet regulations.

Tivoli Endpoint Manager provides the visibility and control retailers need to meet PCI DSS compliance. For the set of requirements that concern data residing on the endpoint, the solution offers key advantages including:

- Continuous compliance, eliminating the need for costly, audit-focused compliance activity
- Rapid deployment in days or weeks, supporting up to 250,000 endpoints with a single management server and console
- Proven ability, helping multiple retail businesses manage remote, intermittently connected devices over low-bandwidth and high-latency links

Tivoli Endpoint Manager can secure and manage endpoints that house sensitive data regardless of the type of device. It can efficiently produce compliance reports—even over low-bandwidth connections—avoiding the need to gather information in person at each location or to conduct lengthy scans of every machine. By ensuring continuous assessment and remediation, it can replace slow, reactive compliance and audit procedures with faster, more effective processes.

Case study: Compliance for hundreds of locations

For O’Charley’s, Inc., a restaurant group operating more than 350 locations in the United States, cost-effective security and systems management have always been high priorities. Meeting PCI security standards is key among its security goals, but to manage the 2,100 PCs and PC-based POS terminals installed in its restaurants, O’Charley’s faced the daunting prospect of sending technicians around the country to install software, patches and updates in person.

As is common in retail environments, relatively slow 56k data lines connected the restaurants to the O’Charley’s data center, complicating remote administration and application processing. The company was able to deploy its Tivoli Endpoint Manager solution across all its distributed equipment within days, creating a centrally managed system that enables remote management and reduces IT workload and related costs.

Meeting compliance requirements at the endpoint

Tivoli Endpoint Manager addresses the following PCI DSS standard requirements. For each requirement, there are two tasks: implementation and validation. Tivoli Endpoint Manager helps with either or both of these tasks for the requirements listed.

Description	Solution component	Implementation	Validation
Implement personal firewall software on mobile and/or employee-owned computers used to access the organization's network via the Internet	Personal firewall functionality ensures consistent policy enforcement and system protection whether installed on a fixed desktop or a roaming laptop.	√	√
Always change vendor-supplied defaults for items such as passwords and SNMP community strings before installing a system on the network.	Configuration management enables assessing and enforcing compliance with corporate and PCI data security standards.		√
For all system components, develop configuration standards that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Configuration management covers security parameters such as ensuring production systems are hardened by removing unnecessary services and protocols.	√	√
Deploy antimalware software on all systems (particularly personal computers and servers) commonly affected by malicious software.	Multiple antimalware options deliver real-time visibility, scalability, and unified management	√	√
Ensure that all antimalware mechanisms are current, actively running and capable of generating audit logs.	Antimalware features consolidate management to inform IT not only about which endpoints are about to fall behind or already have fallen behind in their antivirus definition updates but also about endpoints running non-standard and rogue applications.	√	√
Develop and maintain secure systems and applications.	Features for vulnerability, patch and security configuration management provide best in-class capabilities.	√	√
Regularly test security systems and processes.	Security configuration and vulnerability management features include host-based vulnerability assessment with severity scoring, ability to define and assess compliance to security configuration baselines, and ability to set alarms for anomalous conditions or suspected rogue activities.		√

For more information

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



© Copyright IBM Corporation 2011

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

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

IBM, the IBM logo, ibm.com, 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

BigFix is a registered trademark of BigFix, Inc., an IBM Company.

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.



Please Recycle

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.