BIGFIX

Bringing retail endpoints into compliance (and keeping them there)

HOW BIGFIX SUPPORTS THE PCI STANDARD

BigFix's high performance systems and security management is uniquely positioned to provide retailers with the visibility and control needed to effectively meet PCI compliance. For the set of PCI requirements that concern data residing on the endpoint, BigFix stands apart in offering several key competitive advantages:

- Continuous compliance, which eliminates the need for costly, audit-based compliance activity
- Rapid deployment in some of the most challenging and mission-critical retail environments
- Proven ability to help multiple retail clients centrally manage tens of thousands of remote, intermittently connected devices over low bandwidth/high latency links

These capabilities help to contain costs, improve speed to audit, and ensure continuous assessment and remediation with little to no end user impact.

> "In our environment, getting machines up to speed for an audit was an intensely time-consuming, expensive process, because we operate on multiple platforms, have extremely limited bandwidth to our stores and distribution centers, and needed to send IT support staff to many affected sites. With BigFix, we have automated many of our compliance-related activities, and they take place on an ongoing basis—so time to audit is minimal, with no additional cost or resource requirements."
>
> *—Large Retail Customer with a network of over 150,000 endpoints*

Retail IT Compliance and Operational Challenges

No single solution exists that addresses all of the PCI compliance challenges end to end. For retail and other organizations to successfully meet compliance requirements, they must combine components that most effectively meet a subset of the requirements, piecing together an overall PCI solution.

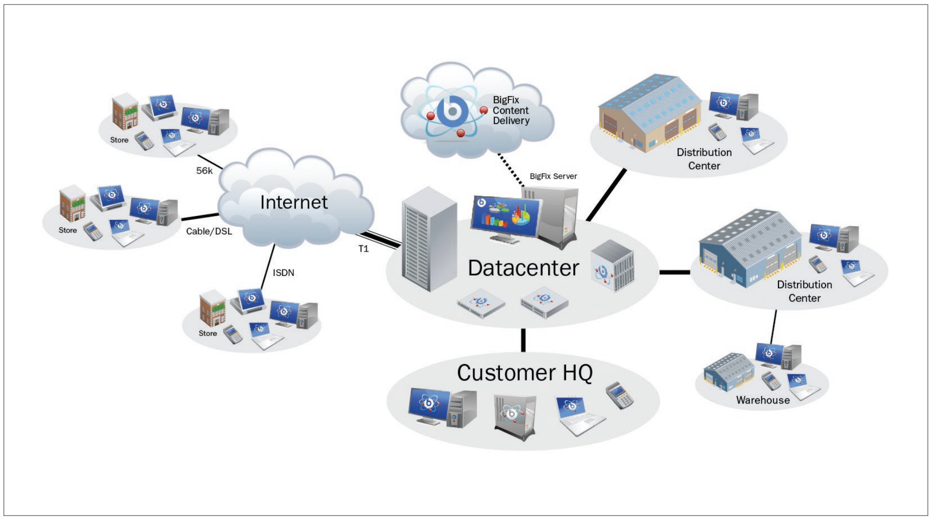
BigFix fits into this overall solution by securing and managing endpoints that house sensitive data, whether the endpoint is a desktop computer, a server, or a roaming laptop. BigFix provides a number of capabilities that meet PCI DSS requirements both through specific products and through the overall BigFix technology's visibility, policy enforcement, and customization features.

In an ideal world, retailers would be able to devote full attention to their business, delighting their customers, addressing time to market and budget constraints, and so on. Instead, PCI compliance often forces a shift of focus to the IT/back-end component of an organization. The following characteristics of the retail environment add to the complexity and challenges of attaining PCI compliance:

- Highly distributed IT infrastructures operating over low-bandwidth, high latency links
- Close ties between retail systems and supply chain systems
- Intense cost and efficiency pressures
- A reactive compliance stance that negatively impacts speed to compliance

For each of these challenges, the BigFix solution offers a feature that helps promote compliance for the retail customer:

Challenge: Retail IT infrastructures tend to be highly distributed, and management must be conducted over bandwidth-constrained links. Particularly with bricks-and-mortar retail, infrastructures are spread across a region, the country, or the globe, with only a few computers per location.



BigFix is purpose-built for managing systems over highly distributed, bandwidth-constrained networks

These can be a mix of desktop computers and embedded Windows devices in cash registers, point of sale terminals, kiosks, and wireless/mobile inventory tracking devices. Because typical end users of these devices are not trained in systems administration, their interaction with these devices can be a distraction from their main jobs—running a store or restaurant, serving customers, and so on—and creates the potential for "breaking" IT administration security and maintenance processes. Compounding the problem of wide distribution, retail infrastructures typically run over low-bandwidth, high latency networks. As a result, systems and security management tasks can take up a high percentage of available bandwidth, slowing network performance—and end user productivity.

BigFix Solution: Effective remote service delivery over low-bandwidth/high latency networks. The "smart client" BigFix architecture works very well in the low-bandwidth networks typically seen in retail environments, such as satellite, shared MPLS, VSAT, and "skinny" networks of 56Kbps or less. In fact, with BigFix one global hotel chain was able to push Windows XP Service Pack 2 to all of its endpoints in a single day—despite having links of only 8Kbps. BigFix users can reach out and touch distributed networks without physically dispatching service personnel or requiring action from end users. This saves tremendous amounts of money in time and travel, decreases the potential for errors and eliminates end user productivity distractions.

Challenge: Retail systems are closely tied into ERP/logistics supply chain systems. A cash register, point of sale terminal, or inventory-tracking device is really a front-end data collection node, feeding mission-critical information back to headquarters, to distribution centers, or even directly to suppliers. Thus, adding compliance tools to the infrastructure creates concerns about disrupting the supply chain.

BigFix Solution: Remote computing management. BigFix can consolidate management of remote devices such as distributed servers and roaming laptops. Maintaining tight controls on these devices helps ensure a well-performing and "honest" supply chain. Because the lightweight BigFix Agent consumes less than 2% CPU on average, there is no impact to end users of mobile devices.

Challenge: Cost and efficiency pressures are always intense. For retailers, competitiveness revolves around being the low-cost producer of a good or service. Thus, management is often reluctant to spend money on IT, and IT staff may feel pressured to advocate for and deliver cost savings from the bottom up.

The Real Costs of Noncompliance: Fines and Lost Business

Many of the forces driving the development of the PCI standards are intangible. Data leaks and breaches make big, unpleasant news, damage reputations, and turn off customers. Customers won't buy from places where they think their privacy isn't respected or protected.

However, noncompliance can lead to other measurable effects as well.

Within the PCI community, credit card companies have started issuing fines to merchants caught storing magnetic stripe data, These fines start at $10,000 a month for the first three months; escalate to $50,000 a month for the next three months; and rise to $100,000 a month for all months thereafter. At least forty-four states have enacted privacy laws that require businesses to notify customers of loss of personal information and allow those customers to sue for civil damages.

Beyond fines, organizations found out of compliance with PCI face jail terms or loss of the ability to accept credit cards payments—which would effectively put many retail establishments out of business.

BigFix Solution: Cost containment. BigFix helps reduce costs in a number of ways:

- Because the BigFix Agent enforces compliance on the endpoint, BigFix solutions require an absolute minimum of additional, dedicated management infrastructure. A single $5,000 class off-the-shelf server is capable of managing infrastructures of up to 250,000 managed endpoints. BigFix solutions can scale to address almost any size retail infrastructure, from hundreds to hundreds of thousands of managed endpoints.
- Time to implementation can be measured in days for most customers, enabling rapid time to value.
- Continuous compliance enforcement by the agent and real-time endpoint visibility makes the audit process extremely cost-effective.
- Process improvements afforded by other integrated capabilities, such as patch management, NAC, and software updates, cut time and labor costs.

Challenge: Speed to audit compliance is compromised by lack of continuous compliance monitoring. Most retail PCI compliance solutions available to date have been reactive—that is, compliance activities are triggered by an upcoming audit rather than conducted continuously. Because of this reactive nature, many organizations struggle to get systems into compliance within the time frame presented by the audit.

BigFix Solution: Continuous compliance. BigFix monitors and remediates compliance continuously, in real time, so there is never a need to rush for an audit—or a worry about being out of compliance for an audit. BigFix not only assesses compliance problems, it fixes them in real time.

In addition to the specific features listed above, the BigFix solution offers the following high-level benefits for retail customers working toward the objective of PCI compliance:

Infrastructure consolidation. BigFix can replace a number of point tools, reducing licensing costs, administrative complexity, and clutter. BigFix's multiplatform capabilities also simplify administration of heterogeneous environments. BigFix has the ability to service environments running multiple generations of Windows as well as Unix, Linux, Mac, mobile, and virtualized computers from a common console and management infrastructure.

Real-time visibility. Not only does pervasive real-time visibility vastly improve management oversight over remote/distributed computers, but it can help instantly flag problems such as unauthorized software on machines.

Reporting. Implementation is only one component of compliance; validation is the other. Reporting is a key tool in presenting compliance results to auditors and regulators. Complementing BigFix's continuous assessment are reporting options that enable an organization to prove compliance whenever requested.

Drawbacks to Existing Compliance Approaches

As mentioned, the entire PCI compliance arena is a relatively recent phenomenon. Thus, it is not surprising that many compliance solution efforts have demonstrated significant disadvantages. These drawbacks fall into two broad categories: One, because of the lack of continuous compliance, organizations find themselves constantly assessing and correcting changes—which puts pressure on both the administrators and the existing architecture and leaves an organization exposed between assessments. Two, these solutions very often fail to provide the scalability, visibility, and flexibility required for complete compliance across all systems within the unique challenges of IT in the retail industry. With these approaches, companies are likely to be left taking a reactive approach towards the full spectrum of PCI requirements and systems—and may even be forced to leave some requirements unaddressed completely. This combination of issues accounts for the fact that recently only one-third of audited organizations were found to be in compliance with PCI.

Existing compliance solutions can be broadly grouped into the following models:

- Server-centric
- Network-based
- Manual/homegrown

Each of these models presents obstacles for retail IT organizations in attaining full compliance—and for each, the BigFix solution presents a contrasting approach that promotes compliance, as follows:

Legacy Model: Server-centric. Many information security solutions are based on a server-centric model, where most of the "work" is done by a central server. This architecture often requires many servers to manage a large number of endpoints, leading to a heavy infrastructure that involves high hardware costs and resource-intensive system management. Perhaps even worse for a retail environment, the server-centric model produces slow response times, as data needs to be pushed from the endpoint to the server for evaluation. This in turn causes high bandwidth consumption and a lack of real-time results, as the server can only analyze data pushed from the last scan—which might have taken place several hours before. In highly distributed retail environments, the end result of a server-centric model is either extremely high network traffic or an ever-escalating number of servers distributed out to manage various network links.

BigFix Approach: Processing at the endpoint. Because decision making and processing in the BigFix solution occurs continuously at the endpoint, infrastructure requirements are small, and results can be achieved in real time. Bandwidth throttling ensures that only minimal bandwidth (<2% CPU on average) is used for system management tasks, with the rest freed for user productivity—ensuring no end user disruption.

The Real Costs of Noncompliance: The Criminal Underground

It may sound like something out of a spy novel, but credit card trafficking has created a billion-dollar international criminal underground that thrives on hacking networks to steal valuable data.

The New York Times recently reported that stolen credit card numbers were on sale in membership-only cyberbazaars operated by people from the former Soviet Union. According to the report, credit card and identity theft costs the global financial system $1 billion or more a year.* In the infamous TJX case, where 45 million card numbers were stolen, it was reported that they sold for $20-$100 each, though lower-quality databases can go for as little as $.50 per record. Data is made available on websites that are posted for a few days only, making tracking extremely difficult.

Another rising cybercrime is blackmail, where a hacker will steal data or ruin a website to prove they have the capability, and then blackmail the victim company by threatening to make the data public. Unethical companies have even hired hackers to blackmail a competitor.

* Source: http://www.wired.com/techbiz/media/news/2002/08/54427

Legacy Model: Network-based vulnerability scanners. While this type of solution can alleviate the cost and management resource drain of the server-centric model, it contains a number of key limitations. Because these solutions must perform scans and then separately analyze the scan data, they cannot provide real-time results—which translates to an inability to provide continuous compliance. Additionally, network-based scanning often results in low accuracy rates, with high false positive percentages, simply based on the fact that specific configuration information can only be found on the endpoint, not through network probes and port scanning. Finally, most solutions of this type cannot perform remediation, so while they may provide information on an endpoint that is out of compliance, they do not have the ability to bring the machine back into compliance.

BigFix Approach: Host-based management. The BigFix solution provides full, real-time access to information not provided through explicit system APIs, allowing continuous assessment and automated enforcement and remediation. This ongoing, automatic enforcement reduces the possibility of risk due to configuration drift, and provides the ability to assess and enforce both on-network and off-network systems.

Legacy Model: Manual/homegrown scripts. Similar to the network-based approach, manual and homegrown scripts do not allow for robust, continuous compliance. Furthermore, these scripts are difficult to maintain and are not easily adaptable if policy changes occur.

BigFix Approach: Customization and integration. BigFix includes open interfaces and scripting capabilities that make it possible to add customer-specific capabilities to a BigFix solution and to integrate it into more comprehensive retail automation and payment card support solutions. BigFix customization capabilities offer customers options to create and enforce company-specific PCI compliance policies across their organizations.

Protecting Data at the Source:

The BigFix Solution Ensures Compliance at the Endpoint

BigFix components address the following PCI standard requirements. For each requirement, there are two tasks: implementation (I) and validation (V). BigFix components help with either or both of these tasks for the requirements listed.

Requirement	Description	BigFix Component	I	V
2.1	Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	BigFix Security Configuration Management provides the ability to assess and enforce compliance with corporate and PCI data security standards. This capability covers use of non-vendor-supplied passwords.		X
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	BigFix Security Configuration Management covers other security parameters such as ensuring all production systems are hardened by removing unnecessary services and protocols. Specifically, BigFix provides configuration checklists for FDCC, DISA STIG, and SANS vulnerability lists.		X
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Customers can choose BigFix's own Anti-Virus solution or manage existing anti-virus products with BigFix. In either case, customers benefit from the real-time visibility, scalability, and unified management provided by the BigFix platform.	X	
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	BigFix Client Manager for Anti-Virus can manage widely used third-party (McAfee, Symantec, Trend Micro, etc.) anti-malware clients. Consolidating management of heterogeneous clients through a common visibility and control infrastructure improves IT staff effectiveness. For example, BigFix can tell you not only which endpoints might have fallen behind in their anti-virus definition updates, but correlate this with endpoints that may be running non-standard and rogue applications.		X
6	Develop and maintain secure systems and applications.	BigFix Security Configuration and Vulnerability Management provides best in-class vulnerability, patch, and security configuration management.	X	X
11	Regularly test security systems and processes.	BigFix Security Configuration and Vulnerability Management consolidates key security configuration management services including security patch management. Features include host-based vulnerability assessment with severity scoring, ability to define and assess client compliance to security configuration baselines, and ability to set alarms to instantly notify administrators of anomalous conditions or suspected rogue activities.		X

BIGFIX™

Bring Your Distributed Environment Under Control with BigFix

BigFix is the only solution that provides pervasive real-time visibility and control in large, complex, distributed environments, especially those with bandwidth concerns and limited IT staff. BigFix addresses the needs of retail organizations looking to enable IT policy enforcement across a distributed and largely isolated retail and branch office real estate. In many environments, installing BigFix has significantly reduced system administrator workloads while improving the effectiveness of system management.

BigFix's Anti-Virus, Security Configuration Management, and Security Configuration and Vulnerability Management products, built on the BigFix platform, enable organizations to operationally implement technical controls to address many of the core PCI data security standards.

References

View the full standard:

- https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

General information about the standard:

- PCI Compliance Guide: http://www.pcicomplianceguide.org/
- CSO: http://www.csoonline.com/article/221189/All_About_the_PCI_Data_Security_Standard
- Cyber Security Alliance: http://www.csialliance.org/issues/pci_data_security_standard/index.html
- MasterCard: http://www.mastercard.com/us/sdp/index.html
- VISA: http://usa.visa.com/merchants/risk_management/cisp.html

About BigFix

BigFix®, Inc. is a leading provider of high-performance enterprise systems and security management solutions that revolutionizes the way IT organizations manage and secure their computing infrastructures.