HCLSoftware

Accelerate and Automate PCI-DSS Compliance

HCL BigFix Compliance PCI Add-on helps protect sensitive data, lower operational costs and mitigate noncompliance risk.

HCL BigFix

Table of contents

Introduction

Although new digital methods of payment have entered the marketplace, credit and debit cards are still hugely popular. In fact, they still account for two-thirds of all purchases. But the convenience of using payment cards also comes with a price—criminals can easily convert payment card data into cash, making the data a highly attractive target for attack.

To help safeguard sensitive customer data, organizations that process, store or transmit payment card data are required to comply with the Payment Card Industry Data Security Standard (PCI DSS). This global security program is designed to help protect against the theft, exposure or leakage of customers' personal and financial information. Failure to comply with the industry standard can result in significant fines, suspension of payment card privileges, litigation, brand damage, and loss of customer, partner and supplier confidence.

By maintaining PCI-DSS compliance, organizations are better positioned to keep data safe. Created in 2001, the industry-backed program is periodically updated to keep up with changing technology and evolving security threats. It establishes specific technology and operational requirements an organiza- tion must meet in order to comply with protection standards. Plus, the PCI Security Standards Council—comprised of card companies such as Visa, MasterCard, American Express and Discover—has proposed specific milestones to help organizations prioritize compliance efforts and focus on the greatest risks first.

The challenges of PCI-DSS compliance

Data security breaches are increasingly common—and can occur on a massive scale. In the past few years, breaches at major retailers have affected tens of millions of cardholders. And each new report of a data breach leaves consumers a little more concerned about their personal information being compromised. Meanwhile, the loss of business is not the only consequence if a security breach occurs. Noncompliant companies can be fined up to USD500,000 per incident. Audit requirements can increase, and credit card activity can be shut down entirely.

PCI-DSS compliance helps protect everyone involved in the payment card industry. Consumers can gain peace of mind, while companies can maintain a positive image, avoid fines and reduce the risk of data breaches. However, there are some key challenges in achieving PCI-DSS compliance, including:

Complex and changing requirements. PCI-DSS includes 12 core requirements, supported by more than 200 sub-requirements and more than 400 testing procedures. Understanding how to apply all of these to a specific environment can require a lot of time and a lot of work. In addition, the requirements keep expanding to respond to changing technology and evolving security threats, with the most recent version (PCI-DSS v4.0) released in March 2022.

The challenge for constant enforcement in complex environments. Today's organizations have to secure a variety of platforms and applications across geographically distributed locations. To maintain compliance in these complex environ- ments, they need global, real-time visibility. In fact, to stay ahead of advanced malware and emerging threats, continuous compliance enforcement is required; periodic assessments are not enough. The need for specialized skills and costly processes. The IT experts needed to map PCI-DSS requirements or testing procedures to platform- or application-specific configuration checks are generally in short supply. Manual processes to mitigate risks or remediate noncompliance can also be very time-consuming and costly.

Using BigFix Compliance to mitigate risk

As with many other things in life, having the right tools can make a world of difference. HCL BigFix Compliance can reduce the cost and complexity of maintaining compliance in today's highly distributed, heterogeneous environments. Using a sienagslye-to-manage, quick-to-deploy solution, organizations canhelp ensure continuous security compliance for a massively diverse range of endpoints—from servers to desktop PCs and "roaming" Internet-connected laptops, as well as specialized equipment such as point-of- sale devices, ATMs and self-service kiosks.

BigFix Compliance provides accurate, up-to-the-minute visibility of security configurations for all endpoints, both on and off the corporate network. It can automatically assess and remediate security policy configurations using thousands of best-practice checklists, based on benchmarks from Center for Internet Security (CIS), Defense Information Systems Agency Security Technical Information Guides (DISA STIG) and many more. An intelligent agent on every endpoint monitors, manages and reports on the security status of endpoints, regardless of the operating system (OS) type or location.

By using BigFix Compliance, organizations can:

Continuously enforce security policies in real time, regardless of the network connection status of an endpoint. This can significantly reduce overall security risk. Manage hundreds of thousands of endpoints, and discover unmanaged endpoints, regardless of location, connection, type or status. Automatically patch and remediate noncompliant systems, within a matter of minutes—reducing risk and labor costs.

Gain a single point of control for endpoint protection, centralizing updates and health-checks of third-party endpoint protection solutions. Help improve security with policy-based quarantines of noncompliant systems, disabling network access until compli- ance is achieved. This can help prevent malware propagation.

Achieving PCI-DSS compliance with BigFix Compliance PCI Add-on

BigFix Compliance PCI Add-on extends the capabilities of BigFix Compliance with more than 2,000 PCI DSS-specific checks. It is designed specifically to help organizations comply with PCI-DSS requirements across the enterprise in a cost-effective manner, while also reducing the overall risk of data breaches.

BigFix Compliance PCI Add-on helps enforce continuous PCI-DSS compliance with continuous monitoring and automatic remediation. The solution provides specialized dashboards and reports that summarize compliance status based on specific PCI-DSS requirements, milestones or platforms. (As shown in Table 1, BigFix Compliance PCI Add-on addresses all of the IT-related PCI-DSS requirements; the others are operational requirements not covered by software.)

Table 1. BigFix Compliance PCI Add-on addresses core PCI-DSS requirements

Control objectives	PCI-DSS requirements	BigFix
Build and maintain a secure network and system	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.	✓ ✓
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.	✓ ✓
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.	✓ ✓
Implement strong access control measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.	✓ ✓ ✓
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.	* *
Maintain an information security policy	12. Maintain a policy that addresses information security to all personnel.	*

✓ Requirements addressed by HCL BigFix Compliance PCI Add-on

* Operational or process-oriented requirements not covered by software

Eliminating compliance drift

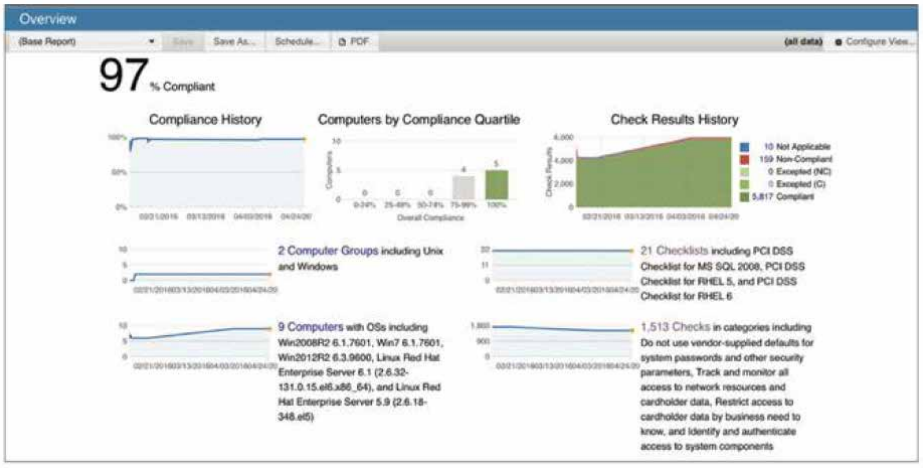
Traditionally, organizations would periodically assess compliance and mitigate risks. But this meant that even if an endpoint passed an audit, it could quickly fall out of compliance again. A manual remediation approach—for patch deployment, software updates and vulnerability fixes—can also leave organizations exposed to periods of high risk.

BigFix Compliance PCI Add-on supports a "set it and forget it" approach to policy management. The solution can provide accurate, real-time visibility of endpoint security configurations, identify and report on any configuration drift, and immediately remediate noncompliant systems. As a result, organizations can eliminate high-risk periods and lower their total costs.

A stair-step, continuous-compliance approach eliminate the risk, cyclical costs and configuration drift that can occur with traditional techniques

Gaining full visibility into your compliance posture

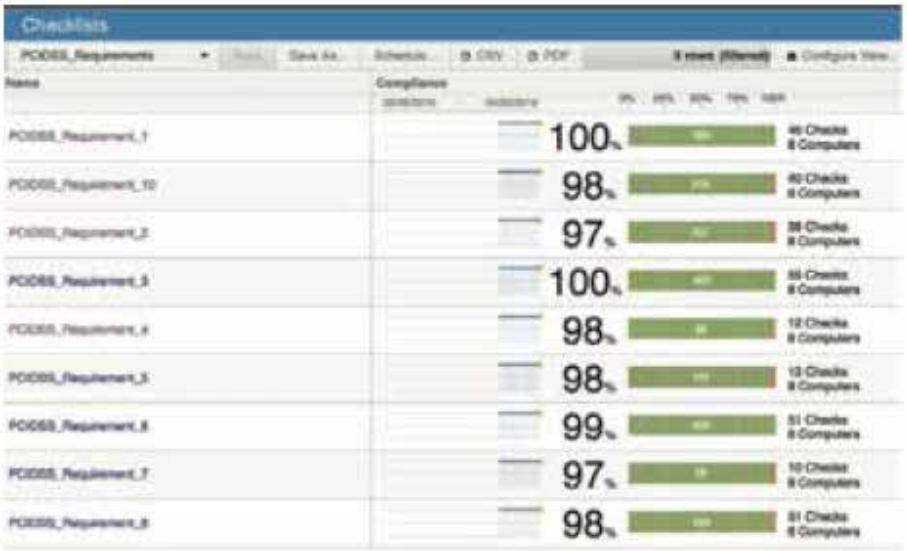
Using the BigFix Compliance PCI Add-on specialized dashboard, IT teams can quickly obtain the overall compliance posture for the entire organization. It shows the overall progress and trends toward continuous compliance, displays the history of check results across all endpoints, and summarizes key deployment data, including the associated checklists, checks and endpoints.



BigFix Compliance PCI Add-on has specialized dashboards that provide real-time visibility into progress the organization is making to meeting PCI-DSS requirements.

Simplifying audits and demonstrating compliance progress

BigFix Compliance PCI Add-on enables IT operations and security teams to share visibility and control of PCI-DSS efforts—helping lower costs and reduce risk. At any time, they can access an at-a-glance look of the organization's compliance status based on PCI-DSS requirements, milestones, endpoints or endpoint groups, and platform-specific checklists. (Each check- list contains technical checks that assess security policies and configurations on each endpoint, provide remediation steps to fix vulnerabilities and provide reporting capabilities.) They can then drill down to get more details on areas of noncompliance.



In addition, BigFix Compliance PCI Add-on supports the PCI Security Standards Council's prioritized approach to compliance, helping companies focus on six specific milestones to address the greatest risks first. The PCI-DSS milestones include:

- Milestone 1: Remove sensitive authentication data and limit data retention.
- Milestone 2: Protect systems and networks, and be prepared to respond to a system breach.
- Milestone 3: Secure payment card applications.
- Milestone 4: Monitor and control access to your systems.
- Milestone 5: Protect stored cardholder data.
- Milestone 6: Finalize remaining compliance efforts, and ensure all controls are in place.

BigFix Compliance PCI Add-on features milestone-based reports that help organizations monitor the compliance status of all six PCI-DSS milestones at a glance. IT and security teams can easily see the progress that's been made in a phased compli- ance project, and they can identify milestone areas that require additional effort.

Conclusion

BigFix Compliance and the BigFix Compliance PCI Add-on provide industry-leading capabilities to help organizations mitigate payment card-related risk and comply with the latest PCI-DSS requirements. In addition to helping companies avoid noncompliance penalties, these solutions help reduce operational costs. There's no need for highly specialized skills or costly manual processes. Using a single, centralized dashboard, organizations can enforce continuous security compliance across the entire enterprise—automatically remediating areas of noncompliance or quarantining systems to help prevent the spread of emerging threats.

Organizations can also realize significant value by deploying additional modules from the HCL BigFix platform, beyond BigFix Compliance and BigFix Compliance PCI Add-on. The broader BigFix platform addresses the convergence of endpoint management and security requirements by delivering capabilities for asset discovery and patching, software distribution, OS deployment, software usage and compliance, incident response, and more. Because BigFix so that all functions operate from the same management server, adding more capabilities is a simple manner of a license key change.

For more information

To learn more about HCL BigFix Compliance, please contact your BigFix Sales Specialist or BigFix Business Partner, or visit https://www.hcltechsw.com/bigfix/offerings/continuous-compliance.

HCLSoftware

hcltechsw.com