IBM Security
Solution Brief

Extending the power of BigFix Compliance with Patch Reporting

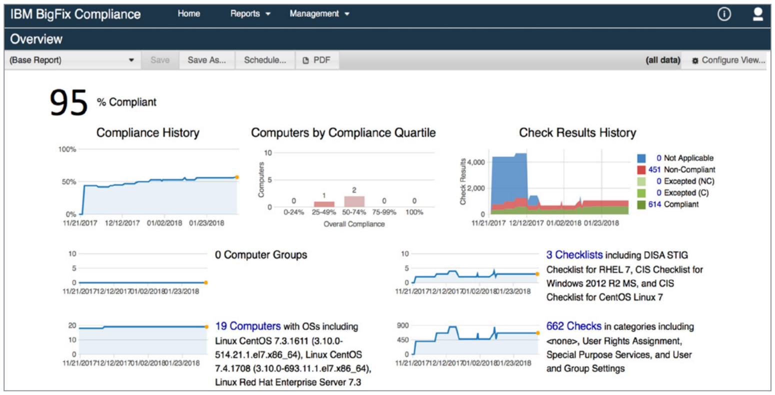
Highlights

- Extend the analytics and reporting capabilities of BigFix Compliance from security configuration to security patching
- Gain a comprehensive and timely view of patching activity and progress to assess the security posture
- Identify the critical and high severity patches and their remediation status to determine the next priority
- Track when patches are released and whether the patches have been applied to demonstrate compliance and pass audits

What is Patch Reporting in BigFix Compliance?

IBM®BigFix® Compliance helps organizations ensure continuous compliance with government regulations and corporate security policies while reducing costs and mitigating security risks. The BigFix infrastructure and best-practice checklists are implemented based on benchmarks published by CIS, DISA STIG, USGCB and PCI DSS.

BigFix Compliance provides near real-time visibility into security configurations across an organization while facilitating continuous, automated policy enforcement to endpoints. This includes laptops, desktops, servers, automated teller machines (ATMs) and point of sale (POS) devices, whether they are on or off the corporate network.



0 Computer Groups

3 Checklists including DISA STIG Checklist for RHEL 7, CIS Checklist for Windows 2012 R2 MS, and CIS Checklist for CentOS Linux 7

19 Computers with OSs including Linux CentOS 7.3.1611 (3.10.0-514.21.1.el7.x86_64), Linux CentOS 7.4.1708 (3.10.0-693.11.1.el7.x86_64), Linux Red Hat Enterprise Server 7.3

662 Checks in categories including <none>, User Rights Assignment, Special Purpose Services, and User and Group Settings

Figure 1: BigFix Compliance - Overview

Patch Reporting is a new feature in BigFix Compliance that tracks, analyzes and reports on the current status and historical trends of patching activities across endpoints in a BigFix deployment. Using the same Compliance Analytics engine and a similar reporting methodology, this feature allows BigFix Compliance to provide additional benefits to the security, IT operations and compliance teams within an organization:

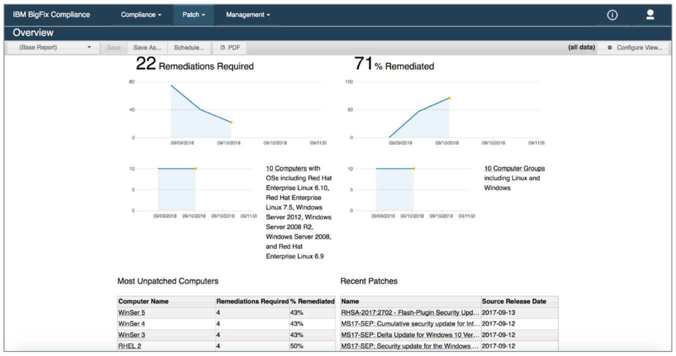
- Complete assessment of the patching posture by SOC or IT operations managers
- More efficient prioritization of vulnerability remediation by IT operations specialists
- Effective demonstration of compliance with regulations or organization policies by compliance specialists

Patching posture assessment

When patches are applied to applicable endpoints, organizations need a comprehensive and timely view of the progress of the patching activities. This is to assess the patching effort efficiency and how vulnerabilities have been remediated by the patches.

Patch Reporting provides analytics and reporting for the current status and historical trend of the applicable patches across endpoints. An IT operations manager or a SOC manager can use the Patch Overview Report to get an assessment of the current and historical patching posture including:

- The total number of remediations to be applied and how it has changed over time. (A remediation means one patch applied to an endpoint.)
- The percentage of the remediations completed and how this has changed over time
- A list of the endpoints that have the most patches yet to be applied
- A list of the most recently released patches



10 Computers with OSs including Red Hat Enterprise Linux 6.10, Red Hat Enterprise Linux 7.5, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Red Hat Enterprise Linux 6.9

10 Computer Groups including Linux and Windows

Most Unpatched Computers

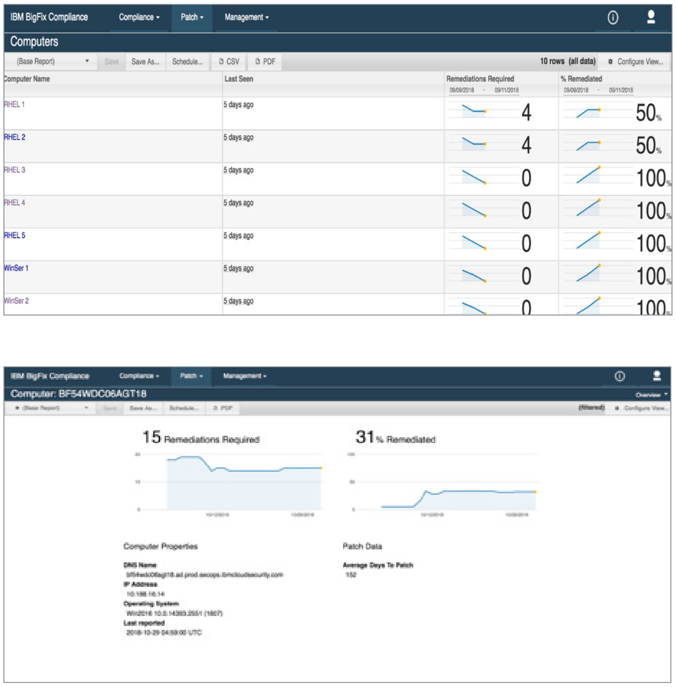
Computer Name	Remediations Required	% Remediated
WinSer 5	4	43%
WinSer 4	4	43%
WinSer 3	4	43%
RHEL 2	4	50%

Recent Patches

Name	Source Release Date
RHSA-2017:2702 - Flash-Plugin Security Upd...	2017-09-13
MS17-SEP: Cumulative security update for Int...	2017-09-12
MS17-SEP: Delta Update for Windows 10 Ver...	2017-09-12
MS17-SEP: Security update for the Windows ...	2017-09-12

Figure 2: BigFix Compliance Patch Reporting – Overview

The patching posture information is also available for various levels of detail, including a computer group, an individual computer or an individual patch. For each endpoint, the report shows the patching posture of the patches applicable to the endpoint and each patch's properties and remediation status. For each patch, the report shows the patching posture of the endpoints the patch is applicable to and each endpoint's properties and remediation status.



Computer Name	Last Seen	Remediations Required 09/09/2018 - 09/11/2018	% Remediated 09/09/2018 - 09/11/2018
RHEL 1	5 days ago	4	50%
RHEL 2	5 days ago	4	50%
RHEL 3	5 days ago	0	100%
RHEL 4	5 days ago	0	100%
RHEL 5	5 days ago	0	100%
WinSer 1	5 days ago	0	100%
WinSer 2	5 days ago	0	100%

Computer: BF54WDC06AGT18

15 Remediations Required

31 % Remediated

Computer Properties

DNS Name
bf54wdc06agt18.ad.prod.secops.ibmcloudsecurity.com
IP Address
10.188.16.14
Operating System
Win2016 10.0.14393.2551 (1607)
Last reported
2018-10-29 04:59:00 UTC

Patch Data

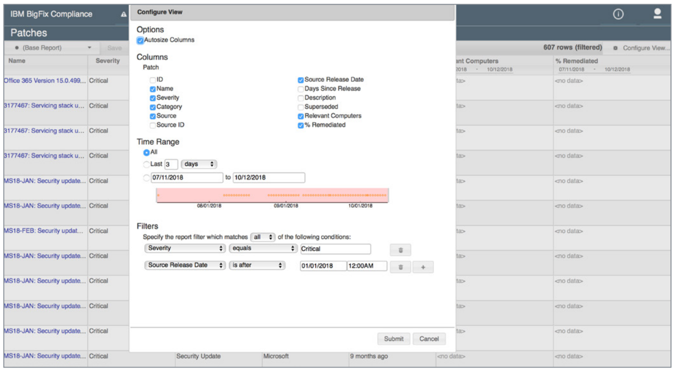
Average Days To Patch
152

Figure 3: BigFix Compliance Patch Reporting – Computer List and Computer views

Remediation task prioritization

Many organizations continue to look for ways to bridge the gaps between security and IT operations. It is even more important for endpoint management and security, because typically there are numerous vulnerabilities discovered by the security team and there are always patches to be applied by the IT Operations team. To improve security posture, an IT operation team needs more information to help them prioritize patching efforts.

With Patch Reporting, an IT operation specialist can use the embedded sorting and filtering functions to identify the critical and high-severity patches and their applicable endpoints. Specialists can immediately learn their current remediation status, to determine the next remediation priority.



Configure View

Options
☑ Autosize Columns

Columns
Patch

□ ID	☑ Source Release Date
☑ Name	□ Days Since Release
☑ Severity	□ Description
☑ Category	□ Superseded
☑ Source	☑ Relevant Computers
□ Source ID	☑ % Remediated

Time Range
● All
○ Last 3 days
○ 07/11/2018 to 10/12/2018

Filters
Specify the report filter which matches all of the following conditions:
Severity equals Critical
Source Release Date is after 01/01/2018 12:00AM

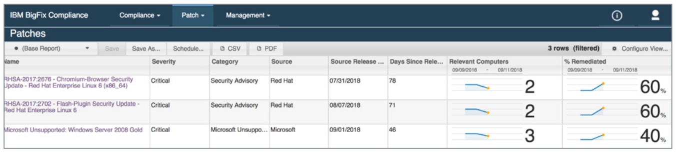
Name	Severity
Office 365 Version 15.0.499...	Critical
3177467: Servicing stack u...	Critical
3177467: Servicing stack u...	Critical
3177467: Servicing stack u...	Critical
MS18-JAN: Security update...	Critical
MS18-JAN: Security update...	Critical
MS18-FEB: Security updat...	Critical
MS18-JAN: Security update...	Critical
MS18-JAN: Security update...	Critical
MS18-JAN: Security update...	Critical
MS18-JAN: Security update...	Critical
MS18-JAN: Security update...	Critical

Figure 4: BigFix Compliance Patch Reporting – Filtering the Patch List view

Patch compliance reporting

Many security regulations have specific mandates for the timeliness of applying security patches. For each patch in the scope of regulatory compliance, an organization must track when the patch was made available and when it was applied to the applicable endpoints. This is to demonstrate its compliance and to help pass compliance audits.

With Patch Reporting, a compliance specialist can effectively track when patches are released and whether the patch has been applied to applicable endpoints. Or, if not, the current status. Reports can easily be exported to a CSV file or a PDF document as proof of compliance or for auditing purposes.



Name	Severity	Category	Source	Source Release ...	Days Since Rele...	Relevant Computers 09/09/2018 - 09/11/2018	% Remediated 09/09/2018 - 09/11/2018
RHSA-2017:2676 - Chromium-Browser Security Update - Red Hat Enterprise Linux 6 (x86_64)	Critical	Security Advisory	Red Hat	07/31/2018	78	2	60%
RHSA-2017:2702 - Flash-Plugin Security Update - Red Hat Enterprise Linux 6	Critical	Security Advisory	Red Hat	08/07/2018	71	2	60%
Microsoft Unsupported: Windows Server 2008 Gold	Critical	Microsoft Unsuppo...	Microsoft	09/01/2018	46	3	40%

Figure 5: BigFix Compliance Patch Reporting – Patch List view

Supported platforms and applications

Patches for Microsoft Windows platforms and applications and RHEL platforms are supported by Patch Reporting. The list of supported platforms and applications will continue to expand. For the complete list of supported platforms and applications, please visit the IBM Knowledge Center.

From security configuration to security patch to vulnerability

Patch Reporting extends the analytics and reporting capabilities of BigFix Compliance from security configuration to security patching. It allows an organization to monitor, assess and report the current and historical posture of these two important endpoint security areas. It allows for a more complete picture of the organization's overall security and risk posture.

Security Configuration
Security Patch
Vulnerability

Figure 6: Extending BigFix Compliance to security patch to vulnerability.

For more information

To learn more about IBM BigFix Compliance, contact your IBM representative or IBM Business Partner, or visit: ibm.com/software/products/en/ibm-bigfix-compliance.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
November 2018

This document is current as of the initial date of publication and may be changed by IBM at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♲ Please Recycle