

# How to Evaluate your Server Compliance Posture

A Comprehensive Manual for  
Server Compliance Audits



## 01

### SECTION 1

- 1.0 How to Use This Guide 1
- 1.1 Key Concepts 2

## 02

### SECTION 2

- 2.0 Assessing Compliance Posture 5
- 2.1 Interpreting Results 6

## 03

### SECTION 3

- 3.0 Integrating Compliance Tools 8
- 3.1 Selecting Tools 8
- 3.2 Implementation 8

## 04

### SECTION 4

- 4.0 Implementing Compliance Analytics 10
- 4.1 Dashboards 11

## 05

### SECTION 5

5.0	Enhancing Compliance through Automation	12
5.1	Monitoring	12
5.2	Remediation	12

## 06

### SECTION 6

6.0	Maintaining and Improving Compliance	13
6.1	Reviews and Updates	13
6.2	Analyzing Data	14
6.3	Continuous Improvement	15

## 07

### Conclusion

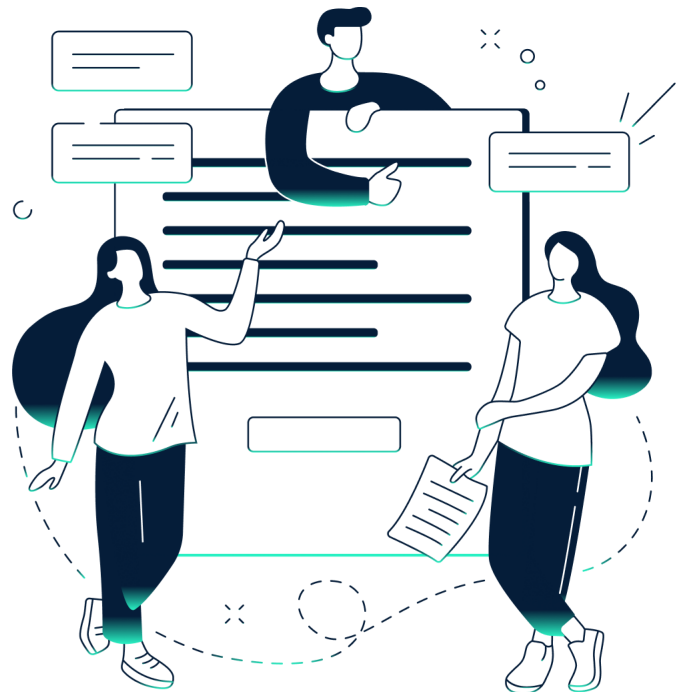
16

## 1.0 How to use this Guide

---

This guide is written for senior IT leaders in the retail sector who are responsible for managing server compliance. Whether you're looking to evaluate your current compliance posture or seeking ways to improve it, this comprehensive manual will provide you with the insights and tools you need.

You'll find structured approaches to assessing your current state, integrating essential tools, implementing analytics, automating processes, crafting strategies, and maintaining improvements.



## 1.1 Key Concepts

### » Patch Management

Regular updates to software to fix vulnerabilities, improve functionality, and ensure security.

#### ◆ Effective patch management involves

- **Identifying:** Keeping track of all software and systems that require patches.
- **Assessing:** Evaluating the criticality of each patch to prioritize based on risk.
- **Testing:** Ensuring that patches do not negatively impact existing systems.
- **Deploying:** Applying patches in a timely and organized manner to minimize downtime.
- **Monitoring:** Continuously tracking the status of patches to ensure compliance and security.

**Patches Catalog** 0 patches selected + CREATE ACTIONS

**PATCH BUNDLES**

Search Included Excluded Approval Status Operating System Endpoint Name Smart Group Remediation Plan Patch Status

Search... Not A... +3 Select... Select... Select... Select... Not In...

■	Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Remediation Plan	Needed On	Vulnerability Provider	Approval Status
<input type="checkbox"/>	UBUT-JP:2034 focal-updates multiverse	LINUX_UBUNTU_20_X x64	Ubuntu Server Focal	Updates	Unspecified		-	4515	3		Not Approved
<input type="checkbox"/>	UBUT-JP:1834 bionic-updates multiverse	LINUX_UBUNTU_18_X x64	Ubuntu Server Bionic	Updates	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBUT-JP:1434 trusty-updates multiverse	LINUX_UBUNTU_14_X x64	Ubuntu Server Trusty	Updates	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBUR-JP:2032 focal-updates restricted	LINUX_UBUNTU_20_X x64	Ubuntu Server Focal	Updates	Unspecified		-	4515	3		Not Approved
<input type="checkbox"/>	UBUR-JP:1832 bionic-updates restricted	LINUX_UBUNTU_18_X x64	Ubuntu Server Bionic	Updates	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBUR-JP:1432 trusty-updates restricted	LINUX_UBUNTU_14_X x64	Ubuntu Server Trusty	Updates	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBUM-JP:2231 jammy-updates main	LINUX_UBUNTU_22_X x64	Ubuntu Server Jammy	Updates	Unspecified		-	4515	3		Not Approved
<input type="checkbox"/>	UBUM-JP:2031 focal-updates main	LINUX_UBUNTU_20_X x64	Ubuntu Server Focal	Updates	Unspecified		-	4515	3		Not Approved
<input type="checkbox"/>	UBUM-JP:1831 bionic-updates main	LINUX_UBUNTU_18_X x64	Ubuntu Server Bionic	Updates	Unspecified		-	4515	2		Not Approved
<input type="checkbox"/>	UBUM-JP:1431 trusty-updates main	LINUX_UBUNTU_14_X x64	Ubuntu Server Trusty	Updates	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBRU-JP:2013 focal universe	LINUX_UBUNTU_20_X x64	Ubuntu Server Focal	Release	Unspecified		-	4515	3		Not Approved
<input type="checkbox"/>	UBRU-JP:1813 bionic universe	LINUX_UBUNTU_18_X x64	Ubuntu Server Bionic	Release	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBRU-JP:1413 trusty universe	LINUX_UBUNTU_14_X x64	Ubuntu Server Trusty	Release	Unspecified		-	4515	1		Not Approved
<input type="checkbox"/>	UBRT-JP:2014 focal multiverse	LINUX_UBUNTU_20_X x64	Ubuntu Server Focal	Release	Unspecified		-	4515	3		Not Approved

Page: 1 Items per page: 20 1 - 20 of 7078

## » Endpoint Security

Measures to protect network endpoints, such as desktops, laptops, and mobile devices, from cyber threats.

### ◆ Key components include:

- **Antivirus and Antimalware:** Tools to detect and eliminate malicious software.
- **Firewalls:** Systems that monitor and control incoming and outgoing network traffic based on security rules.
- **Encryption:** Protecting data at rest and in transit to prevent unauthorized access.
- **Access Control:** Ensuring that only authorized users can access specific systems and data.
- **Endpoint Detection and Response (EDR):** Solutions that provide continuous monitoring and response to advanced threats.

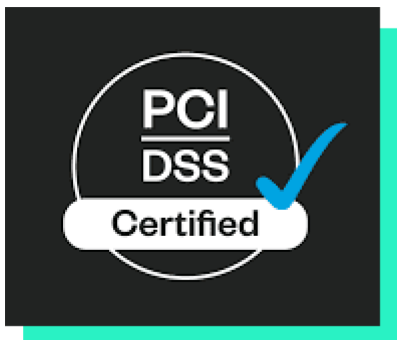
## » Regulatory Requirements

Standards and laws governing data security and privacy, which organizations must comply with to avoid penalties and ensure customer trust.

### ◆ Key regulations include:

#### » PCI DSS (Payment Card Industry Data Security Standard)

A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.



### ◆ Key requirements include:

- Building and maintaining a secure network.
- Protecting cardholder data.
- Maintaining a vulnerability management program.
- Implementing strong access control measures.
- Monitoring and testing networks.
- Maintaining an information security policy.



## » GDPR (General Data Protection Regulation)

A regulation in EU law on data protection and privacy for individuals within the European Union and the European Economic Area.

### ◆ Key principles include:

- Lawfulness, fairness, and transparency.
- Purpose limitation: Collecting data for specified, explicit, and legitimate purposes.
- Data minimization: Ensuring data is adequate, relevant, and limited to what is necessary.
- Accuracy: Keeping personal data accurate and up to date.
- Storage limitation: Retaining personal data only as long as necessary.
- Integrity and confidentiality: Processing data in a manner that ensures security.



## » HIPAA

U.S. legislation that provides data privacy and security provisions for safeguarding medical information.

### ◆ Key aspects include:

- Ensuring the confidentiality, integrity, and availability of all electronic protected health information.
- Detecting and safeguarding against anticipated threats to the security of the information.
- Protecting against anticipated impermissible uses or disclosures.
- Certifying compliance by their workforce.

These key concepts form the foundation for understanding and implementing effective server compliance strategies, ensuring that your organization's IT infrastructure remains secure, reliable, and compliant with relevant regulations.

## 2.0 Assessing Compliance Posture

---

Assessing your server compliance posture is crucial for maintaining a secure and efficient IT environment.

This section provides a step-by-step guide on how to evaluate your current compliance status using advanced tools like JetPatch.

By following these steps, you can identify and address gaps in [patch management](#) and endpoint security, ensuring your organization meets industry standards such as Cisco IOS, SOX, HIPAA, and PCI.

### » Initial Assessment and Diagnostics

Ensure your systems are ready for diagnostic tools by verifying that all endpoints and servers are accessible and properly configured for data collection. This preparation is crucial to address industry standards like Cisco IOS, SOX, HIPAA, and PCI.

### » Configuration

Set up tools to identify gaps in patch management and endpoint security. JetPatch Insights provides a comprehensive overview using advanced data analytics. Access the insights dashboard to view critical indications and quick how-to-improve actions.

### » Using JetPatch Insights section

#### ◆ JetPatch Insights has two main sections:

- **Insights Overview:** The main insights dashboard lists critical insights, each with a critical indication, details in the report, and quick how-to-improve actions.
- **Report View:** A detailed explanation of report insights with meaningful insights, easy-to-understand graphs, and how-to-improve actions. This feature is part of JetPatch's Remediation Plan Compliance Report, which offers a detailed overview of your compliance status, including insights into installation plans and failed updates.

For more details, visit our [Configuration Compliance page](#).



## 2.1 Interpreting Results

### » Understanding Diagnostic Output

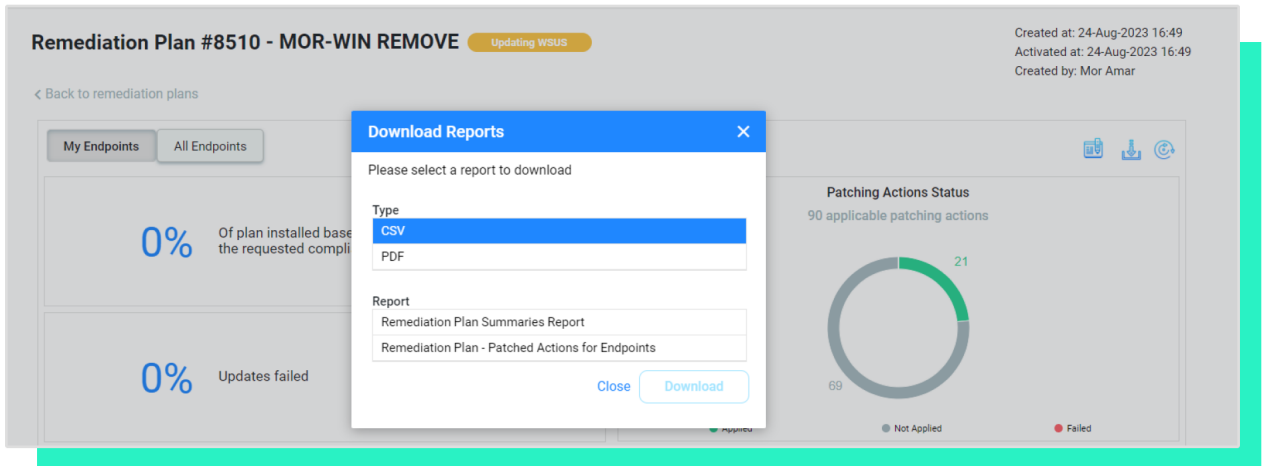
Learn to interpret the results from diagnostic tools, focusing on criticality thresholds and identifying high-risk areas.

### » Criticality Thresholds

JetPatch not only identifies gaps but also provides criticality thresholds to prioritize issues based on severity. Examples include:

#### ◆ Examples include:

- **Patches Compliance:** Insights related to patch compliance in the environment.
- **Endpoints Compliance:** Insights related to endpoint compliance.
- **Patches by Age:** Insights on the age of patches.
- **Endpoints by Oldest Missing Patch:** Insights related to endpoints with the oldest missing patches.



The screenshot displays the JetPatch interface for a remediation plan titled "Remediation Plan #8510 - MOR-WIN REMOVE". The plan is currently "Updating WSUS". The interface shows a progress bar for "Of plan installed based on the requested compliance" at 0% and "Updates failed" at 0%. A "Download Reports" dialog box is open, allowing the user to select a report to download. The dialog has a "Type" dropdown menu with "CSV" selected and "PDF" as an option. Below the dropdown, there are two report options: "Remediation Plan Summaries Report" and "Remediation Plan - Patched Actions for Endpoints". The "Download" button is highlighted. In the background, a "Patching Actions Status" chart shows 90 applicable patching actions, with a donut chart indicating 21 actions are completed (green) and 69 are not applied (grey). The chart also shows 0 failed actions (red).

## » Prioritizing Risks

Address the most significant risks first to enhance security posture. Use the real-time compliance reporting features to monitor the status of patches and identify any issues promptly. JetPatch's real-time compliance monitoring quickly identifies and resolves compliance issues, minimizing the risk of prolonged non-compliance and potential penalties.

## » Self-Assessment Checklist

- Have all endpoints and servers been verified for accessibility and proper configuration?
- Are diagnostic tools properly set up and configured?
- Have critical insights been reviewed and prioritized?
- Is there a process in place for continuous monitoring and real-time reporting?

## 3.0 Integrating Compliance Tools

---

Integrating the right compliance tools is essential for maintaining a secure and efficient IT environment. This section provides a comprehensive guide on how to select and implement compliance tools that align with your retail platform's needs. By following these steps, you can automate and streamline your compliance processes, ensuring optimal performance and reduced manual effort.

### 3.1 Selecting Tools

---

#### » Evaluating Needs

Determine the specific needs of your e-commerce platform. Research and select compliance tools that fit well with your technology stack and business needs. Consider factors such as the size of your IT environment, regulatory requirements, and the specific security challenges you face.

#### » Trial and Selection

Test shortlisted tools to ensure compatibility and effectiveness. Conduct pilot programs to evaluate how well each tool integrates with your existing systems and meets your compliance requirements. Gather feedback from your IT team and make data-driven decisions to select the best tools for your organization.

### 3.2 Implementation

---

#### » Preparing Systems

##### ◆ following these steps:

- **Verify System Compatibility:** Ensure that the selected tools are compatible with your existing software and hardware.
- **Update Software and Hardware:** Perform necessary updates to your software and hardware to support the new compliance tools.
- **Configure Network Settings:** Adjust network settings to ensure seamless integration and optimal performance of the new tools.

#### » Integration Techniques

Automate and streamline compliance processes using JetPatch's capabilities, reducing manual overhead and enhancing efficiency. Leverage features such as automated patch management, real-time compliance monitoring, and remediation planning to ensure continuous compliance and minimize the risk of security breaches.

## >> Detailed Steps for Preparing Systems

### ◆ Update Software and Hardware:

- **Schedule Updates:** Plan software and hardware updates during low-traffic periods to minimize disruption.
- **Backup Data:** Ensure all critical data is backed up before initiating updates.
- **Perform Updates:** Execute the necessary updates for your operating systems, applications, and hardware components.
- **Verify Updates:** Confirm that all updates have been successfully installed and systems are functioning correctly.

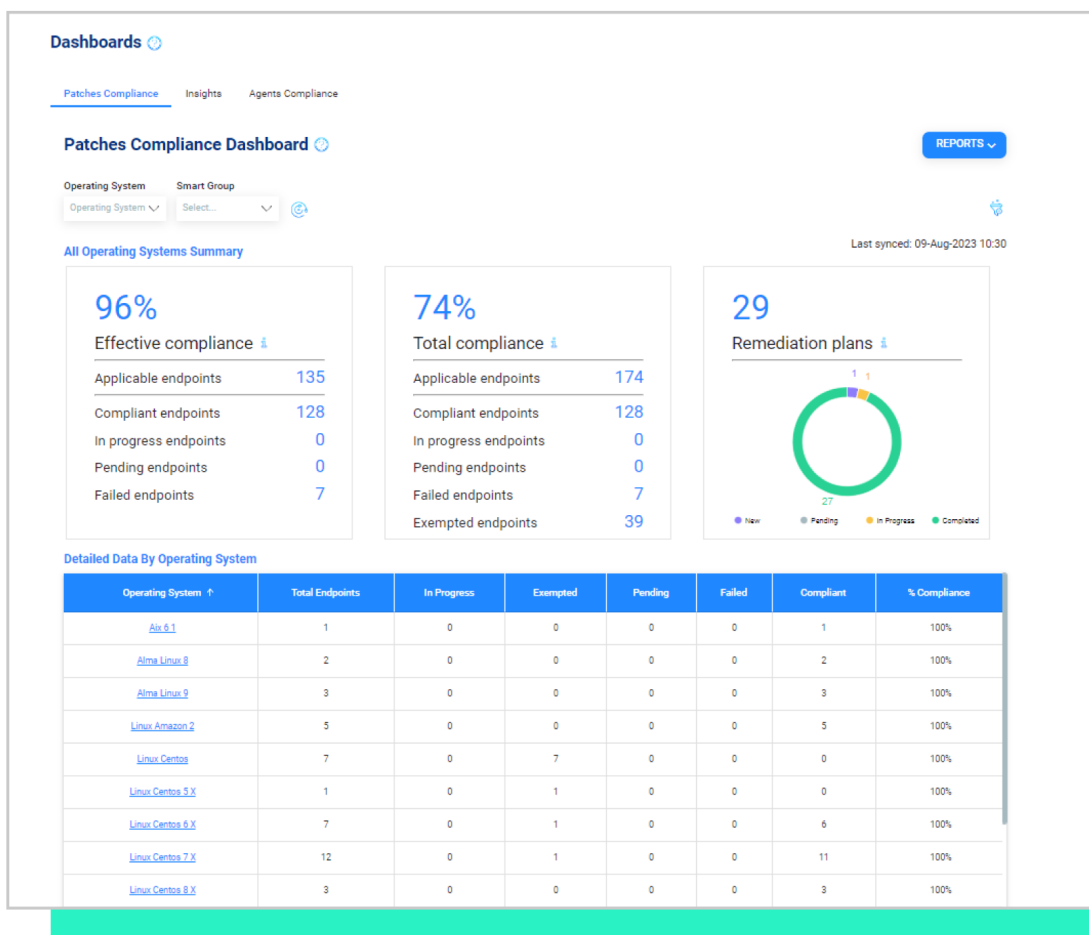
### ◆ Configure Network Settings:

- **Network Assessment:** Evaluate your current network configuration to identify necessary changes.
- **Adjust Firewall Settings:** Update firewall settings to allow communication between the compliance tools and your network.
- **Configure IP Addresses:** Ensure that IP addresses and network configurations support the new tools.
- **Test Network Connectivity:** Perform connectivity tests to ensure that the tools are properly integrated and can communicate with other systems.

By following these detailed steps, you can ensure a smooth and effective integration of compliance tools into your existing IT environment, optimizing performance and maintaining a high level of security compliance.

## 4.0 Implementing Compliance Analytics

Implementing Compliance Analytics Is Crucial For Maintaining Visibility And Control Over Your IT Environment. This Section Provides A Detailed Guide On Setting Up And Utilizing Compliance Dashboards And Analytics Tools To Monitor And Improve Your Compliance Posture. By Leveraging These Tools, You Can Make Data-Driven Decisions That Enhance Your Security Measures And Ensure Continuous Compliance.



## 4.1 Dashboards

### » Setting Up Dashboards

Set up and customize compliance dashboards.

◆ **Follow these steps to ensure your dashboards are effective:**

- **Choose Key Compliance Metrics:** Identify the most critical compliance metrics for your organization, such as compliance percentages, aging of patches, and endpoint security status.
- **Use Visual Tools:** Implement visual tools like graphs and charts to represent data clearly. This helps in quickly identifying trends and issues.
- **Customize Views:** Tailor the dashboard views to the specific needs of different stakeholders, ensuring that relevant information is accessible and actionable.

**Automatic Remediation Plans Rules** + Add

Create automatic Remediation Plans rules based on existing patch bundle.  
 JetPatch will create Remediation Plans for enabled rules and will activate them if configured

Search  Patch Bundle  Modified By  Automatic Activation  Emergency  Next Creation From Date  Next Creation To Date

Name ↑	Patch Bundle	Modified By	Status	Repeat Schedule ↑	Next Creation	Automatic Activation	Emergency	
test	test	anastasia anastasia	<input checked="" type="checkbox"/>	Daily at 00:00 US/Samoa	28-Aug-2023 00:00 US/Samoa	No	No	
test77	mor test	Mor Amar	<input checked="" type="checkbox"/>	Daily at 00:00 Pacific/Honolulu	-	No	No	

Page: 1    Items per page: 20    1 - 2 of 2    |< < > >|

## 5.0 Enhancing Compliance Through Automation

---

This section provides a step-by-step guide on how to leverage automation tools to monitor compliance and remediate vulnerabilities effectively.

### 5.1 Monitoring

---

#### » Automating Compliance Monitoring

- **Install and Configure Automation Tools:** Choose and implement the right automation tools tailored to your specific compliance needs.
- **Set Up Triggers:** Establish triggers for automated reactions to compliance failures, such as missing patches or outdated software.
- **Ensure Process Functionality:** Consistently test and verify that your automation processes are operational and effectively addressing compliance issues in a timely manner.

### 5.2 Remediation

---

#### » Automating Remediation Plans

- **Create Automated Remediation Plans:** Formulate remediation strategies for detected vulnerabilities, detailing the automated actions to be initiated.
- **Implement Remediation Actions:** Set up your systems to automatically carry out these remediation actions upon detection of vulnerabilities.
- **Review and Improve:** Persistently assess the efficiency of automated responses and refine them as necessary to boost performance.
- **Utilize JetPatch's Auto-Generated Remediation Plans:** Utilize JetPatch's advanced capabilities to create and apply remediation plans informed by critical insights, thereby closing compliance gaps efficiently and maintaining the security of your IT environment.

## 6.0 Maintaining And Improving Compliance

---

Maintaining and improving compliance is an ongoing process that requires continuous monitoring and regular updates. This section outlines how to keep your compliance measures current and effective through continuous improvement strategies and the use of compliance analytics.

### 6.1 Reviews And Updates

---

#### » Continuous Monitoring

It ensures that your compliance measures are not only current but are also resilient against evolving threats and changes in regulations. This proactive stance is essential for maintaining the integrity and security of your operations.

Activity	Frequency	Priority Level
Update Compliance Protocols	As scheduled	High
Adjust for New Threats	As needed	High
Perform Compliance Reviews	Annually/Bi-annually	High



## 6.2 Analyzing Data

### » Regular Monitoring

Monitor compliance data regularly to maintain an up-to-date view of your security posture.

#### ◆ Here's how to effectively analyze the data:

- **Pre-Filtered Graphs from JetPatch:** Use pre-filtered graphs from JetPatch to show relevant insights clearly. This includes visual representations of compliance status, patch aging, and endpoint vulnerabilities.
- **Data Interpretation:** Analyze the data to make informed security decisions. Look for patterns and anomalies that may indicate potential compliance issues or security threats.
- **Real-Time Updates:** Ensure that your dashboards provide real-time updates to reflect the current compliance status and any recent changes.

Detailed Data By Operating System

Operating System ↑	Total Endpoints	In Progress	Exempted	Pending	Failed	Compliant	% Compliance
<a href="#">Linux Ubuntu 22.X</a>	3	0	0	0	0	3	100%
<a href="#">Solaris 10</a>	2	0	1	0	0	1	100%
<a href="#">Windows 10</a>	3	0	0	0	0	3	100%
<a href="#">Windows 11</a>	2	0	0	0	2	0	0%
<a href="#">Windows 7</a>	1	0	0	0	0	1	100%
<a href="#">Windows 8.1</a>	1	0	0	0	0	1	100%
<a href="#">Windows Server 2008 R2</a>	1	0	0	0	0	1	100%
<a href="#">Windows Server 2012 R2</a>	2	0	1	0	0	1	100%
<a href="#">Windows Server 2016</a>	1	0	0	0	0	1	100%
<a href="#">Windows Server 2019</a>	3	0	1	0	0	2	100%
<a href="#">Windows Server 2022</a>	3	0	0	0	0	3	100%

## 6.3 Continuous Improvement

Compliance Analytics involves the use of data analysis tools to monitor, evaluate, and improve regulatory compliance processes, ensuring organizations adhere to legal standards and internal policies.

» Using Compliance Analytics for the following compliance improvements:

Activity	Frequency	Priority Level
Update Compliance Protocols	Bi-annual	High
Conduct Security Briefings	Quarterly	High
Perform Annual Audits	Annually	Medium
Analyze Compliance Failures	As needed	High
Assess Risk Levels	As needed	High
Implement Changes	As needed	Medium

If you handle server compliance in-house, or plan to, you should be prepared to invest heavily in the right resources and commit to long-term maintenance. Managing compliance is an ongoing process that becomes increasingly complex over time.

## Common Challenges

- ▶ **Resource Intensive**  
Compliance management requires significant financial and time investments.
- ▶ **Complexity**  
As your IT infrastructure grows, maintaining compliance becomes more complicated.
- ▶ **Responsibility**  
You're responsible for ensuring all servers and endpoints are secure and compliant.

## How We Can Help

- ▶ **Automated Patch Management**  
Simplifies patching across multiple operating systems, reducing manual effort, frequency of human error, and saving money.
- ▶ **Compliance Analytics**  
Provides real-time visibility into your compliance status, helping you monitor and demonstrate compliance effectively.
- ▶ **Continuous Monitoring and Remediation**  
Ensures vulnerabilities are promptly addressed, maintaining a high level of security.

## Proven Benefits

- ▶ **75% Reduction in Remediation Time**  
Automation significantly cuts down the time to address vulnerabilities.
- ▶ **70% Reduction in Manual Efforts**  
Frees up IT resources for other critical tasks.
- ▶ **75% Reduction in System Downtime**  
Efficient patching processes minimize disruptions.

**JetPatch** integrates with your existing IT operations and security tools, ensuring complete process automation and full visibility for all stakeholders.

To explore how we can streamline your compliance strategy and simplify patch management, [schedule a demo](#) with one of our experts today or start a [free trial](#).