Solution Document

Windows Patch Management

Powered by Motadata ServiceOps

Summary

Effective patch management is a cornerstone of enterprise IT security and operational continuity. The Windows Patch Management solution, natively integrated within Motadata ServiceOps, provides a centralized, policy-driven, and scalable approach to managing Windows updates. Designed for IT teams, compliance officers, and enterprise architects, this solution streamlines patch lifecycle management while reducing risks and manual effort.

This document presents a comprehensive overview of the solution's architecture, capabilities, deployment options, and benefits.

Introduction

Cybersecurity threats continue to exploit known vulnerabilities in operating systems, leading to security breaches and service disruptions. Timely patching is essential to mitigate these risks, meet compliance requirements, and maintain system reliability.

Managing Windows patches across distributed networks presents real-world challenges, such as:

- Optimizing bandwidth consumption
- Avoiding maintenance window conflicts
- Tracking patch compliance
- Validating patch deployment success

The Motadata ServiceOps Patch Management solution addresses these concerns with a policy-driven, automated patching system embedded within our ITSM platform.

Product Overview

Motadata ServiceOps delivers an integrated Patch Management module that brings:

- Centralized control over patch activities
- Real-time visibility into patch health and compliance
- Automation from patch discovery to deployment
- Seamless integration with Asset Management and CMDB

Architecture Components

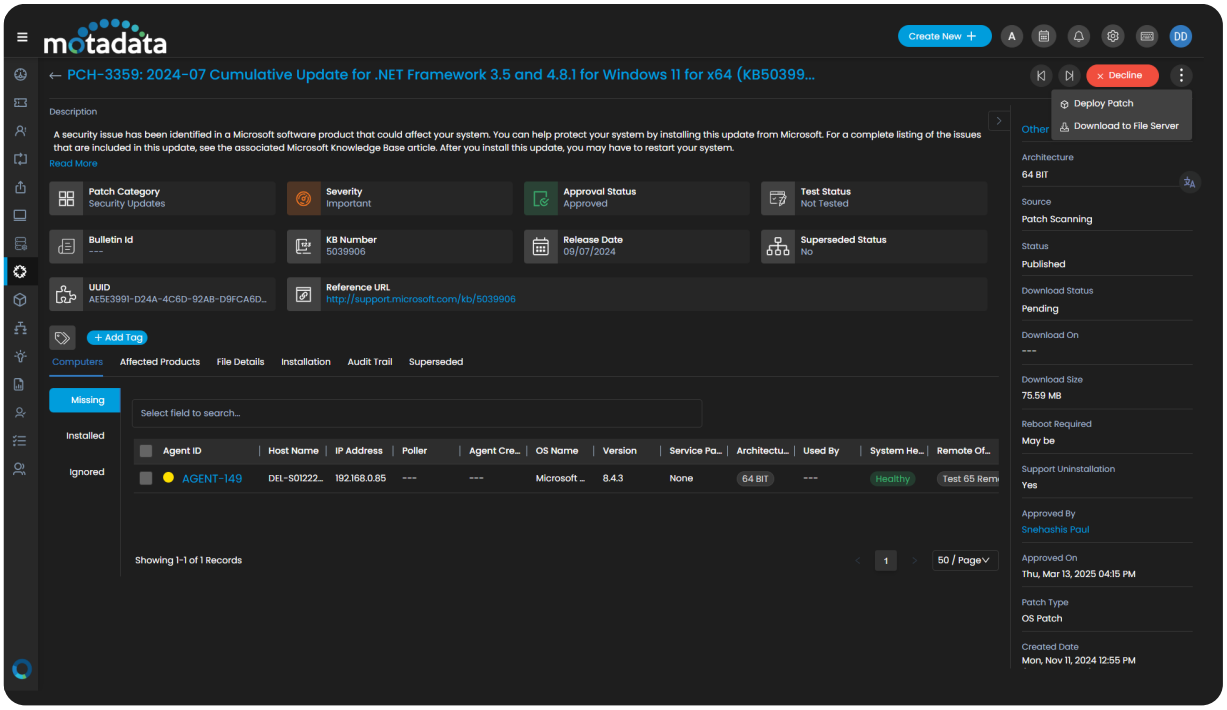
- Patch Repository Server: Syncs with Microsoft Update Catalog or WSUS
- Motadata ServiceOps Server: Orchestrates policies, workflows, and reporting
- Endpoint Agents: Installed on Windows devices to scan and apply patches
- Deployment Server (optional): Used for distributed environments to cache patches locally

Unified Platform Advantages

- Single Agent for discovery and patch operations, simplifying endpoint management
- Unified Portal for ServiceDesk, Asset, CMDB, and Patch Management
- Single Server Deployment model that supports High Availability (HA) and Disaster Recovery (DC/DR) out of the box
- Optional Distribution Server for optimizing network bandwidth in multi-location environments

Key Features

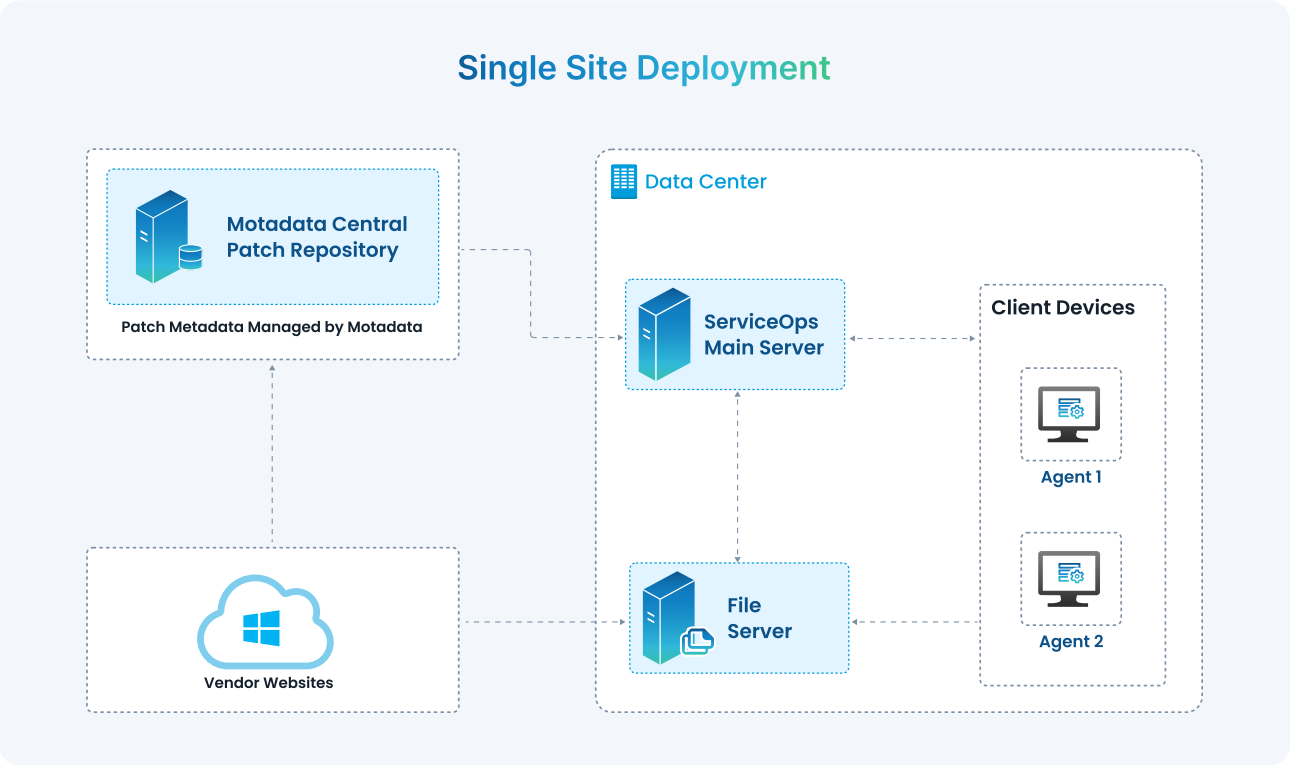
- Automated Patch Scanning: Detect missing patches for OS and supported Microsoft applications.
- Patch Deployment Policies: Schedule deployments during maintenance windows with fallback actions.
- Approval Workflows: Role-based workflows for patch approval prior to deployment.
- Rollback Support: Uninstall failed or problematic patches.
- Bandwidth Optimization: Use of peer-to-peer or distribution server-based deployment.
- Compliance Dashboard: Visualize patch compliance across sites, departments, or devices.
- Notification System: Email or portal notifications for pending and failed patch deployments.



Deployment Architecture Options

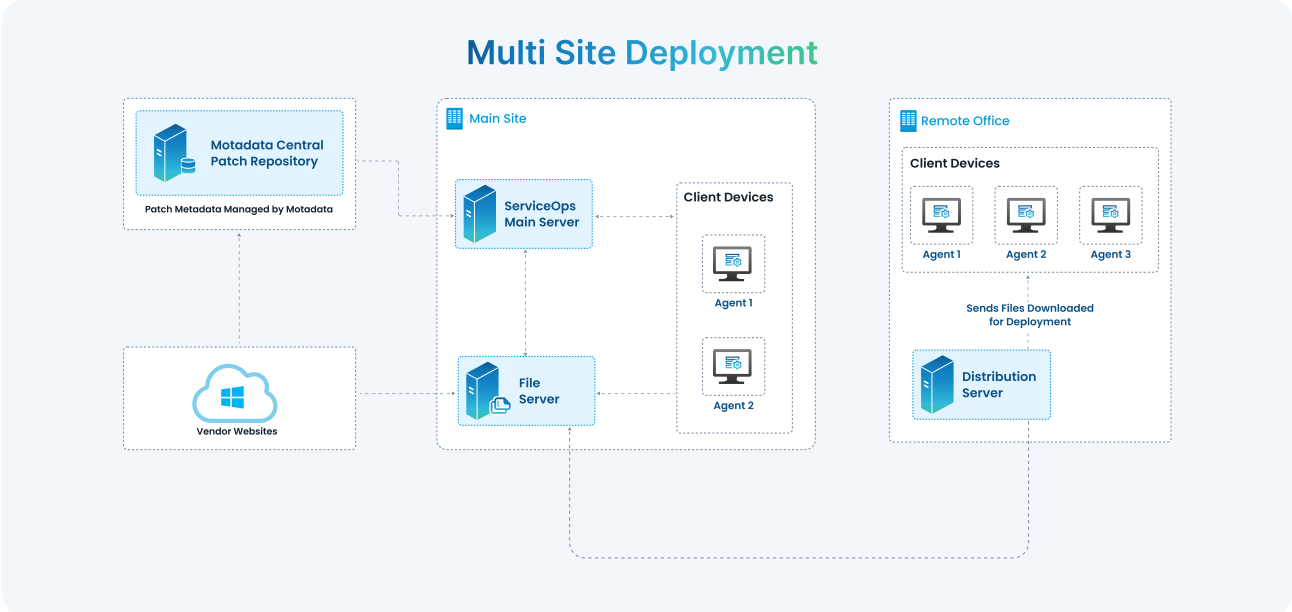
Single-Site Setup

- Central Motadata ServiceOps server + Patch Repository
- Agents directly communicate with server



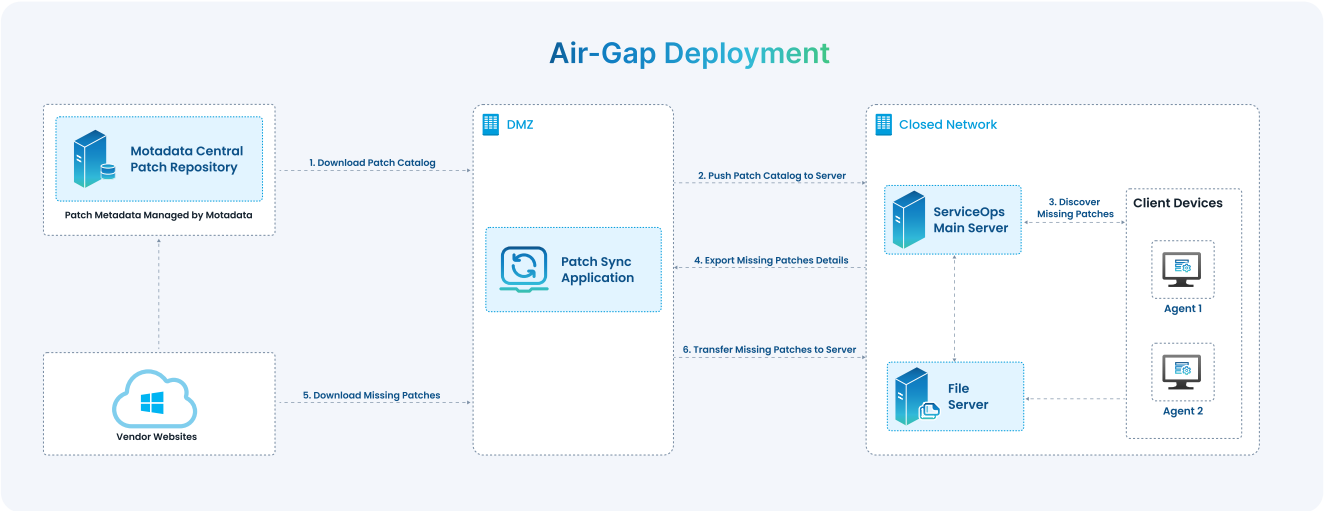
Multi-Site Setup with Distribution Server

- Ideal for geographically distributed networks
- Reduces WAN load by caching patches locally



Air-Gapped Environments

- Central server downloads patches via proxy
- Internal deployment servers handle distribution in DMZ/firewalled zones



Patch Management Process Overview

Gain Visibility into Asset Inventory

- Centralize all Windows asset data scattered across spreadsheets, databases, and tools into a unified repository.
- This consolidated view ensures accurate targeting and supports efficient patch operations.

Scan for Missing Windows Updates

- Initiates a comprehensive scan of all Windows endpoints.
- Identifies missing security and non-security patches to prevent potential vulnerabilities.

Fetch Latest Patches from Microsoft

- A centralized patch repository regularly synchronizes with Microsoft Update Catalog.
- This metadata is then synchronized with Motadata ServiceOps, enabling accurate detection of missing updates across all assets.

Prioritize Patches

- Use risk-based assessment to categorize and prioritize patches.
- Deploy critical and high-severity patches first to minimize exposure.

Test Patches in Controlled Windows Environments

- Allows updates to be tested in sandboxed or isolated environments.
- Reduces risk by identifying compatibility issues before broad deployment

Deploy Patches to Live Environment

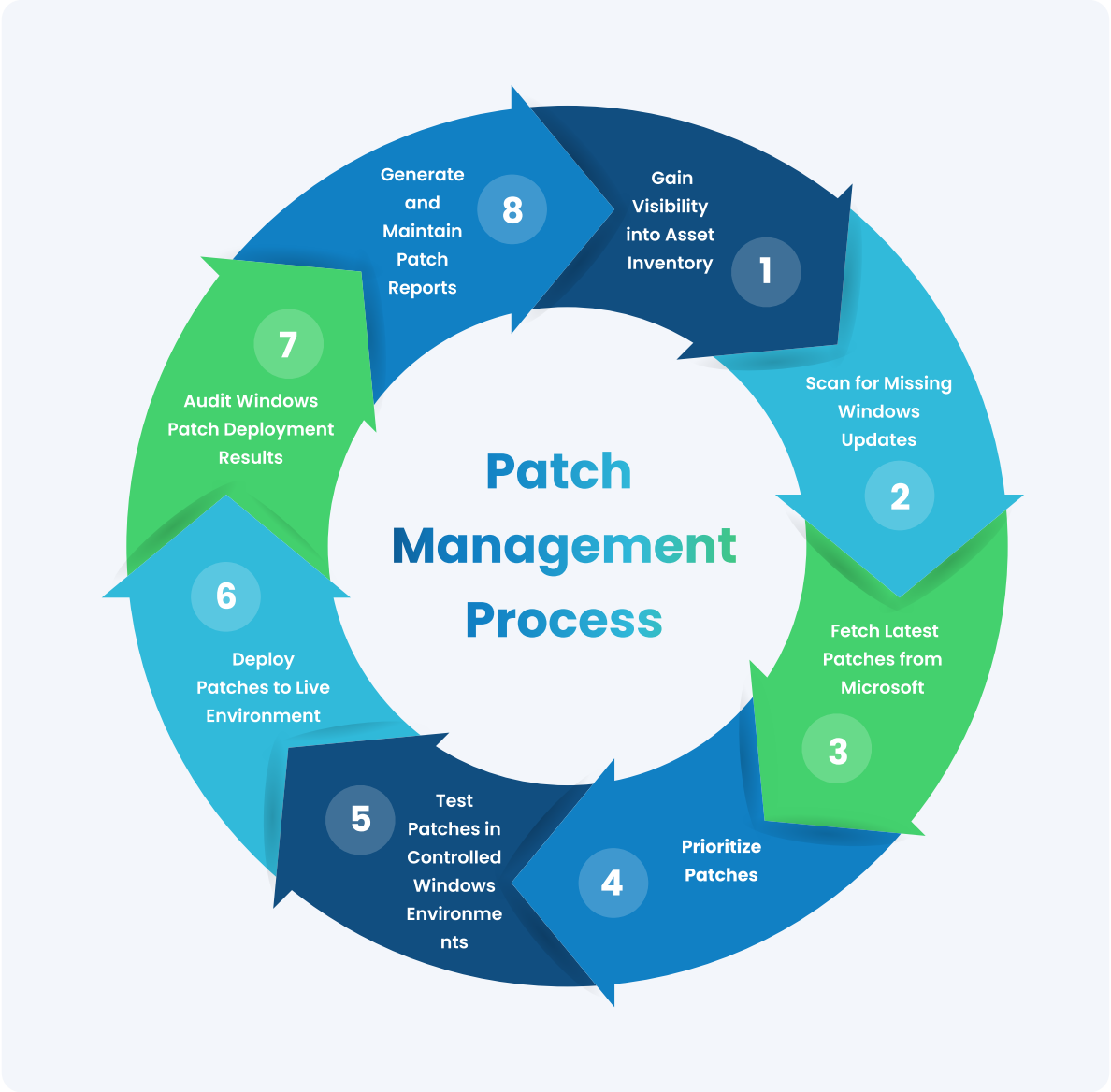
- Roll out tested patches across live systems based on defined deployment policies.
- Leverage scheduling, bandwidth throttling, and reboot management to ensure seamless updates.

Audit Windows Patch Deployment Results

- Continuously tracks patch status—successful, pending, or failed.
- Supports retry mechanisms and helps maintain patch compliance.

Generate and Maintain Patch Reports

- Offers comprehensive reports including patch coverage, deployment timelines, and device compliance.
- Supports audit readiness and strategic patch planning.



Supported Platforms

Windows Client Operating Systems

- Windows 7*
- Windows 8
- Windows 10
- Windows 11

Windows Server Operating Systems

- Windows Server 2008*
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

*End-of-life versions are supported under extended scenarios depending on Microsoft's patch release policies.

Microsoft Office Support

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft Access
- Microsoft Publisher

Microsoft Office applications through native Click-to-Run technology.

Supported Windows Update Types

Motadata ServiceOps supports the following categories of Windows updates:

- Security Update: Refers to updates that address vulnerabilities related to security.
- Cumulative Update: Includes all previously released fixes. If previous updates are already installed, only the latest changes are downloaded and applied.
- Non-Security Update: Covers updates that are not related to security fixes. These can include bug fixes, feature improvements, and other changes.
- Critical Update: Addresses important, non-security bugs that could impact system stability or performance.
- Service Pack: Cumulative set of security, critical, and other updates. May include design changes or customer-requested features.
- Update: General bug fixes that are not classified as critical or security-related.
- Update Rollup: A bundled set of updates (security and non-security) for a specific product or component.

Scalability & Performance

- Designed for 10,000+ endpoints
- Supports parallel deployments and load balancing
- Auto-throttling ensures minimal network impact
- Validated across 20+ branch environments

Security Considerations

- All agent-server communication uses HTTPS/TLS
- Role-based access control (RBAC) for patch approvals
- Checksums verification of patches
- Comprehensive audit logging of patch operations

Compliance & Reporting

- Flexible architecture to support compliance requirements such as CIS, NIST
- Device-wise, patch-wise, and department-wise compliance reports
- Audit-ready reports with timestamps and technician actions

For more information

www.motadata.com

© 2025 Mindarray Systems Pvt. Ltd. All rights reserved.

All trademarks, service marks, trade names, trade dress, product names and logos appearing on the site are the property of their respective owners. Any rights not expressly granted herein are reserved.