



# END-TO-END AUTOMATED PATCH MANAGEMENT AND VULNERABILITY REMIEDIATION



AUTO-DISCOVERY OF  
ENDPOINTS & PATCHES



COST-SAVINGS & PATCH  
SUCCESS SIMULATION

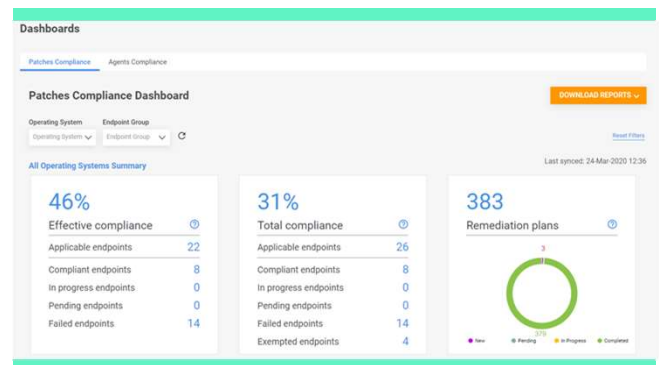


PATCH GOVERNANCE &  
COMPLIANCE DASHBOARD

New software vulnerabilities are exposed at an alarming rate, compelling vendors to release multiple patches, overwhelming IT and InfoSec teams. At the same time, the key approach to dealing with vulnerabilities - Patching - is comprised of manual steps and handshakes that makes this critical process tedious and inefficient.

## THE JETPATCH SOLUTION

JetPatch eliminates patch blindspots with full discovery of all endpoints, OSs, and applications and compares installed patches to an official security baseline. When it discovers new vulnerabilities and required patches, JetPatch deploys them with governed processes during scheduled maintenance windows and based on fully automated workflows that combine industry best practices and your organization's needs, establishing continuous compliance across complex IT environments.



## SECURITY OF COMMUNICATION

JetPatch management of individual endpoints is based on the JetPatch Connector, which must be installed on managed endpoints. The JetPatch Connector can be pre-installed (e.g. as part of a base image), or it can be deployed remotely by JetPatch deployment team.

The secured communication protocols between JetPatch to the Connectors are SSH, SMB, HTTPS.

## CONSOLE AND API SECURITY

JetPatch's console and API use industry-standard methods and mechanisms for authenticating user identities, and a role-based access control (RBAC) scheme to provide each user with access to specific functionality. Standard encryption methods are used to ensure data confidentiality.

## JETPATCH SOLUTION BENEFITS

- Fast Time to Remediation
- Cost Savings and Resource Optimization
- Elimination of Manual Tasks
- End-to-End Workflow Automation
- Patch Process Governance
- Patch Success Simulation
- Continuous Compliance Across Environments
- Minimized Downtime

## PREDICTIVE PATCHING INNOVATION

JetPatch simulates the future success of a cycle before it is executed, using a multi-layer machine learning model, which generates a variety of actionable insights, helping IT and security teams fix root causes of remediation process delays

## JETPATCH AT A GLANCE - TECHNICAL SPECIFICATION

### SERVER REQUIREMENTS

- Red Hat Enterprise Linux or CentOS version 7.x
- PostgreSQL Server from version 9.4 or RDS Connectivity

### ENVIRONMENT DISCOVERY

- JetPatch automatically discovers multiple environments
- Cloud: AWS, Azure
- On-Premise: vCenter, WSUS, Active Directory

### PRE-REQUISITES

- OpenSSL ver. 1.0.1g
- Oracle Java JDK 8
- NGINX 1.9 and above

### SUPPORTED PLATFORMS

- Red Hat Enterprise Linux
- CentOS
- Oracle Linux
- Amazon Linux AMI
- Amazon Linux 2
- Windows Desktops
- Windows Servers
- Oracle Linux
- Solaris
- SUSE Linux Enterprises Server

- Ubuntu
- AIX\*

\* Support for this platform is expected in the next product version

