JioCloud

Vulnerability Assessment and Remediation

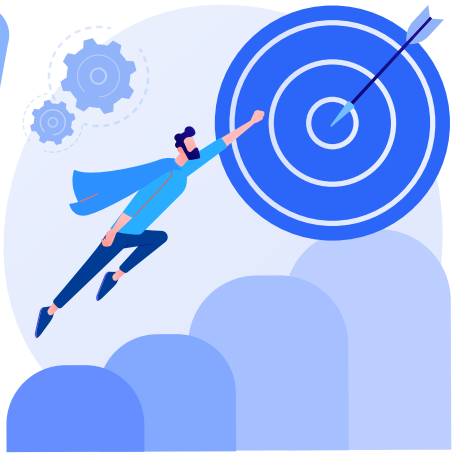
Reduce Vulnerability Exposure by Up to 70% — with Automated Patching and Real-Time Insights

JioCloud

From assessment to remediation — automate 80% of patches, prove compliance, and respond faster

The Challenge

- **Too many vulnerabilities, too little time**
  Security teams struggle to stay ahead of constant threats — especially when patching still depends on manual effort.
- **Blind spots across the environment**
  Unpatched systems, outdated software, and misconfigured assets leave silent openings thats attackers can exploit.
- **Lengthy reports, no clear action**
  Many tools surface long lists of issues — without helping you decide what matters or what to fix first.



The JioCloud Solution

Clarity to Act, Confidence to Improve Prioritise What Matters - Patch Without Delay

JioCloud Vulnerability Assessment and Patch Management helps you take control of your environment — without the manual burden. It identifies high-risk vulnerabilities, shows you what matters most based on business impact, and automates the patching process end to end. You get clear risk scores, real-time visibility, and policy-based workflows, so your teams spend less time reacting and more time securing. Whether you are managing a hybrid fleet or dynamic workloads, JioCloud helps you fix issues faster and prove compliance with less effort.

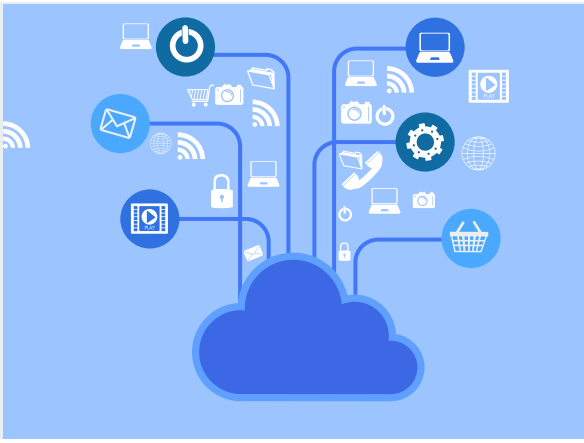
Key Features

- **Asset discovery made easy**
  Sort vulnerabilities by CVSS score, asset sensitivity, exploit availability, and patch deadlines.
- **Automated patch management**
  Deploy patches based on policy by severity, group, or window — without manual effort.
- **Continuous scanning**
  Use lightweight agents to detect new risks in real time.
- **Patch validation and rescanning**
  Confirm patch success automatically, with no manual checks.
- **Blackout and maintenance Controls**
  Avoid disruptions with scheduling built for production systems.
- **Exception management**
  Track exceptions with business justification and expiry controls — all audit-ready.

JioCloud

What You Gain

- **Up to 70% reduction in exposure**
  Fix high-risk gaps before attackers can exploit them.
- **Automated patch cycles**
  Eliminate spreadsheet tracking and manual change requests.
- **Stronger compliance posture**
  Generate audit trails and meet SLAs without extra overhead.
- **Aligned security operations**
  Focus on what matters most, based on context, not just counts.
- **Faster time to remediate**
  Move from detection to fix in hours, not weeks.



Use Cases in Action

Patch what matters first

A new CVE affects production. JioCloud flags the impacted internet-facing assets and auto-schedules patches.

Fix without manual intervention

Automated patching — on your terms. Continuous scanning detects issues, the user sets the patch window, and JioCloud handles deployment, validation, and reporting.

Govern exceptions with confidence

When a legacy app cannot be patched, JioCloud enables a controlled exemption with mandatory business case logging, security controls, and automated expiry — balancing compliance with operational needs.

Who It's For

CISOs and security leaders - Minimise risk exposure and demonstrate improvement.

IT Ops and cloud teams - Automate patching across platforms without slowing operations.

Compliance and audit teams - Maintain policy alignment and evidence trails.

DevOps engineers - Secure fast-moving environments with built-in workflows.

Why JioCloud

Risk-based intelligence: Prioritise what to patch now—with business context and exploit insights.

Enterprise-grade framework: Built for large, regulated setups - with policy enforcement and audit logs.

Integrated ecosystem: Works with your CMDB, ITSM, cloud, and DevOps pipelines.

Backed by experts: Trusted by critical sectors, supported by JioCloud's security leadership.

JioCloud

Ready to Minimise Risk - Without Manual Headaches?

Reach us at jpl.cloudsales@ril.com or visit (website)