ORACLE

OCI Fleet Application Management

Transforming full-stack patching for Financial Services

The Threat Landscape

A cornerstone of cybersecurity, Patch management is now more critical than ever as organizations face increasing risks from data breaches, ransomware, and other costly cyberattacks. The surge in software vulnerabilities, combined with the relentless pace of cyber threats, adds to the challenge. At the same time, enterprises must safeguard an ever-growing, complex footprint of applications, environments, and data - making patch management even harder.

Financial institutions, regardless of size, acutely experience these challenges. The sensitive data they manage, the critical nature of their operations, their scale, and the high stakes of their business have made them prime targets for cyberattacks. These companies struggle to keep up with software patching, not only to defend against attacks but also to meet strict regulatory and compliance requirements.

Regulation further underscores the patching imperative

Among other requirements, regulation mandates that:

- Core Banking Systems - patched on a quarterly schedule, with critical fixes patched within 24-48 hours
- Payment Processing and Fraud Detection systems – updated monthly, immediate fixes for high-risk issues or breaches
- Online and mobile banking apps - bi-weekly updates, critical fixes within 7 days.
- ATM operations software - patched monthly, critical patches within 72 hours.

These are enforced by various regulatory bodies and standards world-wide.

In the US these include the Federal Reserve (Fed), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Payment Card Industry Data Security Standards (PCI DSS), the Federal Financial Institutions Examination Council (FFIEC), Consumer Financial Protection Bureau (CFPB), National Institute of Standards and Technology (NIST), and more. The European Banking Authority (EBA), European Central Bank (ECB), European Payment Services Directive 2 (PSD2), EBA Guidelines on ICT and Security Risk Management, Financial Conduct Authority (FCA) in the UK, Central Bank of the UAE, Dubai Financial Services Authority (DFSA), and other institutions in the different geographies mandate similar policies.

Financial Services struggle to keep up

FSIs face a relentless patching cycle due to the fast-evolving threat landscape and the complexity of their technology stacks.

These stacks often include dozens, sometimes hundreds, of interdependent components—from operating systems to application tiers—that require regular patching across various environments.

All of this must be managed under strict service-level objectives (SLOs), security, and compliance requirements. Siloed processes, manual handoffs (with many patch operations still tracked using spreadsheets and emails), and skills shortage further exasperate the problem.

Stop chasing spreadsheets or manual processes, scrambling to fix deployment failures, or losing sleep over your next audit. Discover how OCI Fleet Application Management can help! >

OCI Fleet Application Management

Simplify centralized management and full-stack patch compliance at scale for *any* technology deployed in OCI

By reducing the complexity, effort, and cost around day2 patch operations, OCI Fleet Application Management helps financial services improve IT productivity, stay current with the latest patches, reduce risk, and enhance their compliance and security.

Connect with us:

Contact your Oracle representative to discuss your needs

Learn more about the service: oracle.com/cloud/fleet-application-management

Take the pain out of patch management!

With auto-discovery of software inventory and patch data, easy management with Fleets, and a catalogue of prebuilt, customizable Runbooks, OCI Fleet Application Management enhances standardization, governance, and operational efficiency across the enterprise.

Key capabilities:

- **Easy management with Fleets**: Organize cloud resources across your portfolio in hierarchical groupings based on the type of resource, environment, installed software, business applications, or custom tags. Centralize operations – report, manage and apply patches and updates across the entire fleet with one click.

- **Support any environment:** Consolidate patch and IT operations across OCI, multicloud, hybrid and on-premises infrastructure (*Coming soon!)

- **Enable Continuous Compliance**: Auto-discovery of the software inventory deployed in your fleets, along with its patch compliance data, audit reports against policy rules, and automatic drift detection -- all help ensure that you’re always running the latest, most secure patch version.

- **Full-stack touchless patch management:** Easily patch specific components, an entire stack, or roll out a patch across thousands of resources. Hardened processes, state management, and validation of the patch are handled automatically. You can schedule touchless patching to run during specific maintenance windows or trigger patching on-demand to remediate compliance issues.

- **OOTB patching for Oracle Products and popular technologies**: Prebuilt runbooks enable customers to automatically discover, verify and patch Oracle Linux, Oracle Fusion stack - prevalent in Oracle industry applications including Oracle Banking, Oracle Human Capital Management (HCM), WebLogic, Java, Exadata Database service, and more. Windows, Apache Tomcat, and other technologies are also supported, with more added on-going. In addition, customers can customize the runbook to enable patching of other 3rd-party software or support their specific processes.

- **Powerful IT automation with Runbooks & Scheduler:** Intuitive GUI, customizable prebuilt runbooks, and the ability to connect your existing automation scripts enable you to trigger patches and other IT processes based on compliance / environment state, governance policies, recurring schedule, or maintenance window.