

How Chef Solves Your Infrastructure Challenges



1. Orchestrate Incident Response

- Identify and isolate the affected nodes
- Run a compliance scan
- Execute controlled shutdown and remediation
- Implement rollback safeguards



6. Execute Ad-Hoc and Scheduled Jobs

- Access the centralized dashboard
- Execute jobs ad-hoc or schedule later
- Customize your DevSecOps workflows
- Leverage consolidated reporting and monitoring



2. Streamline Patching Across Your IT Estate

- Create a tailored node list
- Perform patch deployment in batches
- Schedule jobs during low-traffic intervals
- Automate documentation and reporting



5. Be Prepared for Compliance and Audits

- Filter nodes automatically by OS, application or compliance state
- Schedule recurring compliance scans that generate detailed reports
- Save non-compliant nodes to a result list and automatically trigger remediation workflows



3. Perform Controlled OS Upgrades

- Identify and target specific node groups
- Execute upgrades sequentially
- Monitor and roll back if necessary
- Leverage real-time reporting



4. Perform SSL/TLS Certificate Rotation

- Monitor nodes for expiring/expired certificates continuously
- Orchestrate the entire certificate renewal process - from validation to deployment
- Maintain automated, interruption-free certificate updates and reduce manual errors



Automate. Orchestrate. Accelerate



[Request Free Trial](#)