DATASHEET

Patching Service

Business challenge

Organizations are constantly trying to stay secure and keep their systems up to date, but patch management isn't a simple process. In fact, applying the patch itself is just one part of the overall workflow, which involves multiple teams and various steps. This process flow is usually planned weeks in advance.

A majority of the workflow varies based on the level of automation in place. Some teams rely strictly on manual updates, while others have automated pieces of the workflow but still have several manual steps.

Challenges:

- **Communication:** Scheduling and coordination between teams can be difficult, resulting in more downtime and unsuccessful patching runs.
- **Visibility:** Access to patching data is fragmented, status of patches can vary and reporting is dispersed through multiple tools.
- **Managing multiple OSes:** There is no single workflow to patch all OSes because each OS requires different tools, like Red Hat Satellite, WSUS, etc.
- **Time-consuming:** Even with some automation in place, coordinating maintenance can take weeks.
- **Error-prone:** Manual updates are tedious and can lead to complications like partially applied patches, downtime, and misconfigured servers.

Customer benefits

- Standardize the patching workflow and reduce constraints on internal resources.
- Reliably deploy patches and update machines with increased confidence.
- Ensure systems are up to date and patched on a regular cadence.
- Mitigate risks associated with patching systems at scale.
- Verify machines are patched to the required level.

Expected outcomes

- Console-driven, API, or CLI patching workflow
- Support for both Linux and Windows OS patching
- Self-service patching availability backed by role-based access control
- Systems can be consistently patched and updated
- Scheduling windows for patch automation to be applied
- Blackout windows defined to avoid making changes during peak times
- Improved scalability through patch standardization
- Standard workflow for compliance and security alignment

puppet

Who will benefit?

Are you falling behind on your patches? Does coordinating patches between teams and systems require significant time and effort? Are you maintaining spreadsheets to track patching state, schedules and blackout times? Do you find your teams struggling to keep up with patching needs and building one-off fixes that don't scale?

A Puppet professional can help standardize your patching workflow, build out tasks to trigger that workflow via Puppet Enterprise, and scale it out to your teams via RBAC and self-service jobs.

What you can expect

Puppet's patching service is your one-stop shop for ensuring your organization can patch its machines quickly and reliably. A Puppet professional will help you set up a standardized, automated patching workflow that will scale, and help you deploy it in a way that allows others in the organization to trigger the workflow in a self-service manner, with appropriate scheduling windows.

Assumptions

- Pricing will vary based on duration of engagement.
- The customer is on PE 2017.3 or later, or 2019.1+ (with scheduling).
- The customer has access to the machines.
- The current environment is functional, with Puppet workflows in place.
- The customer will provide the Puppet professional with an environment to test Puppet code for required compliance reporting
- The customer has the ability to install additional modules from the Puppet Forge.