PTM

Privileged Task Management

Privileged Task Management runs automatically on behalf of your team members without granting insecure and unaccountable direct access to any privileged accounts – allowing SysAdmins to safely delegate complicated multi-step tasks without fear of human error, by reducing execution to a single click.

SAFELY DELEGATE PRE-PACKAGED TASKS

Any business process can be packaged up as a task.

- Privileged tasks can be run with a single click - without granting insecure and unaccountable access to privileged accounts
- Allow for risk-free delegation to 3rd party or untrained staff
- Run automatically, or with user-defined schedules.

INCLUDE FILE UPLOADS/ DOWNLOAD ACTIONS

Tasks can contain as many actions as you need them to.

- This includes uploading to, and downloading from devices
- Start a task with a file import to verify whether it requires further execution
- Logs can be downloaded for diagnostic purposes without requiring privileged access.

DEFINE KNOWN FAULT WORKAROUNDS

Design tasks to fix problems that are commonly encountered.

- Problems on systems and devices that have well-known fixes can be fully automated
- Delegate these fixes without the need to escalate to more senior members of your team
- Known faults fixed immediately with a single click.

EXCEPTIONAL MULTI-PROTOCOL & API SUPPORT

Tasks can run against a range of devices with a variety of management interfaces.

- SSH, Telnet, RDP, VNC, RPC, vSphere, HTTP(S) and even bespoke API contracts
- Full programmatic interactivity between devices - highly optimised tasks, per device.

AUTOMATED EMAIL ALERTS & DEVICE BACKUPS

Automatically deliver email alerts to devices or owners whenever a task has been performed.

- Summarise the user, task, target device and confirmation of successful completion
- Automatic backups using vendors' own commands, storing them securely.

COMPLETE CHANGE TICKET AUTHENTICATION SYSTEM

Optionally require change ticket authentication to perform actions, ensuring full accountability.

- PTM allows for free text input to be used as a change ticket reference
- These are logged within the audit trail of a task, and can later be used as search criteria.

WHAT IS PRIVILEGED TASK MANAGEMENT?

With Privileged Task Management, Osirium's PxM Platform combines the benefits of security, efficiency, time saving and accuracy.

Every time a user is given access to a Privileged Account a risk is created. Privileged Task Management (PTM) is the cleanest and safest way of granting the ability to perform a series of known, auditable tasks without granting excessive privileges to the user. The actual tasks can all run under the same Privileged Account and Osirium will keep track of who issued the commands and the parameters used.

Taking a simple example of a command line task that needs to be run across several machines before PTM, we find that the user has to find the credentials for each system, login, issue the commands, logout and then move on to the next system. With Osirium's PxM Platform, they select the task, check the systems required and submit the job. Typically a 20 minute task can be reduced to an error and risk-free 8 seconds.

DELEGATE THE TASK, NOT THE PRIVILEGE

With the PxM Platform's automation of SysAdmin tasks, login sessions become unnecessary – instantly mitigating your most vulnerable attack surface whilst increasing workflow efficiency.

Privileged Task Management runs automatically on behalf of your team members without granting insecure and unaccountable direct access to any privileged accounts – allowing SysAdmins to safely delegate complicated multi-step tasks, without fear of human error by reducing execution to a single click.

Privileged Task Management is a great way of delegating those repetitive tasks to the most appropriate department by wrapping business tasks up into a 'first-call fix'. As a result, your team can dispense with wading through loathsome run books, hunting down shared login credentials, etc. and can instead more effectively focus on delivering an IT infrastructure fit to grant them a competitive edge.

INFRASTRUCTURE & SYSTEM REQUIREMENTS (PXM PLATFORM)

Virtualisation:	VMware 5 through 6, Xen, Hyper-V, Azure, AWS.
Osirium appliance allocations:	IP Address, 40GB storage, 2 x CPU cores, 8GB RAM.
Desktop Client Requirements:	Microsoft Windows & Microsoft .NET Framework v4.5.2 / macOS 10.9 or later
Minimum Browser & Plugins:	Internet Explorer 10 / Chrome 50