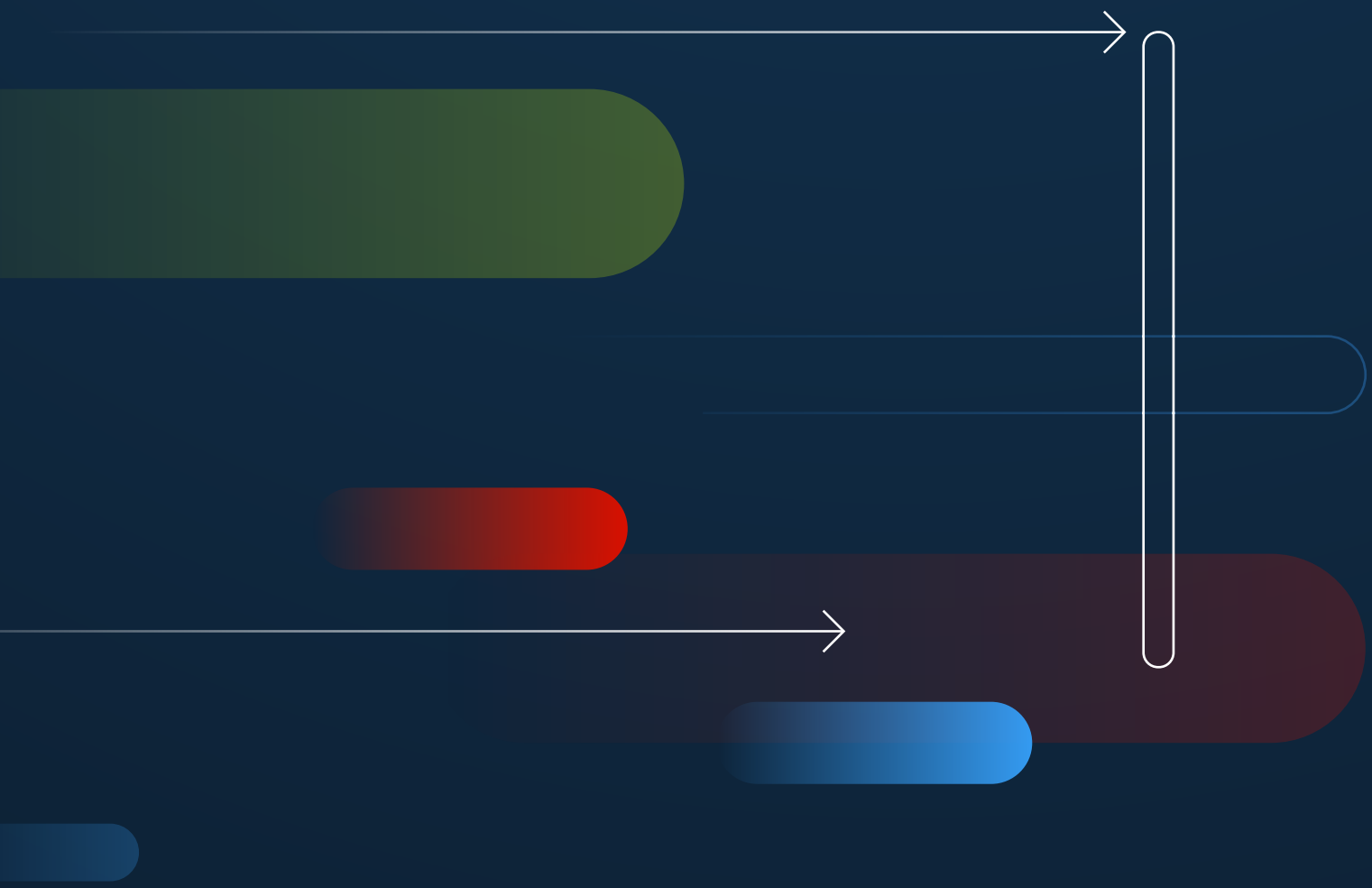
TuxCare
We Take Care of Linux

WHITEPAPER

Integration of KernelCare (and LibCare) into 3rd party management platform with ePortal hosted on TuxCare's side



www.tuxcare.com

PART 1

Registration and Activation

(scheme next page)

Installation of KernelCare agent:

A lightweight agent, mere hundreds of kilobytes in size, is effortlessly installed on the targeted systems using a simple command-line interface (CLI) command.

During the registration process, either Random Registration Keys or Customer's IDs may be employed.

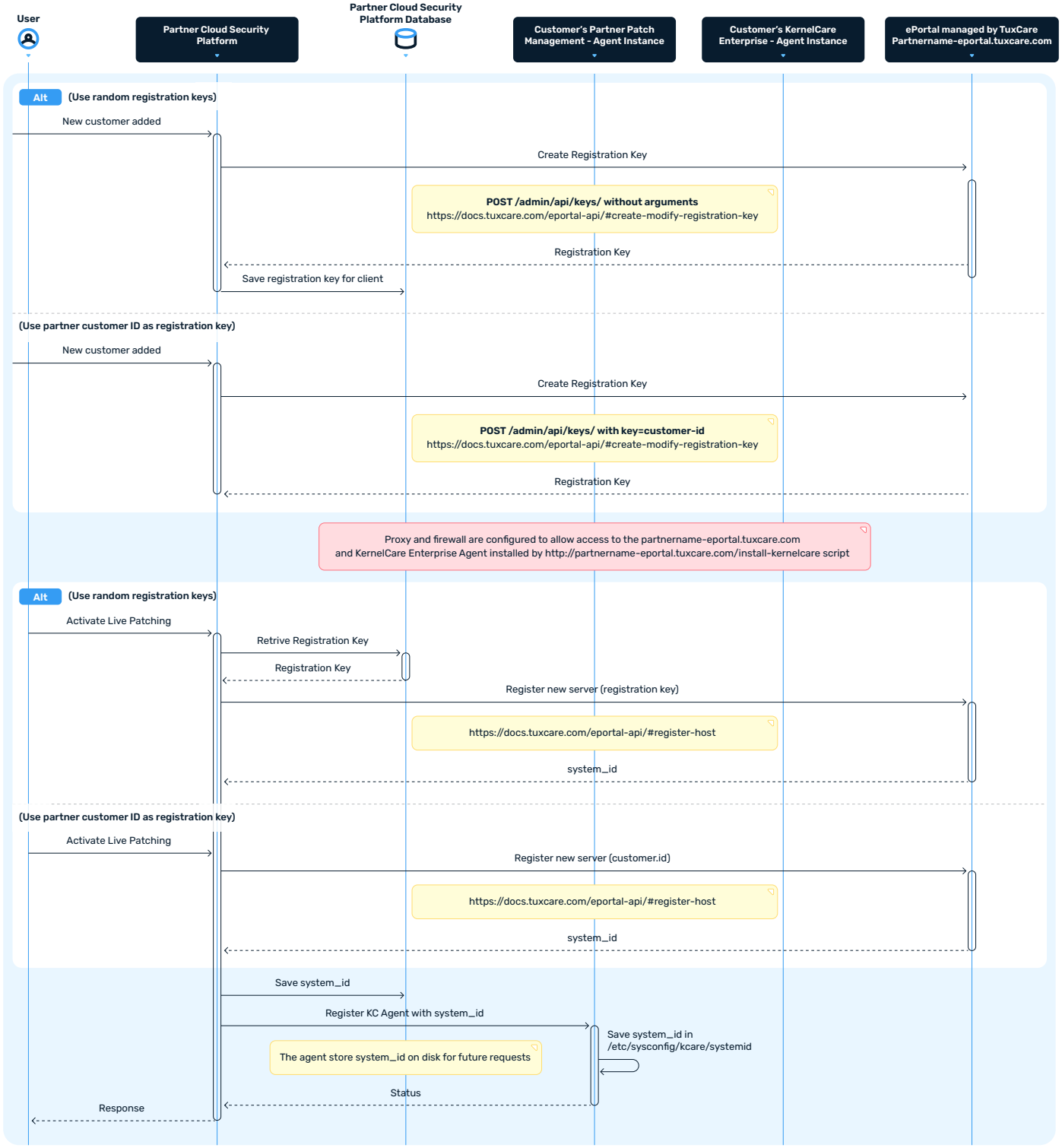
Registration Key creation:

1. The customer initiates the key creation process by selecting "Create a Key for LivePatching".
2. Command is dispatched to ePortal (TuxCare), prompting the generation of a key. This Registration Key is then relayed back to the customer and simultaneously stored within Partner's Management Platform, whether it be in the cloud or on-premises.

Activation of LivePatching functionality – two scenarios:

1. **Utilization of Random Registration Keys**
   - 1.1. Customer activates LivePatching by selecting "Activate LivePatching". The registration key is retrieved from the Partner's Management Platform (cloud or on-prem).
   - 1.2. The customer selects "Add new server", pushing system information along with the key to the ePortal hosted on TuxCare side.
   - 1.3. The ePortal returns System ID to the Partner's Management Platform (cloud or on-prem).
2. **Utilization of Customer ID for registration**
   - 2.1. The customer selects "Add new server", pushing system information along with the Customer's ID to the ePortal hosted on TuxCare side.
   - 2.2. The ePortal returns System ID to the Partner's Management Platform (cloud or on-prem).
   - 2.3. The System ID is retained and stored by KernelCare agent.

Registration



PART 2

Operation

(scheme below)

Registration Key creation:

1. The customer initiates a vulnerability scan by selecting “Scan for vulnerabilities” and receives a scan results from his Vuln Scanner.
2. The customer then selects “Check for available Live Patches (for Kernel or shared libraries)”. Metadata containing information about covered Common Vulnerabilities and Exposures (CVEs) and available patches is retrieved from the ePortal hosted by TuxCare.
3. The data from Vuln Scanner and the ePortal is systematically mapped resulting in a comprehensive list of vulnerabilities eligible for in-memory patching (LivePatching).
4. Upon identifying vulnerabilities the customer selects “LivePatch found vulnerabilities”, triggering the creation of a Job to fix the identified vulnerabilities. The patch is downloaded from the ePortal, undergoes security checks, and subsequently pushed to the agent for application.
5. The outcome of the Job is then displayed in the UI of the Partner’s Management Platform whether it is hosted in the cloud or on-prem.

Normal Operation