
infraguard
UNIFIED CLOUD SERVER MANAGEMENT
SECURE SCALABLE SOLUTION TO SUPERCHARGE YOUR MANAGED SERVICES OPERATIONS.

Table of Contents:

Table of Contents: 2

EXECUTIVE SUMMARY 3

Patching 4

- Traditional Patching Workflow 4
  - Technically Challenging 4
  - Highly Skilled Resources required 4
  - Repetitive Process 4
- InfraGuard Workflow for Patching 5
  - Patch policy 5
  - Patch Execution 5

Operations and Automation 6

- Traditionally 6
- Automation in InfraGuard 7
  - Examples of SOP: 7

Security In-Built 8

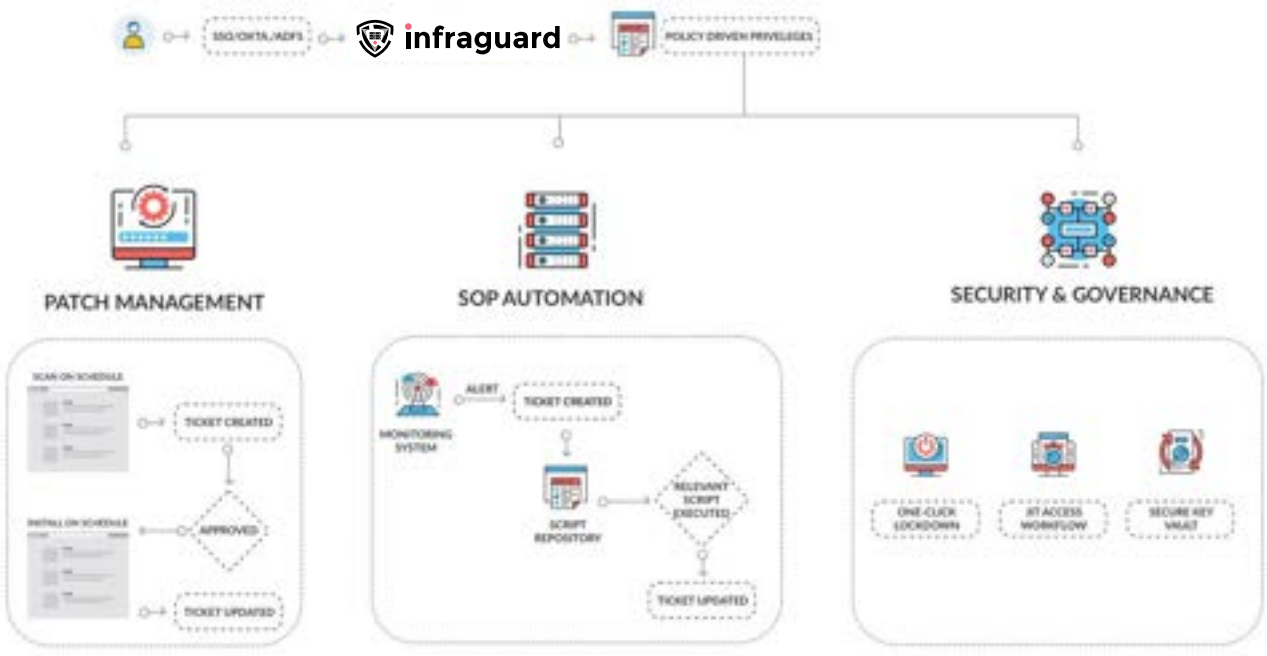
- Just in Time Access (JIT) 8
- Keys in Vault 9
- Key rotation 9
- Lockdown 9

EXECUTIVE SUMMARY

The InfraGuard Platform Consists of the following modules:

1. SSO
2. Patching Module
3. Access Management
4. Automation Platform

Managed Services operations need all these modules, starting from Authentication -> Followed by Policy based privileges to take action on the environment -> To capability to lockdown the environment to get absolute control when needed.



1. Patching

Traditional Patching Workflow

Patching traditionally required war-scale planning and execution across multiple teams in the organization. A typical patching story of the old world has been shown below.

Technically Challenging

Multiple phases are involved:

1. Patch Scan
2. Project Management to coordinate with all stakeholders
3. Backup of all different types of system
4. Patch Execution

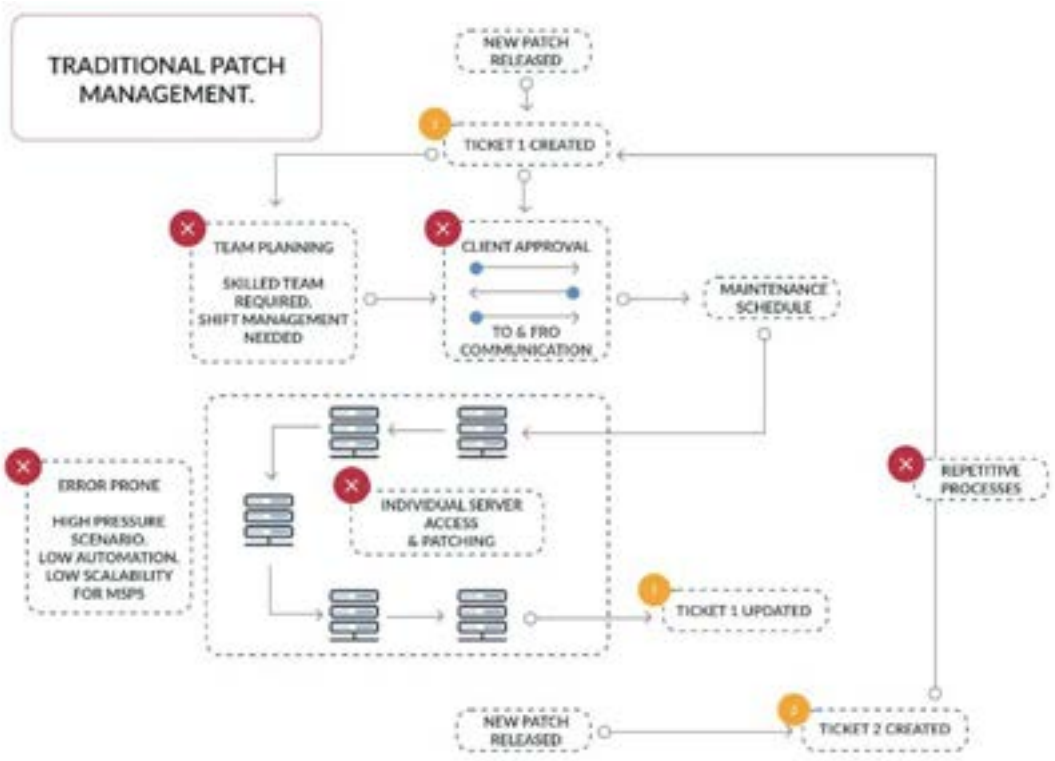
Highly Skilled Resources required

Variety of skilled resources are required to execute patching:

1. Multiple skills needed
    a. System Administrator
    b. Backup Administrator
    c. Project Management
    d. Patch Administrator

Repetitive Process

In every patch cycle the process is repeated and it's a war-scale planning every time.



InfraGuard Workflow for Patching

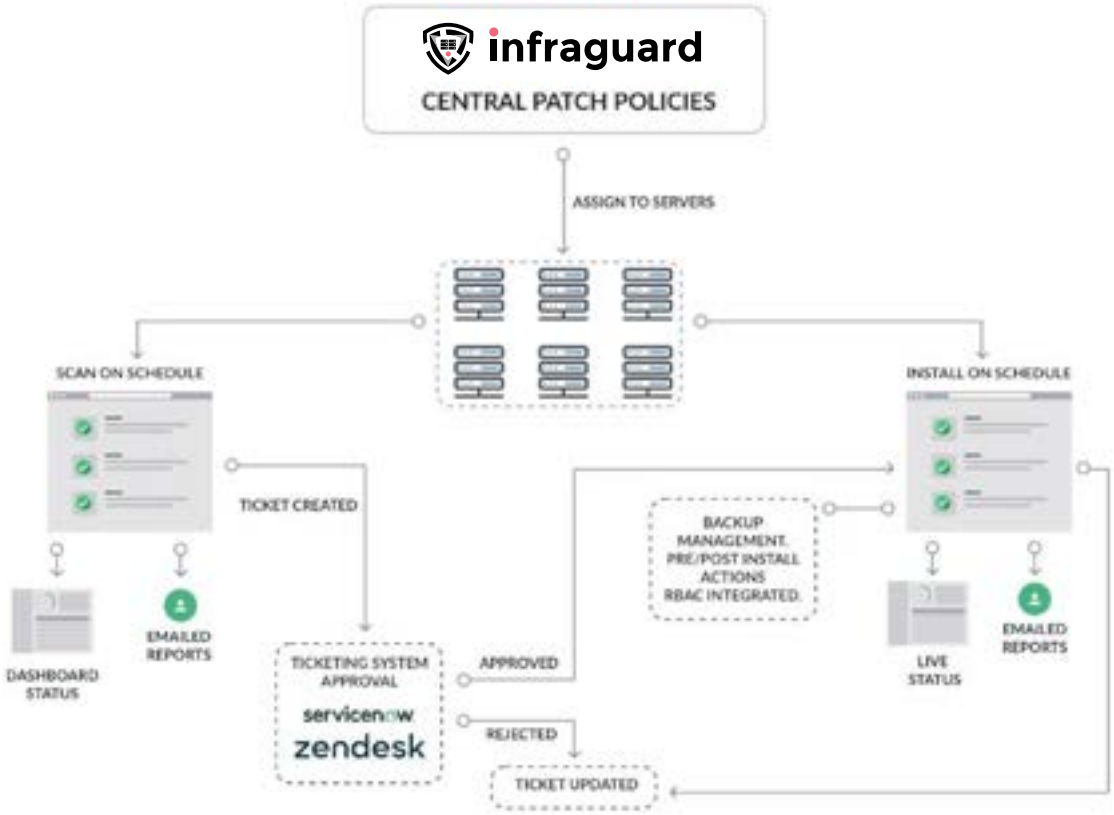
Patch policy

We recommend pre-approved patching policy for scanning and for patch execution.

Patch Execution

The whole of the patching workflow has been automated, and it's just a button click to complete patches on as many servers simultaneously or in a sequence.

The patching workflow in InfraGuard is as below:



2. Operations and Automation

Traditionally

Onboarding of customers has been a time-consuming and human-error prone project. Installing agents in the customer environment to deliver services used to be difficult as someone needed to login on each server and run install agent commands.

Traditionally operations have mostly been team driven and some automation using scripts or cron jobs.

SOP - has been defined in documents, and steps to execute the SOP is written in words which the operations team follow to execute.

This process has been highly dependent on few skilled resources, and everytime a resource leaves, the knowledbase of the environment is lost.

Automation in InfraGuard

We have a script repository for each Standard Operating Procedure, and that repository can be shared across business units in the organization.

All SOP is converted into script and can be kept in the script repository.

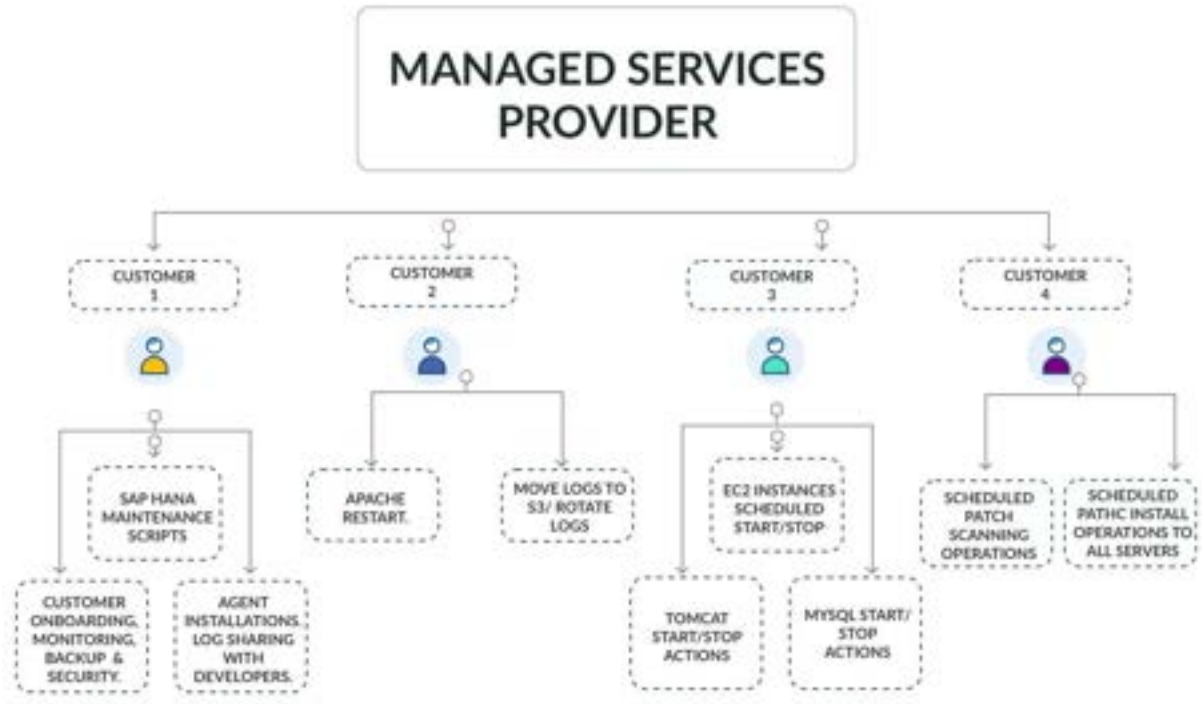
That way the organization builds a knowledge base which is not dependent on resources leaving the team.

Execution of SOP can be scheduled and can be triggered from the ticketing system.

Examples of SOP:

This is how a typical Managed Services Partner would be using InfraGuard to onboard and execute different kinds of SOPs for a variety of customers they may have.

InfraGuard takes care of security by itself at a very granular level.

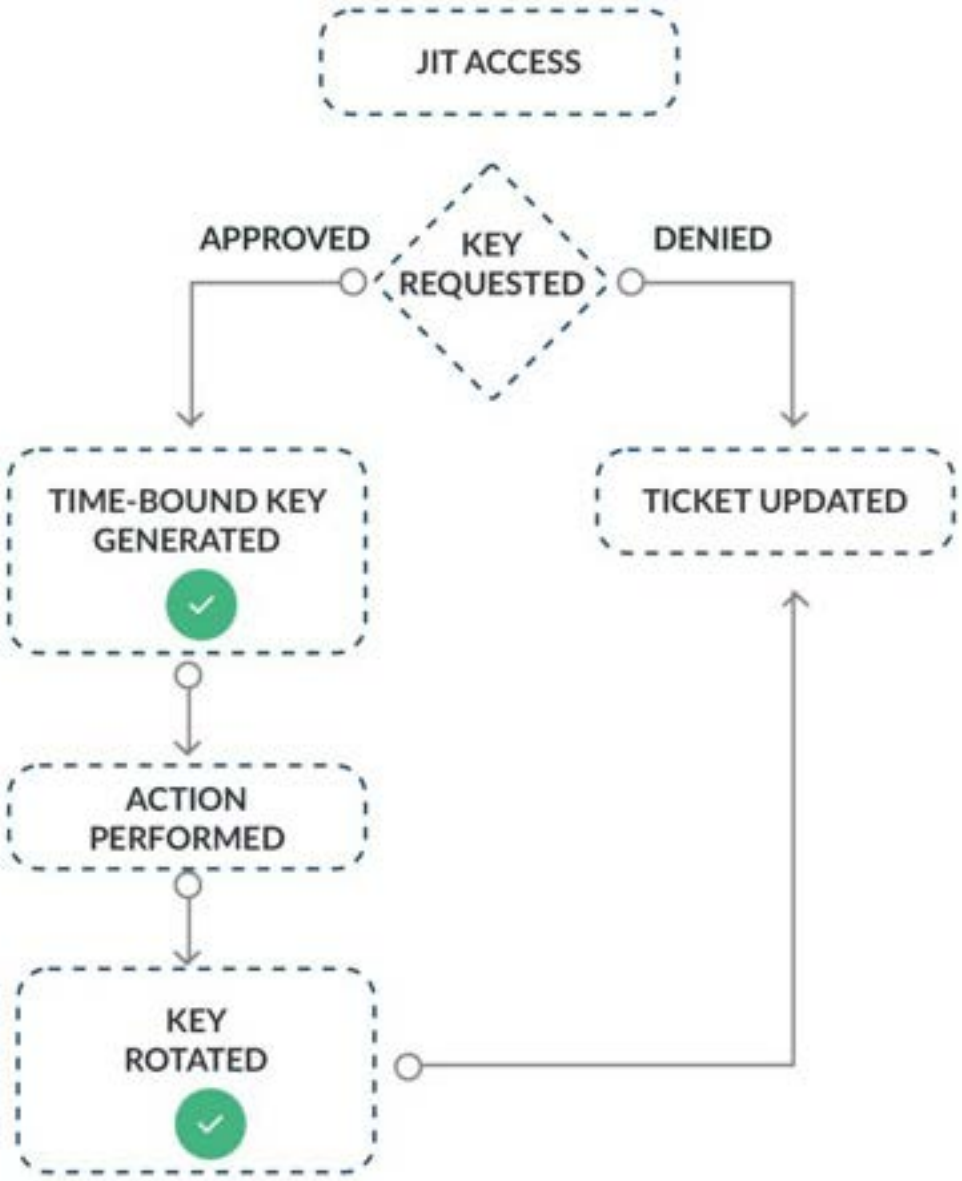


3. Security In-Built

Just in Time Access (JIT)

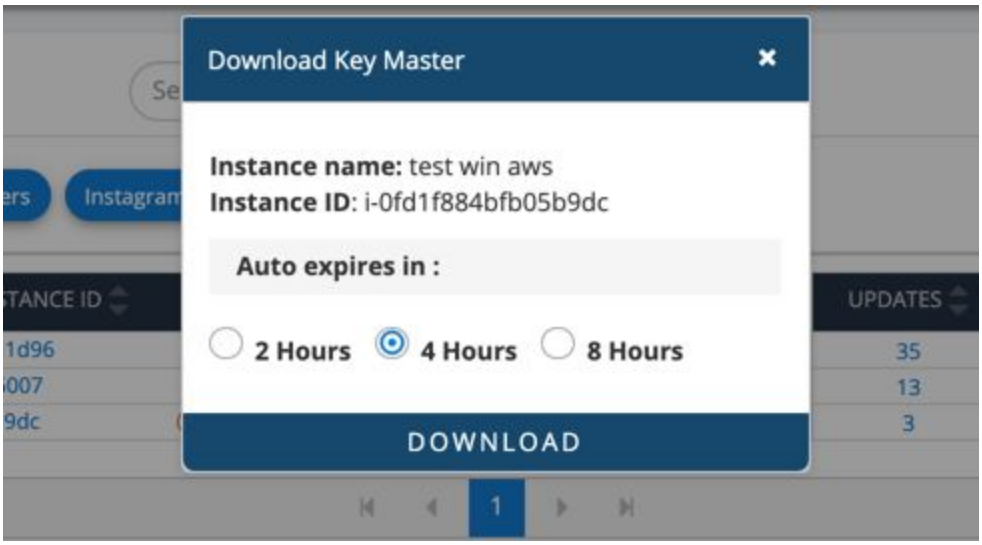
Access in this scenario is defined by the ticketing system. When an approved ticket is assigned to a user, his keys will be enabled at that time. The keys will be time-bound either expiring at a predefined time interval or via input from available integrations with tools such as Shift Management API.

As soon as the action is completed, user access is revoked and the ticket is closed.



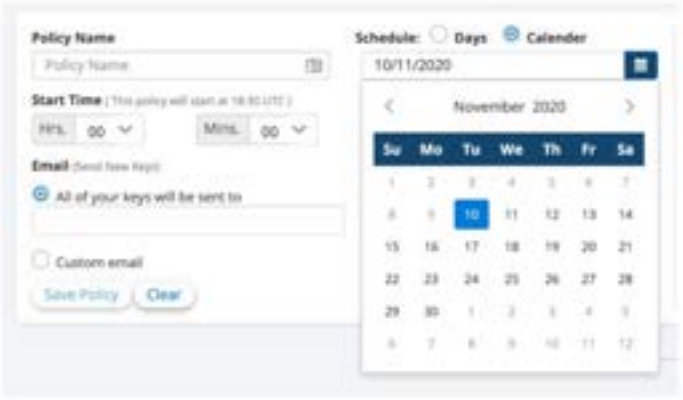
Keys in Vault

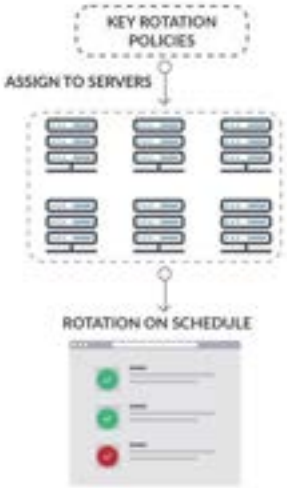
In conjunction with a ticketing system approval based workflow as above, InfraGuard also comes pre-built with an Encrypted Vault to store access keys. Fundamentally, no one should have a live key lying around. When needed, users with the required privileges on InfraGuard (managed by granular RBAC) can download an access key. They key will mandatorily be auto-rotated within a maximum of 8 hours from the time of issue.



Key rotation

The centrally set Key Rotation policies are assigned to servers based on custom groupings. So servers in a high-critical environment could be given more frequent rotation policies. The immediate benefit is that rather than worrying who has live keys, one can rotate all at defined intervals to reduce any risk.





Lockdown

InfraGuard's way of Managed Services is built around preventive security and faster response times. If your servers are under attack, it might take time for your security team to find the cause and rectify. But while that happens, a single 'Lockdown' button on InfraGuard can immediately terminate all remote connections and prevent any new ones to be established. Once the attack has been tackled, the servers can be unlocked from the same single-click. This feature too is strengthened by the RBAC so that only right-privilege users can take the actions.