infraguard

UNIFIED SERVER MANAGEMENT

PATCH MANAGEMENT | ACCESS MANAGEMENT | SOP AUTOMATION

For Demo
contact@infraguard.io

WHAT MAKES US DIFFERENT

Customisable Patch management Flows that simply work On-Demand & On-Schedule across all Operating Systems.

Granular Access Control with In-Built Role-Based privileges that make it easy to prevent unauthorised actions.

Combination of Script repository, Open API and 3rd party integrations for seamless custom SOP automation.

KEY FEATURES

- MULTI-ACCOUNT MANAGEMENT
- UNLIMITED SCALABILITY
- CUSTOM INTEGRATIONS
- OPEN API

The InfraGuard Value

What if all your servers across accounts, regions and Cloud Providers could be visualised in a single dashboard with In-built Role Based Access Control and sophisticated automation workflows? That is **InfraGuard**. An ISO & SOC2TYPE2 Compliant software that works across all Operating Systems and Cloud providers to create Centres of Excellence around Access Management, Patch Management and SOP Automation.

InfraGuard.io
contact@infraguard.io
SINGAPORE | AUSTRALIA | INDIA | PHILIPPINES

infraguard

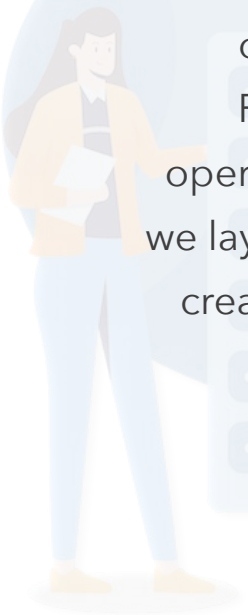
UNIFIED SERVER MANAGEMENT

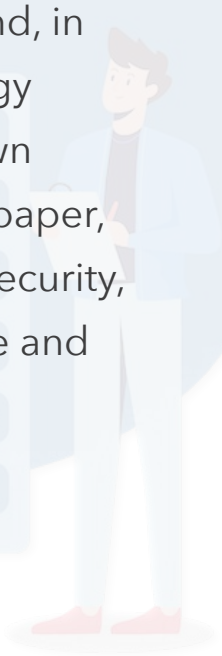
COMPLETE

SECURITY FOR YOUR SERVER INFRASTRUCTURE IN 2021

WHITE PAPER

In the Post-Covid world, even the traditional businesses will increasingly move online and thereby to the Cloud. How we create, structure and secure the server infrastructures will define how successful & efficient the future will be. This is not a small responsibility and, in order to perform it adequately, the Technology Professionals will need to ensure that their own operations are secure and scalable. In this white-paper, we lay down an achievable roadmap to enhance security, create efficiency and utilise automation in a large and hybrid server infrastructure.





Created By: InfraGuard.io

infraguard

GOVERNANCE VISION

With the advent of cloud technologies, majority of businesses are now cloud-first and those that are not, are migrating fast. In the context of Server Administrators, DevOps & SecOps teams, this means that not only are the workloads getting more intensive, they are also getting more complicated. To get work done, it is often a race between Operations and Security - and more often than not, Security takes a backseat.

For server infrastructures to be truly secure, we recommend a layered approach to security that covers ***Insider Threats, External Threats & Operational Processes.***

INSIDER THREATS

How does your enterprise allocate access of internal & client infrastructure to employees? How does monitoring of such access happen and how are threats dealt with?

EXTERNAL THREATS

How secure and updated are your systems from vulnerabilities that can be exploited? How is access prevented from external agencies?

OPERATIONAL PROCESSES

What role does automation play in your operations? How ad-hoc are server actions? Are they being regulated and monitored?

> *"There's no silver bullet solution with cyber security, a layered defence is the only viable defence.*
>
> - James Scott, Institute for Critical Infrastructure Technology

infraguard

A WORD ABOUT THIS NEW WORLD

POST-CORONA CHANGES

As the world reels under the health & economic impact of the Covid-19 pandemic, we, as technologists, are under an additional responsibility to become the backbone of revival.

In the last couple of decades tech industry has evolved at a breathtaking pace, often choosing Go-To-Market above everything else. Today, we urge the community to place security & stability at an equal footing. Prevention will always be better than cure. And as our workloads expand with traditional businesses moving online and virtual interactions becoming the norm, we must recognise that technology will change from being an enabler to becoming a necessity.

In our individual roles, in our own capacities, let's be steadfast in bringing the world back to its feet.

INSIDER THREATS IDENTIFICATION & MANAGEMENT

Good security practices start from inside out. In our years of managing large enterprise infrastructures, we have often seen the most sophisticated of security softwares failing due to internal employees performing unwanted actions (knowingly or unknowingly).

We recommend enterprises to follow the following 5 steps of the Complete Security Framework.

1. ROLE-BASED POLICIES
2. JUST IN TIME ACCESS
3. SINGLE POINT RESPONSIBILITY
4. AUTOMATED KEY ROTATIONS
5. POST-ACTION AUDITING

1. ROLE-BASED POLICIES

All roles are not created equal. Right at the onset, it is important for enterprises to divide their teams (**internal employees & external contractors**) into roles based on the level of access required. This division should take into account, not only "*Who has access to which servers*" but also "*What action they can take on each server*".

This is a very important distinction as too often enterprises simply create roles on the former point without having a way to enforce the latter.

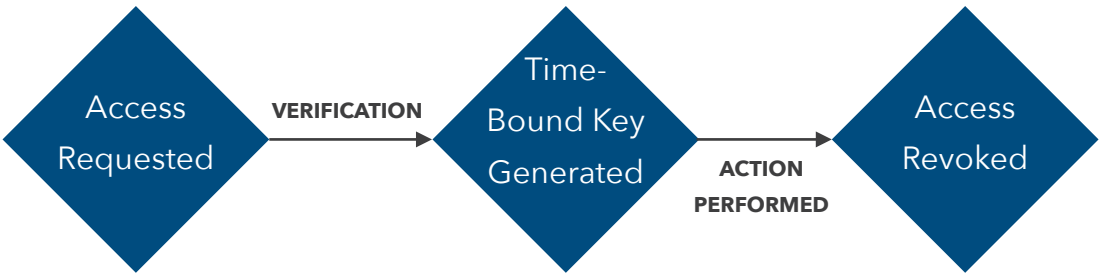
infraguard

Part of the problem lies in the way usual access protocols (SSH/RDP) are structured. They are made to function as a monolith door - Once the key to that door is given, the authorised person can perform any actions. That leaves a lot of scope for unwanted operations. Furthermore, even when using Identity & Access Management solutions, enterprises often ignore the **KEEP IT SIMPLE** principle. If you use a complex way of assigning & managing roles - it will neither be efficient nor enforced.

At **InfraGuard**, we recommend against using SSH/RDP for routine server operations and have built a simple workflow to enforce secure role-based access that enables actions right from the dashboard.

2. JUST IN TIME ACCESS

Server access should always be on an IF-NEEDED and WHEN-NEEDED basis. While the *if-needed* part can be handled by role-based access, to enforce the *when-needed* paradigm, workflow changes are often needed.



This workflow can be initiated by the requester or the approver, and in both cases a ticket number and a reason for access is to be provided before approving/rejecting the request. In the case when the request is genuine - a time bound access is provided. which expires on its own accord once the action is completed.

Such a workflow ensures that no access-keys are lying around that can be used for unauthorised actions in future.

3. SINGLE-POINT RESPONSIBILITY

A robust & locked facility that keeps its master-key with 10 different personnel can hardly be called secure. Unfortunately, this is one of the ways in which operation-alertness has been prioritised over secure standards. Multiple people can access the servers at any point - often all with the same username and key. This makes it easy to shift blame and difficult to allocate responsibility.

Beyond the first two points explained above, every access key must have a single caretaker. In the event that that key is misused or misplaced, the diagnosis and the treatment of the issues will be faster. Furthermore, it will give a direct recommendation on the how to avoid similar issues in the future. **InfraGuard's** auto-key rotation (explained in next point) includes Single-Point Responsibility as its core driving force.

4. AUTOMATED KEY-ROTATIONS

Security best practices discourage extensive and prolonged reuse of Access Keys. While most of our partners choose somewhere between 30 to 90 days for an enforced key rotation action, for sensitive servers this duration could be as low as a few hours. This action should always be automated since putting this in the realm of a manual process would defeat the entire purpose of an extra security layer.

Even for servers which have not been accessed for some time, or with keys that have never been used, it is a good practice to enforce auto-rotation and allocate new credentials to the required personnels.

5. PERIODIC POST-ACTION AUDITING

Too often auditing happens only after disaster has struck. As such, it is more an exercise on allocating blame than one which is preventive in nature. Regular auditing of server actions can be done both manually as well in an automated manner. Major checks should include at least the following:

- What are the common actions being taken on servers - what commands and scripts are being run?
- Which employees are accessing the servers - are they all in alignment with allocated roles?
- How many remote users are present in your servers - are they all necessary?
- When was the last key rotation date? What is the enforced key rotation duration?

Identification and management of insider threats is a tricky issue, susceptible to be pushed under the carpet. While enterprises have to ensure security, they also have to ascertain that employees do not feel a lack of trust. Hence, clear and pre-stated policies should be defined right at the onset. Checks and balances should be in place. And finally, periodic reassessment of above policies should be done by the management team so that preventive actions can be taken before disaster strikes.

EXTERNAL THREATS IDENTIFICATION & MANAGEMENT

Mitigating external threats (beyond Access Management covered in previous section) is all about reducing/removing the number of attack vectors that can be exploited by a malicious party. A periodic security assessment of your cloud architectures that checks your public/private servers, whitelisted IPs and open ports is always beneficial. Too often, gaps creep in during the time of cloud migration or expansion in these areas. That said, one of the simplest and critical actions is to keep your servers updated and patched.

All major Operating Systems release regular fixes to vulnerabilities. The problem arises when enterprises are slow to react to these patches and this leads to a vulnerable period. Patch Management has also taken on the image of an unmanageable overhead that can break systems and lead to downtime. Too many enterprises use their servers without updating for years - leading to even more complexities when they eventually decide to apply all fixes at once.

A clear and enforced Patch Management policy can save plenty of future headaches.

57%

of cyberattack victims report that their breaches could have been prevented by installing an available patch.

- Service Now Study with Ponemon Institute, 2018.

infraguard

A clear Patch Management policy can be easily enforced, and created just by designing on the below three points.

1. COMPLIANCE MONITORING
2. AUTOMATED SERVER SCANS
3. DEFINED & AUTOMATED PATCH INSTALLATION FLOWS

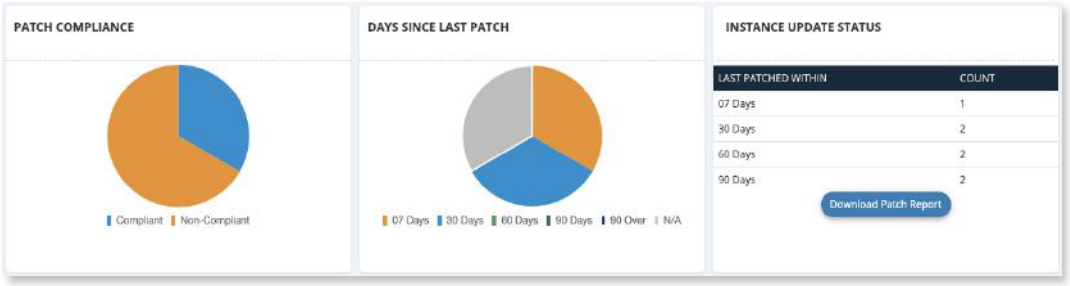
1. COMPLIANCE MONITORING

With large-scale infrastructure, a central Compliance Dashboard is essential. If the processes are based on individually checking each server across accounts, regions & providers, it is almost certain that critical patches will be missed.

A central dashboard, like the one which **InfraGuard** provides, gives a bird's eye view on the the overall scenario and at a minimum should show the following details:

- **How many servers are Non-Compliant** as per the centrally set standards. These standards should ensure that no Security or Critical patches are pending.
- **When were the servers last updated**. Given the frequency of new patch releases, if your servers are left unattended for months, it reflects a security gap.
- **Which servers have crossed the alerting threshold**. If there are servers which have crossed the threshold set (such as not updated in 90 days) then those should be clearly depicted.

- **Downloadable and Shareable reports**. A dedicated schedule should be set up, whereby the Compliance Reports are analysed and remediative action is taken.



2. AUTOMATED SERVER SCANS

Whether you are running 10 servers or 1000, scanning for updates is a task best done by automation. It is a recurring task and one that is easily configurable. Ideally, a dedicated Patch Manager role will be used for this purpose, to ensure that there is Single Point Responsibility to monitor the update status.

An efficient Server Scan Workflow could look something like this:

- Scan all servers every 7 days.
- Have a defined format for pending patch reporting that includes at least the Name of patch, Category and Severity.
- Ensure that the report is auto-emailed to necessary stakeholders as well as available for viewing from a central dashboard.
- Integrate the Scan Reports to a Ticketing System to create an automatic Change Request whenever patches are pending to be installed.

- Ascertain that update status is reflected accurately in the Compliance Dashboard.

3. DEFINED & AUTOMATED PATCH INSTALLATION FLOWS

Patch Installation is a high-criticality task that should be treated in the same manner as you would any other Mission-Critical process in your organisation. The need should be ascertained & defined, the servers categorised based on your operational processes, approval-matrix defined and automated policies implemented. Once done, these should be subject to periodic reviews and improvements.

InfraGuard recommends following general guidelines to get started on.

- Segment your servers into **projects** based on your most important parameters. Example segmentations can be around: Production & Non-Production servers, Servers in a particular Region/ Availability Zone, Servers with different Operating Systems or Servers with similar applications installed.
- Define the stakeholders who will approve the pending patch list, coordinate the maintenance window schedule and receive the reports before and after installations.
- Define the **Patch Installation Policy** for each project. This should include:
  - The category of patches that need to be installed.
  - The schedule for maintenance windows (on fixed dates or after a set interval).
  - Backups to be created either Pre-Install, Post-Install or both times.
  - Exclusion list of patches which need secondary approval and should not be installed automatically.

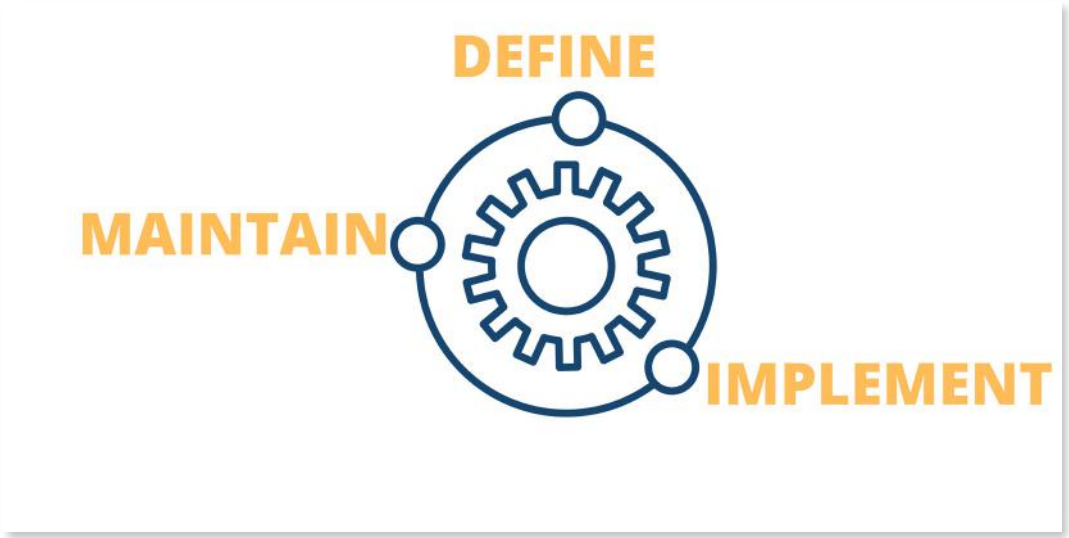
- Custom actions such as server rebooting or scripts that need to be run after installation.
- Post-Installation system checkups & reporting.

Patch Management has become a complicated task due to manual and inefficient workflows. This resulted in servers simply not being patched for months or years. This can be rectified if the policies are defined, automated and incrementally improved. It is possible that for the initial few patch events you would need to supervise the automations, but eventually the task will be driven by the system choices you make, leaving you free to analyse and enhance the automations as needed.

OPERATIONAL PROCESSES SECURED BY COMPLIANCE & GOVERNANCE

The Operational Processes need to keep both a micro and a macro perspective in mind during the design phase. While they need to perform the function for which they were conceptualised, they must also form an integral part of the overall compliance vision of the company.

InfraGuard recommends creating **Centres of Excellence** that accommodate Operations & Governance in a single flow.



Each Centre of Excellence should ideally have three phases **Define, Implement and Maintain**.

Let's look at the use case of Patch management to understand these further.

1. DEFINE

This phase will bring together all the stakeholders including internal and external parties, consultants & service providers. The Operations team (which will perform Patch Management) and the Compliance team (which has to ensure update standards are maintained) will take the inputs of development Teams, customer facing teams and others to draft a Patching Policy that will define:

- The RACI matrix (Responsible-Accountable-Consulted-Informed) group for each operation.
- The frequency of updates
- The standards to be maintained (as in the Security patches must be installed within 7 days of release)

- The sequence of servers to be patched
- The escalation & remediation steps in case of any patching problems.

2. IMPLEMENT

This phase will put into action the steps defined above. With **InfraGuard**, this means dividing the servers into projects and creating policies that are configured accordingly. These policies will include the schedules, reporting emails, sequences, backups and scripts to be run. They will be assigned & attached to the appropriate servers.

During the initial few runs, the policy executions will be monitored from the **InfraGuard** Live dashboard and post-installation reports analysed. If any patches fail to apply, the errors will be checked and rectified, before retrying the execution.

3. MAINTAIN & OPTIMISE

Once the Define & Implement phases have been through their test runs, the policies will be in automated mode requiring little to no manual intervention. The role of the stakeholders at this time shifts to maintaining the policies and attaching them to any new servers that are added to the infrastructure.

Periodically, they will analyse the parameters set for any improvements. These improvement could come via new feature added in **InfraGuard** or internal Organisational changes.

Using a **Centres of Excellence** paradigm for Operations ensures hassle-free processes while remaining flexible enough to change with future requirements. Coupled with Compliance & Auditing features such a log maintenance & management, Compliance dashboards, hygiene practises such as enforced MFA - the organisation can easily maintain a robust & secure infrastructure even at a large scale.

CONCLUSION

The roadmap outlined for Complete Server Security is meant to be achievable and implementable in any existing infrastructure. **InfraGuard** is created for technology teams of any size to be able to manage cross-provider and cross-platform servers from a single dashboard. It is available as a SaaS solution, as self-hosted enterprise deployment and as an API Integration. InfraGuard works seamlessly across AWS, Azure, GCP and Data Centres to offer comprehensive solutions for Patch Management, Access Management, SOP Automation and Governance.

If you would like to work with us in strengthening your server administration, lowering costs and enhancing automation. Drop us a line.

THANK YOU!

infraguard

UNIFIED SERVER MANAGEMENT

SINGAPORE | AUSTRALIA |
INDIA | PHILIPPINES

CONTACT
FOR A DEMO

WWW.INFRAGUARD.IO
EMAIL: CONTACT@INFRAGUARD.IO