giniminds

CASE STUDY:
VDI solution with Ransomware safeguard

VPNless VDI solution with safeguard from Ransomware

Exec. Summary: Work From Home (WFH) culture during and post COVID19 pandemic

Every organization; irrespective of size had Work From Home (WFH) policy as a choice. But COVID-19 has made it necessary for every organization to enforce WFH policy "mandatory".

WFH introduces concern around Productivity and Security for the management. It needs cultural change to ensure success of WFH policy. "Trust" is key ingredient and also change from "Activity based" to "Outcome based" culture is required to ensure desired Productivity is achieved with WFH policy.

To enable WFH for the employee, Organization need to ensure following

- Setup or scale Backend infrastructure (Internet Bandwidth, VPN or VDI Infrastructure, Security policy enforcement etc.)
- Home setup (laptop/desktop, Un-interrupted internet connection, UPS, Mouse, Monitors, printers/scanners etc.)

In the current situation, it is becoming difficult to make company owned and configured laptop/desktop to be made available to each and every employee at their home. The viable option is to allow employee(s) to use their personal devices (laptop, desktop, mobiles etc.) to connect corporate network security and carry out their daily official
activity.

Giniminds has a cost effective and state of the art "VPNless VDI solution" to fast track roll out of WFH policy to employees in "days" rather than "weeks".

Following are key & capabilities of the solution

- **Highly available, massively scalable, data redundant, software defined, fully secure (micro segmentation).**
- **Can be deployed on bare metal servers (whole range of intel hardware including commodity servers. No vendor lock-in)**
- **Enforce granular QoS at each VM level, Load balancing, Thin provisioning, Hybrid environment (different OS and templates within same node or cluster)**
- **Transparent USD re-direction, app publishing platform, single control pane.**
- **Centralized management, Self-Service & Role based access, Centralized patch management, User based profile (persistent, Pooled and shared pool), multiprotocol support.**

All above features and capabilities @ a cost 50% less than the competition per user/month.

Ransomware Attacks:

With Organizations enabling more and more employees to Work From Home (WFH) during this COVID 19 pandemic situation, the employees home network and unsecured devices are becoming new threat vector for Cyber Attacks. Frequency of Phishing and Ransomware attacks have increased many folds.

In case of Ransomware attack, one of the key infrastructures that need to be safeguarded is Data Protection setup to ensure quick and safe recovery from cyber-attack or data breach and resume business operations.

Following are the key elements that need to be included as part of Resiliency framework to recover and resume business operations as quickly as possible

- Automation and Orchestration: for Recovery of Platforms and Application Data
- Write Once, Read Many: Immutable Storage Technology to Prevent Corruption or Deletion
- Air-Gapped Protection: as a Fail-Safe Copy Against Propagated Malware
- Efficient Point-in-Time Copies: and Data Verification to Quickly Identify Recoverable Data
- Regulatory Reporting and Assurances: Validating Transaction Capture Through Regulatory Reporting Processes

Giniminds has a solution with above capability helping organization rapidly recover clean and secure data copies and enabling application restoration and resumption of business operations faster (in hrs/days rather than weeks) after or during destructive cyber incident.