Hybrid Cloud Solutions from Nfina Protect Your IT Ecosystem from Ransomware Attacks

Ransomware is designed to fully encrypt a victim's file system, possibly causing permanent loss of data if you are not properly protected. Ransomware is a major money-making business for cybercriminals. Don't be their next victim.

Ransomware Protection from Nfina

Nfina is a premier Hybrid Cloud hosting provider. Nfina's Hybrid Cloud and computing solutions facilitates ransomware protection and make it easy to backup and restore data if you find yourself dealing with an unforeseeable event such as a ransomware attack. It is a true private cloud, public cloud hosting, cloud backup, and disaster recovery business continuity solution.

Many midsize and small businesses haven't fully implemented a disaster recovery solution because they believe it is too expensive or too complicated to implement. Fortunately, Nfina's Hybrid Cloud backup and recovery service are not only effective, but they are designed to be affordable for businesses of any size and make it simple and easy to safeguard business continuity. We combine on-premise edge computing cluster in your own private cloud with the security of public cloud backup & disaster recovery, all as a monthly service. Nfina's hybrid cloud ransomware recovery solution gives peace of mind with geo-redundant backup storage and disaster recovery plus the ability to run your applications from multiple geo-redundant locations.

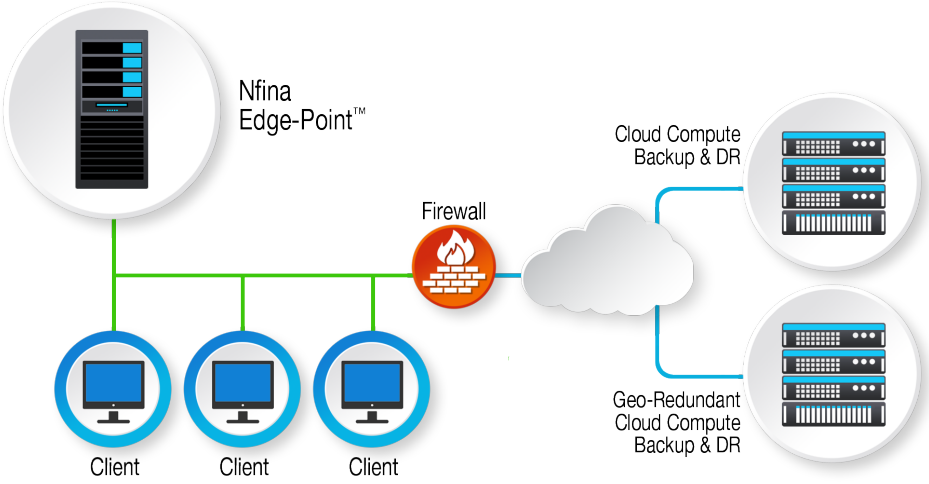
HYBRID CLOUD SOLUTIONS

CYBER SECURE SERVERS

DATA STORAGE

BACKUP & RAPID DR

n-fina HYBRID CLOUD SOLUTIONS



A model Nfina Hybrid Cloud small business solution

All Nfina Hybrid Cloud solutions includes Nfina-Store™ and Nfina-View™ software. Nfina-Store™ storage architecture is a Copy-Modify-Create New Block file system employing immutable snapshots to track changes in the file system. Immutable snapshots provide ultimate ransomware data protection from cybersecurity attacks as they are read-only and cannot be altered, overwritten, or deleted plus they are fully AES encrypted. Adding to ransomware security, Nfina-Store has geo-redundancy built into the architecture allowing immutable snapshots to be stored in multiple locations such as a local NAS, a colocation facility, another campus, and/or other geo-redundant cloud locations. Having backups stored in geo-redundant locations provides protection from unforeseeable events that could prevent you from keeping your on-premises operations up and running. Nfina-Store snapshots are also beneficial because they are smaller in size, not intrusive on compute and storage resources, and can be taken much more frequently than conventional backups. All data is backed up with immutable snapshots, including both the on-premise edge computing stack and the geo-redundant cloud data. At any point in time, you will have 12 copies of the data (4 on prem and 8 cloud backups in Nfina's cloud). This insures that your data is protected and will be available when you need it the most.

In the event of an on-prem outage or ransomware attack, Nfina's hybrid cloud management service, using the Nfina-View SaaS application, can facilitate rollback to a snapshot taken prior to the event causing the disruption. Nfina-View's rapid disaster recovery allows you to rollback or failover in minutes (not hours or days) which translates into less disruption and downtime for your organization. Nfina-View software provides monitoring on-prem and cloud, cloning, failover, rollback, and backup testing. Failover, cloning, and rollback are simple single click operations and do not require rebuilding and reinstalling data. This allows you to remove viruses easily and effectively using the built-in snapshot backup and data restoration mechanism. Nfina's cloud is a true cloud based server hosting implementation so your applications can effectively run on the edge with lower latency or in Nfina's public cloud if disaster strikes.

Managed Services Included

Nfina's Hybrid Cloud solutions also include Managed Services, so we can deal with the challenges of monitoring, troubleshooting, and optimizing your IT environment, while you focus on your business goals. Our entire team of world class qualified engineers with decades of real-world experience will consult, design, and manage your edge and cloud IT Ecosystem. We are able to customize a hybrid multi-cloud solution to fit each client's individual business requirements. Nfina's Hybrid Cloud backup and restoration capability provides an affordable disaster recovery solution.

Patch Management

Patch Management is the process of distributing and applying updates to software to keep your computers up to date. Patches are an important part to maintaining the system's health and security, and they ensure that software is fixed, up to date and protecting against vulnerabilities and bugs that may be present. Patches also help reduce system-related failures which improve productivity and save on the costs associated with poor patch management.

Nfina engineers install, test, and maintain current knowledge of available patches. We make decisions on what patches are appropriate for each client's system, ensuring that patches are installed properly and that your system is tested after installation.

Escalating Remediation Recovery

We make it easy to maintain and recover your company data in the event of data loss through software or hardware failure, or from a ransomware attack. Our backup and restore solution combines the entire process into a single service. Storage, design, testing, monitoring, failover, reporting and more.

Tier-1 Escalating Remediation Recovery

Currently, most ransomware attacks are Tier-1.

- Nfina restores your data from a snapshot taken prior to the attack thus removing the ransomware virus
- Nfina can restore the system in-place
- Time frame is minutes/hours

Tier-2 Escalating Remediation Recovery

In the event Tier-1 recovery is ineffective and the production environment immediately re-infects after recovery, Tier-2 escalation is the next step. More sophisticated Tier-2 attacks may come from "sleeper" infections that lay dormant for weeks or months before attacking.

- Your snapshots are installed on Nfina's Clean Room and software is used to remove the infected files before restoring your environment
- Uses signature malware software (Bitdefender, Malwarebytes, Trend Micro, etc.) to scrub the virus off the infected files
- Tier-2 Recovery – Fee-based. Time frame can be hours/days

Tier-3 Escalating Remediation Recovery

In the event Tier-1 and Tier-2 recovery fails to detect the virus, Tier-3 escalation must follow. The latest and most advanced sleeper ransomware encrypts files and avoids detection of the commercial signature-based malware software due to their "newness".

- Your snapshots are installed on Nfina's Clean Room where AI and machine learning virus software are implemented to remove the infected files before restoring your environment
- Uses non-signature malware software that deploys AI and machine learning techniques (Hammer IT) to scrub the virus off the infected files
- Fee-based. Time frame is open-ended

Conclusion

Organizations from small businesses, mid-size enterprises, to large corporations are more reliant on their data than ever and managing and protecting that data grows more difficult year-over-year. Nfina only recommends solutions proven to guarantee file consistency, as well as recoverability in the event of system failure, virus infection, or user error. Nfina's Hybrid Cloud solutions with Nfina-Store™ and Nfina-View™ management tools clearly fit this bill.

1. Don't wait until you've been attacked to create a Backup & Disaster Recovery plan with built-in Business Continuity. If you wait and your organization is attacked, it's too late.
2. Know the health and status of your infrastructure by monitoring your private and public cloud, test your backups, and failover processes frequently.
3. Creating geo-redundancy by backing up your systems, on-site and in multiple cloud locations is the most essential step.
4. Train your employees and educate yourself. Employees should recognize the signs of a phishing attack and make sure they know not to click on executable files or unknown links.
5. Patch and block. Installing the latest patches and updates significantly reduces the available entry points.
6. Duplicate your IT ecosystem (e.g. cyber security software suite or network stack design) in our public cloud.
7. Implement early threat detection systems. Use a firewall that will block unauthorized access to your computers, server, and network and provides an activity log of blocked attempts.
8. Install anti-malware / ransomware software. It is crucial to update regularly.
9. If infected, activate your DR plan. If hit with ransomware, immediately shut down your organization's network operations to prevent the infection from spreading. Isolate and remove the infected system(s) from the corporate network and disable the computer's wireless, Bluetooth, and any other potential networking capabilities.

Nfina Technologies sales@nfina.com nfina.com
820 S. University Blvd. Suite 4E, Mobile, AL 36609 251.243.0043