Ransomware Proof Your Business With Nfina's Hybrid Cloud Solutions

Ransomware Facts and Statistics

In 1989 the AIDS Trojan was the first strain of ransomware documented. Cybercriminals used floppy disks to spread their ransomware across computers considering it was long before acceptance of the modern-day internet. 30 years later, ransomware is a major money-making business for cybercriminals. Safeatlast estimates the global cost associated with ransomware recovery will exceed $20 billion in 2021, with ransomware perpetrators carry out more than 4,000 attacks daily.[1] In 2021, ransomware attacks against businesses will occur every 11 seconds, up from every 40 seconds in 2016.[1] 95 new ransomware families were discovered in 2019 with 1 in 3,000 emails passing through filters containing malware.[1] Attacks in the education sector rose by 388% between Q2 and Q3 of 2020.[1]

Ransomware is designed to fully encrypt a victim's file system, possibly causing permanent loss of data. The Beazley Breach Briefing reports that small-to-medium-sized businesses, which tend to spend less on information security, are at a higher risk of being hit by ransomware than larger firms.[2] In 2021 organizations averaged paying a ransom north of $300,000.[1] The average downtime following a ransomware attack was 22-days[3] and the cost of downtime was almost 50 times greater than the ransom demand.[1] Companies also need to pay for all the working hours required to restore their systems, clean up the damage caused by the attack, and strengthen their cybersecurity.

Protect Your Organization's Data with Proper Backup

The best defense against ransomware is to outmaneuver cybercriminals by not being defenseless to their threats. Backup important data so if your servers and computers are compromised, you won't be forced to pay to recover your data.

Ransomware doesn't just infect computers and servers, most cybercriminals search for backup systems to encrypt and lock, too. Figure 1 illustrates a simple flat network where client application files are stored on the file server and

HYBRID CLOUD SOLUTIONS

CYBER SECURE SERVERS

DATA STORAGE

BACKUP & RAPID DR

n-fina HYBRID CLOUD SOLUTIONS

backup is stored on the local NAS, both located on the same LAN. This elementary design is very vulnerable to attack and will almost ensure that your organization will be obligated to pay some form of ransom to recover their data or risk losing it.

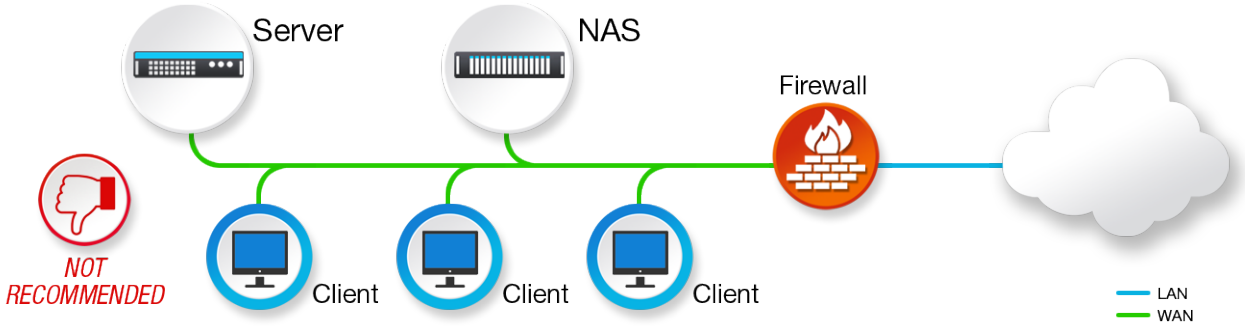

Figure 1 – Simple Flat Network

To prevent intruders from gaining entry to backup storage, the NAS should connect directly to corporate servers via an isolated storage backup network and not connect through the LAN nor have direct, wireless, or Bluetooth connections with any other machine or client. Figure 2 illustrates a more robust network, where the NAS is not mapped onto the LAN, residing on its own storage backup network, isolated from the LAN. This example shows how geo-redundancy can be achieved by storing backup data on-premise and in multiple cloud locations.

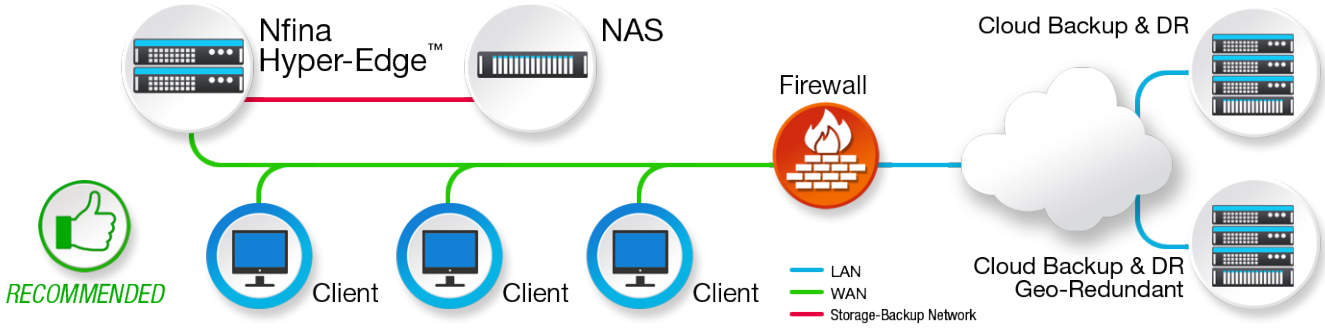

Figure 2 – Robust Network

In addition to managing your network infrastructure, the storage architecture used is an equally important factor in being able to use backup storage to restore ransomware-infected data.

Figure 3 to the right illustrates Conventional Read-Modify-Write (RMW) storage architecture. This design copies, modifies and writes all of the data, all of the time. This process places a burden on the application server, which must allocate CPU and memory to read and stream data to process backup jobs. Full backups are usually scheduled for off-peak periods such as weekends, while incremental backups are typically run after hours. To store compounding data, backup storage must be expandable. In many cases, to conserve space, overwrite retention policies are implemented where new backups overwrite the preceding one. In this case, if the ransomware virus was downloaded and a backup occurred before it was discovered, the backup will be corrupt.

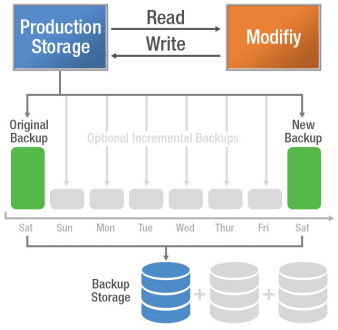

Figure 3

820 S. University Blvd. Suite 4E, Mobile, AL 36609 251.243.0043
nfina_sales@n-fina.com n-fina.com

Nfina's Hybrid Cloud solutions include EdgeStore™. EdgeStore™ storage architecture is a Copy-Modify-Create New Block file system employing snapshots to track changes in the file system. The first snapshot records the baseline, before any changes. In Figure 4 below, this is the Original Block Tree. The snapshot contains the original version of the file system, while the live file system contains any changes made since the snapshot. No additional space is used. As new data is written to the live file system, new blocks are allocated to store this data. This is shown below where blocks C has been modified creating C+. When blocks are updated, added or deleted the indirect or parent blocks are also modified in the live file system. At this point a New State (Block Tree-1) is created by combining the previous snapshot with the live file system plus the updated block(s) and a new snapshot is created from the New State and the process repeats at the defined intervals.

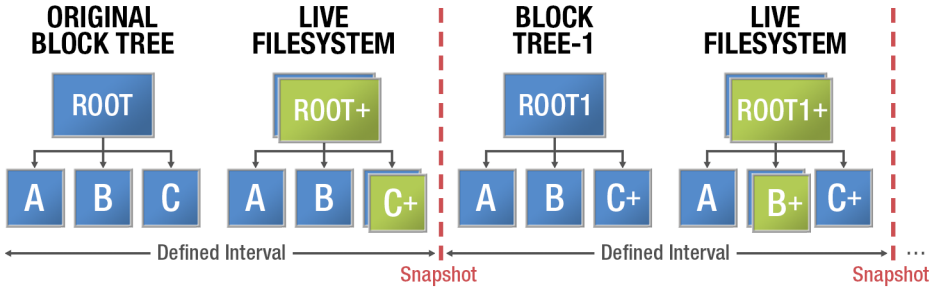

Figure 4 – Nfina's EdgeStore™ Copy-Modify-Create New Block Transaction

This method has additional advantages. Only the deltas are recorded, so Nfina's EdgeStore™ snapshots provide disk savings. The original block is not copied out of the way, so there is no performance decline. It is non-intrusive, allowing snapshots to take place during production as often as necessary, hourly, or even at five-minute intervals.

Snapshots allow you to rapidly restore data in minutes from a point in time and can be mounted as read-only to recover any previous version of a file. In a ransomware attack, you restore uncontaminated data by reverting to a snapshot saved before the attack. Even if the server is being protected with nightly off-site backups for disaster recovery purposes, restoring the server from the local NAS over the storage backup network will be much faster than restoring from off-site storage via the internet. In addition, restoring from the local NAS will not impact the performance of the internet or client network because it is isolated from both.

Nfina's Hybrid Cloud with Rapid Backup & DR and Escalating Remediation Recovery

Nfina's Hybrid Cloud is a fully managed solution designed to protect and ransomware proof your business. We make it easy to maintain and recover your company data in the event of data loss through software or hardware failure, or even from a ransomware attack. Nfina's Hybrid Cloud solution combines the entire process into a single contact solution. Storage, design, testing, monitoring, failover, reporting and more. We maintain copies of your critical data on-site and off-site. Redundancy ensures your information is insulated and always available for recovery and minimizes your downtime.

Tier-1 Escalating Remediation Recovery

Currently, most ransomware attacks are Tier-1.

- Nfina restores your data from a snapshot taken prior to the attack
- 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

Because data integrity should always be the essential concern, 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 EdgeStore™ and NfinaView™ management tools clearly fit this bill.

You're still largely on your own when it comes to fighting ransomware attacks, but there are steps to take to protect your organization from attack:

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 you're 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.
2. Creating geo-redundancy by backing up your systems, on-site and in multiple cloud locations is the most essential step. Keep your information backed up in safe and reliable locations that cybercriminals cannot easily access.
3. 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.
4. Patch and block. Installing the latest patches and updates significantly reduces the available entry points.
5. Duplicate your IT ecosystem (e.g. cyber security software suite or network stack design) in our public cloud.
6. 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.
7. Install anti-malware / ransomware software. It is crucial to update regularly.
8. If infected, disconnect. 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.

Sources

[1] Forbes https://www.forbes.com/sites/forbestechcouncil/2021/07/29/seven-factors-analyzing-ransomwares-cost-to-business/

[2] Beazley Breach Briefing https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html

[3] Statista https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/