FALCONSTOR

10 Rules to Ensure Secure Backup in the Age of Ransomware

How strong is your last line of defense?

Executive Summary

The age of ransomware is upon us. In the event an attacker gets in, backups are sometimes the last line of defense. They allow operations to be restored to a point-in-time prior to the attack. However, many organizations are still concerned about the security of their backups, which must be reliably secured for up to 10 years to adhere to regulatory and corporate compliance requirements. Are your backups as secure as they need to be? How fast can you recover from a ransomware attack? Adhere to these rules, to ensure your last of defense exists when you need it.

#1: Maintain a complete backup onsite for rapid recovery

The "2" in the time-tested "3-2-1" backup standard indicated the need for two complete backup copies, but one complete backup copy is mandatory onsite. This will be used to rapidly restore mission-critical servers after the attack. Backups ensure an image from prior to the attack is available, versus a high availability solution that gets impacted just as the main site is when replication happens.

#2: Maintain at least one backup replica offsite for safety

3-2-1 also stresses the need for one backup copy to be offsite, somewhere other than the primary data center, to ensure safety. Maintain a minimum of one backup copy offsite to protect against site disasters, blackouts, burglary, fire, flood, and ransomware.

In the past, this copy was mainly in the form of LTO tape and the copy was transported off to a secure warehouse for long-term storage. Today, that is just one option, since companies:

- Replicate on-premises data to a disk-based target at a remote location.
- Replicate the data to a storage service at a major cloud provider like AWS, Azure, IBM, or Google or to a managed service provider.
- And yes, many still write to tape and use trucks to store them safely offsite in a mountain.

TIP: Use deduplication and compression technologies to shrink the backup image, ensuring the fastest possible transfer of information to secondary data centers and cloud services. For example, organizations have experienced 20:1 deduplication for IBM i workloads, helping ensure that the backups always complete within the desired backup window

TIP: Consider storing a third copy of select data at a third location. Some data may be so sensitive that a third copy is required, and when doing so,

consider a different target. For instance, a larger organization may replicate the second copy to its own data center, and a third copy to a cloud service provider or simply output that copy to tape. A smaller organization may opt for two cloud copies in lieu of owning and operating a secondary data center.

#3: Encrypt all backups at every step in the process

If the ransomware attacks of past have taught us anything, encryption must be woven into the process from first copy, in-flight, and on the final target, at-rest. While many will tout the value of the latest security capabilities such as firewalls and strict operational procedures, AES-256 encryption of data remains the highest standard of care and protects data when those other security capabilities and procedures inevitably break down.

TIP: Apply encryption after deduplication and compression to get the savings benefits. Encryption must happen after deduplication and compression, based on the math involved.

#4: Optimize for long-term retention with immutable backups

IT organizations remain split over the implementation of information archives. For larger organization in regulated industries like financial services and healthcare, designated archives have been required for decades. But for the vast majority, purpose-built data archives are simply beyond the scope of the services they can provide. As a consequence, backups can be used to serve the objective of long-term data preservation with the right techniques and the right capabilities at the target, which means capitalizing on immutable media. When immutable media is used, the target cannot be over-written or manipulated, thus preserving the data in perpe-

tuity. When tape is used as the target, immutable LTO tape can be used to preserve data. When a disk-target is used in an owned data center or in the cloud, immutable storage, referred to as WORM media for Write Once, Read Many, can be targeted.

TIP: Consider your archival intervals – how frequently you hold a complete immutable copy – to keep the cost of data retention in check. Use RBAC so admins have only the rights they need, when they need them.

#5: Understand your encryption key management

While encryption in-flight and at-rest need to be part of the backup operation, the entire operation can be compromised without sound key management. The encryption keys need to be assigned and maintained by the backup software to ensure the right folks get access to the right copies. But what happens when the backup servers go down? This highlights the need to be able to export of a designated encryption key manager on-premises or at a cloud service provider. Many organizations have taken this step to protect data against external and internal threats.

TIP: Even if your software keeps track of your encryption keys for you, an independent copy should be made, and yes, encrypted and stored in an offsite vault. Further, encryption key rotation is a best practice to generate updates and protect the data as employees, with access privileges, leave the organization.

#6: Automate the detection of corrupt backups

Even organizations with all the proper systems and operational procedures in place can fall victim to the challenge of corrupt backup copies, which is the silent challenge of backup. This corruption, frequently known as “bit rot,” happens when the data decays and becomes unreadable by the backup application and therefore is not restorable. To fight this challenge, certain backup technologies employ checksums, such as CRC32, to compare original copies to current copies that can detect this form of corruption and help remediate it before further damage can occur. While still novel within the industry, incorporating the detection of corruption has moved from the periphery to essential in backup operations, and even more so when backups are used as a data archive.

#7: Automate the detection of data tampering

Hashing the backup sets increases the confidence of data protection teams that the data has not been maliciously altered. At the time of the backup, the backup data is hashed, often using SHA256, to generate a hash value for that backup, which is then stored in a table. Intermittently, the system

can take another hash of the backup currently in place and compare that to the original hash value.

Differences in hash values provide valuable clues that can be used to verify when tampering has occurred and lead to remediation. Knowledge is power when it comes to malicious actions and hashing backups has emerged as a key means of gaining that knowledge and put a stop to tampering.

#8: Move beyond passwords with two-factor authentication

The era of relying solely on passwords has passed. Too many employees and outside contractors come and go within IT organizations to ensure that passwords can effectively limit access to information. The news remains rife with stories of insiders retaining access to systems long after leaving companies, which compromises every sound security measure put in place. Two-factor authentication, known as 2FA, has emerged as the standard over the past decade and even more so with more remote workers, augmenting a user's password access with a second form of identification via token. Many cloud service providers employ 2FA as a standard for accessing cloud services, and IT organizations are continuing to invest in 2FA for the general employee population. Don't overlook the need to deploy those same kinds of controls over IT-centric applications like backup systems and storage targets.

#9: Test and Test Again

Effective data protection teams regularly test their backup systems and procedures. This discipline is often hard to maintain in the face of dead-

lines for new application rollouts and overworked teams. But testing the ability to provide different service level agreements (SLAs) for recovery point objectives (RPO), the point to which the data is protected, and recovery time objectives (RTO), the ability to restore at a particular rate (e.g., within one hour of attack), is essential. There is simply no way that a team can meet the challenge of a ransomware attack without practicing responding to the event. Bear in mind that this level of assurance is what an organizations' C-Suite is looking for.

TIP: Look for vendors, both service providers and technology providers, that will not only help define the playbook for backup but will actively participate in testing data restoration, essential to business continuity.

#10: Optimize Annually

Technology and procedures should be reviewed annually to improve the security of backup operations. While larger and better resourced teams may be able to contract for a security audit or use a third-party security scorecard application to assess the security posture, most teams will simply need to set aside the time to do a proper review to weigh the costs and benefits of improving security measures.

TIP: Again, look for service providers and vendors that are ready to provide the information, best practices, and assistance needed to examine the backup process and bring ideas on how to optimize security for the long haul.

The Role of FalconStor®

FalconStor (OTCQB: FALC), headquartered in Austin, TX, was founded in 2000 by a team of experts with decades of experience in storage software solutions and a track record of proven success. The company's engineering and management teams are seasoned veterans of enterprise storage and software and continue the spirit of innovation with StorSafe VTL, which offers market-leading virtual tape library (VTL) technology to power the most modern data protection solution - spanning on-premises to the Cloud.

FalconStor StorSafe® VTL delivers the right technology at the right time, ensuring backup data, your last line of defense, can be protected and stored onsite for rapid restores, transmitted remotely for protection, and secured with AES-256 encryption in-flight and at-rest. Embedded hashes and checksums also help to fight against data corruption and misuse, as well as periodic data health and readiness checks for recovery. Immutability is provided by the erasure coding that is currently used in warm tiers of cloud-based object storage. And WORM properties can provide an effective immutable barrier against ransomware and other malware.

There is also role-based administration, so nobody is given more access rights than they need, and full multi-tenancy is implemented to keep each department or organization isolated from each other – as well as facilitating bill-back for services used. The StorSafe VTL management GUI, StorSight®, provides a real-time dashboard that is updated every 10 seconds to ensure your last line of defense is solid.

Visit us at https://www.falconstor.com/products/storsafe/ to learn more.