



# Backup Strategies & Best Practices

## Backup Strategies That Impact Recovery & Restoration

Arctic Wolf's Incident Response (IR) perspective sheds light on how certain backup strategies stack up against modern cyber attacks. The following are ordered by fastest to slowest restore times our team typically sees:

### ***SAN Snapshots\****

SAN Snapshots act as a grand-scale "redo" function. Their infrastructure allows for easier segregation from typical network access, the ability to "revert" to a previous snapshot of data without forensic evidence lost, and are almost impossible to encrypt. However, they require ample data space to function which can be costly. Organizations should consider replication to a Secondary SAN with proper deduplication and compression to minimize storage usage.

### ***On-Premise Hardware\****

On-premise hardware can provide secure backups for quick, singular restores. This type of environment can typically survive a cyber attack thanks to their requirement for non-Domain credentials for access, built-in storage that can be immutable (a backup copy of data that cannot be altered, deleted, or changed), their ability to store offsite to the cloud, and are nearly impossible to encrypt.

### ***On-Premise Server\****

An on-premise server is usually the best option for a one-time restore when servers crash or when files are missing or deleted. They are hard to hide from attackers without proper network segmentation. An on-premise server can also store a second, immutable copy of data off-site to the cloud to ensure backups are safe and redundant.

### ***Cloud Backups\****

Cloud backups can be disconnected from a network to a safe external site, stored in multiple regions to protect against localized disasters, end-to-end encrypted to secure data, and protected with Multi-Factor Authentication (MFA). Immutable backups are also available. For threat actors, cloud backups are more difficult to delete / remove and are nearly impossible to encrypt, however, they require a high network bandwidth to function properly for organizations.

***\*Depending on your organizations' needs, we recommend configuring these backup strategies to bare metal to capture the operating system, applications, and files rather than file-level only.***

IN PARTNERSHIP WITH



## Modern Threat Actors, Cyber Attacks, and Backup Etiquette

Having a backup is crucial as it acts as a safeguard against data loss from hardware malfunctions, accidental deletions, or cyber attacks. This ensures your organization can restore vital information like key documents, financial records, system settings, etc.

It's best to follow the **3-2-1** principle of backups:

3 – Keep 3 copies of data (1 primary and 2 backup copies)

2 – Keep 2 copies stored (in separate locations)

1 – Keep 1 stored off site (ideally in a secure private cloud with proper credentials and Multi-Factor Authentication enforced)

## Need help with your cybersecurity strategy?

Talk to Arctic Wolf's team for proactive remediation:



**Cybersecurity  
Remediation &  
Hardening**



Third-party service providers discussed herein, though not affiliates of The Hartford, are pre-approved by The Hartford to provide cyber-related services. You are not required to avail yourself of their services. Sharing any information with any such vendor is at your sole discretion. References to any vendor are provided for your convenience only and are not intended as a substitute for your own due diligence and selection of vendors to suit your company's needs. The vendors are independent contractors that charge their own rates. Discounted rates offered by any vendor are not offered by The Hartford, nor on any premium for a policy of insurance. Any such vendor discount is subject to change without notice and is not guaranteed by The Hartford. The Hartford does not warrant the performance or services of the vendors or their websites. The Hartford assumes no responsibility for the control, correction or legal compliance of your cyber security measures or other business practices and operations. Notice of any claim, act, fact or circumstance to a vendor does not constitute notice thereof to The Hartford. Approved vendors are current as of March 2025 and may change at our discretion at any time, with or without notice.

The Hartford Insurance Group, Inc., (NYSE: HIG) operates through its subsidiaries, including underwriting company Hartford Fire Insurance Company, under the brand name, The Hartford®, and is headquartered at One Hartford Plaza, Hartford, CT 06155. For additional details, please read The Hartford's legal notice at [www.TheHartford.com](http://www.TheHartford.com)