The Seven-Step Checklist to Secure Backup Data

Practical and imperative measures to implement today.

Introduction

Ransomware attacks are increasing at an alarming rate, with an attack occurring 15 times every second[1]. Backup software and appliances are often targeted using stolen credentials, putting critical backup data at risk. It is more important than ever for executives to act and ensure their teams are proactively securing critical backup data. Don't leave your data protection infrastructure vulnerable to unauthorized access or modification. By following this seven-step checklist, your organization can dramatically improve its security posture and strengthen defenses against cyber threats, ultimately safeguarding your most valuable assets. Share these actionable steps with your team today and emphasize the importance of implementing them to protect your organization from potential attacks.

Seven Simple Steps

1. **Enable Multifactor Authentication (MFA)**
   Actively integrate multifactor authentication with your existing identity and access management policies

2. **Elevate Veritas Appliance Security Level with Lockdown Mode**
   Prevent unauthorized access or modification to the underlying operating system

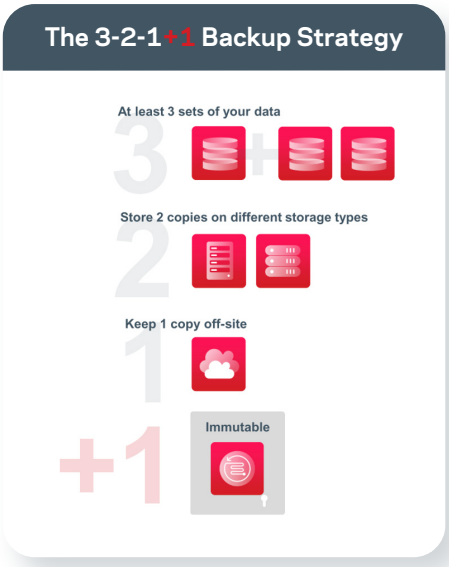
3. **Implement an Immutable Data Vault to Secure Data**
   Use NetBackup Flex Appliances, NetBackup Flex Scale, and NetBackup Access Appliances for secure and tamper-resistant storage; adopt a 3-2-1+1 backup strategy

4. **Secure Credentials with Privileged Access Management**
   Deploy external password management solutions, such as CyberArk privileged access management (PAM)

5. **Reduce Network Exposure by Implementing Network Access Controls**
   Implement network segmentation and create an isolated recovery environment (IRE) using NetBackup™ and NetBackup Flex Appliances

6. **Keep All Systems and Software Updated**
   Proactively update Veritas software and install security patches to leverage new capabilities and enhanced security features

7. **Enable Encryption**
   Configure strong encryption everywhere—on-premises and in the cloud—to prevent unauthorized data access and theft



Act Now: Share this checklist with your team and encourage them to implement these crucial steps to protect your organization's data and strengthen its security posture. For more information and up-to-date recommendations, visit veritas.com.

1. 2023 SonicWall Cyber Threat Report

2625 Augustine Drive, Santa Clara, CA 95054 | +1 (866) 837 4827
veritas.com

V1875 04/23