Quorum Business Continuity & Disaster Recovery Solution

Once common wisdom had it that backups were a low priority when it came to security. While IT leaders focus heavily on stopping attacks and preventing breach repercussions – loss of customer faith, regulatory fines, and compromised data– protecting backups from attackers traditionally just hasn't been at the top of the security list.

Yet backups are the last line of defense when criminals take over your system. Attackers know this, and many head straight for your backups to remove any hope of recovery. So why do so many IT teams fail to secure their backups like the valuable insurance they are?

If your team has yet to integrate your backup and disaster recovery ecosystem into your security program, here are 5 practices to get started.

Practice Redundancy
If you're still relying on physical backups, realize they can be vulnerable to theft and consider adding an additional layer of security in the form of cloud backups. Another vulnerability: the end of the tape or disc lifecycle. Be sure to thoroughly destroy them to keep sensitive data from being exploited.

Take Advantage of Detection Tools
The longer criminals are in your system, the higher the likelihood they'll spread through your network – including infiltrating any backups they can find. Detection tools that can identify unauthorized users, or users employing valid stolen credentials, can go far in doing damage control.

Include Backups in your Response Plan
When creating and testing your recovery plan, make sure your backups are present and accounted for. If you're booting up one set of backups and leaving others on the bench, remember to check on whether they've been compromised.

Use Advanced Security Controls
Each individual virtual network that connects to the DR recovery node should be isolated by a dedicated firewall; any data centers hosting your applications should offer Tier 1 architecture

and be certified with PCI, HIPAA & SOC 2. If necessary, ask your vendor how they handle data migration, cloud tenancy and remote access.

Secure Your Backups

Criminals who want to hold your information hostage, like ransomware attackers, are especially interested in seizing your backups. Your best option for protecting them: encryption. Even if your backups are accessed or stolen, encryption will disguise the data from their unauthorized eyes. (You might also get any regulatory financial penalties and notification requirements reduced.) Any backup stored in the cloud should pass through a 128 bit AES encrypted session over a 256 bit AES VPN tunnel before leaving your network; the data should be encrypted again while at rest in the cloud. Any link used to connect or upload your data should be secured through SSL or other protocols as well.

Typical methods for rendering data unreadable include encryption algorithms like AES, Blowfish, RSA and 3DES, truncation, index tokens and pads, and one-way hashing. But skilled cryptography must be paired with other security protocols as well, such as restricting access to encryption keys, protecting transmission over open networks, using best practices for wireless networks, and cracking down on transmission of sensitive data over email, chat and other casually used technologies.

Maybe you believe your backups are already protected. If so, great. Just be sure to regularly evaluate those controls. With the explosion of Big Data and the growing complexity of many BDR systems, many organizations find their backups aren't as well-protected as they thought. Weak encryption key management or a gap in backup disk disposal can easily become a habit, opening a door to data loss. Backups have always served as your organization's insurance; by giving them the protection they deserve, your team can unlock a stronger level of BDR security and greater peace of mind.

Quorum tightened up security too.

If there's one concerns our customers bring up again and again, it's ransomware. Teams want a vendor who can help them recover fast enough to beat demands for exorbitant ransoms. They also want a solution that can securely hold their data, so they don't need to worry about it falling into the wrong hands.

Quorum is a private cloud provider for this reason – your data can only be seen and accessed by you. We further protect you through the most advanced encryption in the industry. All backups of your server image, apps and data are compressed and encrypted at motion and at rest. We know we represent your last line of defense, and onQ pulls out every stop possible to ensure your data can't be seen or used by other people. That's it for today. In our next post, we'll walk you through onQ's advances in deduplication, performance and our incredibly convenient new user interface. We’ll also explain how enterprise leaders can solve your scaling challenges with onQ.

QUORUM IS YOUR LAST LINE OF DEFENSE AGAINST RANSOMWARE

Relying solely on prevention to avoid Ransomware is only a partial solution. So how should you protect yourself? That can be a tricky question. IT admins will want to build a wall around their systems in the form of a next gen firewall, IPS, host/server antivirus, access controls, etc. There are multiple ‘defense in depth’ guides you can follow.

These defense in-depth guides do a great a job preventing known threat signatures and behaviors. But what happens when an ill-advised user circumvents your security barriers? Or when that zero-day ransomware exploit makes its way inside your system?

That's where onQ comes in. It's hardened appliance hardware and encrypted snapshots can immediately boot a snapshot of your production servers in the event of an infection. Our scalable hardware is designed to deliver the same levels of workload performance as your production systems, to seamlessly take over for the compromised server. onQ gives you the time to you need to clean the infected server and get it back online

Quorum internal network (Xen, ZFS, CentOS/OnQ) is highly secured as it is not exposed to Production network/domain

1. The Hypervisor, onQ and Filer run in a separate dedicated Internal network with their own internal IP’s and subnet. This safeguards the internal architecture from any external or internal network threats.
2. SAN storage is also secured with a passphrase.
3. The VSAN volumes are also encrypted to protect the data (volume encryption)
4. The SAN storage cannot be accessed from outside the appliance.
5. All communication to storage and hypervisor happens through onQ internal IP Address.
6. Data stored in Storage is also fully encrypted (data encryption)
7. Data cannot be viewed through hypervisor or OnQ.
8. Every snapshot is dynamically merged with RN giving recovery from every snapshot.
9. Filler (Storage) is not accessible to avoid internal threats. Users cannot delete data from Quorum

QUORUM Offers 256 AES Encrypted at Rest and In-Motion

Your data is always either at rest or in-transit. When it is at rest it is not actively moving from server to computer network, between computer networks, or so on, and when data is in-transit, it is. Encryption at rest and encryption in-transit means that your data is fully encrypted in both cases.

With AES encryption, both the sender and the receiver of the data must have the same key in order to decrypt and read data. 256-bit AES encryption is the mathematical equivalent of 2^{256} key possibilities. So both at rest and in-transit, your data is secure.