Ensure maximum uptime for ALL of your mission critical applications, data and systems with our unified approach.
Uptime and Recovery Challenges

An essential function for today’s IT staff, is the challenge to maintain system uptime.

Because this falls directly on their shoulders, IT leaders need a reliable solution to ensure their critical systems can recover quickly and painlessly in the event of a mishap.

With ever-evolving technologies, finding the balance between critical data protection and reliable application availability has become somewhat of a balancing act.

To make it more difficult, there are significant challenges in the search for a reliable solution.
Challenge #1
Research:

The research necessary to sift through, uncover, and understand new disaster recovery (DR) solutions that promise ease-of-use and speed has become a significant undertaking.

Challenge #2
True Differentiation vs Marketing Fluff:

There are so many vendors in the data protection arena – most of which promote largely similar claims of innovative, cutting-edge capabilities and self-proclaimed advantages.

It’s difficult to decipher between true differentiation and marketing fluff.

Challenge #3 Legacy
Backup and Recovery in the DR Space:

Many in the DR space have deep roots in legacy backup and recovery (BAR) that continue to influence their approach.

As a result, as customer requirements change, they essentially ‘bolt-on’ new functionality (sometimes courtesy of third-party technology licensing) to meet the recovery requirements of today.

The outcome is a mixed bag of various levels of integration, capabilities, support and overall customer experience.
It’s no secret that budget requests for DR improvements face heavy scrutiny. Why? Because, more often than not, legacy solutions are viewed as ‘good enough’.

And, in all fairness, for those not directly involved in the failover and failback processes, this could be considered a valid assessment and why budget requests for DR fall upon deaf ears.

However, those deeply entrenched in the uptime battle know too well that “good enough” solutions fall short in the end. The reality is legacy DR technologies have not kept pace with changing and evolving requirements, as well as the new environments they are part of.

An investment in a new DR approach may seem optional to a layman because it is so rarely activated in response to a recovery event.

They envision it collecting dust – providing value only during the rare Mother Nature-inspired outage.

They discount the following realities:

» Over 90% of service interruptions have nothing to do with Mother Nature.

» Service interruptions are the bi-products of hardware failure, software failure, and human error.

» Customers expect perfection. With the increase in Internet technologies, customers, users, employees, and management expect an instant response for every website, application, and server with every click. Always! Any amount of downtime is no longer acceptable.
The Quorum onQ Difference

Quorum’s onQ technology is purpose-built and military-grade, originally developed for U.S. Naval combat systems to enable failover and failback capabilities.

Introduced commercially in 2010, onQ technology has evolved to include many new capabilities. Yet, the solution is built entirely by Quorum developers from the ground up to ensure tight, end-to-end integration for the best possible user experience.

Quorum’s unique approach to DRaaS leverages onQ to provide a powerful, unified approach to recovery with capabilities and benefits that traditional server backup and data protection products simply cannot match.
Like many competitive solutions, onQ leverages VM clones for speedy recovery of applications, data and systems. However, we have taken this approach to the next level with what we call, PREcovery. What do we mean by this?

Fast and Reliable Failover

The recovery VMs are prebuilt from incremental backups and stored locally for HA and remotely for DR to allow fast failover using the desired image, thus reducing recovery time to mere minutes.

Automatic Pretesting

Your Quorum recovery VMs are pretested automatically each and every day (power-up, login, and isolated TCP/IP stack testing) — without disrupting your daily workload.

How does that sound? In addition, not only does onQ DRaaS enable you to easily recover anything (a file, an email, a directory, a server, every server in your datacenter), but it also includes functionality that will increase your productivity and speed ROI.
Known for its reliability, Quorum onQ core technology was originally created for U.S. Naval combat systems.

Introduced commercially in 2010, onQ's comprehensive and powerful combination of technologies provide functionality well-beyond our competitors' approach to recovery.

As a result, not only do you benefit from ease of use and superior reliability, but onQ also enables you to speed ROI with its powerful key features and unique set of capabilities.
Replication

While the Recovery Node (RN) is being created or updated, the deduplicated data (recorded by the local onQ appliance) can then be replicated to a second onQ appliance at a designated DR site – either your remote site, or in the Quorum Cloud. This replication is not only sending the delta, but the data is also compressed and encrypted to minimize any network traffic-related bottlenecks and to ensure maximum data transfer speeds, while maintaining the utmost security.

Once the data transfer is complete, the DR solution completes the same process of keeping a repository of data and creating/updating RNs to continually provide the benefits of a fully PREcovered and unified recovery solution for all of your critical applications, data and systems that you make part of your onQ deployment.

Instant Recovery

Once you have identified a server as a PN, and its first backup is completed, an exact replica of that server will be created as a VM clone called a Recovery Node (RN). The RN is stored locally on the onQ high availability (HA) appliance and updated with each incremental backup.

When needed, the RN can be spun-up within a few minutes – literally the time it takes to boot the VM. At this point, the server, associated applications, and data will be available to users.

As discussed earlier, we refer to this as PREcovery because not only are the recovery VMs prebuilt and ready-to-run, but they are also pretested – ensuring superfast and reliable failover.

In addition, when recovery in hours – as opposed to minutes – is deemed acceptable, RN recovery on-demand is available as a cost-saving measure.
Migration Tools

Failover to onQ is easy – just a single click of your mouse, or a tap on your smartphone or tablet. However, as you know, failover is only half the battle. Ease of failback to the production environment is equally important, and with other HA, disaster recovery (DR), and disaster recovery as a service (DRaaS) solutions, this can prove difficult.

Dealing with multiple recovery products and platforms also adds to the difficulties as opposed to addressing all of your recovery needs in a unified way. onQ enables you to easily perform bare metal restore (BMR) to dissimilar hardware and/or platforms – physical-to-virtual, virtual-to-virtual, virtual-to-physical, or physical-to-physical.

Another advantage of onQ is that not only can it perform a full BMR, but it can also perform incremental failback. For example, instead of requiring enough downtime to restore your entire 2TB file server, which could take hours, you would only need downtime sufficient to recover the amount of data changed since the failover.

So, if only 20GB changed, that could be recovered in minutes – limiting your downtime and ensuring the most efficient recovery possible. It’s a win-win!

Archive

onQ Archive Vault is a natural extension to the onQ platform, enabling policy-based migration and long term storage of deduplicated data (virtually unlimited) that must be retained for extended periods of time (i.e., compliance, eDiscovery and litigation requirements).

Auto Self-Test

One of the most popular features of onQ is the ability to conduct automated testing of the RNs and associated networking. You can conduct these tests on a daily basis, schedule them in advance, and be notified if any failures occur.

Gain peace of mind via automated, non-intrusive testing of every protected server. Know that when you call onQ into action, it will perform as intended.

Sandbox

onQ’s integrated sandbox can be used for performing a full DR Test without disrupting production. It can also be used for testing patches, new apps, and configurations – before you push them to the production environment.

And, because the onQ sandbox contains exact replicas of your PNs, you can be assured that testing is both reliable and convenient.
## Quorum onQ Technology

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>Customer Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backup</strong></td>
<td>Data, applications and entire servers quickly and efficiently.</td>
<td>Meet recovery point objectives (RPOs), as well as backup windows and security requirements. These technologies are integrated into onQ and there is no need to manage them separately.</td>
</tr>
<tr>
<td><strong>Deduplication, Encryption, and Compression</strong></td>
<td>Reduce backup data and time, transferred and stored data amounts and secure data during transfer and at rest.</td>
<td>Meet recovery point objectives (RPOs), as well as backup windows and security requirements. These technologies are integrated into onQ and there is no need to manage them separately.</td>
</tr>
<tr>
<td><strong>Replication</strong></td>
<td>Flexible and efficient replication of data, applications and server information between appliances and the Quorum Cloud.</td>
<td>Allows instant recovery to support aggressive Recovery Time Objectives (RTOs) – even in the event of entire datacenter failures – and without the requirement to first set up a new infrastructure and restore the data.</td>
</tr>
<tr>
<td><strong>Flexible Recovery Options</strong></td>
<td>Recovery of individual files, messages, servers and entire datacenter using file-level recovery (FLR), bare metal restore (BMR) and windows snapshot recovery (WSR).</td>
<td>Depending on the size of the disaster, you can recover as little as needed, or even an entire datacenter which makes business continuity within minutes a reality.</td>
</tr>
<tr>
<td><strong>Auto Self-Test</strong></td>
<td>Recovery Nodes are tested automatically after each backup or as scheduled. onQ's isolated network stack is also tested.</td>
<td>Ensure that the Recovery Nodes will run (and be accessible by users) when needed and that the recovery will be successful.</td>
</tr>
<tr>
<td><strong>Migration Tools</strong></td>
<td>BMR to physical and virtual environments independent on the source environment.</td>
<td>Using onQ as a migration tool while running the Recovery Nodes. Migration between different environments is possible and switchover times are reduced to minutes.</td>
</tr>
<tr>
<td><strong>Instant Recovery</strong></td>
<td>Individual servers, or even entire datacenters can be started within minutes. Recovery time is reduced to the time it takes to boot-up the Recovery Nodes (virtual clones).</td>
<td>Aggressive RTOs can be met in support of your comprehensive business continuity plan. Recovery within mere minutes of a disaster is a reality, and can be initiated from any web browser – even by non-IT staff, as no special training is required.</td>
</tr>
<tr>
<td><strong>On-Demand Recovery</strong></td>
<td>Dedicated Recovery Nodes can be built on-demand. The recovery time depends on the amount of data.</td>
<td>Save money by identifying servers that are not critical – where availability within hours as opposed to minutes would be acceptable.</td>
</tr>
<tr>
<td><strong>DRaaS / Hybrid Cloud</strong></td>
<td>Replication targets are SOC2, Type II Quorum data centers in the US (bi-coastal – HIPAA and PCI certified) and the UK (PCI compliant).</td>
<td>Benefit from offsite replication without the need of a secondary site. Additional services include maintenance of compliance standards, active monitoring and more.</td>
</tr>
<tr>
<td><strong>VLab / Sandbox Basic</strong></td>
<td>onQ provides an environment separate from your production environment, including a test network – without the requirement of additional infrastructure.</td>
<td>Use your onQ appliance as a development system, or to test patches, upgrades as well as new applications and configurations before pushing to production. Secondary tasks such as database reporting can be run in this environment as well.</td>
</tr>
<tr>
<td><strong>Datacenter Power Outage Protection / Remote Failover</strong></td>
<td>Replication to a separate DR site or Quorum Cloud provides a virtual copy of the protected environment that is independent of the production infrastructure.</td>
<td>If your datacenter infrastructure is not available for any reason (e.g. power failure, HVAC malfunction, natural disaster, water damage, etc.) easily and remotely failover an entire site with a few mouse clicks.</td>
</tr>
<tr>
<td><strong>Dynamic Resource Allocation</strong></td>
<td>Compute resources can be over-allocated and assigned to customers on an “as needed” basis.</td>
<td>Save money by reserving DR compute resources only when needed – as opposed to all of the time.</td>
</tr>
<tr>
<td><strong>Additional Configuration Options</strong></td>
<td>Server protection can be configured based on your needs (instant recovery, on-demand recovery, local high availability, or backup only).</td>
<td>Flexible configuration options enable you to design your business continuity model according to your specific needs and within your budgetary constraints.</td>
</tr>
<tr>
<td><strong>Solution Administration and Monitoring by Quorum</strong></td>
<td>Quorum's DRaaS team monitors all onQ systems, administrators and manages onQ Cloud components.</td>
<td>Peace of mind knowing that your Recovery Nodes are always up-to-date, monitored for resource limitations, regularly tested and more.</td>
</tr>
<tr>
<td><strong>Archiving Option</strong></td>
<td>Archiving provides long-term retention capabilities beyond the standard retention period in a DR system. JBOD storage is available from Quorum. Optionally you can leverage your existing storage to further reduce costs.</td>
<td>Quorum onQ appliances are built to retain approximately 45-days of data, application and system images. Using the optional onQ Archive Vault (JBOD) you can set policies to migrate your data to lower cost storage, where it can be maintained for years (i.e., regulatory compliance, e-discovery, etc.).</td>
</tr>
</tbody>
</table>
Regardless of the protection model you choose, an onQ Appliance will be deployed in your local datacenter to provide the HA component.

If you choose DRaaS as a solution, the appliance would connect to the elastic cloud infrastructure. Optionally, if you choose the DR solution, a second onQ Appliance can be deployed at your DR site.

Quorum’s patented onQ technology is at the heart of all Quorum unified recovery solutions:
- High availability (HA)
- Disaster recovery (DR)
- Hybrid cloud disaster recovery as a service (DRaaS)

Sizing Considerations

In order to ensure proper sizing, and thus reduce the likelihood of unplanned upgrades, Quorum takes a proactive approach and asks that potential customers speak directly with our systems engineers when trying to determine which onQ appliance will provide the best experience in terms of processing power, memory, and storage requirements.

Sizing discussions/calculations take into consideration more than twenty variables that can have a significant impact on the planned usability of the appliance.

Continue
onQ Archive Vault

Quorum onQ appliances are generally sized to store up to 30-40 days backups. However, many customers will require longer retention periods, perhaps driven by HIPAA, PCI, or e-discovery. These can easily be accommodated using onQ Archive Vault, which provides virtually unlimited scalability.

**onQ Archive Vault Options**

- **onQ Archive Vault Appliance** is a JBOD device you can purchase from Quorum. A single instance of the Quorum onQ Archive Vault can be extended to more than 200 TBs across 8 disks of storage modules. It is possible to have multiple instances of the Archive Vault, thus allowing unlimited scalability.

- **onQ Archive Vault Gateway** allows you to take advantage of your existing storage hardware by using it as the repository for your Archive Vault Data. It is connected either by iSCSI, or a fibre channel to your storage.

  The onQ Archive Vault virtual machine is managed by your onQ appliance. Scalability is limited only by the size of the storage you want to attach.

**Sizing Considerations**

As with the onQ Appliance, several variables must be considered when calculating storage requirements to ensure proper sizing.

Contacting a Quorum system engineer is required before you place an order.
Solutions

Quorum onQ DRaaS, DR, and HA solutions not only protect, but boost the productivity of your business by addressing the needs of users, IT staff and budget owners too.

onQ is a win-win-win!

This chart provides a checkbox comparison of the available onQ solutions.

<table>
<thead>
<tr>
<th>Quorum onQ Solution</th>
<th>DRaaS</th>
<th>DR</th>
<th>HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Deduplication, Encryption, Compression, Application, Consistency</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Recovery Options (FLR, BMR)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Auto Self-Test</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Migration Tools</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Instant Recovery</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>On-Demand Recovery</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Replication</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DRaaS / Hybrid Cloud</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>VLAB / Sandbox Basic</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DC Power Outage Protection / Remote Failover</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Dynamic Resource Allocation</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Configuration Options</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Administration and Monitoring</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archiving Option</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Why Consider Quorum onQ DRaaS?

- Quorum Cloud is maintained within SOC2, Type II datacenters in the US and the UK.
- Quorum Cloud is flexible and allows for instant and on-demand Recovery Node (RN) configurations and extended retention periods.
- Hybrid Cloud DRaaS provides the convenience and reassurance of both local and remote testing and recovery capabilities.
- Your DRaaS environment is maintained using PCI & HIPAA compliance standards.
- Your DRaaS environment is protected and monitored by a 24×7 PCI-certified security solution.
- Your DRaaS configuration is proactively monitored to ensure customer backups and RN builds are always up-to-date in support of DR readiness in the event of a disaster.
- Daily data transfer to the Quorum Cloud is monitored to ensure your tunnel is available and functional.
- Your networking and firewall rules are created, tested, and maintained by Quorum's DRaaS Support Team.
- You are provided with Public IPs assigned specifically to your organization.
- Your protected systems are proactively updated to the latest version of onQ. All upgrades are performed by the Quorum DRaaS Support Team, so there is no action required on your part.
- The Quorum DRaaS Support Team possesses years of experience in the areas of Business Continuity Planning (BCP) and disaster recovery.
- The Quorum DRaaS Group works closely with your IT department to ensure your DR testing is complete and successful.

Continue
This is a typical HA configuration including an onQ Archive Vault for long term retention. In this example, three critical servers (SQL, Exchange, and Linux) are protected by a single onQ appliance and monitored by the onQ Portal GUI.

**Failure scenario: Single server failure**

In this example, the production Exchange server has experienced some level of failure. Using a single click, an IT staff member is able to start the virtual copy (VM clone or Recovery Node) of the failed Exchange server on the locally deployed onQ HA appliance.

Users need only refresh their interface to the application in order to immediately continue their work.
When deploying onQ in a DR configuration, in addition to the local onQ HA appliance, a second onQ appliance must be deployed at the organization’s DR location.

Changes to locally protected servers (data, applications, and server images) captured by onQ HA are first deduplicated and then replicated to the onQ DR or DRaaS appliance at the secondary location.

**Failure scenario: Complete datacenter failure (e.g., power outage)**

In the event of a complete datacenter outage, IT staff can, with a single click on a web-enabled mobile device, power on and spin up all Recovery Nodes on the onQ appliance deployed at the remote DR site.

The servers will start in a preconfigured sequence including necessary time delays. Users can then use VPN to access the servers, applications, and data on the remote onQ appliance.

Downtime is limited only to the time it takes the VMs to spin-up.
An onQ DRaaS deployment is similar to an onQ DR deployment. However, instead of an organization deploying a second onQ appliance at their own DR site, they have chosen to leverage the Quorum Cloud. Server, application, and data changes captured by the locally deployed onQ HA appliance are replicated to the onQ appliance in the Quorum Cloud. DRaaS deployments enable organizations to more cost effectively ensure both local HA and remote DR as they can avoid the capital expenditures related to designing, staffing, and maintaining a replicated datacenter.

**Failure scenario: Complete datacenter failure (e.g., flooding)**

In the event of a complete datacenter outage, IT staff can, with a single click on a web-enabled mobile device, power on and spin up all Recovery Nodes on the onQ appliance deployed in the Quorum Cloud. The servers will start in a pre-configured sequence, including necessary time delays. Users can then use VPN to access the servers, applications, and data on the remote onQ appliance located in the Quorum Cloud. Downtime is limited only to the time it takes the VMs to spin-up.
“Tapes are not as reliable, and you don’t know how good your backup is until you need it. With onQ, before you have time to think about it, it [your data] is restored – it’s brilliant. Plus the service is excellent! Moving away from tape restore is a big plus for us.”

Sue Hulbert – IT Manager, Weddel Swift

“I really like what I’m seeing here. This Quorum Hybrid Cloud Recovery is the first solution to combine onsite and cloud-based recovery, the first to run its own cloud data center infrastructure [vs. outsourcing] and the first solution that’s capable of doing daily disaster recovery testing.”

Dick Csaplar – Senior Research Analyst, Virtualization and Storage, Aberdeen Group

“From a qualitative point of view, the greatest benefit has been in peace of mind across the organization. The use of Quorum during Superstorm Sandy has shown that our disaster recovery plan — regarding our data, applications and systems — is secure and now proven.”

Doug Feltman – Director of Systems and Applications, 24 Seven, Inc.

“Our data, applications and systems can now be recovered with one click, meaning that downtime has been slashed from one week to minutes. I estimate this saves us upwards of $100,000. Now we’re prepared for any disaster that might come our way.”

Alex Roberts – Associate Director of Technology, Campbell Hall

“With a normal DR solution, we’d have to duplicate our entire infrastructure offsite, which would involve purchasing multiple servers, and more. We chose onQ because it’s an all-in-one solution that gives us complete disaster recovery within a pair of appliances, saving us money and eliminating unnecessary overhead. We love the ease and simple elegance of onQ.”

James Gentile – Chief Information Officer, Arizona Medical Board