Quorum onQ®

Ransomware Edition

Quorum onQ® Ransomware Edition (onQ® RE) is the latest innovation from Quorum. Built on our award winning onQ® Backup and Disaster Recovery platform, onQ® RE is a dedicated recovery appliance built specifically to recover servers infected with Ransomware.

How does it work?

onQ® RE connects to your network and takes snapshots of your production servers. These snapshots are used to create a virtual machine image that can be used in the event of a Ransomware infection. At user determined intervals, new snapshots are taken, encrypted and saved to the hardware appliance. Each snapshot is automatically tested to be sure that it will function in the event of an outage.

What if I'm infected?

In the case of a Ransomware infection, the first thing the IT team must do is isolate the affected system to prevent the spread of the infection. Then the last known good snapshot is selected from the onQ® RE management console and the virtual machine copy is started up. Once fully booted, the system is now on the production network and is ready to take over for the failed server.

> "Over the past 2 years, we have had 3 Ransomware attacks, mostly caused by employees opening documents with infected attachments that looked legitimate. We were able to isolate and recover the infected servers in a matter of minutes. I can honestly say, without Quorum, we would not be in business today."
>
> Confidential Oil and Gas Client

ABOUT QUORUM

Quorum enables IT teams to provide business continuity and the fastest recovery from server downtime in the industry. Our onQ® product was first introduced in 2010 and has evolved into a powerful platform delivering backup, one-click instant recovery, deduplication, replication, automated recovery testing and extensible archiving, all delivered as a hardware appliance, virtual machine or as cloud based disaster recovery as a service (DRaaS).

With offices in the US and the UK serving customers worldwide, businesses of all sizes like the easy installation, flexible deployment options and fast recovery time. To learn more, visit us at **www.quorum.com** or follow us on twitter **@quorumlabs**

Quorum®

Your backups are protected

Quorum has taken several steps to ensure that your snapshots are safe and secure. First, the onQ RE appliance is on its own network segment, which is not a part of the Active Directory domain. This means it is less likely to be targeted by a Ransomware attack. Second, onQ RE also runs a hardened Linux operating system, reducing all security vulnerabilities to an absolute minimum.

Third, if onQ RE snapshots an infected server, and then does an automated start-up test, the network segmentation prevents the Ransomware from spreading to other servers on the main network. Finally, all snapshot data is encrypted in motion and at rest, which means that previous snapshots cannot be infected, ensuring that customers will have an uncompromised snapshot for recovery.

Features

- Dedicated hardware appliance capable of protecting up to 15 servers
- Quad core, 2U server with 64GB of memory
- 22TB of storage
- All data fully encrypted in flight and at rest
- Runs on a separate network segment
- Specially hardened Linux operating system
- Automatic testing of all snapshots
- User defined snapshot intervals

Quorum onQ® RE Protects Your Business