DATASHEET

Quorum Clean Room

Effectively Troubleshoot and Perform Forensics on Ransomware Attacks

In today's digital landscape, ransomware attacks have become increasingly prevalent and devastating for businesses of all sizes. As a result, it is essential for organizations to have a robust disaster recovery plan in place to protect against and recover from such attacks. Quorums onQ offers a comprehensive solution, with a built-in test room environment, which can be used as a clean room to troubleshoot and perform forensics on ransomware attacks effectively.

How to Use onQ Test Network as a Clean Room for Ransomware Troubleshooting:

Once you have taken the preliminary steps of contacting insurance, any police, or forensic experts and made the decision to try and recover, you should proceed in a methodical best practice driven direction.

1. Set up the Clean Room Environment: Create a replica of your production servers and data within the onQ Test Network at a point in time before ransomware took effect. This will serve as a baseline for conducting ransomware troubleshooting activities without risking the integrity of your primary systems.

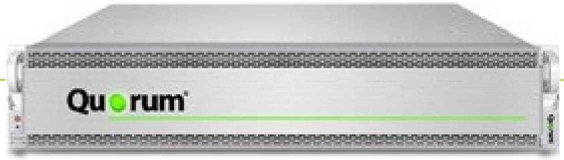
2. Perform Forensics: With the clean environment set up you can use it to perform extensive forensics and ensure the servers are free from infections of ransomware, spyware, and root kits.

3. Clean Network: While working on the servers is a key to recovery, forensics should also be used to identify how your network was breached, and ensure that no back doors were added so you are not re-infected.

4. Document Findings and Recommendations: Keep detailed records of the ransomware troubleshooting process, including the steps taken, recovery outcomes, and areas for improvement. Use this information to refine your disaster recovery plan and enhance your organization's security and resilience against future ransomware attacks. This information should also be given to the FBI or CISA to be used in fighting the ransomware epidemic.

5. Recovery: Once comfortable with the forensics and network status you can move the cleaned servers from the onQ test network back into the production environment, and restore functionality to your company.

About Quorum: Quorum provides all-in-one, easy-to-use disaster recovery and ransomware protection solutions that helps businesses worldwide to protect their mission-critical data with backup, instant recovery and storage replication of your mission-critical data after any storage, system, site failure, or under any circumstances or threat. Quorum serves customers worldwide, with offices in the US, UK and business affiliates with offices in South Korea and the UAE.



Benefits of Using onQ Test Network for Ransomware Troubleshooting:

- Included with onQ solution so you can test as often as you want
- Provides a safe and controlled environment for simulating ransomware attacks
- Enables thorough testing of recovery capabilities
- Facilitates forensic analysis of infected servers without risking production systems
- Helps organizations identify and address vulnerabilities in their network
- Enhances overall security posture and resilience against ransomware attacks
- Ensures compliance with regulatory requirements by documenting recovery processes
- Collaborate with external partners, such as law enforcement and cybersecurity experts, to combat ransomware threats more effectively

In conclusion, leveraging the onQ Test Network as a clean room for ransomware troubleshooting can significantly strengthen an organization's ability to mitigate and recover from cyber threats. By following best practices and using this dedicated environment, businesses can enhance their security posture, protect critical data, and ensure business continuity in the face of evolving cybersecurity challenges.

> “
>
> Over the past 2 years, we 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
>
> ”