CLAIMS

1. A method for efficient data recovery and backup, comprising:

storing data using storage snapshots, from a plurality of first devices, on a plurality of storage arrays via a first network path and a second network path,

determining a condition of data loss, power loss, or a cyber compromise event,

based on determining the condition, instantiating recovery of data using the storage snapshots from the plurality of storage arrays via a third network path, wherein instantiating recovery of data comprises sending the data to a plurality of second devices for scrubbing, analysis, and cleaning.

2. The method of claim 1, wherein the plurality of first devices is associated with a data production environment.

3. The method of claim 1, wherein storing data using storage snapshots comprises:

continuously sending the data from the plurality of first devices to a virtual machine associated with a cyber recovery environment via the first network path.

4. The method of claim 3, wherein the first network path comprises an air gapped first network medium and a control point.

5. The method of claim 3, wherein storing data using storage snapshots comprises:

writing the data from the virtual machine to the plurality of storage arrays via the second network path, wherein the second network path comprises a second network medium.

6. The method of claim 5, wherein storing data using storage snapshots comprises:

utilizing the second network medium to write the data from the virtual machine to a logical unit number (LUN) of the data on the plurality of storage arrays.

7. The method of claim 1, wherein instantiating recovery of data further comprises:

sending the data to the plurality of first devices via a pair of cyber recovery environment storage area network switches.

8. The method of claim 7, wherein instantiating recovery of data further comprises:

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the first devices.

9. The method of claim 8, wherein instantiating recovery of data further comprises:

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with another one of the plurality of the first devices.

10. The method of claim 1, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the second devices.

11. The method of claim 10, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with another one of the plurality of the second devices.

12. The method of claim 1, wherein the plurality of storage arrays stores the data in a read-only manner to make the data immutable.

13. A system comprising:

a memory storing instructions, and

a process configured to execute the instructions to perform operations comprising:

storing data using storage snapshots, from a plurality of first devices, on a plurality of storage arrays via a first network path and a second network path,

determining a condition of data loss, power loss, or a cyber compromise event,

based on determining the condition, instantiating recovery of data using the storage snapshots from the plurality of storage arrays via a third network path, wherein instantiating recovery of data comprises sending the data to a plurality of second devices for scrubbing, analysis, and cleaning.

14. The system of claim 13, wherein the plurality of first devices is associated with a data production environment.

15. The system of claim 13, wherein the system further comprises a cyber recovery environment comprising the plurality of storage arrays, a virtual machine, and a pair of storage area network switches.

16. The system of claim 15, wherein storing data using storage snapshots comprises:

continuously sending the data from the plurality of first devices to the virtual machine via the first network path.

17. The system of claim 16, wherein storing data using storage snapshots comprises:

utilizing the second network path over a fiber medium to write the data from the virtual machine to a logical unit number (LUN) of the data on the plurality of storage arrays.

18. The system of claim 15, wherein the first network path comprises an air gapped ethernet network and a control point.

19. The system of claim 15, wherein instantiating recovery of data further comprises:

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the first devices.

20. The system of claim 14, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the second devices.

21. A method for efficient data recovery and backup, comprising:

storing data using storage snapshots, from a plurality of first devices, on a plurality of storage arrays via a first network path and a second network path,

determining a condition of data loss, power loss, or a cyber compromise event,

based on determining the condition, instantiating recovery of data using the storage snapshots from the plurality of storage arrays via a third network path, wherein instantiating recovery of data comprises:

sending the data to the plurality of first devices via a pair of cyber recovery environment storage area network switches; and

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the first devices.

22. The method of claim 21, wherein the plurality of first devices is associated with a data production environment.

23. The method of claim 21, wherein storing data using storage snapshots comprises:

continuously sending the data from the plurality of first devices to a virtual machine associated with a cyber recovery environment via the first network path.

24. The method of claim 23, wherein the first network path comprises an air gapped first network medium and a control point.

25. The method of claim 23, wherein storing data using storage snapshots comprises:

writing the data from the virtual machine to the plurality of storage arrays via the second network path, wherein the second network path comprises a second network medium.

26. The method of claim 25, wherein storing data using storage snapshots comprises:

utilizing the second network medium to write the data from the virtual machine to a logical unit number (LUN) of the data on the plurality of storage arrays.

27. The method of claim 21, wherein instantiating recovery of data further comprises:

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with another one of the plurality of the first devices.

28. The method of claim 21, wherein instantiating recovery of data further comprises:

sending the data to a plurality of second devices for scrubbing, analysis, and cleaning.

29. The method of claim 28, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the second devices.

30. The method of claim 29, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with another one of the plurality of the second devices.

31. The method of claim 21, wherein the plurality of storage arrays stores the data in a read-only manner to make the data immutable.

32. A system comprising:

a memory storing instructions, and

a process configured to execute the instructions to perform operations comprising:

storing data using storage snapshots, from a plurality of first devices, on a plurality of storage arrays via a first network path and a second network path,

determining a condition of data loss, power loss, or a cyber compromise event,

based on determining the condition, instantiating recovery of data using the storage snapshots from the plurality of storage arrays via a third network path, wherein instantiating recovery of data comprises:

sending the data to the plurality of first devices via a pair of cyber recovery environment storage area network switches; and

sending the data from the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the first devices.

33. The system of claim 32, wherein the plurality of first devices is associated with a data production environment.

34. The system of claim 32, wherein the system further comprises a cyber recovery environment comprising the plurality of storage arrays, a virtual machine, and a pair of storage area network switches.

35. The system of claim 34, wherein storing data using storage snapshots comprises:

continuously sending the data from the plurality of first devices to the virtual machine via the first network path.

36. The system of claim 35, wherein storing data using storage snapshots comprises:

utilizing the second network path over a fiber medium to write the data from the virtual machine to a logical unit number (LUN) of the data on the plurality of storage arrays.

37. The system of claim 34, wherein the first network path comprises an air gapped ethernet network and a control point.

38. The system of claim 34, wherein instantiating recovery of data further comprises:

sending the data to a plurality of second devices for scrubbing, analysis, and cleaning.

39. The system of claim 38, wherein instantiating recovery of data further comprises:

sending the data to the plurality of second devices via the pair of cyber recovery environment storage area network switches to a pair of storage area network switches associated with one of the plurality of the second devices.