How to Set Up a Secure Isolated Recovery Environment (SIRE)

World Backup Day is a great time to dig into the power of modern backup technologies and how they can be leveraged to combat today's threats. That includes one thing every organization should have completed and ready to go: a secure isolated recovery environment (SIRE).

A SIRE should be set up in advance, tested, and in a ready state to be transitioned into quickly after an event. With these steps completed, your infrastructure will be in place, giving you one less thing to worry about when you're being pressured to get the business back up and running with minimal downtime.

Here's why you need a secure isolated recovery environment and how to set one up.

Why Do You Need a SIRE?

Immediately following a breach or event, you should consider your existing environment closed for business until further notice. Don't assume you can salvage even the uncompromised functions. This is because:

- The authorities or investigators may confiscate or quarantine equipment for forensic review
- Insurers may not let you use it
- Internal teams may need it

So what do you need to have ready to get back online as soon as possible? **A secure isolated recovery environment.** This is like having a secure, clean IT environment at the ready so you can **resume critical operations quickly and**

safely until new production capabilities (whether truly newly acquired or reclaimed) can be brought back online.

This means having the hardware, software, and networking infrastructure required to do so—considering your old environment is likely useless for the time being.

You'll need fresh, trusted infrastructure for several reasons:

- To begin recovery while forensics processes are ongoing
- To stage and orchestrate the reintroduction of critical applications
- To test changes before going back into production

Learn how to set up a staged recovery environment

Benefits of a Secure Isolated Recovery Environment

There are multiple reasons this will be advantageous:

- **It creates a "guaranteed point" for the recoverability of your critical data and applications.** You won't use your SIRE for *all* of your applications and data, only those that are critical to operationalize your business in a limited capacity.
- **It's all about speed.** C-level executives are less concerned with the backup environment and whether or not you have an "air gap" or other controls. Their focus is speed: "Is the business back up and running yet? If no, why not, and when will it be?"
- **It will buy you time to complete the forensics review** and get other, less critical systems back online and reintegrated.

6 Steps to Prepare a Secure Isolated Environment

1. Work with business stakeholders to prioritize application recovery needs to appropriately size the environment.
2. Identify the location that the SIRE will be housed in (i.e., on-prem data center or co-location facility such as Equinix or public cloud).
3. Acquire the necessary hardware.
4. Build and test the hardware to ensure it's ready to go when needed.
5. Have built-in snapshot capabilities. Start with snapshots, and plan only to go to backups if you can't get the historical data you need.
6. Make sure backups are clean and don't contain sensitive data that was previously deleted for compliance reasons. Test the backup to make sure it's clean so you're not propagating corrupted code when it's restored, then move to production.

The Most Important Feature of a Good SIRE? SafeMode Snapshots

To really get a jump on the speed that a SIRE is designed to deliver, you'll want to get your critical data into the environment *as quickly as possible*.

Pure Storage® SafeMode™ Snapshots are the best (and only) feature on the market that can give you metadata snapshots that are not only immutable—meaning they can't be modified once written—but they also cannot be deleted, **even by people or processes that might have administrative credentials**. This is an incredible feature that gives you a starting point for recoverability of your data immediately after an attack occurs. And, no having to mess with backups or slow data transfers from offline environments, which also may have been compromised. I cover that in my blog post on why air gaps give a false sense of security.

Learn more about SafeMode Snapshots and start having conversations with your security team today to ensure you’ve got the best recovery environment and strategy possible.