The Top 6
Considerations For IT Resilience & Assurance

The term IT Resilience & Assurance (ITRA for short) is a new term being used by industry pundits to describe technology that enables your business to maintain acceptable service levels even in the event of severe disruptions to your applications, data and the IT systems which support them. ITRA incorporates early detection of pending impact caused by mistakes, malicious activity or mother nature, plus it provides rapid recovery in the event of a failure all in a solution that is affordable, automated and easy to use. The following list provides you with a set of considerations for you to think about when you are evaluating ITRA solutions.

01 Early Warning

One of the key features that a great ITRA solution provides is early detection to predictively identify a risk to your systems. Infrascale's Anomaly Detection allows you to get early warning when something is happening with your your data that could be related ransomware or other type of malware attack. Common symptoms of a ransomware attack include renaming affected files which will cause them to appear as new files when backed up. Alternatively, the ransomware may encrypt the files so they register as "changed" when a backup runs. Infrascale tracks the backup trends for your devices and provides a warning when anomalies such as the quantity of new or changed files increases significantly over the the average.

02 Complete Protection

One of the most obvious, yet crucial elements to an effective ITRA solution is having complete, current and easily accessible copies of your data ready for direct and rapid deployment. This includes usable copies of the systems, applications and data in a portable format and located in safe, accessible locations. It is critical that a solution creates both local and remote copies of your data and that can rapidly move data to a location where the platform can use it. It must support the initial capture of very large volumes of data in an efficient and practical manner.
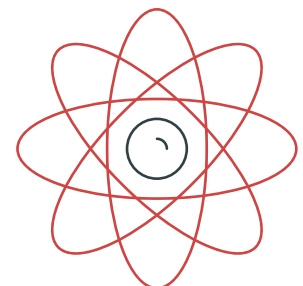
03 Highly Flexible

Look for a solution that provides a local appliance, private cloud, as well as a scalable public cloud component for the remote recovery. The local appliance can be used in the event of a single drive failure including the ability to recover and boot protected systems. For more complex failures, the recovery may require booting workloads remotely in the cloud.
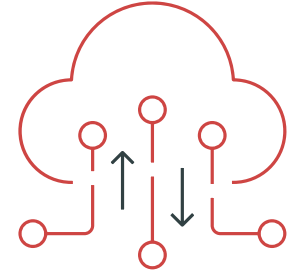
04 Seamless & Efficient Operation

Once the baseline data exists in the secondary location, ensure your solution requires the least amount of data to be moved as possible on an ongoing basis. Because of the size of today's large datasets, it is not feasible to move full images over the internet to the cloud on a daily basis. Look for solutions that leverage deduplication technology to dramatically reduce the amount of data that needs to be transferred. This provides the added benefit of reducing recovery time.
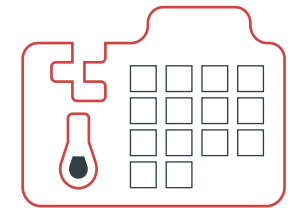
05 Fully Automated

 A data emergency is a stressful time and stress causes mistakes. Be sure your solution provides strong orchestration including fully automated reconstruction of failed systems and all the related dependencies to eliminate human error. In addition, the recovery process should not impose a long list of complicated information required from the operator to initiate it. Lack of automation during the recovery process will lead to delays and potential data loss.

06 Guaranteed

The "A" in ITRA stands for Assurance and you should look for a vendor that not only provides a complete solution, but who stands behind their solution with a clear and compelling guarantee. This guarantee should include commitments in terms of recovery time as well as SLAs that describe what happens if they don't. Only vendors who are willing to back their product with a strong guarantee have the confidence and capability to deliver.