White Paper

The Time For
IT Resilience Is NOW

Infrascale™

Executive Summary

Cloud backup and cloud storage/syncing services are popular because they store data in the cloud, and you can access and restore your data from anywhere -- to anywhere -- fast. Most services even allow you to view and download files from a browser or phone. Where these solutions fall short is they don't provide functionality that allows you to completely recover servers, applications and full business operations in a matter of minutes. Today, what businesses require is affordable and effective IT Resilience. That is, solutions that provide seamless, automated access to your applications and data. Several key pieces of technology must be in place in order for IT Resilience & Assurance (ITRA) to be possible:
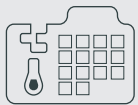
Anomaly Detection

An early warning technology that alerts if out of the ordinary operations are occuring within a data set to warn of potential ransomware or other malicious activity.

Backup

Automated identification, selection, replication and cataloging of data that is not currently protected to a safe location

Deduplicated File System Assisted Replication

Allows for rapid cloning of an entire system or groups of systems by minimizing

Orchestration

Provides a fully automated way of reconstructing failed systems and an orderly restart of the full environment.
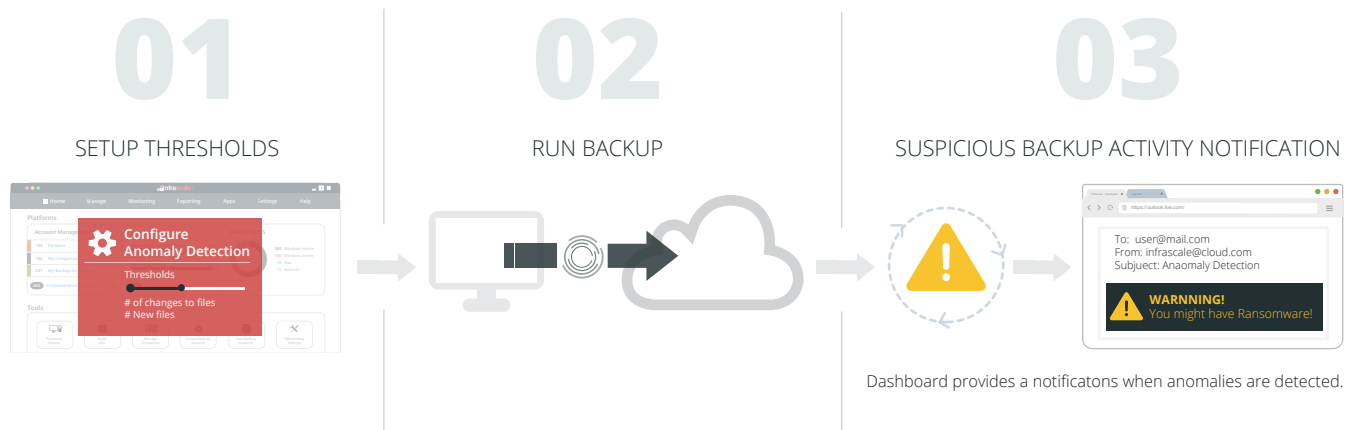
Assurance

A guarantee from your vendor that you will be able to resume full business operation with an SLA for the recovery time.

The purpose of this white paper is to examine the necessary building blocks required for ITRA and to help you understand what to look for when selecting a great solution that best fits the needs for your business.

Anomaly Detection

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.

01 SETUP THRESHOLDS

02 RUN BACKUP

03 SUSPICIOUS BACKUP ACTIVITY NOTIFICATION

Dashboard provides a notificatons when anomalies are detected.
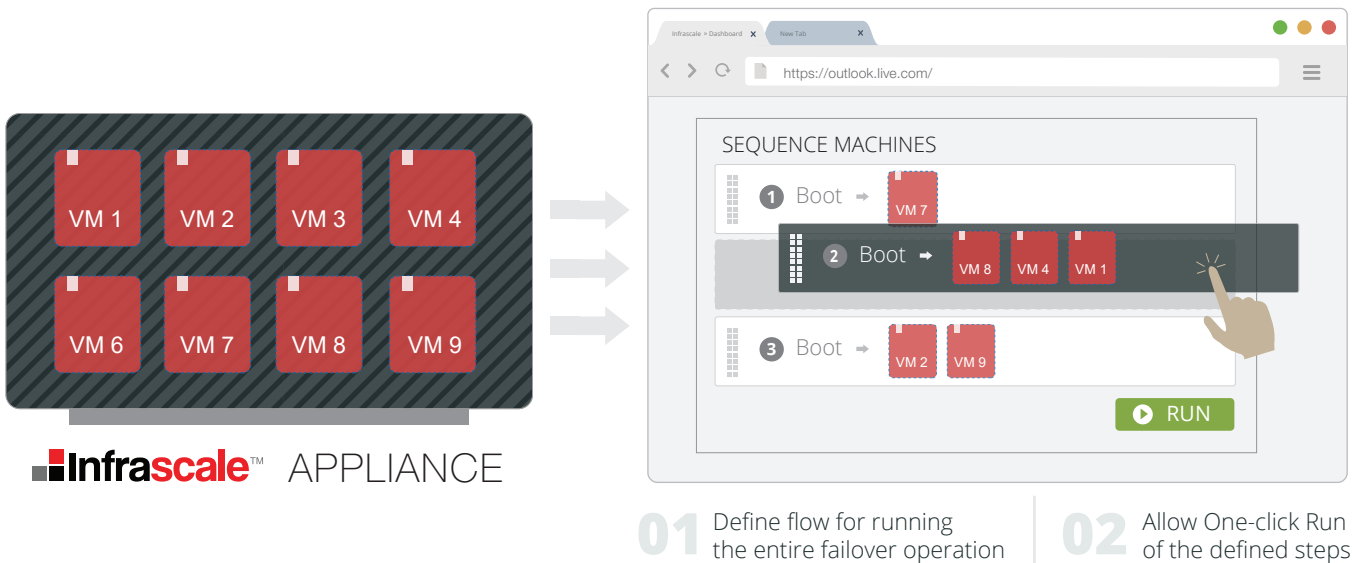
Everything Starts With A Backup

In the event of a single drive failure, you can typically leverage a local appliance to recover and boot a single machine. For more complex failures, a local appliance may not be sufficient. In these cases it is critical to have a usable copy of the systems, applications and data in a portable format and located in a safe, accessible and remote location. This requires replication that can rapidly move data to a location where the platform can use it. The initial capture is often seeded via disk or over the wire. Once the baseline data exists in the secondary location, one of the important capabilities is to be able to move as little data as possible on an ongoing basis especially for very large volumes where complete replication can be prohibitive for recovery time.

Deduplicated File System Assisted Replication

One of the key technologies that Infrascale has developed is DFSAR--Deduplicated File System Assisted Replication. This technology allows you to examine all blocks that exist for a job and compare them to everything that exists on the remote location to see what matches. DFSAR allows you to use blocks that already exist in the secondary location to quickly rebuild that job on the secondary location (Google Cloud or elsewhere). If the system needs to be able to boot, it will create a clone and boot from the clone rather than the backup copy. It's cloning a dedup state of the machine, not the machine itself. This often means that the amount of data that has to be moved is less than 1% of the total volume. This reduction of data being moved results in vastly faster recovery time.
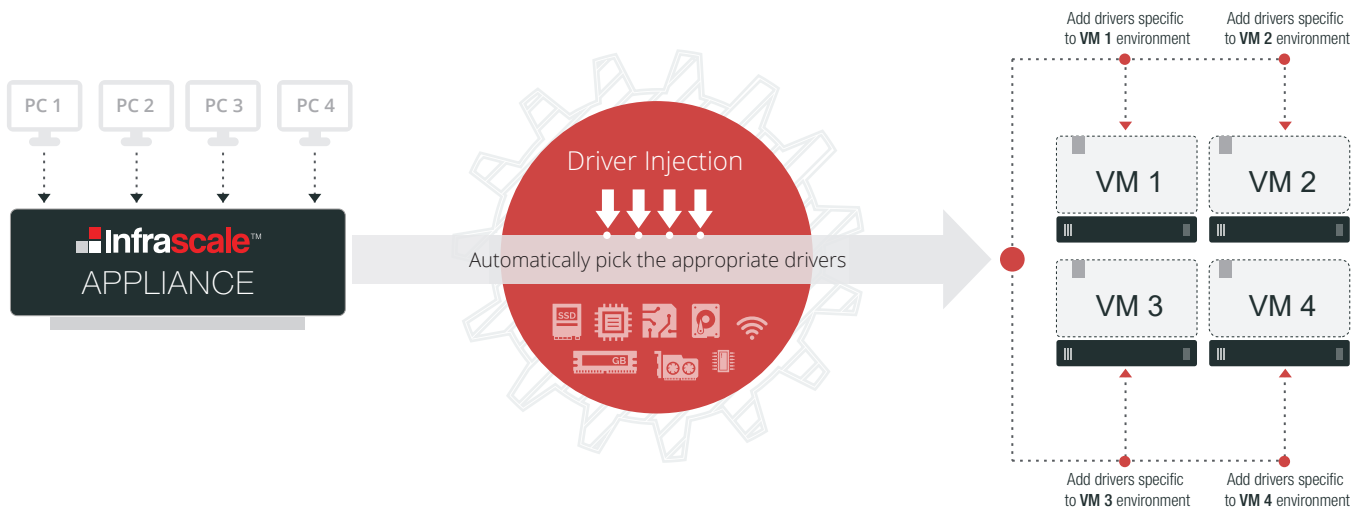
Orchestration

One of the most important components to an IRTA solution is the ability to automate the recovery process to eliminate the risk of human error. Orchestration is critical to a fast and error free recovery. Infrascale's orchestration allows you to drag and drop machines to designate the order that they need to spin up. Without proper orchestration, a Web Server may spin up and try to authenticate against its domain controller which is still booting and although eventually both machines will be technically online, they won't be able to communicate. Infrascale allows you to disable outbound networking so that all the applications can come online in the DR network and you can prove that the entire infrastructure is working and ready to go, but not affecting anything outside the environment. Users need to define which machines are critical to bring up in the event of a disaster. Infrascale provides the ability for self directed orchestration with the drag and drop interface.

Infrascale™ APPLIANCE

01 Define flow for running the entire failover operation

02 Allow One-click Run of the defined steps

A critical component to orchestration are boot groups. Boot groups are collections of pre-defined resources or machines that you can quickly and easily designate to bring back online in a coordinated fashion in the event of a failure. These boot groups are related servers and applications that allow you to designate operational areas to come back on line together or in a designated sequence. In most environments, these systems have dependencies and applications and services have to come back online in a specific order. For example, most every environment has a domain controller and a web server. The web server is often the front end of the business and it will typically spin up much faster than the domain controller. You need to control the startup sequencing of all the machines in order to ensure that everything with dependencies will have the appropriate resources available when they need them. In this example, orchestration may sequence the domain controller to come up first in order to make sure that all the resources and connections required by the webserver are in place prior to the web server coming online.

Assurance

Talking about IT Resilience is one thing, but to be confident that your vendor can actually deliver in the event of an outage, you need assurance in the form of a guarantee. Because of how Infrascale allows simple "point and click" orchestration of multiple systems, the ITRA recovery process is literally one click. Once the orchestration takes over, all your effected systems are back up within a few minutes. The key difference that separates ITRA from cloud backup is that ITRA provides a turn-key business continuity capability that allows you to recover a sophisticated business with interconnected services that can be operational and provides an SLA that assures your full infrastructure will be back up and running within a few minutes. Nested Virtualization allows orchestration to run in a completely automated manner. It allows Infrascale to have not only its core software and orchestration engine running, but also to spin up sub virtual machines that contain your environment with all the applications and data with full automation and no human intervention. These VMs can provide continuous operation or can later be restored to new physical or virtual resources. Driver injection allows the failover to occur from a physical or virtual environment to the virtual environment running in the cloud without concern about the different drivers required to make the systems work in their new hosts. This provides the ultimate flexibility with regard to rapid failover in the event of a disaster.

PC 1   PC 2   PC 3   PC 4

Infrascale™ APPLIANCE

Driver Injection

Automatically pick the appropriate drivers

Add drivers specific to **VM 1** environment   Add drivers specific to **VM 2** environment

VM 1   VM 2

VM 3   VM 4

Add drivers specific to **VM 3** environment   Add drivers specific to **VM 4** environment

Boot it in a dissimilar envronment with diffrent hardware and dirver requirements

Conclusion

If you are looking to take your recovery capability beyond simple backup or folder sync, the best solution is ITRA. When evaluating ITRA solutions, make sure you have a system that supports some type of early warning system, like Infrascale's anomaly detection, so you get an alert of any nefarious activity in your environment and automated action to mitigate possible damage. In addition, make sure you have a solid backup foundation with a capability to take rapid snapshots of large volumes and the ability to boot from the clone. Finally, make sure you have a system that supports strong orchestration and nested virtualization to ensure fully unattended operation. Although the concept of orchestration is powerful, the interface needs to leverage drag and drop to be easy to implement in a self directed manner. Nested virtualization allows you to boot and run entire systems in the cloud. Driver injection takes care of all the differences between source and destination when it is time to failover. Finally, make sure you are working with a vendor that provides assurance in the form of a guarantee that you will be able and an SLA for the recovery time that fits the needs of your business. The result is an affordable and effective IT Resilience solution that provides seamless, automated availability for your business operations. For more information on how Infrascale can help you establish IT Resilience for your business please contact us.