Four Tiers of a Resilient Backup Architecture

Overview

When the unexpected happens—and it will—simplicity, resiliency, and speed are essential. With a tiered backup architecture as part of your response plan, you can build availability and durability into your recovery, reducing major events to non-events. Here's one example of a tiered architecture that you can implement with Pure Storage® technology.

Four Tiers of a Resilient Backup Architecture

1 Active Failover

Tier 1 provides an immediate or nearly immediate failover without the need to restore from snapshots or backups. Technology such as Pure Storage ActiveCluster™ delivers immediate failover between two systems located in close proximity (11ms or less latency between sites) with no data or performance loss should either side of the cluster fail.

For customers outside of the geographical boundaries required to perform synchronous replication, or for those who choose to replicate across longer distances, Pure ActiveDR™ can be leveraged to provide a very low RPO and RTO failover solution.

2 Local Snapshots

Tier 2 enables you to quickly restore from immediate rollback after administrative mistakes or bugs in development. Snapshots of Tier 1 data are taken on a regular, recurring basis—from every 15 minutes to a few times a day. These are kept locally for a relatively short period of time (three to seven days) to provide **near-instant recoverability** should the need to restore occur.

A: Local Snapshot Protection

Additionally, local snapshot protection can extend the recoverability available for a **quick restore from short-term data loss**. Generally, this tier will offload local snapshots from the primary array and store them on a secondary array for a slightly longer period of time (e.g., 14 to 30 days). This frees up storage on the primary array but still provides extremely high-speed restores when necessary. The snapshots all provide immutable and enhanced protections to prevent them from being deleted from the local array.

B: Data Protection Software

Data protection partners and backup vendors can be integrated into this tier, offering a **very fast restore of recent backup data** in the event of a cyberattack. On Pure Storage systems (either FlashArray™ or FlashBlade®), backup vendors can offer advanced recovery options through custom integrations and architectures built with Pure Storage.

3 Primary Data Protection Site (a.k.a. DR Site)

From Tier 2, 30 to 360 days of backup snapshots can be replicated to a Tier 3 site for **medium-term recoverability** from a disaster that might strike an entire, primary data center location, such as a fire or tornado. This tier is meant to be a secondary disaster recovery (DR) site that is physically and geographically separate from the primary site, with advanced backup integrations for fast recoverability. SafeMode™ snapshots provide additional protection from ransomware or the deletion or corruption of backup data.

4 An Optional, Data-only Bunker

Traditionally, Tier 4 may have used tape storage. But today, tape serves little purpose, even for long-term data retention. That's where a Tier 4 data bunker comes into play, serving as an additional, one-way-in vault for **retention of large amounts of data available for immediate use**. Bunkers can be especially useful when an entire geographic region is impacted and/or it is impractical to restore data—but that's not all they can do.

The Third-party Vector Risk

So why are attacks, such as the one on CDK, happening with greater frequency? From the hackers' perspective, it's easy to see the appeal of reaching targets indirectly through vendors and cloud providers. Cybercriminals know that big attractive targets like major financial services and healthcare organizations will have robust defenses around their own assets. But they also know that these organizations likely have relationships with dozens or even hundreds of SaaS applications and other IT providers.

Starting there instead—with third-party software providers—provides access to a multitude of threat vectors that can yield significant results from one exploit. Once attackers gain access to that data and those networks, they can launch ransomware attacks of their own or simply sell access to others.

Will all of these parties maintain comparable defenses? Maybe, maybe not. Just as important: Can the apps' customers—the intended targets—monitor and police all their vendors to make sure they're taking all of the appropriate security measures?

Minimizing the Risk Footprint

> "There's a tremendous amount of inheritance risk that you take on with supply chain software—and you don't always have visibility within your supplier as to what they're doing about security."
>
> **CHIEF RISK OFFICER**

Supply chain and vendor security are top of mind for CISOs, including those who took part in the recent Pure Storage CISO roundtable. They named it one of the biggest InfoSec challenges they face. Here's how CISOs at leading organizations are protecting themselves, reducing risk, and staying out of the headlines.

Ransomware is getting smarter every day, but with Pure Storage backup and recovery solutions, we can outsmart threats together.

PS2657-01-en 08/24