komprise

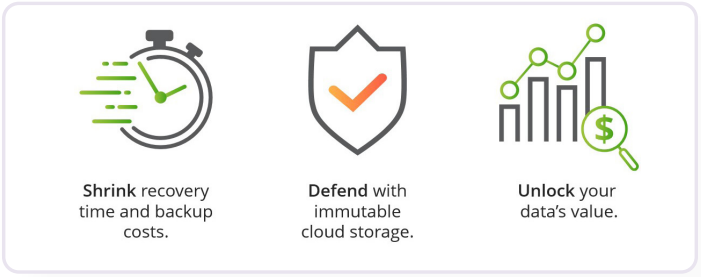
Solution Brief

Protect Unstructured Data from Ransomware

Reduce Attack Surface and Costs with Komprise Intelligent Data Management

Ransomware can enter your organization by infecting any data, not just your mission critical data. This poses a challenge for infrastructure and storage managers who typically focus the best data protection strategies on mission-critical data which is often block data. The large volume, variety and velocity of file data in the enterprise makes this unstructured data the hardest to defend against ransomware attacks and leaves the organization vulnerable.

The large attack surface of file data is risky not only because an attack can enter the network through any one of the billions of files, but also because the attack could spread for months in the enterprise network without detection. Any ransomware defense strategy for file data must consider ways to reduce the active attack surface.



Ransomware Protection at 80% Lower Cost

Komprise Hybrid Tiering Benefits for Ransomware

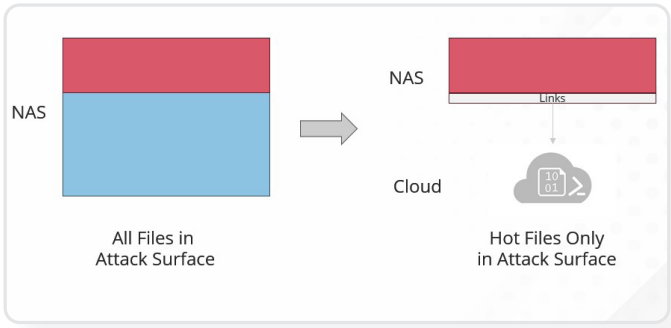
- Hybrid tiering removes the files from the ransomware attack surface, unlike storage-based tiering;
- Tiering to an immutable location adds another layer of defense from potential attacks because any modification to a file causes a new version to be saved.
- Hybrid tiering at the file level is transparent to the snapshot mechanisms, supporting tamperproof snapshots.
- Hybrid tiering at the file level shrinks your storage, backup and DR footprints, reducing costs.

Ransomware defense for file data is difficult and expensive

Defending file data against ransomware attacks is difficult and costly because file data can easily be billions of files and petabytes of data. Most (80%) of this data is cold and not actively used, yet by keeping it in active storage, it is still vulnerable to attacks and must be defended the same way as hot data.

Snapshots are also vulnerable to ransomware attacks

Unfortunately, snapshots may not be an adequate defense to recover from a ransomware attack because snapshots can themselves become infected or corrupted. Storage vendors now offer tamperproof snapshots that protect against deletion. However, most solutions do not allow tiering, as doing so could provide a backdoor access to the destination volume. Komprise is a storage-agnostic solution which works well with tamperproof snapshots.



Komprise Tiering to Cloud Shrinks Ransomware Attack Surface.

Shrink Ransomware Attack Surface with Hybrid Tiering at the File level

Given these constraints, organizations must look for ways to shrink the file attack surface. Transparently offloading cold files through hybrid tiering cuts both costs and risks. Komprise hybrid tiering offloads entire files from data storage, snapshot, backup and DR footprints and leaves behind dynamic links. This allows your users to continue seeing and accessing the tiered files without any change to application or user processes, leveraging **Komprise Transparent Move Technology** (TMT)™.

Reduce Vulnerability to Ransomware Attacks

In summary, most file data isn't mission critical--but it could be your weakest link for ransomware attacks. Komprise hybrid file tiering eliminates cold data from the ransomware attack surface while giving users and applications seamless access. This shrinks your attack surface by 80%+ and it reduces your ransomware defense costs while technologies like tamperproof snapshots work seamlessly.

Learn More

About Komprise as part of your ransomware strategy at **komprise.com/ransomware**

komprise

Komprise, Inc.
1901 S. Bascom Ave. Suite 500
Campbell, CA 95008
United States

For more information:
Call: 1-888-995-0290
Email: **info@komprise.com**
Visit: **komprise.com**

For media requests email
marketing@komprise.com