

## Krome Cloud Backup and Recovery Software

### Already Cloud Ready

Unprecedented data growth is challenging companies of all sizes, placing increasing pressure on their backup and recovery initiatives. With mounting pressure to comply with regulatory requirements and improve disaster recovery practices, companies are experiencing dissatisfaction with traditional backup methods that are falling short regarding efficiency, reliability, and ease of use.

An ever expanding network of central, remote and branch offices further confounds the situation. The need to deliver against strict service level expectations, while managing costs, turns information recovery management into a complex challenge for enterprise data centers of all sizes.

Krome in partnership with Asigra understands the challenge. Our agentless architecture has been developed to deliver an intelligent, elegant, yet easy to implement and simple to use solution with the most robust feature set on the market.

### Empower your enterprise

#### Data Protection Strategy:

You do not need to choose whether to completely manage the entire company data or completely outsource it to an Online Backup Service Provider. Asigra is the only solution available that allows mixing and matching and seamlessly switching between the two strategies without having to reinstall the backup and recovery client software.

#### Public and Private Cloud Data Protection Strategy:

You can leverage the Public Cloud or use your company's Private Cloud to optimise the backup of distributed remote locations, virtual machines and mobile users.

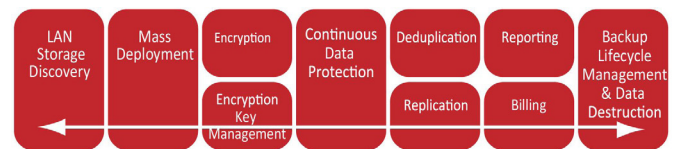
#### Control vs. Custody:

Krome's Asigra solution is the only solution that always ensures your control of backup data. You can easily migrate your backup data from your internal data center to an MSP's facility or vice-versa, without having to reinstall the backup and recovery client software. As your backup strategy changes, retain the custody of your data or outsource it to an MSP, but you always have control over your backup data. Asigra offers a variety of clear, cloud-migration paths.

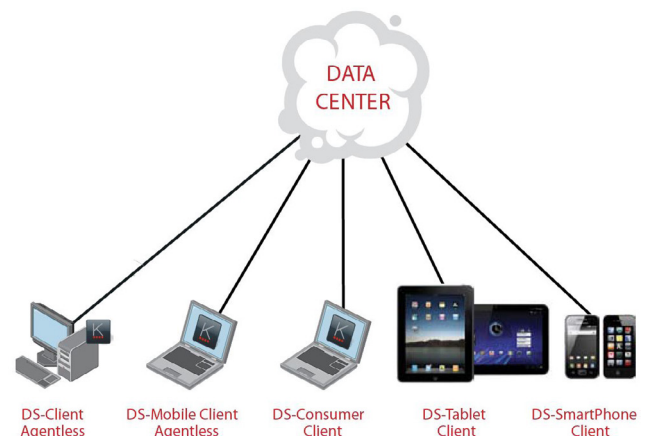
#### Single code base and common platform:

Krome Backup offers a holistic data management solution that includes technologies like LAN Storage Discovery, Mass Deployment, Encryption, Compression, CDP, Deduplication, LAN Resource Discovery, Replication, Backup Lifecycle Management with a single code base an unified platform.

### Single code base and common platform

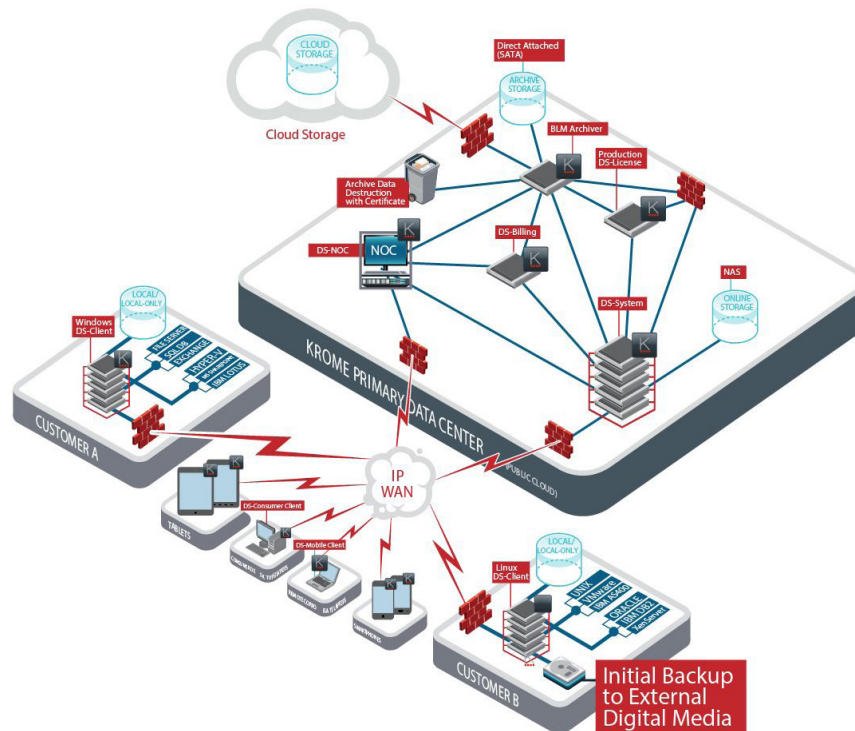


A new industry paradigm shift around backup redesign is finally catching up with virtualisation and public/private cloud computing. Delivered to both small and medium enterprises (SMEs) and large enterprises as a standard (Private Cloud) license, term (Private Cloud) license, or as an online (Public Cloud) backup service, the Krome Backup solution is designed to deliver against strict service level expectations, while managing costs.



### Software

The software is comprised of two major components: the DS Client (one installed at the edge of the cloud) where data needs to be protected); and the DS-System (installed at the vaulting location, or core of the cloud where the protected data resides). This scalability enables Krome to support additional backup loads and multiple Operating Systems, servers, databases, applications, and storage environments. While these features were developed with the storage needs of large businesses and enterprises in mind, our pay-as-you-grow licensing model—which is based on the amount of compressed and deduplicated data stored—makes the solution well suited to SMBs (Small and Medium Businesses).



## Agentless Advantage

Krome's agentless data protection doesn't just match the capabilities of agent-based technology, it exceeds them.

And it does so by no small margin. Like agents, Krome Backup protects all files (visible and hidden), databases, email systems and mailboxes, all standard Unix (including Mac OS X), Linux, Windows, even Systemi Operating Systems. And it does all this by working remotely through the Operating Systems' and application's APIs.

The agentless architecture assures that you experience no Operating System and application disruption or downtime for implementation or upgrades; no security risk because of an open agent port that can be hacked; no server cycles being wasted for agent software. While at the same time you enjoy flexible RPO, including CDP, with incomparably fast and flexible recovery.

**Krome Backup provides agentless backup and recovery support for all leading applications and Operating Systems:**

- |                      |                        |                      |
|----------------------|------------------------|----------------------|
| • VMware             | • DB2                  | • Windows            |
| • XenServer          | • PostgreSQL           | • Linux              |
| • Hyper-V            | • Sybase               | • Unix               |
| • MS SharePoint      | • Lotus Notes & Domino | • AIX                |
| • MS Exchange Server | • GroupWise            | • Novell Netware OES |
| • MS Outlook         | • My SQL               | • Mac OS X           |
| • MS SQL Server      | • Android Tablets      | • System i/Power 6   |
| • SAP                | • SmartPhones          | • Apple iOS 4 & up   |
| • Oracle             |                        |                      |

## Significant Savings

Even if agents from traditional backup and recovery vendors were free, an Asigra solution would still enable huge reductions in operating expenses through its:

- Auto-upgrade to new software versions and Hot Fixes engine
- Central Management GUI interfaces
- Scheduling and automation of tasks, etc.

## Simple licensing

Simply purchase software the same as disk capacity no license fees, no tracking, no overspending on site licenses you only pay for compressed and deduplicated capacity consumed.

## One piece of software to install, manage, upgrade

The software even self-upgrades, so there is no timeconsuming and administrative resource draining pushing of agents or updates out to hundreds or thousands of remote-site systems.

## WAN/LAN/CPU resource conservation

The software runs with negligible impact on servers, workstations, and laptops, eliminating the CPU-cycle hits associated with agent-based solutions.

## Robust, hardcoded security

There are no agents to open hacker-tempting ports in the firewall.

## Elegant scaling

While agent-based solutions compound complexity in rapid growth environments, our agentless backup/recovery solution easily accommodates new capacity, new applications, new sites, and additional backup sources.

## Krome Cloud Backup is comprised of two major components; the DS-Clients and the DS-Systems:

### DS-Client

Installed at the end customer's premises where data needs to be protected. The DS-Client is the collector of the data from all machines, drives, applications and systems on the end customers LAN.

The DS-Client software is agentless - it does not need to be installed on every machine or application it backs up. It can run on a dedicated DS-Client machine or on an existing machine on the LAN that it needs to backup. One DS-Client is sufficient to collect and backup all the data from all the servers, desktops, laptops, network or local drives, structured applications and raw files on the entire LAN.

It is designed to accommodate a range of heterogeneous network backup requirements and transmits data securely to the DS-System onsite or offsite over the Wide Area Network (WAN). The agentless DS-Client is offered for Windows, Linux or MAC environments.

### DS-Mobile Client

Installed on the remote laptop and sends it to the DS-System at the Service Provider's (SP's) or private cloud data centre. The DS-Mobile Client collects data from the remote laptop it resides on. It is designed to accommodate a range of heterogeneous network backup requirements and transmits data securely to the DS-System residing in the datacentre. The DS-Mobile Client has a very light footprint and can be centrally configured and Mass Deployed to any number of laptops within minutes. The agentless DS-Client is offered for Windows environments.

### DS-Smart Phone Client

Installed on the smart phone. The Client collects data from the smart phone and sends it to the DS-System at the Service Provider's (SP's) or private cloud datacentre. The DS-SmartPhone Client for Apple iOS can be downloaded from Apple App Store. The DS-SmartPhone Client for Google.

### DS-Tablet Client

Installed on the tablet. The DS-SmartPhone Client collects data from the tablet and sends it to the DS-System at the Service Provider's (SP's) or private cloud datacentre. The DS-Tablet Client for Apple iOS can be downloaded from Apple App Store. The DS-Tablet Client for Google Android can be downloaded from Android Market or Amazon Appstore.

### DS-Consumer Client

Installed on the consumer desktop or laptop. The DS-Consumer Client collects data from the consumer desktop or laptop and sends it to the DS-System at the Service Provider's (SP's) datacentre. The DS-Consumer Client can be downloaded from the Asigra website.

### 2. The DS-System

The DS-System installed at the Enterprise or Krome's datacentre or core of the cloud. The DS-System is the data aggregator. It receives data from all remote DS-Clients. The DS-System is available in standalone or High Availability (HA) and scalable N+1 configuration.

#### DS-System

DS-System software maintains, manages and validates the online storage repository where the backed up data transmitted by the DS-Clients is saved. The DS-System is typically located in a secure offsite hosting facility. The storage Architecture for the DS-System may be Direct-Attached-Disk, Storage Area Network (SAN) or Network-attached storage (NAS). The DS-System is offered for Windows or Linux.

#### N+1 DS-System

The N+1 configuration of the DS-System is designed to allow for further scalability of the DS-System as well as to increase the availability of the backup service. The N+1 DS-System offers scalable architecture for more nodes in the N+1 configuration, as well as scalable storage through the Extensible Storage functionality. The DS-System is designed to withstand failures of some of its nodes without interrupting the backup service. All nodes in the N+1 DS-System configuration work together to provide backup and restore services to the same DS-Clients. As long as half of the N+1 nodes are available, the backups and restores will not be interrupted. Any DS-System from the N+1 configuration can serve (backup, restore, delete, synchronise, validate, etc.) the DS-Clients. The N+1 DS-System is offered for Windows or Linux.

#### Consumer DS-System

Consumer DS-System software maintains, manages and validates the online storage repository where the backed up data transmitted by the DS-Consumer Clients, DS-Tablet Clients and DS-SmartPhone Clients is saved. Consumer DS-System may be used to provide backup/restore services to one or more DS-Consumer Clients under the same accounts or under different accounts. The Consumer DS-System is typically located in a secure offsite hosting facility. The storage Architecture for the Consumer DS-System may be Direct-Attached-Disk, Storage Area Network (SAN) or Network-attached storage (NAS). The Consumer DS-System is offered for Windows.

#### Mobile DS-System

Mobile DS-System software maintains, manages and validates the online storage repository where the backed up data transmitted by the DS-Mobile Clients residing on remote laptops in the field is saved. The Mobile DS-System is typically located in a secure offsite hosting facility. The storage Architecture for the Mobile DS-System may be Direct-Attached-Disk, Storage Area Network (SAN) or Network-attached storage (NAS). The Mobile DS-System is offered for Windows or Linux.

## Replication and Backup Lifecycle Management (BLM)

### Replication DS-System

The Replication configuration of the DS-System allows storing backed up data into multiple geographical locations for redundancy and high availability reasons. Depending on the Replication configuration, DS-Clients can automatically fall back to replication DS-Systems for their backup, and restore activities if the main DS-System is not available.

Replication DS-Systems can easily be turned into production DS-Systems by simply changing their license parameters. Replication DS-Systems are licensed separately.

### DS-NOC

DS-NOC is a web interface that allows Enterprises or Service Providers to access and monitor DS-System, BLM Archivers or DS-Billing Systems DS-License Server and DS-Clients remotely through web.

Additionally, Service Providers use DS-NOC to enable web access for their end customers or partners to other DS-System, BLM Archiver reports, status updates, account/DS-Client creation on DS-System and web access to the archive data stored in the BLM Archiver.

Users with the DS-NOC web interface have granular access to its functionality based on granted permissions. File restore through web is also available DS-NOC is licensed separately.

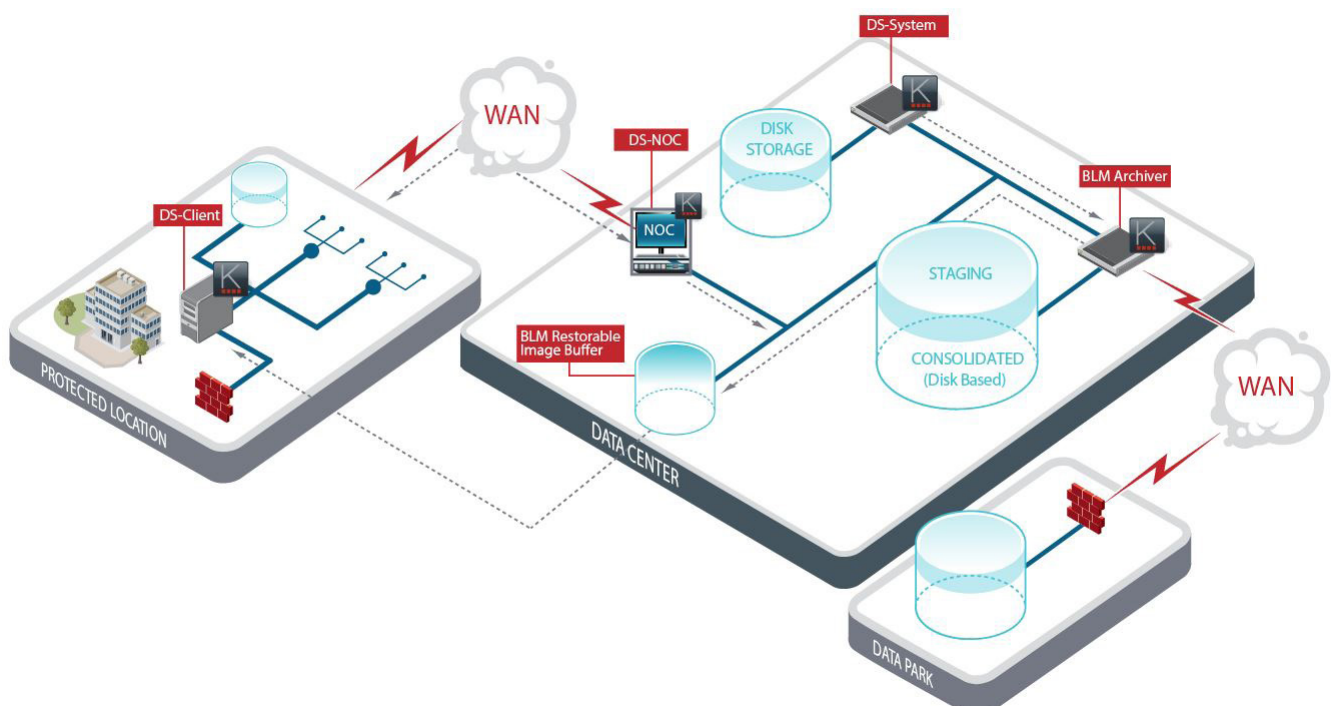
### Backup Lifecycle Management (BLM)

Every business stores data of varying importance. Mission-critical data required for day-to-day operations must be immediately accessible and stored on the DS-System. However, less important data or dormant files for significant periods of time occupy premium real estate on the DS-System and should be saved to less expensive storage and eventually deleted to ensure compliance. The DS-System's online disk-based storage maintains critical data. BLM allows you to archive DS-System data for long term, either for cost or for regulatory compliance reasons.

- Saves money while still offering data protection by archiving obsolete generations and deleted data as well as old data.
- Enables compliance with backup regulations by allowing periodic copy archiving, and by providing data destruction (with certificate).
- Licensed per amount archived. Unlimited restores.
- It is a separately licensed software.

### Backup Lifecycle Management (BLM) Replication

The Replication configuration of the BLM Archiver is designed to accommodate replication data for one or multiple BLM Archivers for redundancy/compliance purposes. Replication BLM Archivers can be easily turned into production BLM Archivers by changing their license parameters and by reconfiguring DS-Systems to archive their data on the new BLM Archivers. Replication BLM Archivers are licensed separately.



## Advanced Modules Overview

Modules are additional software functionality that may augment the core backup/restore capability of the DS-Client and DS-System. The modules are licensed separately, but are pre-integrated with the DS-System. Some of these are licensed separately.

### Autonomic Healing

A veritable storage immune system, this module constantly scans the DS-System and immediately notifies when it encounters a corrupted or otherwise problematic file.

Before the file can cause any harm, Autonomic Healing detects any corruptions (both data corruptions and logical inconsistencies caused by third party technologies such as faulty RAID controllers, file systems, Operating Systems, disk subsystems, network packet loss, etc) and sends notifications so that the personnel can fix the problem before it becomes harmful.

- Allows constant and seamless monitoring of DS-System storage.
- Saves time by identifying potential problems before they become serious issues.
- Ensures backup data is constantly in a valid state to maintain high SLAs for customer restores.

### LAN Storage Discovery

This module completely analyses the entire concentration of data on the LAN before you commit to a backup procedure. This module generates relevant reports that identify possible storage inefficiencies, thereby enabling you to optimise and better manage the backup procedure from both a data and cost perspective.

#### Report data helps to show areas where you can:

- Increase server availability and performance.
- Isolate storage abuses before conducting a costly backup.
- Reduce backup window time.
- Optimise network disk space, which enables you to determine which files require backup.

### Local Storage

This module enables customers to store copies of their backed up data locally, on DS-Client LAN for fast restores in Disaster Recovery scenarios.

### Local-Only

This module enables customers to store backed-up data locally only on DS-Client LAN. This module is capacity-based and is enabled from DS-System. It enables customers to specify data to be stored offsite and/or onsite or on-site only.

### Other Modules

- DS-Recovery Tools
- Disc / Tape Module

