

KOMpliance is secure data software for the enterprise. Optimized to take advantage of today's virtual environments, engineered to secure, protect, preserve and retain data in compliance with the most rigorous government regulations and industry standards. KOMpliance sets the standard for cost-effective, easy-to-implement and maintain, long-term secure data solutions.

OVERVIEW

The KOMpliance software is ideal for any organization that needs to implement data security and privacy, regulatory and corporate compliance, or the long-term archiving of unstructured data. There is no learning curve or retraining required; users can continue to use the same applications without having to change what they do or how they access data. KOMpliance offers the same level of immutability and permanence that has been long associated with hardware based solutions in a pure software deployment. KOMpliance advanced security capabilities extend beyond the basic functionality of WORM Write-Once media to manage the entire lifecycle of all data. KOMpliance is very popular in highly regulated industries including financial and healthcare; federal, state and local government; public safety, insurance and higher education as well as video surveillance and organizations with multiple remote offices.

DATA SECURITY IS NO LONGER A NICE TO HAVE OPTION. IT IS A VITAL PIECE OF ANY BUSINESS. YOUR DATA IS TOO IMPORTANT TO LOSE, TOO SENSITIVE TO BE SEEN OR STOLEN AND TOO CRITICAL TO BE COMPROMISED, CORRUPTED OR MODIFIED.

SECURITY

- **Safety Net** – KOMpliance enforces what users are permitted to do instead of what they are privileged to do; isolating data security from standard access privileges.
- **Future-Proof** – KOMpliance protection moves with the data ensuring that the security will survive the changes in Windows versions, architecture and configuration.
- **Dark Security** – Hide sensitive files and documents rendering them invisible to all those whose are not authorized to know of their existence.
- **Application Verification** – restricts data access and operations to known, qualified, verifiable and authenticated applications.



CHANGING THE RULES ... CHANGES THE OUTCOME ...

KOMpliance presents a new shift in the security paradigm creating another layer of control over the security and privacy of corporate information. The traditional security mechanisms adopted across the globe depend on standard measures including firewalls, proxy servers, anti-virus and anti-malware and most importantly a regiment of LDAP and Active Directory groups and permissions. These measures, though significant, overlook the biggest security risks of all, the users. At the end of the day no matter how secure an organization may think they are, all operations are dependent on access privileges and in fact these privileges are enforced by the operating system which does not understand intent. Any time a user invokes an application, opens an email or clicks on a link they are invoking it in their own context and it is inheriting their privileges. The operating system security model only understand whether you could perform an operation and does not have the ability to determine whether you should. This is a fundamental challenge that faces every organization. Most data breaches and compromises are actually triggered on the inside. They can be accidental or malicious but the outcome is always the same and the cause is simply an inside job.

INTEGRITY

- **Digital Signature** – maintains a verifiable validated SHA-256 digital fingerprint of the contents of retained files and documents across all replicated copies ensuring that the history and contents cannot be altered after the fact (WORM storage)
- **Secure Time** – KOMpliance automatically prohibits tampering with the system time. The server time is protected against power outages, changes in BIOS and fake or untrusted NTP servers to ensure verifiable chain of custody and accurate audit trails.
- **Tamper-proof Protection** – Safeguard file authenticity protection against threats, corruption and manipulation with an accurate audit trail, verifiable digital fingerprints that are validated and maintained across all replicated copies.
- **AES-256 Encryption** – Secures data-at-rest in encrypted tamper-proof volumes to prevent data breaches or theft and enable the creation of encrypted backups.
- **Data Verification** – Files are continually verified against their digital signatures and fingerprints. KOMpliance provides self-healing replication that ensures data protection for seconds, days, years, decades or forever.

DATA SECURITY

Unstructured data represents up to 80% of data in most organizations which by its nature either never changes or changes infrequently. This data can be secured by an IT generalist using the existing IT infrastructure without any disruption to user access or ongoing operations. The data secured and managed by KOMpliance is automatically protected instantly without delay. There are no agents to deploy, no proprietary connectors to purchase or hardware acquisition required and above all no vendor lock.



DISASTER RECOVERY

Most organizations rely on various combinations of backup and replication processes to protect their assets. These processes are always dependent on one simple premise that the data being backed up is the genuine article. Everyone needs a backup plan and the ability to recover from any failure or disaster. However, these backups can only deal with the aftermath of the changes regardless whether they were deliberate or accidental. The corruption of data would always take place outside the context of the backup processes and there is no mechanism for the backup application to intervene or prevent the change from occurring in the first place. KOMpliance radically changes the impact on backup preventing and circumventing illegal /inappropriate modifications to protected files.



BACKUP ASSURANCE

KOMpliance-protected data is immune to modifications, dramatically reducing the size, time and cost of the backup processes. Most importantly the backups would not contain corrupted or compromised data ensuring that the backup is genuine, protected and instantly accessible. Customers can continue to utilize the backup software of their choosing. KOMpliance-protected volumes may be repeatedly backed up as often as required.



DID YOU KNOW? *Standard system security measures enforce user privileges based on what operations are allowed and have no context or understanding of intent. They only understand and enforce what a user could do and have no understanding of what they should not be able to do. All data secured by system based access controls and Active Directory groups and permissions is vulnerable. Even encrypted files are just as vulnerable, they may be obfuscated but a privileged user can still delete, corrupt or overwrite them. KOMpliance security prevents deletion, corruption and modifications ensuring that the data stored is the genuine article.*

COMPLIANCE REQUIREMENTS

- **Government Regulations** – Meet regulatory mandates (e.g., Federal Rules of Civil Procedure (FRCP), SOX, SEC-17a4, FINRA, CJIS, HIPAA, GLBA, PCI DSS, etc.)
- **Data Retention** – Easily create retention rules for unstructured data directories or file types.
- **Instant Retention** – KOMpliance can retain data instantly upon creation. There is no agent, no move required.
- **Legal Hold** – Apply legal hold on any file to override the retention expiry until the litigation hold is removed.
- **Adaptive Retention** – Flexible policies retain files for fixed, permanent “never expire” or indefinite periods that can be expired or lengthened to accommodate the organization’s needs.
- **Persistent** – KOMpliance file retention can be extended but never shortened.
- **Data Deletion** – KOMpliance performs a secure erase / DoD wipe of file contents to delete all copies.
- **Chain of Custody** – Ensures authenticity with accurate audit trails, metadata and verifiable digital fingerprints across all retained file instances.
- **One System** – There is no need to isolate, separate or redistribute data. Not all data is created equal, some files may never require retention.
- **Secure Privacy** – KOMpliance secures both retained and regular files in the same folders allowing users and applications to function normally without any impediments.

REGULATORY AND CORPORATE COMPLIANCE

KOMpliance is ideal for organizations that must comply with regulatory compliance requirements and mandates for data security, privacy, retention, preservation and immutable WORM storage. KOMpliance standard features address the strictest regulatory requirements for data integrity, protection, privacy, security, longevity, availability and disaster recovery with full audit trails. KOMpliance simplifies and automates the enforcement of internal corporate guidelines for data retention, deletion, privacy, protection and risk mitigation. Organizations use KOMpliance to effectively address; information privacy requirements (medical, financial, juvenile, criminal, student etc.) per HIPAA, CJIS and PCI-DSS; immutable record retention requirements per SEC 17a-3, SEC 17a-4, FINRA 4511, GLBA, NCUA, Sarbanes-Oxley and FDA 21 CFR-11; as well as high availability and litigation hold per eDiscovery and Federal Rules of Civil Procedure (FRCP).



LONG-TERM ARCHIVE

The KOMpliance software secures data for seconds, hours, days or decades with unsurpassed integrity and protection in an easy to use and manage interface regardless whether the data resides on-premise, in the cloud or both. Each file is fingerprinted with a SHA-256 digital signature and replicated instantly on geographically separated instances of KOMpliance. Background data integrity audit processes validate replicated file fingerprints to ensure file authenticity without the need for administrative intervention. These self-healing integrity checks, audit digital file signatures and secure time stamps work together to enforce file security with a verifiable chain of custody for each file throughout the retention period.



WORM “WRITE-ONCE” SOFTWARE

KOMpliance patented software-based immutable WORM and encryption unconditionally enforces retention, privacy and secure erasure to meet strict compliance regulations, mitigate risks, and eliminate errors avoiding punitive fines and penalties without having to deploy proprietary hardware. This unique approach to data security allows organizations to continuously modernize their infrastructure to take advantage of advances in storage and server technology while maintaining the same level of security and chain of custody mandated by regulators and legislators.



SCALABILITY AND AVAILABILITY

- **Active-Active Replication** – KOMpliance continuously replicates data across volumes to protect against failures.
- **Sustainable Continuity** – KOMpliance maintains up to 64 concurrent copies that can span across different locations, storage, hyper-visors, configurations and versions of Windows.
- **Failover / Failback** – Native active-active replication protects against site disasters with automatic failover and self-healing synchronization and reconciliation. There is no master or slave and no manual intervention required.
- **Performance & Capacity** – Scale capacity up to multiple petabytes. License the capacity on-demand as required using any storage technology even thin provisioned disks.
- **Obsolescence Protection** –KOMpliance provides organizations with the flexibility to secure data today and in the future as their storage infrastructure evolves without any costly data migrations or conversions.
- **Hardware Agnostic** – KOMpliance is designed to be completely hardware and configuration agnostic, automatically adapting and embracing to changes.

REMOTE AND BRANCH OFFICES

Enforcing corporate compliance guidelines for data that resides in remote or branch offices can be a daunting and overwhelming undertaking for most organizations. Commonly, these remote offices have no local IT personnel and the users are plagued with access delays and network latency issues. The simplest solution to alleviate these IT challenges is to deploy KOMpliance at corporate headquarters and replicate to instances of KOMpliance in each remote office, providing NFS and CIFS shares. All data stored at the branch office KOMpliance instances is instantly protected locally and securely transmitted to the KOMpliance instance at corporate. KOMpliance Active-Active replication allows up to 64 concurrent instances to exist across various locations and geographies affording the same level of security to the local users and replicating the data to the other locations.



ACTIVE-ACTIVE REPLICATION

KOMpliance built-in replication capabilities enable organizations to maintain up to 64 concurrent active-active replicated copies. These replica copies are identical in content but completely independent of infrastructure, storage configuration and even Windows version. Users and applications can access a local copy in their location eliminating network latencies and enhancing disaster recovery. Replica copies can be added on the fly leveraging the KOMpliance self-healing replication design to reconcile and resynchronize the contents across all copies.



SELF-HEALING REPLICATION

KOMpliance always keeps track of the outstanding work and completes the transactions after any outage or loss of connectivity. There are no master or slaves. Failover is simple and transparent. KOMpliance replication can bridge the gap for infrastructure transformation allowing organizations to simply add a physical or virtual machine to the replication group. Using KOMpliance organizations can continuously modernize their infrastructure to take advantage of advances in storage and server technology while maintaining the same level of security and chain of custody mandated by regulators and legislators.



DID YOU KNOW? *Backup and replication technologies cannot prevent data loss, since they have no knowledge or understanding of what is legal or illegal. In fact, they actually are only aware of the changes after the fact. They simply copy or replicate the changes and they cannot prevent or stop the changes from occurring in the first place. Everyone needs backups and replication for disaster recovery, but adding KOMpliance security prevents deletion, corruption and modifications ensuring that the data restored or recovered is the genuine article.*

PRIVACY

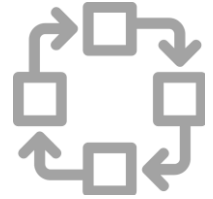
- **Security** – KOMpliance security policies override user access privileges ensuring that files are immune to modifications even when they are not retained.
- **Data Loss Prevention** – KOMpliance security provides unprecedented control to circumvent data breaches, inhibit ransomware, prevent data theft and loss.
- **Encryption** – Files are stored on AES-256 encrypted volumes. There are no external tools or service required.
- **Resilient** – KOMpliance secures digital corporate assets and no single individual could ever jeopardize data access.
- **Authentication** – Users are authenticated with Active Directory and ACL permissions.
- **Audit Trails** – Audit trails report on file access and denied access attempts

EFFICIENT

- **Use Any Storage** – Create secure encrypted KOMpliance -protected volumes using any storage.
- **Reduce Backups** – KOMpliance volumes can be removed from the backup stream, significantly reducing the size of full backups resulting in a fast return on investment based on savings of labor, hardware, media and time.
- **Secure Backups** – KOMpliance prohibits and prevents modifications and corruption that would compromise the validity and integrity of retained data being backed up.
- **Fast Restores** – KOMpliance replication is self-healing to reconcile across all copies from all locations eliminating the need for lengthy scan and restore operations.

FILE LIFECYCLE MANAGEMENT

KOMpliance software incorporates a flexible file lifecycle management engine that controls every aspect of the file lifecycle from creation to disposition. These policies allow organizations to enforce strict controls on what operations are enabled or disabled and override access privileges and permissions to limit who can access or see the data or what they can do. These protection policies further enhance file security with the ability to incorporate Active Directory and ACL permissions to provision who can set or clear file retention or manage litigation hold. Creation policies can screen for legal document and file types preventing the creation of illegal / inappropriate content



MINIMIZE RISKS

KOMpliance isolates the security of the data from the privileges of the user in an independent layer that is not dependent on the user privilege but is dependent on corporate and departmental mandates and policies. The security of data is unconditional and operations that are deemed inappropriate are denied immediately overruling the privileges of the user or even the domain administrator. No other security measure can provide the safety net and shield provided by KOMpliance to protect critical and sensitive data from the power of users and domain administrators. The risks of ransomware and data breaches are real; the damages could be monumental and the punitive fines could be detrimental. Every organization can benefit from KOMpliance security and protection.



MAXIMIZE ROI

KOMpliance is deployed as a software running on Windows Servers. The security and advanced features included in the package are all standard. There is no proprietary hardware, no expensive migrations and no data conversions. Organizations can simply decide to Opt-in or Opt-out without delay. Most organizations can realize the benefits and savings from deploying KOMpliance within 90 days.



CLOUD-READY

- **Archive AnyWhere** – KOMpliance features enable service providers to offer highly secure Archive-as-a-Service with logical, physical and encryption data separation.
- **Online Archive** – An on-premise KOMpliance instance can replicate to a cloud-based KOMpliance-protected archive service. KOMpliance supports one-to-one and many-to-many replication.

EASY TO MANAGE

- **Automatic Archive** – Allows files to be created and secured immediately. There is no need to migrate or delay retention.
- **NAS (NFS/CIFS)** – Leverages Windows file sharing capabilities. Users and applications simply access CIFS/NFS NAS interface to stores files on KOMpliance.
- **Fast, Easy Deployment** – KOMpliance can be installed and configured in minutes. File lifecycle policies ensure files and folders are secured instantly, completely transparent to applications and users.
- **Global Management** – Single pane-of-glass management across all replicated local and remote KOMpliance instances
- **Ultimate Data Protection** – Protecting data with KOMpliance has many advantages over traditional hardware based solutions and backups; including WORM, single file deletion, greater reliability and availability, and replication failover to dramatically reduce RTO
- **Authentication** – KOMpliance supports Active Directory authentication in the enterprise preserving file and folder level NTFS permissions.
- **Lights-Out Management** – Self-managing KOMpliance issues alerts when something needs attention.

GO AHEAD VIRTUALIZE

Increasingly, organizations are taking advantage of the great efficiencies and cost savings to be had by virtualizing their infrastructure. KOMpliance Software, affords organizations the flexibility to protect and secure data in virtualized environments.

Organizations can leverage the adoption of virtualization across all their data and file servers without having to compromise usability, functionality or interoperability. IT administrators can leverage their existing Windows administrative expertise, existing backup tools and even thin provisioned disks behind their virtual machines. There is no need to change what they do or how they manage their virtual machines. Go ahead virtualize and avoid the expense of deploying additional servers or storage to protect data.



NO HARDWARE, NO VENDOR LOCK

Traditionally, hardware based solutions employ proprietary interfaces to implement compliant data storage forcing customers to change how they conduct their day-to-day operations. In most cases, customers have to purchase additional proprietary hardware, replace existing applications, acquire expensive connectors. Every infrastructure deployment has a limited lifespan that is governed by the business needs and the lifecycle of the hardware which commonly becomes outdated, EOL or obsolete. KOMpliance provides a simple and painless pure software approach allowing customers to secure critical data on any storage they choose today, and the flexibility to keep their data secure as their infrastructure evolves in the future. Users can simply drag and drop their data into or away from KOMpliance. There are no costly conversions or migrations required.



CHANGE NOTHING - ZERO IMPACT APPROACH

The KOMpliance pure software approach to data security is rooted in over three decades of experience and based on a deep understanding of the real life data security challenges and regulatory compliance scenarios that customers have to address. KOMpliance allows organizations to deploy secure tamper-proof volumes that address their compliance needs and minimize the impact on users and applications. There is no need to deploy agents, purchase connectors or change how the users access data or upgrade applications. Users simply access the KOMpliance volumes using standard file sharing interfaces to create, store and access files using existing applications; there is no training or learning curve; it just works!



EASY TO USE

- **Non-Disruptive** – Users and applications do not need to change to work with KOMpliance. Any application can have its data securely archived on a Windows Server or Virtual Machine while the application is in production.
- **Override Privileges** – Preserve and enforce file and data security to prevent illegal or inappropriate operations even when invoked by administrators.
- **On-The-Fly Retention** – Users store files that may be retained immediately upon creation without delay and without having to move, or migrate. There are no agents or connectors required.
- **Dynamic Capacity** – License the capacity that you need to protect on demand, independent of the size of the KOMpliance-protected volume and regardless whether it was thin-provisioned or not.

A PROVEN TRACK RECORD

KOMpliance has improved the way a range of industries secure data. Addressing the strict WORM retention requirements of SEC and FINRA in the financial sector. Streamlining processes and reducing costs to secure images, medical records and privacy in healthcare. Protecting public records, confidential information and historic data for state and government agencies. And it provides chain of custody and continuity of information for legal applications. Some of the most common industries served include:

- | | | |
|------------------|------------|-----------------|
| • Financial | • Legal | • Education |
| • Healthcare | • Security | • Insurance |
| • Life Sciences | • Banking | • Surveillance |
| • Transportation | • Courts | • Public Safety |
| • Manufacturing | • Defense | • Government |



LEARN MORE

Discover all the advantages at www.komsoftware.com.

Request a live demo to see how KOMpliance can secure your data.



Phone: +1.613.599.7205

+1.888.556.6462

Email: sales@komsoftware.com

Website: www.komsoftware.com

150 Katimavik Road, Suite # 1000, Ottawa, Ontario, Canada K2L 2N2