VERITAS

Ransomware Protection, Security and Resiliency for Business-Critical Applications

White Paper | January 2024

Executive Summary

The threat of malware infiltration and ransomware attacks is a top concern for businesses of all types and sizes. The impact of application downtime for business-critical applications is substantial, and often has a significant effect on an organization's revenue stream and reputation. This has driven the need for robust and enterprise-focused solutions to help secure data and protect IT services against ransomware attacks and other events that can result in unplanned downtime. A multi-layered cyber resiliency strategy is the best approach to help ensure that your IT services continue to be secure, resilient, and recoverable, while providing the smooth and consistent user experience that your end users expect.

Veritas InfoScale™ is a proven solution for managing availability and resiliency for business-critical applications. InfoScale has evolved to incorporate advanced security and ransomware protection features designed to reduce the impact of malware infiltration and ransomware attacks, with functionality that makes your data immutable and quickly recoverable. InfoScale helps you deliver comprehensive multi-layered cybersecurity, with several key benefits:

- **Protection:** InfoScale's secure file system provides several advanced features, including the ability to make your data immutable, and assistance with quick recovery of primary data in the event of a ransomware attack or data corruption.
- **Security:** Protect your data against unauthorized access and exfiltration. Integrated data isolation functionality helps prevent malware infiltration, and enables you to quickly recover applications.
- **Resiliency:** InfoScale automates application availability and advanced disaster recovery, and can help ensure zero data loss and near-zero recovery times. As a platform-agnostic solution, InfoScale enables you to run applications in any type of environment, including cloud, hybrid cloud, and multi-cloud architectures.

This white paper will provide an overview of how InfoScale can provide security and resiliency for your business-critical applications. By integrating data security and application resiliency into a single comprehensive solution, InfoScale helps protect your applications against any type of disruption, including widespread site outages and ransomware attacks.

Solution Value

As a proven market leader in application high availability, InfoScale is a proven multi-faceted solution that delivers extensive functionality to enhance security, availability, and resiliency for business-critical applications as a single software-defined solution.

InfoScale delivers integrated security and application resiliency to protect your business-critical IT services against ransomware attacks and unplanned downtime.

InfoScale helps ensure your IT services are secure, resilient, and delivering a smooth and predictable end user experience by providing a full spectrum of functionality, including:

- **Ransomware protection:** InfoScale's secure file system feature (SecureFS) enables data immutability for applications by automating the creation of write once, read many (WORM) files and checkpoints that cannot be modified. Checkpoints can be used to recover your applications very quickly in the event of a ransomware attack.
- **Encryption:** Volume and file-level encryption ensures that your data is protected against unauthorized data access, and limits the risk of data being exposed due to exfiltration.
- **Data isolation:** Space-optimized snapshots can be easily provisioned in an area isolated from traffic, to reduce your exposure to malware. Snapshots can be easily recovered using integrated storage management functionality that quickly resynchronizes primary data volumes using the isolated snapshots.

- **Resiliency:** InfoScale supports several advanced high availability and disaster recovery topologies that help keep your business-critical applications highly available and protected against unplanned downtime.

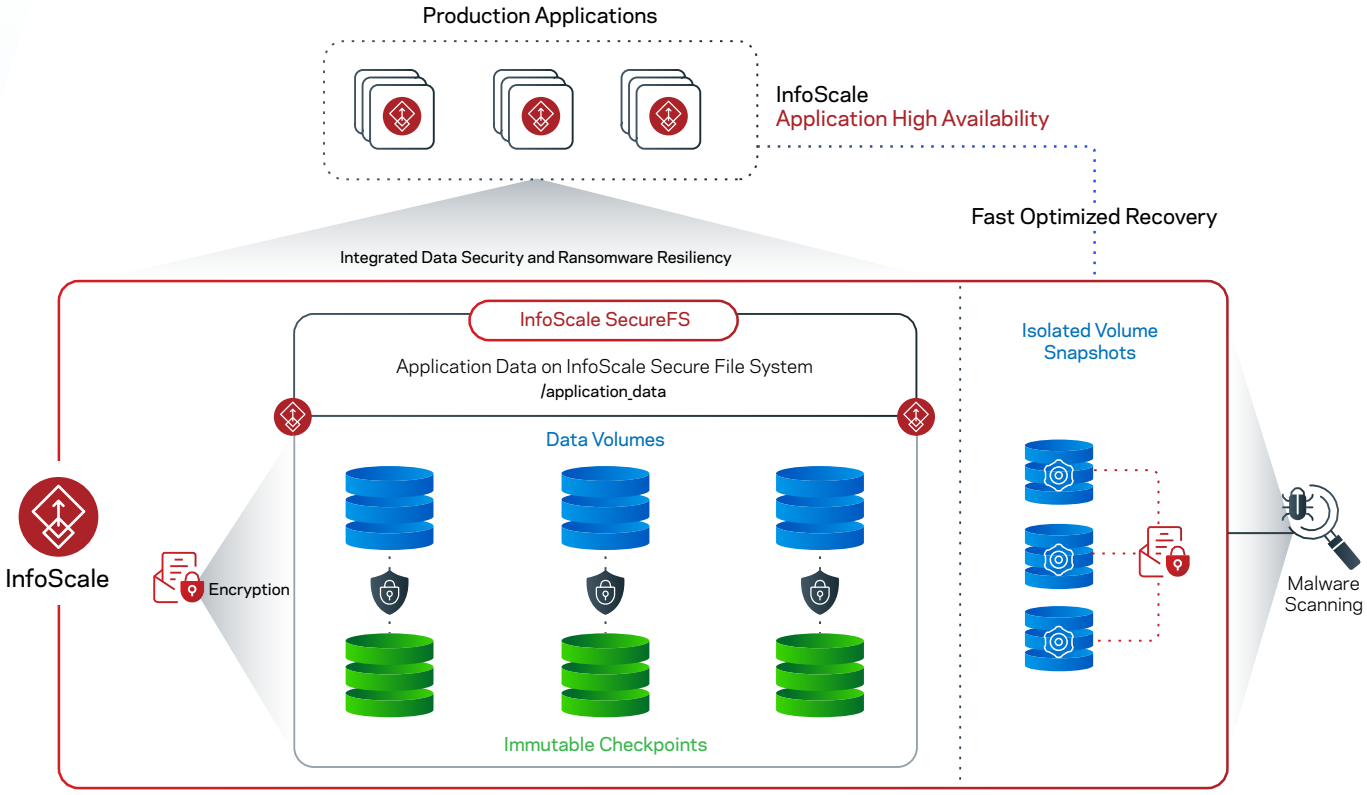

Figure 1. InfoScale security features minimize the impact of malware infiltration and ransomware attacks

Solution Components

InfoScale is a multi-faceted platform for business-critical applications. There are multiple components that work together to provide security and application availability as a single solution:

- **Veritas File System (vxfs):** An extent-based POSIX compliant journaling file system capable of managing large volumes of data, designed to provide high performance and availability for applications. vxfs is fully supported in on-premises deployments and in the cloud, and has several advanced features that provide security, performance, and resiliency benefits for applications. The SecureFS feature of vxfs allows you to seamlessly create immutable data checkpoints so you can quickly recover from ransomware attacks.
- **Veritas Volume Manager (vxvm):** A storage management utility that manages physical disks as logical data volumes that are presented to an operating system as a storage device on which you can create file systems. vxvm volumes can be encrypted to help protect your applications against unauthorized access and data exfiltration.
- **Cluster File System (CFS):** On-premises and cloud-native multi-access block storage services depend on a cluster file system to support parallel access to data by multiple systems. CFS is a feature of the Veritas File System (vxfs) that provides highly available and secure parallel access for applications.
- **Veritas InfoScale Operations Manager (VIOM):** VIOM is a platform and vendor-agnostic centralized management console for InfoScale that also provides some visibility into other third-party infrastructure. Using VIOM, you can easily configure ransomware resiliency and corruption protection for your business-critical applications in an intuitive web-based interface. VIOM can also be used for monitoring, visualization, and management of system and storage resources. It also includes a reporting engine that can help identify issues that may reduce application high availability and disaster recovery readiness.

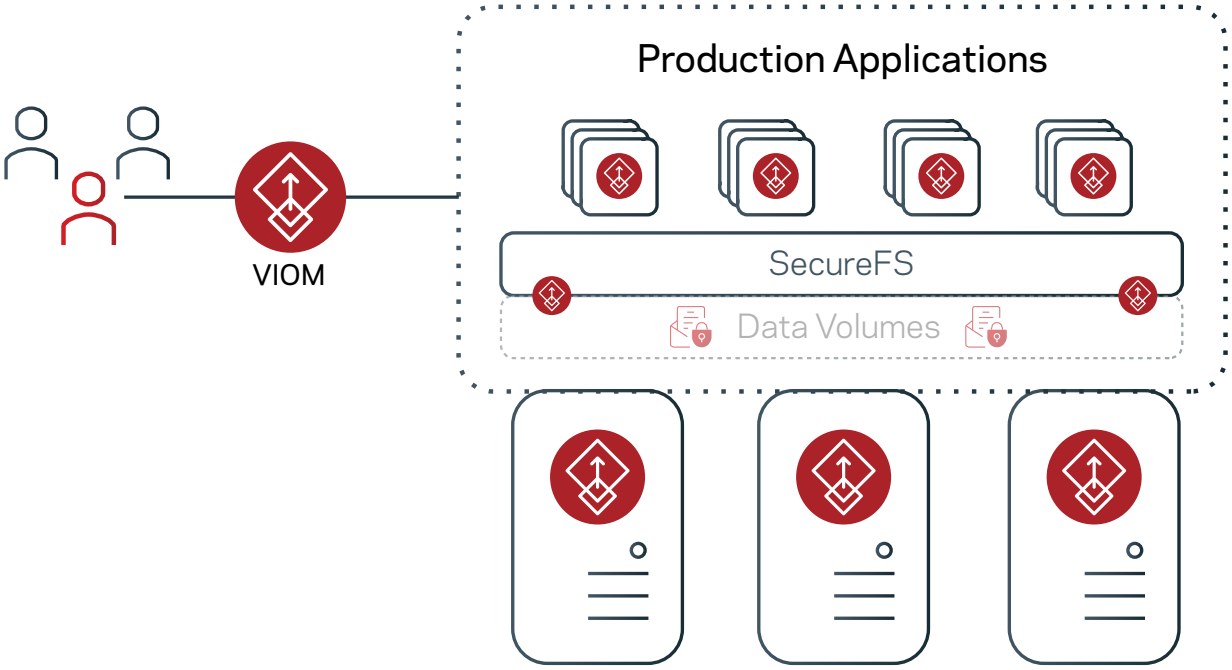

Figure 2. Easily manage InfoScale ransomware resiliency and data security features using VIOM

Ransomware Protection and Security

Malware and data corruption are common factors that can lead to unplanned downtime and other scenarios that can negatively affect your IT services. Protecting your applications from these threats requires a solution designed for enterprise workloads that natively provides data immutability, encryption, and data isolation functionality for your applications without compromising performance and usability. InfoScale offers file system security and snapshot management designed to protect your applications against ransomware attacks and data corruption, as well as volume encryption that ensures your data is protected against unauthorized access. InfoScale also provides the functionality you need to deploy your applications and IT services in highly resilient architectures that can further protect your applications against system outages.

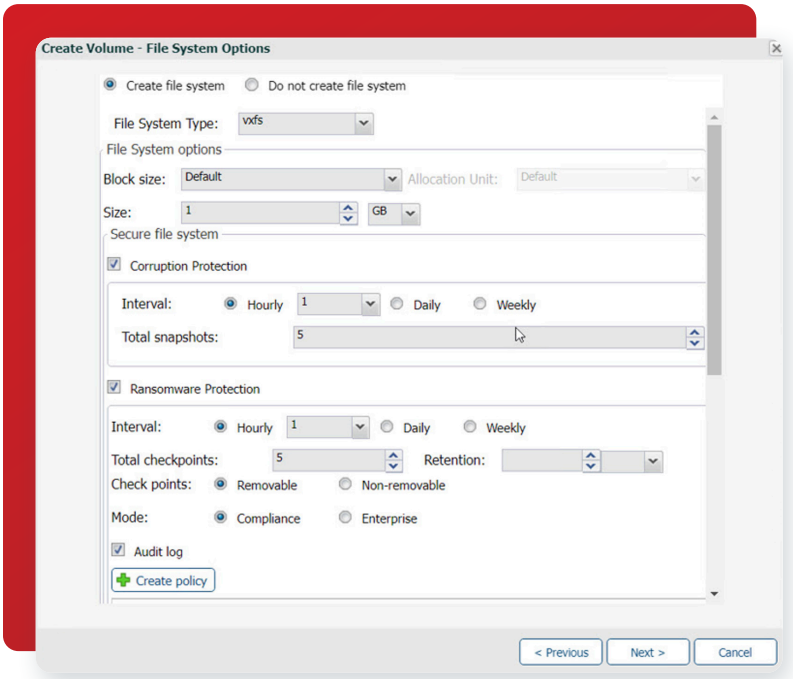

Figure 3. InfoScale's SecureFS is easily configurable, with several options that provide comprehensive protection

File System Immutability

InfoScale's secure file system (SecureFS) allows you to designate files and file system checkpoints as immutable. SecureFS provides WORM functionality that ensures that files and file system checkpoints can only be read but not modified or deleted for a given retention period. After the retention period has expired, the file can then be modified or deleted. There is also a less restrictive WORM option—compliance mode (also known as SoftWORM)—where the root user is given the ability to reduce retention times on files or checkpoints. Running your applications and databases on InfoScale SecureFS will give you better protection against ransomware attacks, with an easy to use solution that requires minimal overhead.

InfoScale's secure file and checkpoint option is a space-efficient, quick, and easy-to-use solution to protect your primary data against ransomware attacks. Immutable checkpoints are created automatically and can be rolled back very quickly to reduce downtime in the event of malware infiltration. Some of the key benefits include:

- **Immutable checkpoints:** Optimized and easy to create, file system checkpoints can be designated as non-modifiable to protect primary data against ransomware attacks. Checkpoints can be rolled back very quickly to provide fast restores of production data when needed.
- **Audit logging:** Ensures there is a proper record of events related to unauthorized modifications within the file system.
- **Data resiliency:** Provides support for file- or volume-level recovery, as well as application/database-level recovery.

The secure file system functionality is customizable, which gives you the flexibility to design templates specifically for different applications and workloads.

InfoScale also provides integrated snapshot management designed to ensure your data is recoverable in the event of system failures and other events that may result in data loss. The snapshot management feature is similar to the ransomware resiliency feature, however the snapshots are not immutable. The optimized snapshots are stored on an alternate storage device that is separate from the primary file system, to reduce the impact of primary system failures.

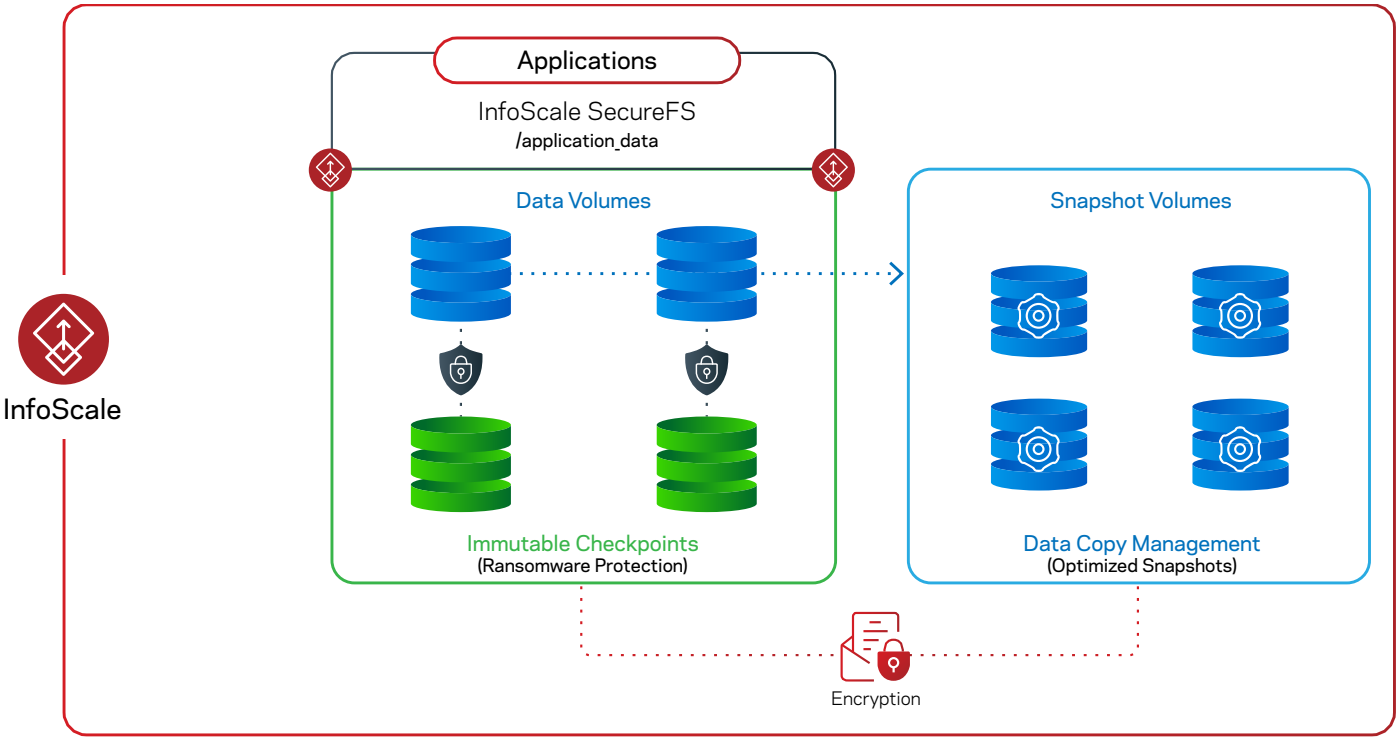

Figure 4. InfoScale protects your applications from ransomware attacks and other forms of data corruption

The InfoScale secure file system feature includes lockdown modes that provide different levels of security:

- **Compliance Mode:** Allows you to set and extend retention periods. In compliance mode, authorized users can reduce or remove a retention period but cannot modify the files or checkpoints. This provides flexibility, as you do not have to wait for the retention period to expire in order to modify data.
- **Enterprise mode:** A more strict option, where you can set or extend the retention period, but you are not allowed to reduce or remove the retention period. To modify data, you must wait for the retention period to expire, then delete and re-create checkpoints or snapshots. This provides maximum data protection.

InfoScale also gives you the flexibility to integrate custom scripts into the data management process to provide additional functionality and data services for your applications. InfoScale volumes and checkpoints can be scanned by a third-party anti-malware solution to ensure there is no known ransomware present, and to remove any threats if ransomware is identified.

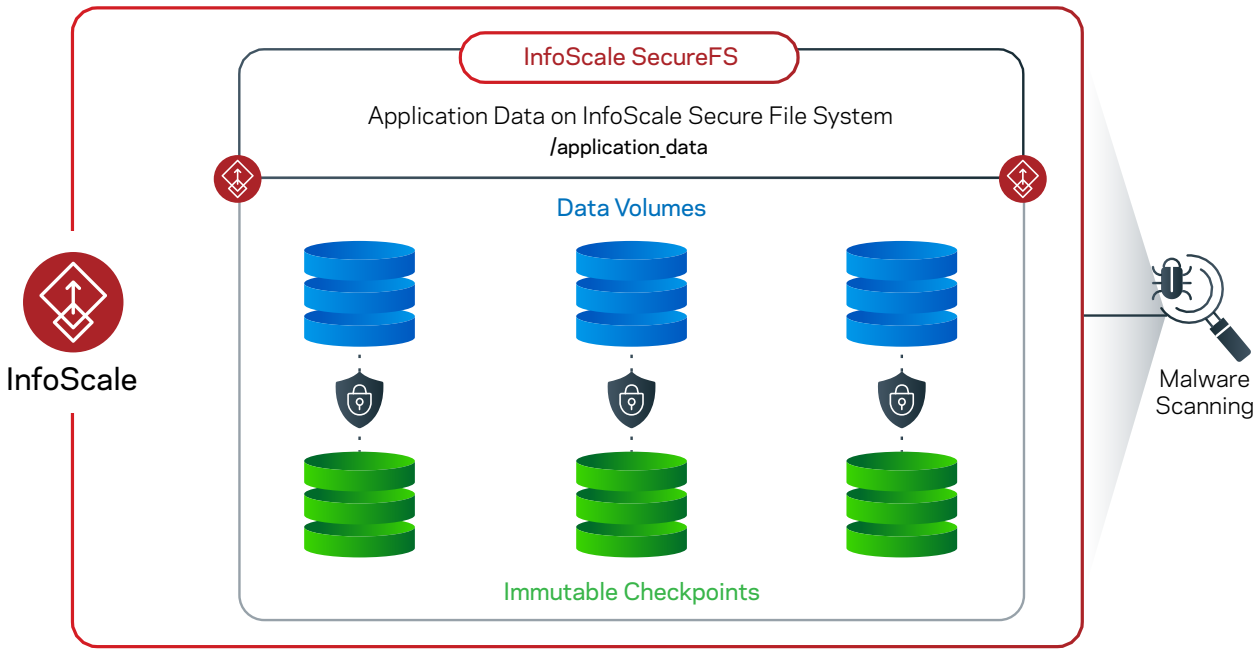

Figure 5. InfoScale's SecureFS operates in parallel with software designed to identify and remove ransomware

Secure Boot

Today's systems have the ability to run many types of software at scale, and it has become increasingly important to ensure that the software you use to support business operations is secure and trusted. Secure Boot functionality is a very reliable way to ensure that the software running on your systems is secure, by verifying software signatures and preventing malicious software from loading when your system starts (boots).

InfoScale fully supports the Secure Boot process for Unified Extensible Firmware Interface (UEFI) systems. InfoScale public keys can be generated online using the Veritas Services and Operations Readiness Tools (SORT) website, and can then be enrolled with your system's UEFI key management function. Once your key is enrolled, the InfoScale software will be loaded with the signed key when your system starts with Secure Boot enabled.

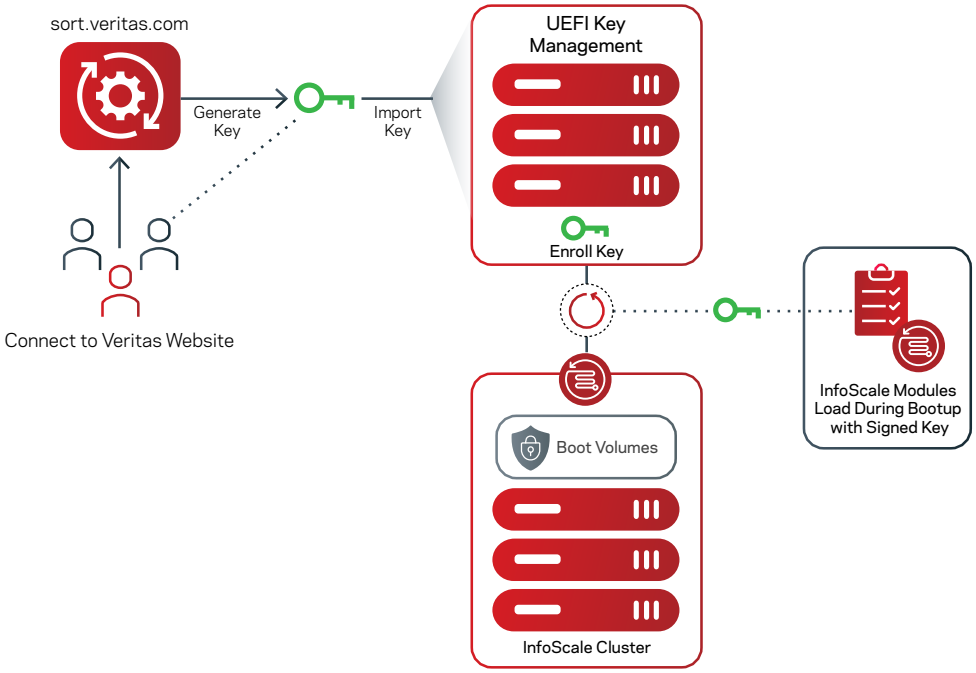

Figure 6. InfoScale supports the secure boot process on UEFI systems

Secure Clock

While secure files and file system checkpoints ensure that your data is secure and unchangeable, it is equally important to manage data retention settings to eliminate attempts at expiring data and subverting immutability. InfoScale's secure clock ensures that there is a method of keeping track of time on your systems that guarantees the filesystem's retention periods cannot be subverted. If a secure clock mechanism were not present, it is possible that a retention period could be expired by simply changing the system clock to some point in the future.

The InfoScale secure clock involves recording the system time to a file at the system level of the filesystem. This mechanism guarantees that ransomware cannot subvert the secure clock by manipulating the system time.

Data Isolation

InfoScale can be deployed in a way that provides isolation for production data by mirroring data volumes and isolating them from new I/O—where an anti-malware engine can be used to find and eliminate ransomware.

InfoScale's volume mirroring and optimized snapshots can be accessed independently of the volumes from which they were taken. By creating a volume mirror and detaching the mirror as a new snapshot volume, this effectively isolates a copy of your primary data from new I/O. At this point, you can automate the process of running an anti-malware scanning engine to scan the new snapshot volume, which will detect and eliminate ransomware. Once the snapshot is validated as safe by the anti-malware engine, you can use InfoScale's FastResync option to quickly reassociate the snapshot plex with its original volume in an optimized manner, where only changed data is synchronized. This gives you a fast and reliable way to protect your production databases from ransomware attacks, with a very low recovery point objective (RPO).

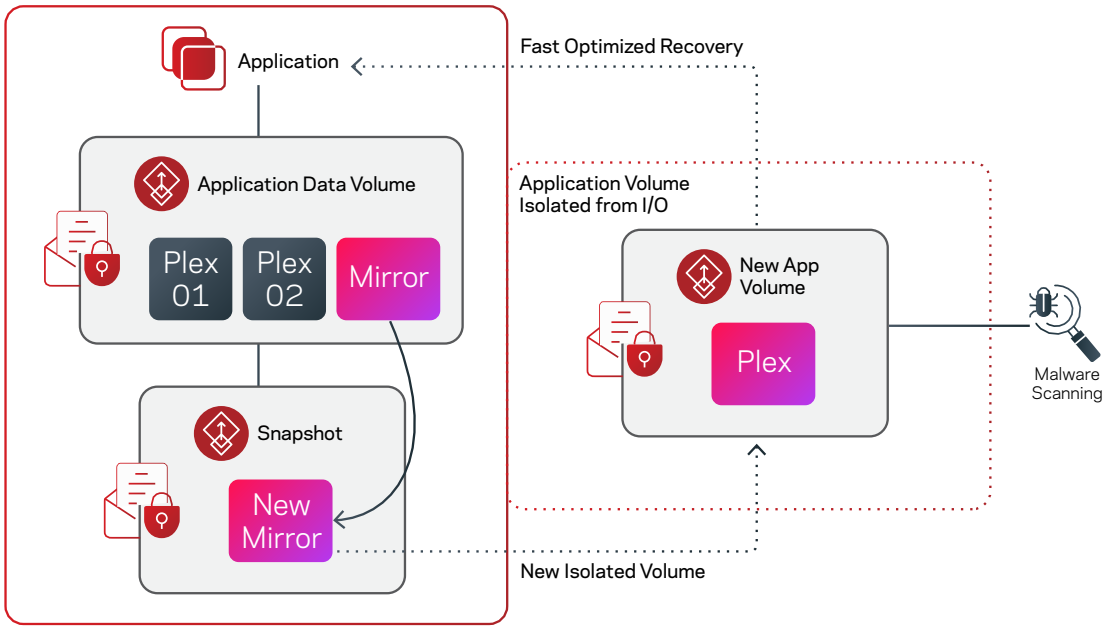

Figure 7. Data isolation with encrypted volumes

Data Encryption

All InfoScale volumes on Linux and Windows systems can be encrypted, which gives you an added layer of security that protects your data against unauthorized access. InfoScale uses AES 256-bit symmetric key encryption and is FIPS 140-2 compliant. Encryption can be enabled automatically when volumes are created to ensure that all I/O going to and from InfoScale volumes is encrypted. If an attacker gains access to your system credentials and is able to create snapshots or make unauthorized copies of your data, InfoScale volume encryption protects you against unauthorized data access and data exfiltration by ensuring that your data is inaccessible to the attackers.

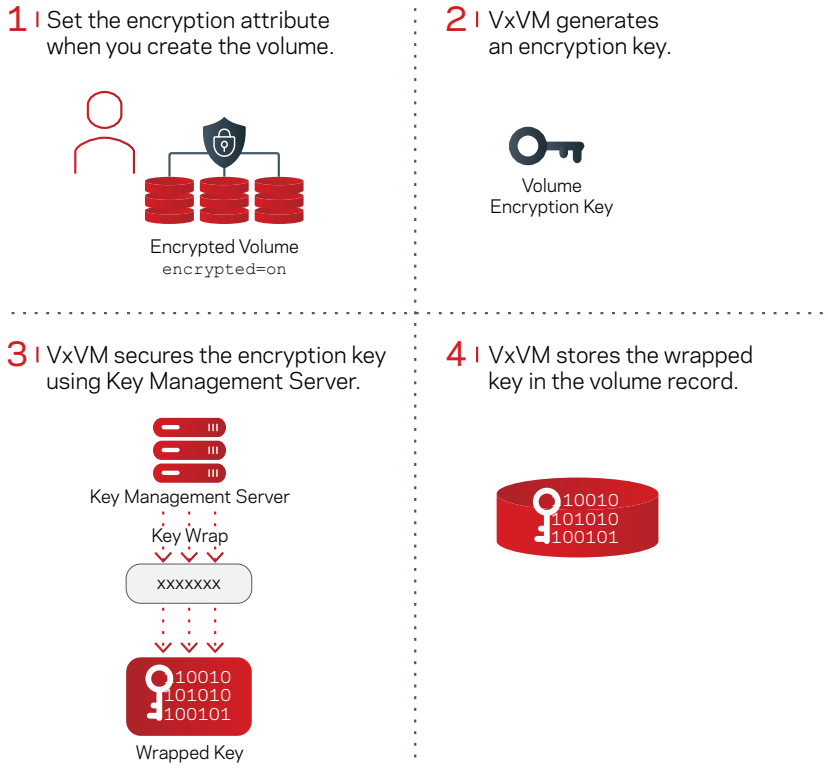

Figure 8. InfoScale volume encryption can be easily configured to help secure your data

Application Resiliency

Unplanned application downtime always has a negative impact on your business, regardless of the cause of the downtime. While protecting your applications against malware infiltration and corruption is a key requirement for avoiding unplanned downtime, there are several other factors that need to be considered and managed to ensure the highest levels of availability and resiliency for business-critical applications. To fully protect your applications against unplanned downtime, you also need a robust solution in place to protect your IT services against outages resulting from other causes such as natural disasters and system failures. InfoScale is a proven solution for managing application-aware high availability and disaster recovery This can be implemented while leveraging InfoScale's ransomware protection and snapshot management features.

Resiliency and Disaster Recovery

Ensuring that your applications are resilient and recoverable with no data loss and minimal downtime is a key requirement for many business-critical applications. While some applications provide a certain degree of native functionality for backup, recovery, and resiliency, achieving zero data loss over any distance, and a near-zero RTO while remaining platform agnostic requires an advanced solution designed for operational flexibility and resiliency.

InfoScale can support zero data loss for business-critical applications using what's known as a bunker configuration (shown in Figure 9). This configuration incorporates a bunker site into a standard primary/DR configuration, which is used to store logs that are synchronously replicated from the primary site. This configuration does not require synchronous replication between the primary and DR sites, which is difficult to achieve and limits your options for geographic distribution of your applications to protect against localized outages. InfoScale delivers geographically dispersed resiliency for applications with zero data loss over any distance, and automated failover that enables near-zero recovery times.

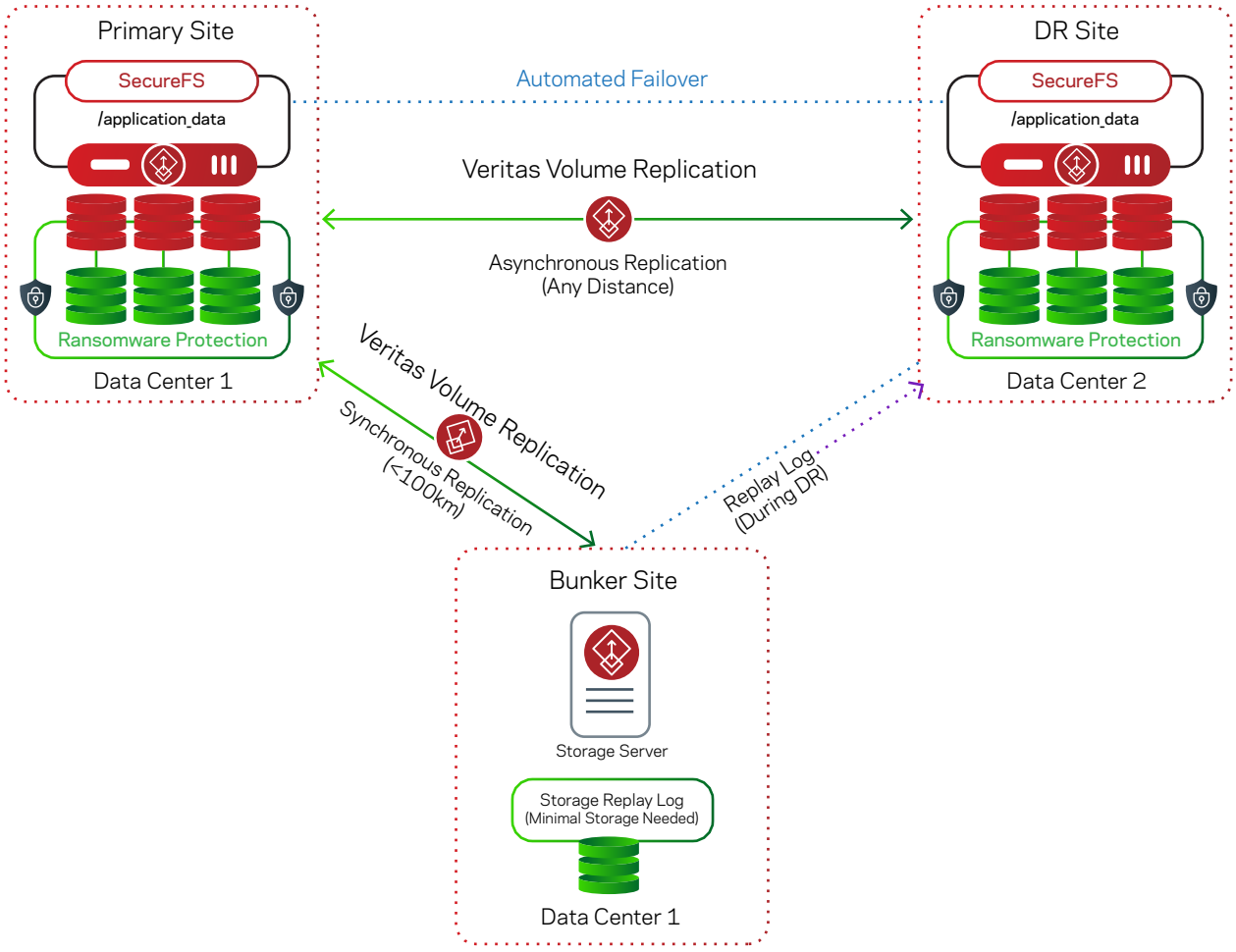

Figure 9. InfoScale advanced disaster recovery and resiliency can provide zero RPO and near-zero RTO for business-critical applications

InfoScale high availability and disaster recovery topologies—including the highly resilient bunker topology shown in Figure 9—can be implemented while using InfoScale's security and ransomware resiliency features such as volume encryption and SecureFS. This gives you protection against malware, as well as the application resiliency your business-critical applications need to be protected against local and widespread system and service outages.

Ensuring Data Integrity

When multiple systems/nodes have access to data via shared storage, the integrity of the data depends on internode communication, ensuring that each node is aware when other nodes are writing data. When the coordination between the nodes fails, it results in a split-brain condition—a situation in which two servers try to independently control the storage, potentially resulting in application failure or even corruption of critical data, which can then require days to recover.

InfoScale's integrated I/O fencing solution ensures data integrity by preventing data corruption. Without I/O fencing, it is not possible to determine which node(s) is/are valid members of the cluster, and subsequent write operations will compromise data integrity. I/O fencing

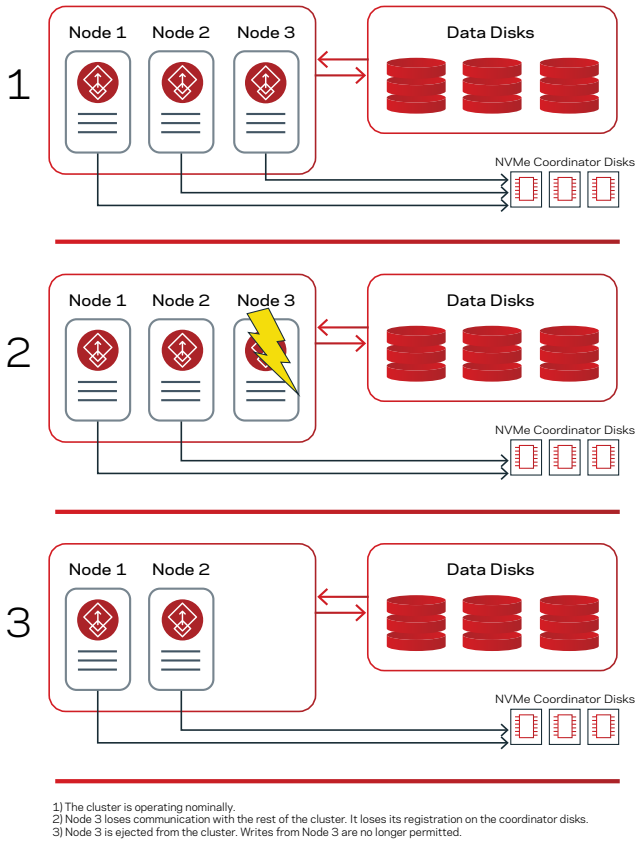

Figure 10. InfoScale I/O fencing ensures data integrity

ensures that errant nodes are fenced and do not have access to the shared storage, while the eligible node(s) continue(s) to have access to the data, virtually eliminating the risk of data corruption.

Fencing is done using industry-standard SCSI-3 persistent group reservation technology, as well as other non-SCSI-3 fencing technology. In public cloud environments where SCSI-3 persistent group reservation compatible disks are not available, I/O fencing is configured using NVMe devices or coordination point servers. Fencing in the public cloud using NVMe disks is a simple yet highly reliable solution for ensuring data integrity. InfoScale fencing with NVMe disks also adds an additional layer of security for your data, as you can block access to the disks to prevent unauthorized access, and you can also prevent disks from being attached to other compute instances without proper authority.

Conclusion

Ensuring that your IT services deliver a premier user experience and are protected from malware and unplanned downtime is always top of mind. InfoScale is a proven enterprise platform that provides ransomware protection, security, and resiliency for your applications, while maintaining a smooth and seamless end user experience. This secure and resilient foundation for your applications also improves operational flexibility by enabling you to operate anywhere—including in cloud, hybrid-cloud, and multi-cloud environments. With InfoScale, your business-critical IT services will be:

- ✓ **Protected:** Primary data immutability that is optimized for fast recovery helps protect your applications against ransomware attacks and data corruption, without sacrificing performance.
- ✓ **Secured:** Primary data encryption and isolation helps further protect your applications against malware infiltration and unauthorized access.
- ✓ **Resilient:** By integrating security with resiliency, InfoScale ensures that your applications are secure and highly resilient, with zero data loss and near-zero recovery time resiliency architectures that can be configured in any environment.

InfoScale is a comprehensive, multi-faceted solution with a proven track record of improving security, availability, and operations for business-critical applications. By delivering a complete solution that helps you ensure application security and resiliency, InfoScale is a key component in a multi-layered cybersecurity strategy and is the ideal foundation for running your business-critical applications with maximum confidence.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1986 01/24