VERITAS

The Veritas Ransomware Resiliency Strategy

Solution overview.

White Paper | April 2022

Contents

Executive Summary

The threat of ransomware attacks is a top concern for businesses of all types and sizes. Ransomware attacks have become commonplace with cybercriminals continuously evolving and creating new, more sophisticated ways to deliver attacks. With demands becoming excessive and the risk of data loss increasing, an advanced multi-layered resiliency strategy is needed to help ensure that your IT services are secure, resilient, and recoverable while providing the smooth user experience that your end users expect.

Veritas provides enterprise IT solutions that ensure your IT applications are protected and resilient. As one of the industry's most comprehensive ransomware resiliency platforms, Veritas offers integrated protection, detection, and recovery features to help ensure business continuity and provide the confidence that your business can successfully defend against and recover from a broad range of threat vectors, including ransomware. With business resiliency as a key focus, Veritas delivers a unique data management strategy based on proven technology that can operate at scale. Some of the key functionality includes:

- Protection for your data using secure, efficient appliances and advanced functionality that provides a wide range of recovery options – with immutable and indelible infrastructure that protects your backup data from ransomware attacks
- Integrated intelligence and analytics that can detect ransomware and anomalous behavior and provide comprehensive, holistic insights into the status of your systems
- Resiliency for your IT services with application awareness that can provide data storage immutability with advanced functionality to protect your applications and data against ransomware attacks and significantly reduce recovery times

This solution overview will discuss the Veritas ransomware resiliency strategy and how to integrate Veritas solutions into a broad multi-layered cybersecurity strategy to protect against malware. Veritas offers a unique integrated solution that ensures your IT services are protected and resilient with the intelligence you need to successfully recover from and minimize the threat of malware infiltration and ransomware attacks.

Solution Value

Veritas provides a holistic strategy for ransomware resiliency designed to provide enterprise-grade storage, data protection and application availability for your IT services. Veritas enables a multi-layered foundation that provides protection, detection, and recovery capability for both your production applications and backup systems. This unique integrated approach to ransomware resiliency has several key advantages:

- ✔ **Secure data protection** – advanced protection for your applications with anomaly detection and secure turn-key appliances designed with integrated immutability, indelibility, and operational efficiency
- ✔ **Improved IT service availability** – ensure business continuity and high availability for any application with several options for faster recovery and automated event-based system process management
- ✔ **Operational intelligence** – holistic insights with ransomware-focused dashboards and heuristics for both production data and backup data footprints ensure that you have visibility into potential threats in real-time

With integration between InfoScale, NetBackup and Data Insight, Veritas delivers a comprehensive ransomware resiliency strategy to meet nearly any Recovery Point Objective (RPO) or Recovery Time Objective (RTO). Figure 1 shows an overview of the Veritas ransomware resiliency strategy and how Veritas enables you to protect your data, detect ransomware and restore your applications and IT services in nearly any environment.

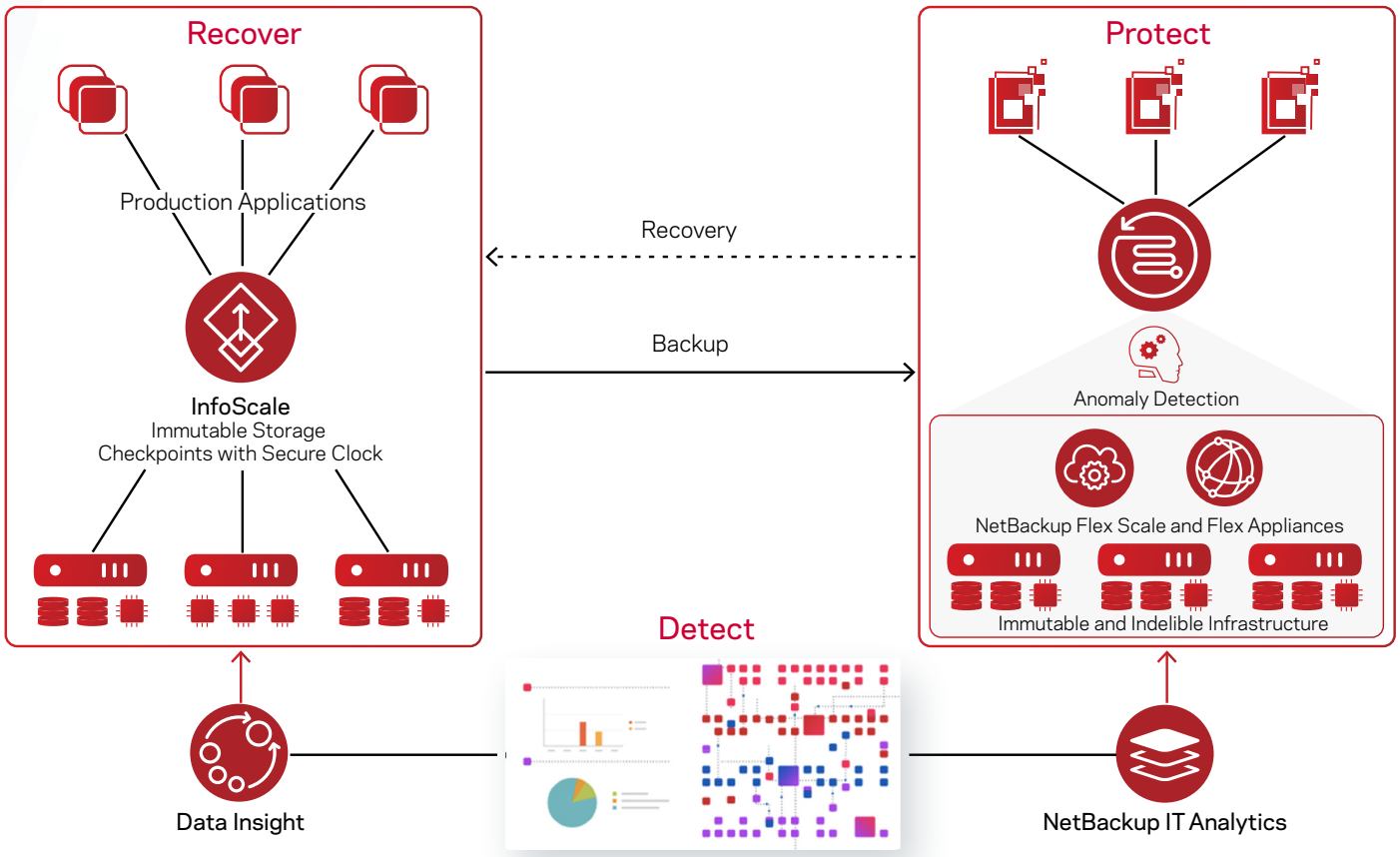

Figure 1. Veritas ransomware resiliency strategy overview

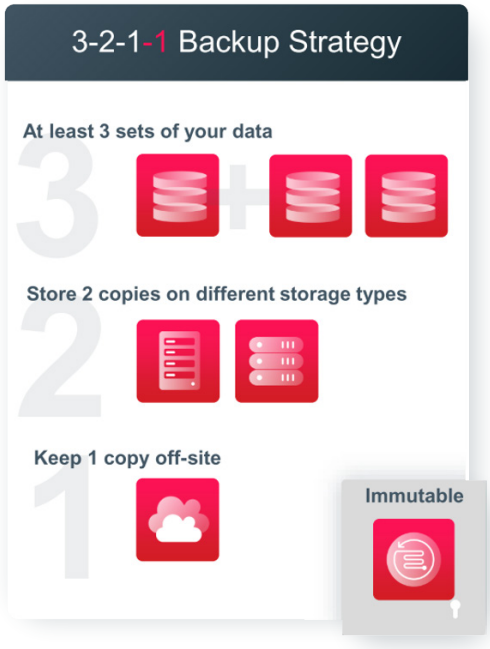

Figure 2. How to implement an effective 3-2-1-1 backup strategy

Protect

Veritas NetBackup is a proven solution to manage data protection for nearly any type of IT application or service. With a strong focus on data integrity to help ensure backup data remains safe and untouched from malicious invaders, NetBackup includes several features and functionality designed to ensure the integrity of your backup data.

Having multiple copies of your data can significantly reduce the impact of data corruption as well as the likelihood of data loss due to malware infiltration and ransomware attacks. Veritas recommends adopting the "3-2-1-1" approach for backing up data, which involves keeping three copies of data on two different media types, with one off-site and at least one copy on immutable and indelible storage. NetBackup can efficiently manage the 3-2-1-1 backup process across different platforms – including cloud and containers – to reduce the risk of data loss and infection by ransomware.

NetBackup has several features designed to combat ransomware while maintaining the scalability and functionality needed to accommodate any enterprise data protection requirement:

- Flexible vendor-agnostic architecture with integrated 3rd party malware scanning that can accommodate a 3-2-1-1 backup strategy with standard support for immutable, indelible, and air-gapped storage
- Auto Image Replication (AIR) enables the replication of backup data between backup domains that can be within the same, or different sites – including cloud. AIR also enables offline air-gapped copies of your backups to further reduce the threat of data access by unintended sources
- NetBackup Flex and Flex Scale appliances provide immutable and indelible infrastructure with autonomous operations in a secure and easily manageable hyperconverged platform that reduces your operational overhead and complexity

Veritas provides a comprehensive solution for managing data protection at scale with integrated security and resiliency features designed to protect your data against malware infiltration and ransomware attacks.

Secure Appliances

With security as a cornerstone for our solutions, Veritas has a long-standing history of engineering backup appliances designed to provide the most secure, efficient, and comprehensive data protection with immutable and indelible infrastructure that safeguards your data against ransomware. NetBackup appliances are built using the following design principles:

- Security and resiliency – NetBackup appliances are designed with a zero-trust architecture and multiple layers of security that limits the ability for malware to alter system configurations or data. Infrastructure resiliency with clustered storage helps ensure there is nearly zero risk of data loss while maximizing storage efficiency and reducing costs
- Operational simplicity – streamline management with orchestrated automation of operations, reducing operational risk and your overall management costs. Manage multiple appliances and multi-site backup operations from a single web-based console
- Flexibility – protect any type of workload efficiently and easily scale as your environment grows. Optimize and manage backup data as part of an overall lifecycle to further improve data security and resiliency across multiple platforms – including air gapped backup targets such as Flex Appliance immutable storage, immutable cloud storage and tape

Protecting your backup data and infrastructure is essential for ransomware resiliency. Veritas Flex and Flex Scale appliances are operationally efficient and provide the most secure way to protect your backup data. They are purpose built for NetBackup with integrated functionality that helps combat the threat of ransomware:

- Zero-trust architecture – appliances have integrated role-based access controls and specially designed lockdown features that provide a higher level of security to protect both backup data and the storage infrastructure
- Data Immutability – ensures data cannot be changed for a determined length of time to protect data against cybercriminal intrusion and internal threats. To further improve security, the backup storage is on a secure data store that is only visible and accessible to the NetBackup storage service, eliminating users and filesystem services from accessing it
- Hyperconverged system – the all-in-1 operational model significantly reduces overhead and is a more secure platform that better protects your data against malware infiltration and ransomware attacks. All components – the OS, drivers, firmware, and software – have been optimized to provide enhanced security at initial deployment and with all system updates

Flex Appliance

The Veritas NetBackup Flex Appliance is an innovative approach to data protection infrastructure modernization that allows you to configure multiple NetBackup primary, media, immutable and optimized cloud storage instances on a single hardware platform. Each NetBackup instance runs in a container and shares the hardware resources available within the Flex appliance. The NetBackup instance configuration can be easily tuned to manage various performance requirements for any workload, while still providing the scalability and advanced data protection features – such as NetBackup optimized duplications and AIR – needed to protect your data from ransomware.

Data security and integrity for the Flex appliance is provided seamlessly with support for several features that help ensure your backup data is secure and less susceptible to malware infiltration and ransomware attacks. Flex appliances are designed with data security and immutability in mind:

- **Immutability and indelibility** – Flex appliances provide a completely immutable and indelible storage solution that prevents your data from being changed for a determined length of time. Flex appliances use a secure compliance clock independent from the operating system time to manage retention periods. Flex appliance immutable storage can also be used as an air-gapped target for NetBackup clients as part of a 3-2-1-1 backup strategy
- **Lock down modes** – can be enabled at any time to create immutable storage instances within the Flex appliance. Appliances hosting immutable storage can move into a heightened level of security to protect both data and infrastructure. Administrators are prevented from making changes to the OS and internal components, all endpoints are secured from unauthorized access, and access to all services is protected and authenticated
- **Platform security** – with a zero-trust security model, Flex appliances have operating system security hardening with a secure hardened Veritas file system. Flex Appliance is a proven platform for secure data protection that also includes internal component logical isolation, role-based authentication and integrated IDS/IPS to further improve platform and data security

Figure 3 shows an example of how the NetBackup Flex appliance is deployed with a choice of integrated immutable storage that keeps your data safe from ransomware attacks. For additional information on Flex appliance security, please refer to the whitepaper in this link.

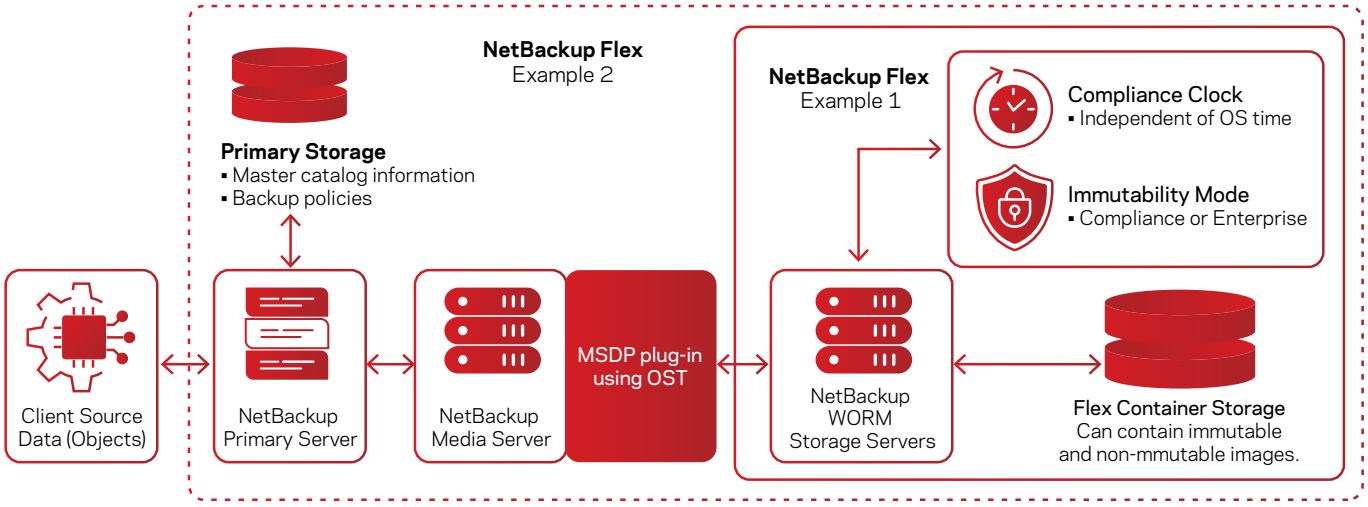

Figure 3. Example of a NetBackup Flex deployment with integrated security and data immutability

NetBackup Flex Scale

NetBackup Flex Scale is a modern hyperconverged data protection platform that provides enterprise scalability and usability and can be easily customized. The NetBackup Flex Scale architecture was designed with security as one of the primary objectives. It was built using containers to provide service isolation, a hardened OS, and a Zero Trust security model. NetBackup Flex Scale takes an in-depth and multi-level approach to preventing any unauthorized access to system data or unauthorized use of system resources, including mandatory access control, limiting (or removing) root access to users and services, secure communication, and enhanced security to the data infrastructure.

NetBackup Flex Scale includes several features to ensure the security and integrity of both the system and backup data:

- **Hardened system** – the full NetBackup Flex Scale appliances stack has been hardened for security, including the Linux operating system, management access, application binaries and configuration settings. It includes proprietary security policies that conform with STIG guidelines as well as enforcing mandatory access control. It also includes intrusion detection and protection services that restricts access to processes and resources and maintains an audit trail of important user and system actions
- **Write-Once Read Many (WORM) storage** – NetBackup Flex Scale includes WORM storage which provides immutable and indelible data protection, ensuring data cannot be modified, corrupted, or encrypted after backup for the length of time set within the backup policy. The retention is determined by a cluster-based immutable compliance clock/timer that is independent of OS time and NTP
- **Container Isolation** – the containerized architecture adds an additional layer of security by providing isolation between NetBackup services as well as internal software firewalls that block unauthorized traffic and ensure that there is no visibility between namespaces

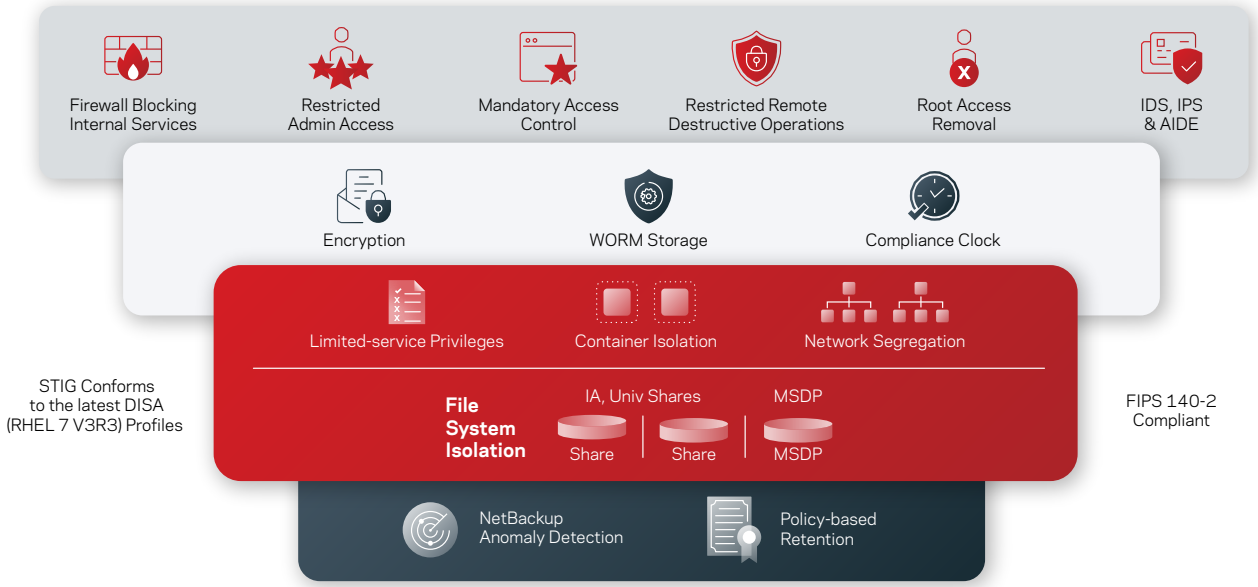

Figure 4. NetBackup Flex Scale's zero-trust model provides multiple layers of protection from ransomware attacks

With a flexible scale-out architecture and focus on data security, NetBackup Flex Scale gives you enterprise data protection capability that can operate at scale, while effectively protecting your data against ransomware attacks. For an operational view of NetBackup Flex Scale's secure design and ransomware protection functionality, please refer to the whitepaper in this link.

Primary Data Isolation

Veritas InfoScale provides high availability for applications and software-defined storage with advanced functionality designed to help protect against ransomware infections. In addition to immutable file and file system checkpoint capability, InfoScale can also 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 has several advanced storage management features, including volume mirroring and optimized snapshots that 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 the 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 data from ransomware attacks with a very low RPO.

Figure 5 shows how this technique can be used with applications deployed on InfoScale storage.

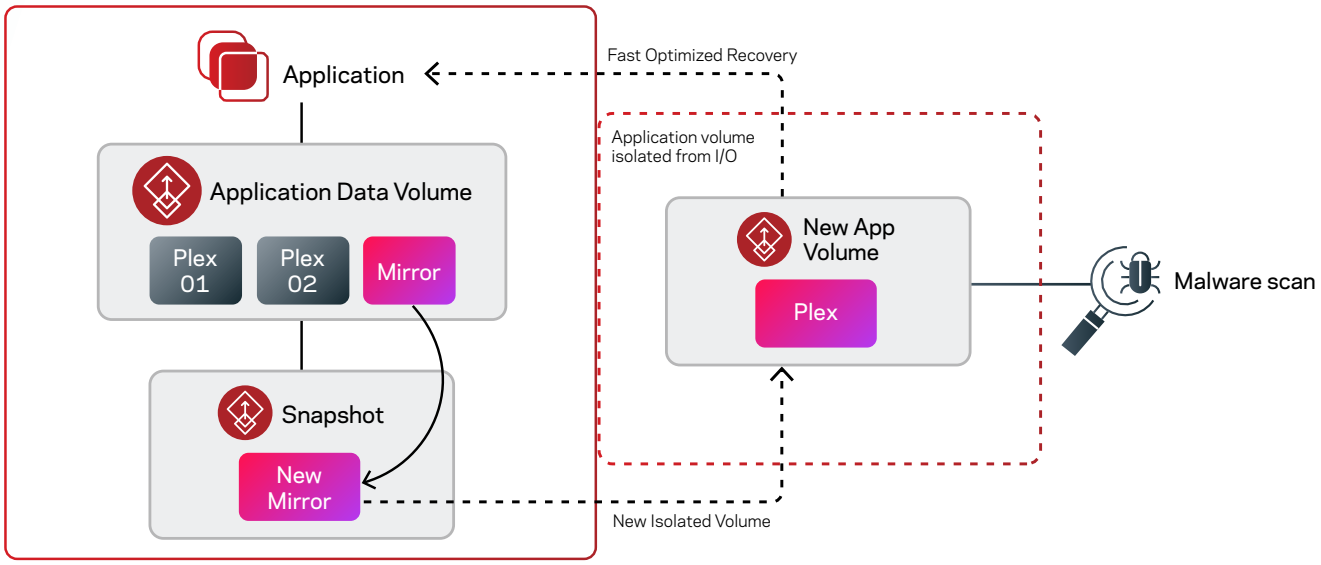

Figure 5. Using InfoScale with a 3rd party malware detection engine

Detect

When it comes to ransomware, having real-time visibility into your data and infrastructure is key. Seconds matter, and understanding what risks and threats are present in your environment in the minimum amount of time allows you to take action to remediate the threat and prevent any data loss or corruption. While it's often very difficult, time consuming and expensive for organizations to create a unified visualization to effectively detect ransomware, Veritas helps make this possible with minimal effort.

Veritas provides operational intelligence and monitoring focused on helping you detect and prevent ransomware from infiltrating your systems. With a focus on both backup data and primary data, Veritas delivers advanced visibility and intelligence that gives you a holistic view of your infrastructure with insights that help combat ransomware.

- **NetBackup IT Analytics** – a single pane of glass solution that provides operational insights and intelligence across cloud, storage, and data protection footprints. NetBackup IT Analytics delivers several dashboards designed specifically to combat ransomware by identifying unprotected systems as well as anomalies with data protection operations
- **Data Insight** – near real-time monitoring of your primary data that can identify the location of known potential ransomware file extensions and automatically take action. Data Insight can detect and alert on malicious or anomalous behavior from user accounts, and it helps in reducing attack surface and minimizing malware damage by discovering over-exposed data – including sensitive data
- **NetBackup** – advanced functionality quickly detects anomalies in the backup process in real-time while backups are running and isolates backups with malware. Integrated malware scanning can be automated based on anomaly detection scores and ensures that your data is safe and free of ransomware prior to recovery

Primary Data Visibility with Data Insight

Protecting your production systems and applications against data corruption and ransomware attacks is a significant concern for businesses today given the need to ensure high availability and resiliency for your IT services. Veritas Data Insight supplements existing malware detection tools by providing an additional layer of security focused on identifying malware and anomalous behavior. Data Insight provides functionality targeted specifically at identifying potential ransomware threats and can monitor and notify administrators when sensitive data access or unexpected user accesses occur.

Data Insight uses advanced behavior and file analytics to identify malware and ransomware attacks in near real time. Some of the key features Data Insight provides to detect ransomware are:

- **Anomalous behavior detection** – understand user activity with anomaly detection policies that have customizable thresholds to quickly identify deviations in behavior in near real time
- **Custom query templates** – out of the box templates for ransomware threat detection and analysis
- **Malware identification** – built in ransomware file group enables reporting on potential ransomware infected files and includes hundreds of known ransomware extensions with the ability to add extensions as they're identified. Integrated optical character recognition can detect ransom notes in files and images, which helps prevent schedule-based attacks when a note is detected prior to the attack

Data Insight enables you to visualize user risk so you can understand which users represent a higher risk of unsafe behavior with the systems and data they interact with. Data Insight creates a baseline of user activity that looks for any anomalies in user account behavior resembling a malware attack. The integrated social networking map combined with user risk analysis makes it possible to visualize and track insider threats with proactive real time alerts, so you can identify risky behavior before it's a problem.

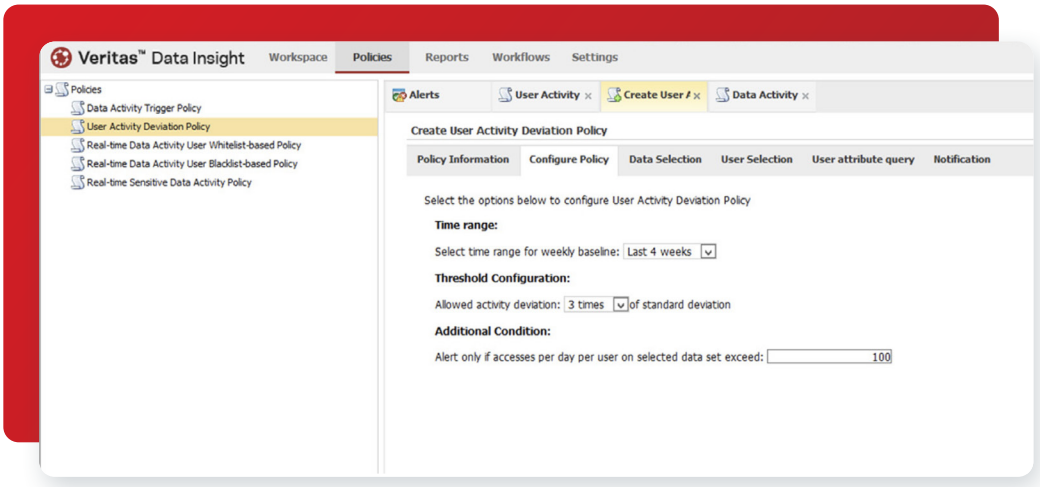

Figure 6. User activity detection policy in Data Insight

InfoScale Integration

Data Insight provides an agent plugin used to monitor access events on Veritas InfoScale file servers. The plugin is included as part of the InfoScale software and is automatically installed on systems using the Veritas File System (VxFS). The plug-in captures events that are then read by Data Insight. This integration with InfoScale provides information on who's using systems managed by InfoScale, as well as information and reporting on file access, permissions and deletes.

Operational Intelligence: NetBackup IT Analytics

Understanding potential ransomware threats and being able to respond quickly is key. Having a holistic view of your infrastructure and data is also of key importance to ensure that all your data is properly protected. This also gives you visibility into areas of potential ransomware exposure. Veritas NetBackup IT Analytics helps you understand the risk factors in your environment in real time so you can take the appropriate actions to prevent or minimize the effect of ransomware – anywhere it may strike.

NetBackup IT Analytics provides a ransomware risk assessment dashboard out of the box. The dashboard gives you a quick view of the preidentified reports that use predictive analytics to understand potential risks within your backup environment. NetBackup IT Analytics helps you ensure that your backup environment is both optimized and secure by providing comprehensive reporting on several data points. This helps you with:

- **Discovery** – track all changes within your backup environment to help detect ransomware and quickly respond. NetBackup IT Analytics includes support for over 850 known ransomware extensions.
- **Visualizing risks** – intuitive graphs give you a historical view of all the risks generated within your environment. Flags hosts that are missing from your backup schedule and visualize applications with failed backups.
- **Backup monitoring** – monitor and identify changes within your backup environment with summary graphs that provide actionable insights. Mitigate risk by identifying anomalies using a baseline of known successful backups

In addition to detecting files with known ransomware extensions, NetBackup IT Analytics allows you to organize this information in a meaningful way so you can execute on a quick plan of action. You can organize the ransomware files detected by hosts, locations with the most ransomware files, types of ransomware extensions and owners of files. Figure 7 shows an example of the NetBackup IT Analytics ransomware assessment dashboard.

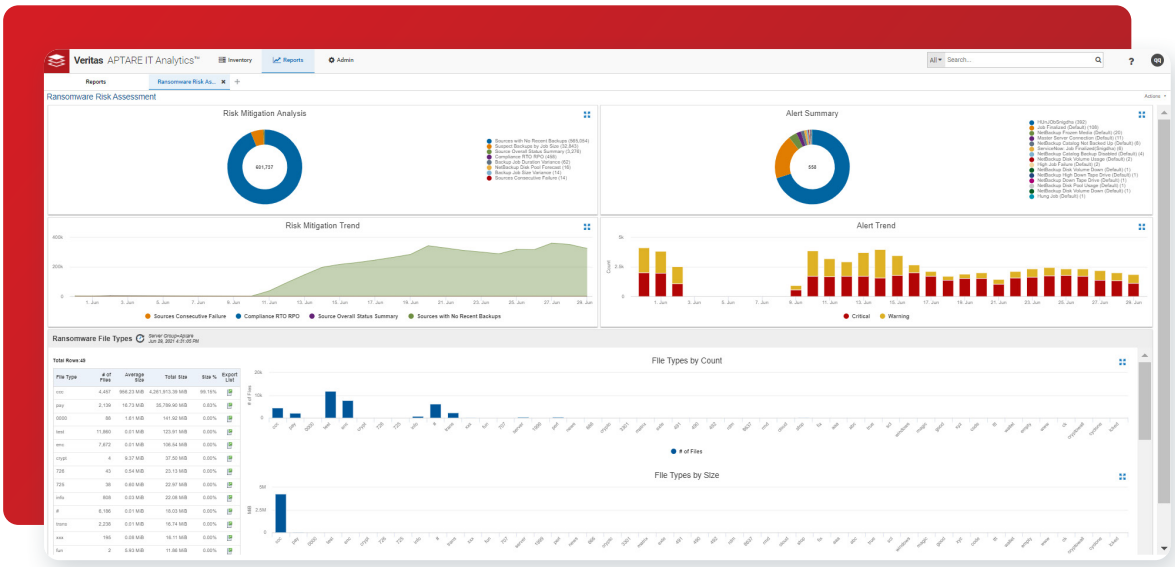

Figure 7. Ransomware assessment dashboard in NetBackup IT Analytics

NetBackup IT Analytics also probes successful backups to identify potential false positives by comparing historical backups against the new backup and identifying anomalies such as significant changes in job durations, image size variations and/or policy configuration changes. This gives you the assurance that your critical IT services are being protected.

Anomaly and Malware Detection

Constantly growing datasets can be difficult to analyze, and this presents unique challenges when it comes to ransomware resiliency. Normal behavior is constantly redefined, and identifying anomalous activity is difficult without an integrated solution that can analyze data as it grows and changes – in real time. NetBackup now provides artificial intelligence-powered anomaly detection that can detect and alert on suspect behavior at the time of backups. This feature ensures your data is always recoverable and enables you to take immediate action when ransomware strikes, isolating backups with malware and limiting the impact of malware on your backup data.

NetBackup anomaly detection can process data fast and efficiently to detect abnormal events, changes or shifts in backup datasets. Designed with machine learning that can constantly analyze the entire pool of data managed by NetBackup, the integrated anomaly detection engine works seamlessly in the background on the NetBackup primary server with the objective of providing advanced warning of a ransomware event.

There are several fields where anomalies can be detected and reported on within the NetBackup WebUI:

- **Backups** – provides the ID number of backup jobs where anomalies were detected
- **Systems and policies** – quickly identify any backup sources (NetBackup clients) and backup policies where anomalies are detected
- **Anomaly score** – a system generated metric based on AI-powered data analysts that tracks and ranks events that fall outside the standard deviation for a particular dataset

In addition to anomaly detection, NetBackup provides automated malware scanning using 3rd party engines to scan backup images and ensure that they are malware free and safe to restore. You can either restore full images that have been scanned and validated as secure, or you can restore individual files. If a file marked for restore is infected, you can restore it from an uninfected backup. This gives you a safe and effective way to recover data without any risk of re-infecting the target machine. Figure 8 provides an overview of the integrated NetBackup malware scanning process.

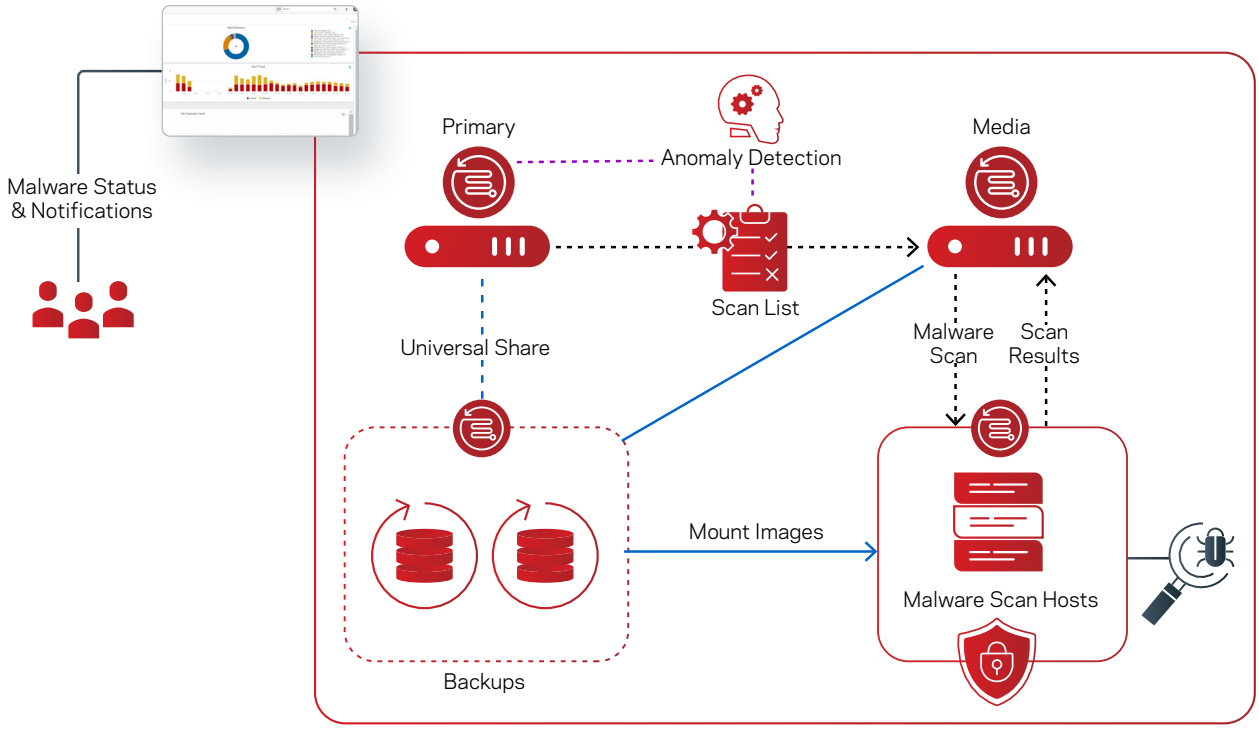

Figure 8. NetBackup integrated malware scanning

Recover

While having an advanced data protection solution is very important, effective recovery and resiliency functionality is a key part of an overall ransomware resiliency strategy. Ensuring that your production applications and data are easily recoverable and have the resiliency needed to withstand ransomware attacks is a primary concern for all businesses.

Veritas InfoScale helps maintain business continuity by providing resiliency for your applications, while NetBackup Resiliency and NetBackup Recovery Vault are designed to help ensure your systems are easily and quickly recoverable in the event of a ransomware attack. As a fully integrated solution for application availability, recovery and resiliency, there are several key benefits:

- Flexibility to use nearly any platform – software and hardware – with integrated security and resiliency features that help protect your production data from ransomware attacks
- Multiple options for configuring application resiliency with support for a wide range of RPOs and RTOs to accommodate applications with varying SLAs as a single solution
- Secure, indelible, and immutable storage options for production data with advanced storage management functionality that can improve application availability with fast, optimized recovery options

Veritas InfoScale and NetBackup Resiliency are fully integrated and can provide availability and resiliency for applications running on nearly any platform – including cloud and containers. A single user console simplifies operations and delivers comprehensive reporting, efficiency, and a smooth user experience.

Primary Data Resiliency with InfoScale

Veritas InfoScale is a proven solution for managing both availability and storage for your critical applications. As a software-defined solution, InfoScale provides both the flexibility to work with nearly any application and infrastructure, while also being a cost-effective way to deliver data services for your applications – including ransomware protection. InfoScale has advanced functionality that can help keep your production applications and data secure and easily recoverable from data corruption or malware.

Some of the key functionality offered by InfoScale to mitigate the effects of ransomware includes immutable storage checkpoints, data isolation capability and integrated security mechanisms that prevent unintended access and changes to system components. The Veritas InfoScale Operations Manager (VIOM) is the graphical management interface that provides an intuitive user experience with visibility into various system metrics and data points across your entire environment. VIOM gives you visibility into specific processes and components that are vital to application resiliency, with the ability to easily report on and log system events.

InfoScale Secure Files and Checkpoints

The Veritas Filesystem (VxFS) enables both files and file system checkpoints to be immutable. The WORM functionality available in InfoScale ensures that both 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 – called SoftWORM – where the root user is given the ability to reduce retention times on files or checkpoints. This functionality is also useful for ensuring that data is available for legal proceedings where data may need to be preserved pending litigation.

InfoScale's secure file and checkpoint option is an efficient, quick, and easy to use solution for protecting your primary data against ransomware attacks. Some of the key benefits include:

- **Infinite retention** – retain data marked as immutable for as long as needed with no limit on retention
- **Immutable checkpoint** – designate file system checkpoints as non-modifiable to protect primary data against ransomware attacks with no impact on recoverability
- **Audit logging** – ensures there is a proper record of events related to illegal modifications within the file system
- **Data resiliency** – support for file level replication of a file system designated as WORM or SoftWORM

InfoScale gives users the flexibility to integrate custom scripts into the data management process to provide additional functionality and data services for InfoScale managed systems. Using custom scripts, InfoScale volumes and checkpoints can be scanned by a 3rd party anti-malware solution to ensure there is no known ransomware present, and to remove any threats if ransomware is identified.

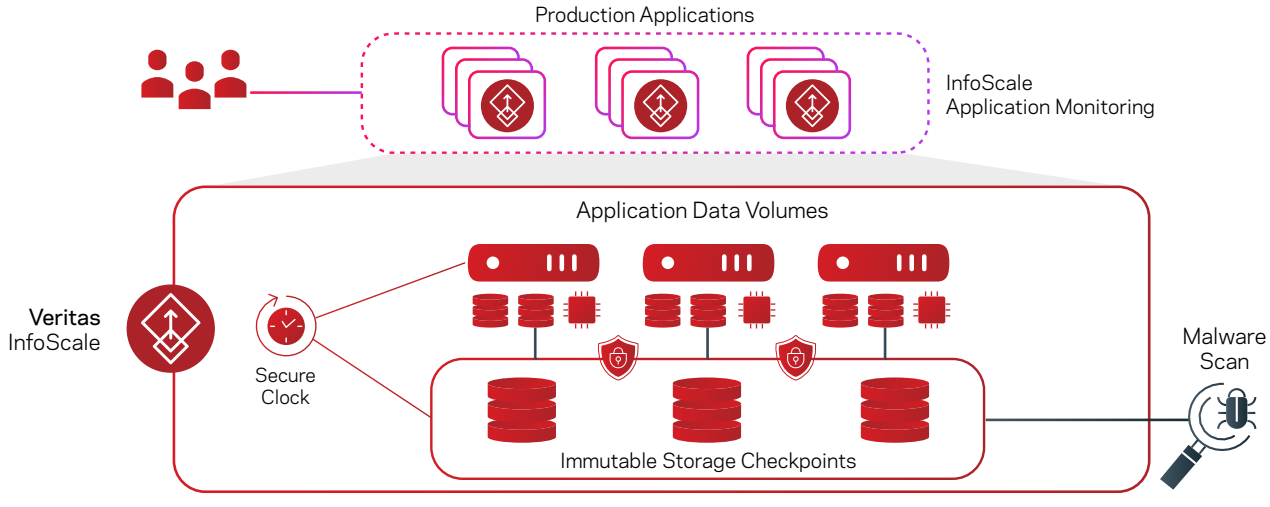

Figure 9. InfoScale immutable checkpoints for production data

Process and Event Monitoring

In addition to secure files and checkpoints, InfoScale can monitor events, as well as system and application processes. If InfoScale detects a process being monitored going offline, this triggers a warning and InfoScale can take action to bring the process back online or move your application to an alternate system within a cluster. This can be a significant benefit in a ransomware attack scenario as you can monitor anti-malware software processes and system security related processes to know if they're intentionally taken offline.

All InfoScale monitored events and audit logs are visible in the VIOM console, which provides a graphical view of all components within InfoScale managed systems – both software and hardware.

Secure Clock

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

The InfoScale implementation of the 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 tampering with the system time.

Continuous Data Protection

NetBackup Resiliency's Continuous Data Protection (CDP) feature provides advanced resiliency for your applications by offering checkpoints derived from real-time replication of your production data that can be used for recovery purposes. CDP augments primary data replication by providing granular recovery for your VM's with a near-zero RPO. This ensures recovery capability for your applications across heterogeneous environments using granular recovery points in addition to near-real-time data replication. With this functionality, CDP provides an additional layer of recoverability from malware or data corruption with a much lower RPO than recovering from a backup copy. NetBackup Resiliency also provides a single interface to manage recovery from both CDP checkpoints and backups, which simplifies the recovery process.

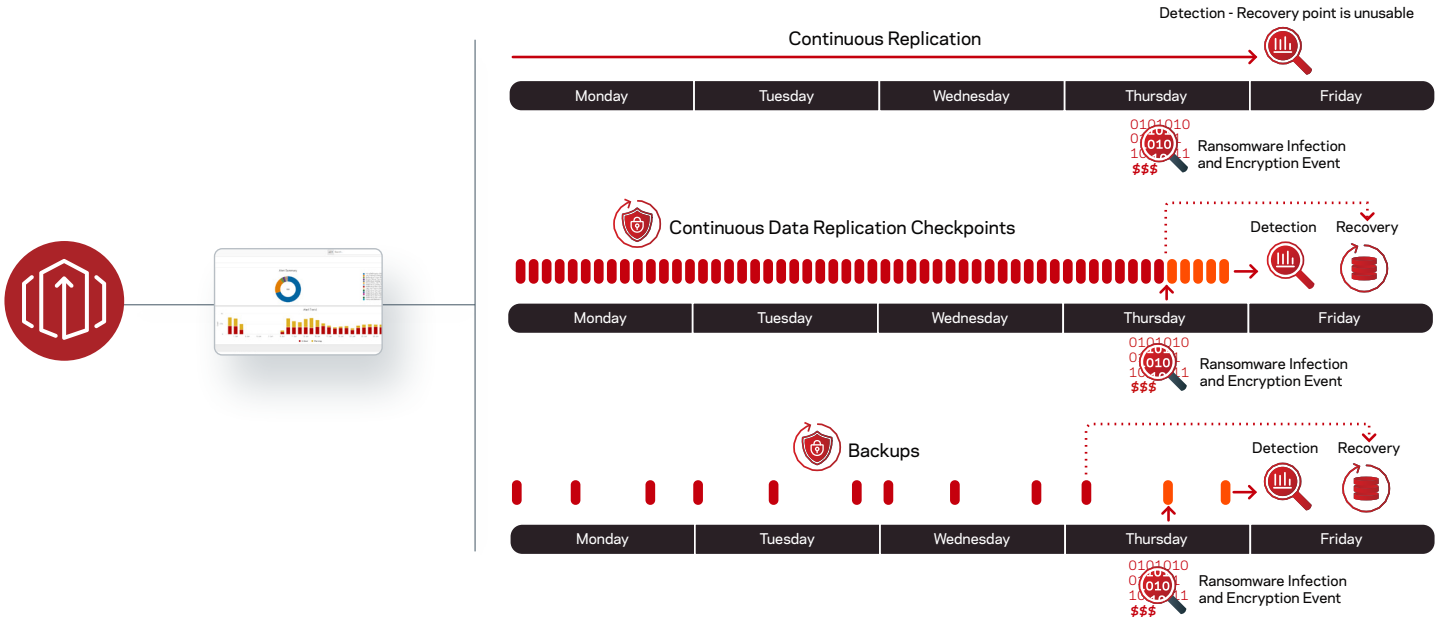

Figure 10. NetBackup Resiliency data checkpoints support a much lower RPO than backup

Orchestrated Recovery

NetBackup Resiliency's Virtual Business Services feature allows you to manage recovery for multitiered applications as a single consolidated entity. With Virtual Business Services, you can completely automate the recovery of a complex, multitier application that spans multiple systems. In the event of a ransomware attack, this provides easier, faster recovery and minimal application downtime.

NetBackup Recovery Vault

Protecting and recovering your data in the cloud can be an effective and efficient way to improve ransomware resiliency. NetBackup Recovery Vault is seamlessly integrated with NetBackup and provides secure cloud Storage-as-a-Service managed by Veritas that is optimized for data protection. Recovery Vault provides:

- **Ransomware protection** – secure air-gapped storage reduces the threat of data loss from ransomware attacks
- **Recover anywhere** – flexibility to choose whether to recover workloads in your data center or in the cloud
- **Optimization** – storage management is provided by Veritas which gives you low-cost long-term data retention in the cloud that can complement tape as an additional option for air-gapped storage

Recovery Vault is an easy and cost-effective way to incorporate data protection tailored cloud storage into an overall ransomware resiliency strategy that helps reduce the risk of data loss, with limitless scalability that can easily accommodate growing data footprints.

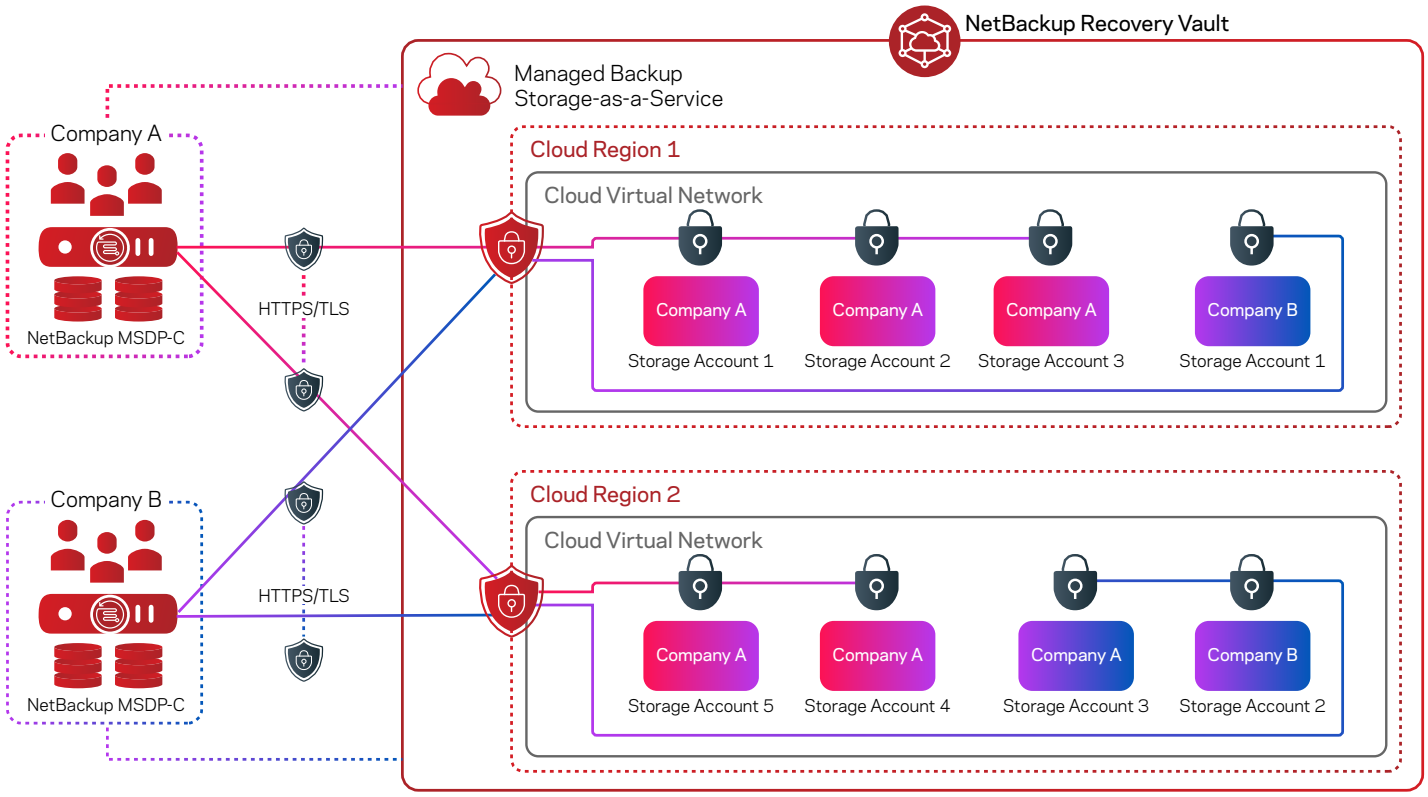

Figure 11. NetBackup Recovery Vault architecture overview

Summary

As ransomware attacks evolve and become more sophisicated, it's of paramount importance for your business to be able to easily adapt to rapidly changing threat vectors to avoid service downtime and data loss. Veritas offers a comprehensive ransomware resiliency strategy that can work with nearly any operating environment and application, with a focus on 3 key principals:

- ✔ Protect – advanced data protection and secure appliances that provide several features to combat ransomware such as integrated malware scanning, a zero trust architecture and immutable and indelible storage
- ✔ Detect – holistic real-time visibility into the status of your applications and data with anomaly detection and tailored insights that help identify malware infiltration in both primary and backup data
- ✔ Recover – advanced storage and fast recovery capability for primary data with integrated storage resiliency, immutability and data isloation capability that ensures the availability of your applications as well as the security and integrity of your data

Having a holistic, multi-layered, and comprehensive cybersecurity strategy is always the best defense against downtime and data loss due to malware infiltration. Veritas understands that this can be a complex challenge and has delivered an enterprise foundation to help protect your IT services as part of an overall cybersecurity strategy. The Veritas ransomware resiliency strategy provides you with the tools, functionality and confidence that your IT services will be highly available, resilient and protected from ransomware.

Appendix

Solution Components

The Veritas ransomware resiliency strategy is based on a combination of Veritas products that work together to provide a foundation for ransomware resiliency. The following products are discussed in this paper:

InfoScale – a software-defined optimization solution for mission-critical applications that abstracts applications from their underlying hardware and software resources. That abstraction enables enterprise-grade optimizations around business continuity, performance, and infrastructure agility across physical, virtual, cloud, and containerized environments. InfoScale provides scalable software-defined storage and availability management for applications running in nearly any environment, with advanced functionality that enables automated system process management, secure data access and immutable data copies to help protect your production applications and data from ransomware attacks. Learn more about InfoScale.

NetBackup – provides enterprise-level heterogeneous data protection for any application in nearly any platform – including containers. It provides cross-platform data protection functionality for a large variety of operating systems and applications. NetBackup uses a centralized management architecture that can be easily scaled to manage data protection for vast enterprise environments. NetBackup includes several comprehensive features – including airgap capability – that are designed to keep your backup data secure and easily recoverable, with integrated machine learning that can detect anomalous behavior and alert users to potential ransomware threats. NetBackup is available in several efficient, easy to manage and secure appliance form factors that add multiple layers of security to the backup process and significantly reduce the threat of data loss or corruption due to ransomware attacks. Learn more about NetBackup. Learn more about NetBackup appliance solutions.

NetBackup IT Analytics – an IT analytics solution that provides advanced insights into storage, backup, virtual and cloud infrastructures as a single platform designed to optimize IT operations, efficiency, and costs in nearly any environment. NetBackup IT Analytics provides holistic visibility into your data center operations and can provide insights into several key data points to help you better understand how resources are used, the costs associated with resource utilization and how your IT services are protected and made resilient. In just a few minutes, NetBackup IT Analytics can provide insights into the breadth and depth of a ransomware attack so you can strategically plan and execute a recovery. NetBackup IT Analytics analyzes data in both on-premises and cloud environments, with a simple deployment architecture that makes it easy to use and operate with a minimal infrastructure footprint. Learn more about NetBackup IT Analytics.

Data Insight – a data analysis tool that provides the analytics, tracking and reporting necessary to deliver organizational accountability for file use and security. Data Insight is designed to work with petabytes of data and billions of files and can help maintain regulatory compliance for data access to protect information from unauthorized use and exposure. Data Insight provides several other services for primary data, including auditing, sensitive data monitoring, anomalous behavior detection, user anomalies, custom query templates and file extension identification that can all be used to detect and alert on ransomware. Learn more about Data Insight.

NetBackup Resiliency – a software-defined disaster recovery and resiliency orchestration solution for physical and virtual systems that enables automated resiliency and disaster recovery for hybrid and multi-cloud environments. NetBackup Resiliency provides multiple options for advanced replication management, including native data replication capability, integration with storage level replication and NetBackup replication. NetBackup Resiliency supports continuous data protection based on real-time replication that provides users with multiple checkpoints that can be used for recovery purposes with a minimal RPO. NetBackup Resiliency also acts as the centralized interface when integrated with InfoScale and NetBackup that provides control and visibility for the overall solution.

NetBackup Recovery Vault – a cloud-based managed backup-as-a-service recovery solution that provides a seamless, fully managed secondary storage option for NetBackup. Recovery Vault is fully managed by Veritas and it provides virtual air-gapped ransomware protection with limitless scalability that can accommodate growing backup footprints. Recovery Vault offers flexible recoverability that gives users the option to recover anywhere – on-premises and in the cloud. Learn more about Recovery Vault.

Table of Figures

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

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

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

V1551 04/22