EBOOK

5 Best Practices for Ransomware Recovery

Rubrik & ePlus: Time for a Datatude Adjustment

Rubrik and ePlus have joined forces to deliver a solid remediation plan that meets the threat of ransomware head-on by arming data-dependent organizations with immutable technology, strategic insight, and unmatched expertise.

> **This partnership combines Rubrik's simplified and automated data management, instant recovery from ransomware, and secure archive to the cloud with the engineering expertise of the ePlus Managed Services team to support setup, configuration, optimization, and management.**

Now organizations can make their data work harder for them by making their backup solution the key to improved business continuity, cloud mobility, multi-cloud management, and regulatory compliance. And the tight integration created by ePlus running their own Cloud Managed Backup service on Rubrik allows a sharper focus on improving customers' business outcomes.

With confident ransomware recovery made possible by the Rubrik/ePlus partnership, organizations will realize a fast track to the cloud and a path to operational excellence that positions them strongly for the future.

BEST PRACTICES FOR RANSOMWARE RECOVERY WITH RUBRIK

As guardians of our customer's data, Rubrik understands that a ransomware attack is one of the worst-case recovery scenarios that customers can face. An impacted customer will likely be dealing with widespread business and logistics issues caused by the attack. Rubrik has helped a number of our customers successfully recover from ransomware attacks. As a result, a set of best practices has been developed to help other customers plan for, identify and remediate ransomware attacks.

Through our experience with customers and industry, Rubrik has organized its ransomware best practices into the following steps: Preparation, Prevention, Detection, Assessment, and Recovery.

- **Preparation:** Organizations put themselves in the best position for success when they prepare for a ransomware attack ahead of time.
- **Prevention:** Rubrik encourages organizations to use third party tools to prevent ransomware from entering and attacking its systems. It is best to catch ransomware before it has a chance to do damage.
- **Detection:** Rubrik can help detect where ransomware has attacked via Radar so that surgical remediation can be made.
- **Assessment:** During the Assessment step, it is important to decide what needs to be recovered first and when.
- **Recovery:** Data is recovered once the ransomware has been neutralized and cannot reinfect the data.

The next sections describe these steps in detail as well as the actions to take during each one.

PREPARATION

Taking the time to prepare for a Ransomware attack is a key success factor for recovery. The steps below outline some of the tasks that Rubrik has found to be successful.

- **Build a plan:** Develop a ransomware response and recovery plan and supporting playbook. This plan should be updated and reviewed periodically. Additionally, the plan should be stored in a secure location that cannot be attacked by ransomware. A printed copy is good for this.

  By following an established plan during an attack, confusion will be limited as everyone will know what to do. Also, a plan will help expedite the identification and neutralization of the ransomware, to reduce the impact by reacting in an efficient and effective manner.

- **Who will respond:** Identify key stakeholders across management, IT, system/application teams, etc. and who will be responsible for executing and managing the incident response. Make sure those people know their responsibility and how to execute their portion of the recovery plan. A key success factor is timely and thorough internal communication within the affected organization.

- **Communication:** Identify methods of communication that are available during a Ransomware event. Corporate email and phone systems may be impacted and unavailable. Provide for alternate means of communicating both internally and with outside vendors such as Rubrik.

- **Prioritization:** Identify the criticality of each system and its data to the business. Knowing which systems in the business need attention first and how they interact with other business systems will allow for a smooth and orderly recovery. Based on each system's criticality level, document a recovery plan of what systems would be recovered in which order.
- **Identification:** Implement tools like Rubrik Radar to identify at a file or object level what data has been infected with ransomware. Having this data during an attack will be invaluable to speeding up recovery and preserving uninfected data.
- **Protection:** Ensure all necessary systems and data are being protected with the required levels of data retention. Here it is better to include extra data and exclude as needed rather than only including targeted systems/data. In this manner, all data needed for recovery will be in the data protection system.
- **Recovery plan:** Determine what recovery methods will be used for each type of recovery. Options like Rubrik Live Mount will allow systems to be recovered in minutes as they run on the Rubrik CDM storage. This method, however, rolls entire systems back to a safe point in time. Uninfected data may be lost. File-level and database level restores for infected data may be more desirable. The appropriate method needs to be evaluated ahead of time so that it can quickly be selected during an attack.
- **Automation:** A key factor during the recovery phase is automation, as it minimizes the risk of human error. It also speeds up recovery and aids in progress tracking. Rubrik has a full set of APIs and SDKs to help automate recovery. These can be integrated with automation tools such as Ansible, Terraform, Puppet, Chef, PowerShell, and Python. Once a recovery plan and prioritization have been established, automation is the next step in building a more robust recovery capability.
- **Isolation:** Have a plan to isolate infected systems so that the spread ransomware can be prevented on the network. Also, have a plan in place to recover data and systems in isolation of the main network. If the ransomware cannot be safely neutralized, recovery to a new set of systems on a separate network may be the only course of action.
- **Storage:** Determine where backup copies will be stored (locally and/or offsite). Local copies stored on Rubrik's immutable CDM platform will allow for faster recovery to local systems. Remote copies of the data will be required if the recovery plan calls for recovery at an alternate site.

  Special attention should be given to how data is stored offsite. If replication to another Rubrik appliance is used, data immutability is built in. On the other hand, data stored in offsite archives may not be immutable and subject to attack by Ransomware. This is because the storage platforms on which the backups are stored are not necessarily immutable. For example, an NFS archival location could be accessed outside of Rubrik and the data attacked by the ransomware. Cloud archives can also be externally accessed when not properly secured. If archival locations will be relied upon to recover from ransomware attacks, steps should be taken to secure those locations.
- **Testing:** Periodically test data recovery to be prepared for an actual incident. Without testing the recovery plan, there can be no assurance that it will work when an attack happens. Testing also provides the experience and confidence to staff members that an attack can be successfully and quickly remediated.

  Tests should be made as realistic as possible without disrupting business operations and performed at both planned and unplanned intervals. One purpose of testing is to be prepared for the unexpected.

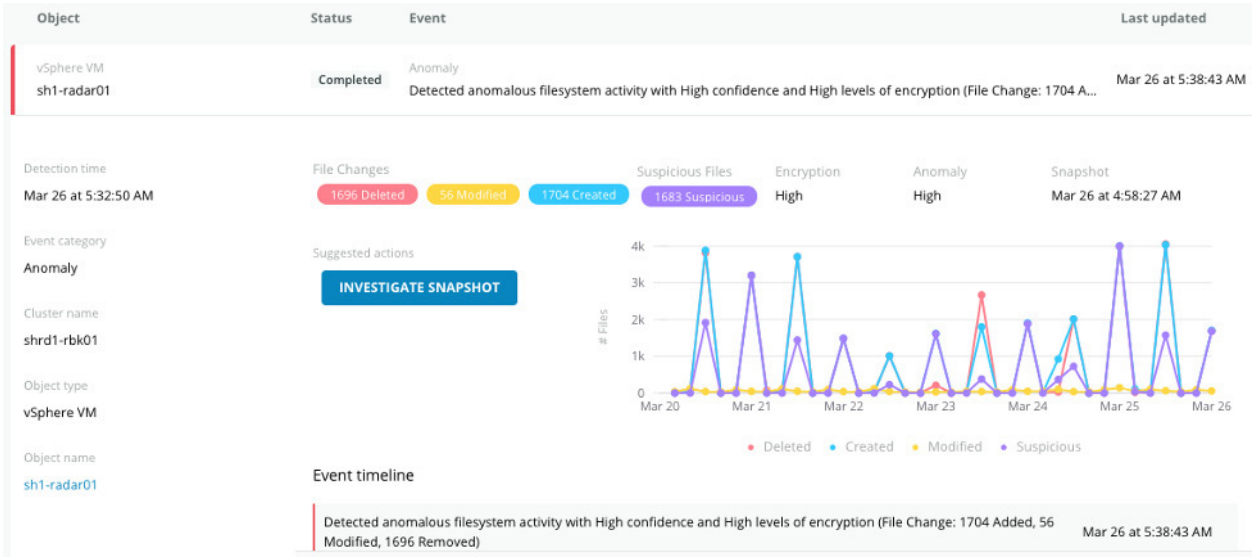
  Various validation frameworks are provided by the Open Source Community. One such framework is provided on Rubrik Build[7].

PREVENTION

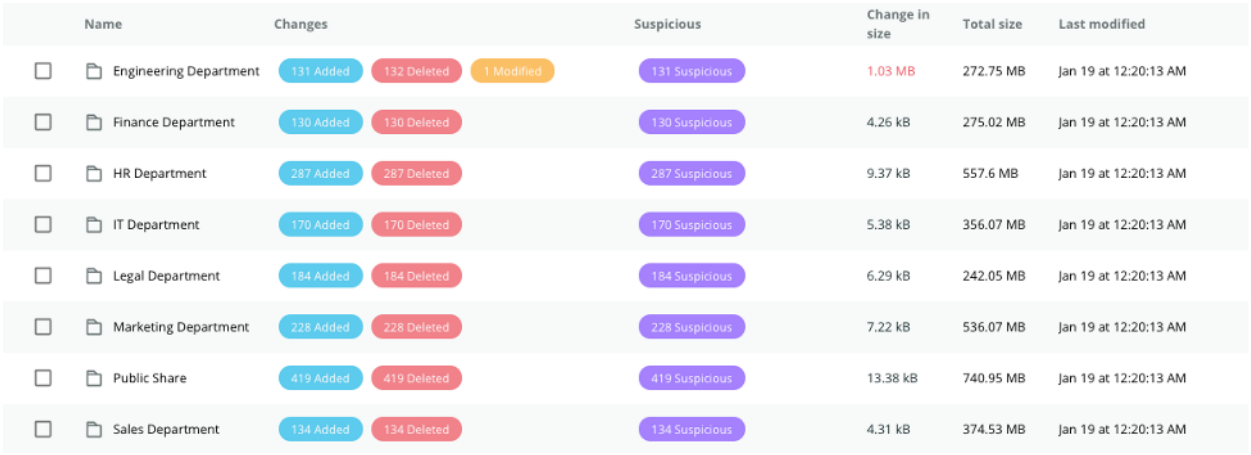
While Rubrik does not play a role in the prevention of ransomware, plenty of best practices and third-party software offer this protection and guidance. Information about prevention is available from places like Cybersecurity and Infrastructure Security Agency (CISA)[8] and The Federal Bureau of Investigation[9].

DETECTION

In the event that ransomware circumvents the Prevention methods, processes and tools should be put in place to detect ransomware before it has fully activated. The first line of detection is from real-time detection tools. Analysis of backup data is the second line of defense.

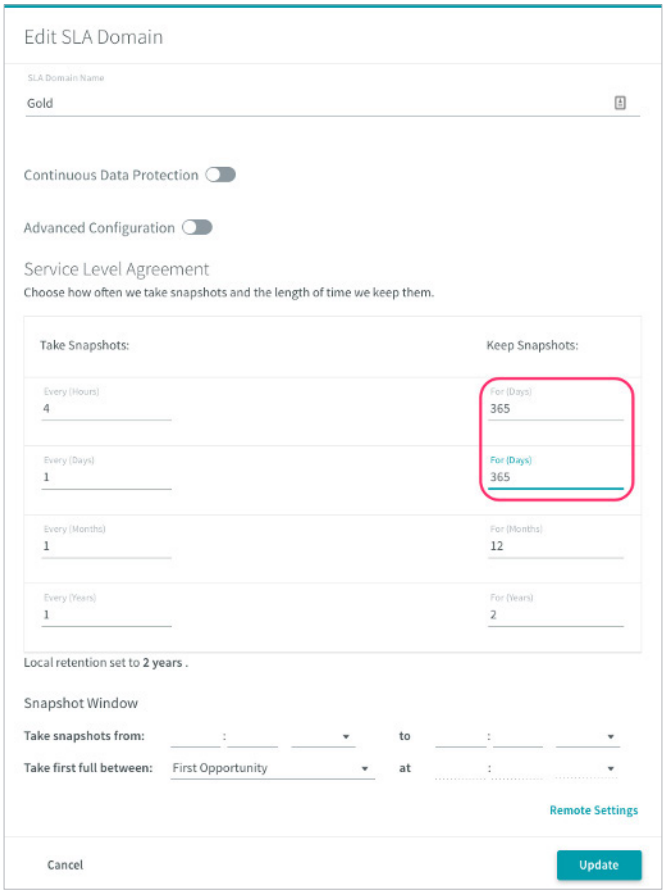


Rubrik Radar helps with Detection by leveraging a Deep Neural Network (DNN) to build out a full perspective on what is going on with the backups through analysis. The network is trained to identify trends that exist across all samples and classify new data by their similarities without requiring human input. The analysis is largely based on file system behavior and content analysis. Rubrik Radar's File System Analysis performs behavioral analysis on the file system metadata information looking at items like number of files added, number of files deleted, and so forth. Once outlier behavior is detected, File Content Analysis can be performed on the backup to identify if encryption has occurred. A list of the infected files is then presented to the system administrator.



ASSESSMENT

- **Isolation:** Systems that are suspected of or have been confirmed to be infected with ransomware should be isolated. This will prevent the ransomware from spreading to other systems on the network.
- **Extending or Pausing snapshot expiration:** Once ransomware has been detected, snapshot expiration should be carefully reviewed to ensure no valid snapshots expire which would affect data recovery. SLAs with near term retention policies should be extended to at least one year for the duration of the ransomware event. Be sure to make note of the original retention periods so that they can be set back after the ransomware event is over. As a second precaution, Rubrik support can pause the expiration of snapshots until the event has ended. Contact Rubrik support as soon as a ransomware attack is suspected to request this service.



These steps will help prevent the accidental expiration of backups that may be needed for recovery.

- **Notification:** All stakeholders should be notified of the ransomware attack so that they can start to execute their portions of the recovery plan. Notification should also include Rubrik support for assistance with recovery. Early notification of stakeholders, Rubrik support and other vendors even while the attack is still being assessed will allow time for them to respond.

  Engage Rubrik and open a priority 1 support case at your first opportunity. Even if the event is still in the investigative and/or neutralization phase, Rubrik Support may be able to be of assistance. Ensure management, technical stakeholders, and all technology vendors such as Rubrik are collaborating, communicating and aligned on priorities, the order of operations and action items. Please help to ensure all internal and vendor technical stakeholders are copied on all case updates to maintain overall situational awareness. It is best to over-communicate in these situations. Rubrik is very happy to collaborate with all other technology vendors to assist in your environment's recovery.

- **Assess the scope of the attack and neutralize:** Ascertain the current status & impact and scope of the situation. Obtain answers to the following questions/actions:
    - Has the attack been neutralized?
        - Restoring before the attack has been neutralized can reintroduce the ransomware and reinfect systems. This can lead to a cycle of recovering the same systems over again.
    - Identify the scope of the attack.
        - What business functions have been or may be impacted?
        - What systems and data were compromised?
            - This includes archive and cloud data repositories.
            - If Rubrik Radar is available it can be used in this step to identify compromised files.
        - Was the network/authentication infrastructure compromised?
        - When was the ransomware software introduced?
        - How was the ransomware software introduced?
        - When did the attack first happen?
    - Identify the strain of ransomware that has attacked the systems or data.
        - Use tools like ID Ransomware[10] to identify the ransomware strain.
    - Identify a safe point in time for a restoration point?
        - Not selecting a safe recovery point could reintroduce the ransomware if it is already in the backups.

- **Pausing protection to affected systems:** As the scope of the ransomware attack is understood, the appropriate action must be taken to stop the spread of the ransomware. When possible, pause protection on only the compromised infrastructure vs. a global blanket pause in protection. This will limit the impact to only the parts of the business which were attacked. For Rubrik CDM it will also minimize impact to snapshot chains and minimize subsequent full & deltas, which can result in more cluster space being utilized and jobs taking longer to run.
- **Review the disaster recovery/ransomware incident plan:** While the initial response is taking place, be sure to review the disaster recovery/ransomware incident plan. This will ensure that steps in the detection, assessment, and recovery from the ransomware attack are not missed.
- **Establish recovery priority based on the affected systems and the recovery plan:** Once the affected systems and/or data has been identified prioritize recovery based on the established recovery plan. This will allow those systems and data to be recovered quickly and in accordance with the business' needs.
- **Identify where the backups will be restored from (local copies or archives):** Determine if local copies of the backups are available or if they will need to be brought back from archives. The recovery point that was determined for each system based on when the infection occurred will help to dictate this. Also, determine if the archival and/or cloud data has been compromised. If so recovering from an alternate copy will be necessary.

RECOVERY

Before starting the recovery process, it's important to know what type of recovery is required. If the ransomware only attacked files on servers or user shares on a NAS, a file-based recovery method can be used. If, however, the ransomware attacked the virtual disk images for a hypervisor or the MBR records of a physical system, a full system recovery may be needed. The best practices for recovering from each of these attacks is covered here, along with general best practices for all recoveries.

GENERAL RECOVERY BEST PRACTICES

These best practices apply to all recovery scenarios.

- **Recover safely:** Only begin recovery operations after the ransomware has been neutralized. This may mean that data needs to be recovered in isolation or to new systems. Restoring systems or data before the ransomware has been neutralized may result in the system/data being attacked again. If the ransomware cannot be isolated and neutralized in a timely manner, the alternative is to recover where systems cannot be reinfected.
- **Decrypt data:** Recovery may not be necessary if there is a decryptor for the ransomware strain that was identified. When possible, decrypt existing data to prevent data loss. Decryption should be done in a safe environment. If the ransomware could not be neutralized, decryption in isolation may be required.
- **Isolated recovery:** Often ransomware attacks are so pervasive that recovering back to original locations will only result in secondary attacks. Recovering to an isolated environment where the ransomware did not have access is the best prevention for a secondary attack. During the Preparation phase, an isolated environment should have been identified and tested. During the Recovery phase, use the isolated location to securely recover data if needed.
- **Prioritized recovery:** As planned for in the Prevention phase, recovery will be based on the prioritization of applications and lines of business. The prioritized list of what to recover and when should come from the Assessment phase. Ensure that foundational services required for basic functionality, such as DNS, DHCP, and Authentication, are running or restored first. Without these, the recovered systems may not function properly.
- **Use automation:** Use the tested automation that was developed during the Preparation phase. Automated recovery via automation tools and Rubirk's APIs and SDKs will speed up recovery times. Proven and tested automation will also add to the accuracy of the recoveries. Automation may not be required for all types of recoveries. Some examples of where automation can be particularly helpful are:
    - Recovering NAS systems with tens or hundreds of shares.
    - Recovering complete virtual environments with hundreds or thousands of VMs.
    - Recovering database servers with many databases.
    - Recovering filesets across multiple servers to or near the same point in time.

FILE-ONLY RECOVERY BEST PRACTICES

These best practices apply to scenarios where only files and directories need to be recovered.

- **Verify the operating system:** Verify that the underlying operating system can be trusted and was not compromised by the ransomware attack.
- **Recover to clean systems:** If the original system cannot be trusted, recover files to a known good system. This may be a newly-built system that is in isolation.
- **Identify files for recovery:** Use a tool like Rubrik Radar to identify which files were attacked by the Ransomware and recover them.

VIRTUAL MACHINE AND DATABASE RECOVERY BEST PRACTICES

These best practices apply when the VM itself cannot be used. This may happen if the NAS storage that the VM is running on has been compromised. It may also happen if the ransomware renders the VM unbootable.

- **When to use Instant Recovery:** (Smaller data sets) Recovery efforts can be sped up by utilizing Rubrik's Instant Recovery feature. This allows VMs and databases to be mounted directly from the Rubrik storage, saving the time that it takes to copy backups back to primary storage before making resources available. Once mounted, VMs can be moved back to primary storage in the background while providing their regular services. Databases can be run until a planned outage can be taken to move the database back to primary storage.

  Instant Recovery is a good option for a smaller number of VMs, which may include mission-critical systems. Care should be taken with Instant Recovery so that the Rubrik cluster is not overloaded. The Rubrik cluster is not a substitute for primary storage. Also for VMs, the time and resources required to storage vMotion VMs back to primary storage are higher. This is due to the storage vMotion protocol and the ability for multiple users to access the VMs at the same time.

  Instant Recovery is a good option for smaller numbers of databases because the Rubrik storage is not designed with the same performance characteristics as primary storage. Additionally, databases cannot be storage vMotioned to primary storage. Instead, they must be shut down during a maintenance window and moved offline. The trade-off of gaining access to the database immediately needs to be weighed against having to move it later.

- **When to use Export:** Rubrik's Export function recovers or copies the database or VM directly to primary storage. Once copied the database or VM can be brought back online. This method provides the fastest data transfer performance back to primary storage and is best for recovering many VMs. The entire Rubrik cluster's performance can be used to move the data back to primary storage. There is no contention with workloads that are also writing data.

- **When to Mix Instant Recovery with Exports:** Instant Recovery and Export workloads can be mixed on the Rubrik Cluster. Doing so should be done with extreme care. Exports will utilize the full resources of the Rubrik cluster to move data back to primary storage. Instant Recovery may have to contend with the traffic that is being recovered. This may cause degraded performance in the databases and VMs that have been Instantly Recovered. Use of this mixed workload should be evaluated on a case-by-case basis.

HYPERVISOR MANAGER RECOVERY BEST PRACTICES

Coordinate the recovery of vCenter(s) with the appropriate support team to ensure a smooth recovery.

- **vCenter Recovery:** Care must be taken if vCenter has to be recovered or when recovering VMs into a new vCenter. Rubrik CDM uses the MOID of a VM for tracking. Duplication or reuse of the MOID can lead to issues during the recovery of VMs. If vCenter has been compromised, it is better to restore it from backup than to create a new empty vCenter and recover the VMs into it.

  When vCenter Service Appliance (VCSA) is used, Rubirk snapshots of it can be recovered directly to an ESXi host. Contact Rubrik support for more details.

  Other vCenter platforms can be recovered from vCenter's built-in backup. The backup files that this creates can be protected by Rubrik CDM. After restoring the backup file, contact VMware Support for more details on recovery options using this method.

- **Recovery and/or re-installation of non-vSphere Hypervisor Managers(s):** When hypervisor managers such as Microsoft's System Center Virtual Machine Manager (SCVMM) or Nutanix Prism are protected using Rubrik snapshots, please engage Rubrik Support for recovery options. When the hypervisor manager is protected using built-in backup methods, please engage the hypervisor vendor in addition to Rubrik Support. These hypervisor managers are usually prioritized higher in the recovery workflow to ensure that Rubrik can focus on the individual VMs afterward.

CONCLUSION

Ransomware has become more prevalent over the years and is costing companies millions of dollars. During this time ransomware has also evolved and become more sophisticated. It not only will block access to systems, but it will also encrypt or delete active data, including backups.

When the prevention of a ransomware attack fails, having an immutable backup that cannot be attacked becomes crucial. Being able to intelligently identify and remediate encrypted data makes recovery efforts easier, less time consuming and reduces data loss.

By following the best practices outlined in this document, the odds of recovering from a ransomware attack successfully and in a timely manner are greatly improved. Of course, the best defense is prevention but in the event that preventative measures do not work, Rubrik has demonstrated success in recovering from ransomware.

SOURCES AND NOTES

1 https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

2 https://www.rubrik.com/blog/immutable-backups-protection-ranswomare/

3 https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf

4 https://pages.rubrik.com/DataIntegritywithRubrik_Registration.html

5 https://www.rubrik.com/wp-content/uploads/2017/02/Data-Sheet-Data-Encryption-1.pdf

6 https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf

7 https://build.rubrik.com/use-cases/backup-validation/

8 https://www.us-cert.gov/ncas/tips/ST19-001

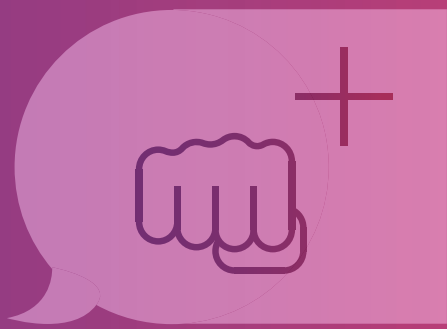
9 https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

10 https://id-ransomware.malwarehunterteam.com/

Get A Readiness Assessment

You've begun your datatude adjustment and realized that backup is just the beginning of what the Rubrik/ePlus solution can do for you. Now it's time to take the next step by having our engineers perform a thorough analysis of your current infrastructure, needs, and processes. We'll make strategic recommendations that show you a path to simpler data management, smart automation, and considerable cost savings.

datatude.eplus.com



For more information, visit eplus.com/datatude