Competitive Intelligence Report
April 2019

DCIG

Creating a Secondary Perimeter to Detect Malware in Your Enterprise Backup Environment:

A Comparison of How Backup Solutions from Asigra, Dell EMC, and Rubrik Detect and Respond to Malware Attacks

By Jerome M Wendt

Asigra.

Table of Contents

April 2019

DCIG

Competitive Intelligence Report

Creating a Secondary Perimeter to Detect Malware in Your Enterprise Backup Environment:

A Comparison of How Backup Solutions from Asigra, Dell EMC, and Rubrik Detect and Respond to Malware Attacks

Executive Summary

Malware represents one of the more insidious threats that companies face in their day-to-day operations. Due to the numerous ways in which malware can find its way into a company coupled with malware's rapidly changing nature, first line defenses such as anti-virus software and firewalls can no longer ensure that malware will not find its way past them into production data stores and, by extension, into corporate backups. Companies must now take steps to create a secondary perimeter to ensure their backups remain safe from malware attacks as well as free from malware to ensure they can recover from a malware attack.

Sandbox
Test IT environment setup to test for presence of malware.

Data Analysis
Analyzes backup metadata and file content for changes and anomalies.

Inline Scan
Backup software leverages cybersecurity software to scan for malware.

In response to these corporate demands for malware-free backups, there are three distinct methodologies available from Asigra, Dell EMC, and Rubrik that companies may use to detect malware in their backups. These include:

1. ***Create a sandbox.*** Using a sandbox isolated from their production environment, companies first recover their backups. Once recovered, they can scan the data for the presence of malware. Alternatively, if they suspect the backups contain a strain of malware that is still unknown to anti-virus software, they can allow it to detonate in the sandbox so they can observe its behavior and develop counter measures.
2. ***Do data analysis on snapshots.*** Using this approach, software analyzes file metadata and file content in system snapshots. Then using sophisticated machine learning algorithms, the software looks for anomalies and significant changes to the data to determine if malware may exist and be active in the production environment.
3. ***Perform an inline scan in which the backup software leverages cybersecurity software to scan for malware during backups and recoveries.*** Using this technique, the backup software provider embeds cybersecurity software in its software. The cybersecurity software then scans for malware as the backup software backs data up and then again when it recovers data.

Each of these three approaches has its respective merits and best use case. To make the best choice, companies will want to give preference to the methodology that provides them the fastest, easiest, and most reliable means to detect the presence of malware in their backups. In almost all circumstances, embedding cybersecurity software inside the backup software to scan for malware during backups and recoveries, such as Asigra Cloud Backup does, will be the best approach.

By embedding cybersecurity software in its backup software such as Asigra has done with its Cloud Backup software, companies can ensure that their most important data—the data they deem worthy of being backed up—has an extra layer of protection around it. In this way, should malware ever penetrate their perimeter defenses and compromise their production data, they can have a high degree of confidence that the backups they use to recover is free from malware and they can use it to quickly recover from this type of attack.

Creating a Secondary Perimeter to Detect Malware in Your Enterprise Backup Environment:

A Comparison of How Backup Solutions from Asigra, Dell EMC, and Rubrik Detect and Respond to Malware Attacks

The Scourge of Malware

The city of Atlanta.[1] Del Rio City Hall.[2] Hancock Health Hospital.[3] The San Francisco Municipal Transportation Agency.[4] There is one characteristic that these and many other institutions throughout North America and the world share: malware has hit every one of them in the last few years.

During this time, malware in its various forms has become nothing short of epidemic.[5] Consider:

2016
RANSOMWARE ATTACK EVERY 0:40 SEC.

2017
RANSOMWARE PAYMENTS OF $1B

2019
MALWARE ATTACK EVERY 0:14 SEC.

2021
MALWARE ATTACK EVERY 0:11 SEC.

- A business fell victim to a ransomware attack every 40 seconds in 2016
- In 2017, the FBI estimated ransomware payments approached $1billion annually
- In 2019, a business will fall victim to a malware attack every 14 seconds
- By 2021, a business will fall victim to a malware attack every 11 seconds by 2021

These statistics illustrate how malware has become a worldwide outbreak for which all institutions, public or private, must prepare to respond. Cybersecurity Ventures estimates that cybercrime will cost the world ***$6 trillion annually*** by 2021 which represents 6.7% of world GDP. Assuming this forecast holds true, cybercrime will create more profits than the profits from all major illegal drugs combined and would represent the biggest transfer of wealth in history.[6]

Malware's Two Primary Sources of Revenue

Malware's forecasted financial revenues have hackers the world over dedicating IT resources to make ever more potent strains of it. As a result, malware continues to rapidly evolve as hackers develop new forms of it to generate revenue. Ransomware and cryptojacking represent the two forms of malware that companies will most likely encounter and must be prepared to defend against.

In the case of ransomware, it attacks companies by first encrypting their data. Once encrypted, the hacker demands payment (a ransom) from the affected company. In return for payment, the hacker provides a key to the company that will decrypt its data. Unless the company pays the hacker for this key within a specified time, the company may not be able to decrypt its data.

Cryptojacking represents the other primary form of malware that has also recently gained momentum. Once cryptojacking malware finds its way onto a server, it attempts to run silently and undetected as a background process on the server. When running, it performs revenue generating tasks such as bitcoin mining on behalf of the hacker.

Cryptojacking malware does not overtly charge companies in the same way as ransomware. Companies may not even know that cryptojacking malware resides and runs on their systems since their applications still work.

They may only notice it when applications running on those servers experience degraded performance. Alternatively, they may get an unexpectedly high bill from their cloud provider due to the cryptojacking malware consuming abnormally high levels of CPU and memory resources on their cloud VMs.

Generating Revenue is Malware's End Game

Malware distinguishes itself from other types of hostile software such as computer viruses or spyware in that it seeks to illicitly make money off a company either through extortion (ransomware) or by using its computing resources without its permission (cryptojacking). These both present a significant risk to companies (financially and technically) and their abilities to operate without business interruption.

1. https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-may-cost-the-city-17m.html
2. https://www.bleepingcomputer.com/news/security/del-rio-city-hall-forced-to-use-paper-after-ransomware-attack/
3. https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
4. https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/
5. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf, Pg. 7
6. Ibid.

The Difficulty in Detecting Malware's Presence

Companies already largely recognize the threat that malware presents to their operations and many take precautionary steps to ensure it does not infect their data stores. At the perimeter of their organization, they use standard defenses such as anti-virus software and firewalls that scan incoming data to detect for the presence of malware. On those occasions when malware does slip past these perimeter defenses and infects their production data, they can use backups to recover from a malware attack.

On the surface, these two best practices may sound satisfactory to prevent a malware attack and recover from one should perimeter defenses fail. However, there are two flawed assumptions associated with only using this two-tiered approach to detect, prevent, and recover from a malware attack.

FLAWED ASSUMPTION #1:
Perimeter Defenses Such as Anti-virus Software and Firewalls Stop All Incoming Malware

Anti-virus software and firewalls leave multiple gaps on a company's perimeter for various reasons. Whether used separately or together, they often cannot detect every occurrence of data as it enters companies to scan for malware. Data may still find its way into corporate data stores from multiple sources which include (to name a few):

- Web links embedded in email
- File attachments
- Internal network file shares
- External internet file sharing software such as Dropbox
- Managed service providers (MSPs) that utilize software such as Kaseya to provide remote support
- Remote Desktop Protocol (RDP)
- Thumb drives
- Data generated or received by internet of things (IoT) devices
- Data downloaded through web browsers

Purchases of "approved" corporate applications or software updates to them may also can contain malware. Software companies produce up to 111 billion new lines of code every year that they routinely and systematically distribute to their clients.[7] While new software or software updates should be malware-free, companies get no guarantees that they are.

Even should a company manage to ensure its anti-virus software and firewalls scan all data coming in through all these different sources for malware, malware itself constantly changes. A 2017 study published by G DATA security experts revealed they discovered a new malware strain about every 4 seconds.[8]

This massive number of malware strains makes it improbable that anti-virus software and firewalls can alone identify every new strain of malware as it enters a company. Further, this can also result in variations of documented strains such as Locky, NotPetya, and WannaCry slipping through undetected.

FLAWED ASSUMPTION #2:
Backups are Immune from Malware

Companies may think that if even on the rare occasions where malware gets past their standard perimeter defenses, they can always turn to their backups to recover. Here again companies get no guarantee that they can use backups to successfully recover from a malware attack.

To use backups to recover from a malware attack, two conditions must hold true:

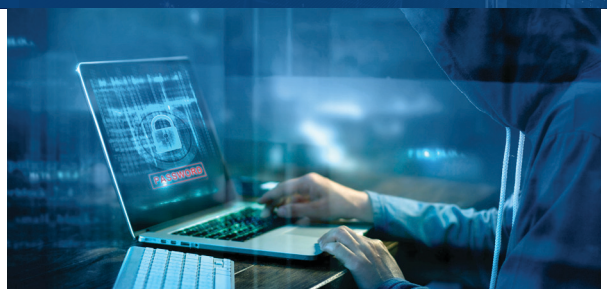
1. Good backups exist that they can use to recover.
2. The recovered backups will not re-introduce the malware back into the production environment.

As some companies have found out, ransomware has evolved to identify and attack backups. Some recent versions of ransomware may delete or encrypt backup files stored on disk or on network file shares where some backup software products store the backups they create.

One recent example is Zenis Ransomware. It scans for files with extensions such as ".bak", ".bkp", ".old", and about 20 others. If it finds files with any of these extensions, it encrypts them as well.[9]

Perhaps the most insidious form of an attack involves malware that remains dormant and undetected for some

7. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf , pg. 5
8. https://www.gdatasoftware.com/news/2017/04/29692-a-new-malware-strain-was-discovered-every-4-2-seconds-in-q1-2017
9. https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/



time. Once inside a company, it first infects production files over a period of days, weeks or even months before it detonates. During the malware's incubation period, companies will back up these infected production files. At the same time, they will, as part of their normal backup operations, delete their expiring backups.

After a few weeks or months of routine backup operations, all backups created during this time will contain infected production files. Then when the malware does detonate in the production environment, companies may get caught in a Zero-day Attack Loop.

In this circumstance, when companies attempt to recover, they discover they have neither good backups nor good recovery points. Instead, they can only restore files previously infected with the dormant malware which will re-introduce the malware back into their environment.

Recovering with Confidence Starts with a Golden Copy

To deal with these challenges that malware presents to backup data stores, companies increasingly look to backup software providers to help them confidently recover from a known good copy of data. This good copy of data should be free from malware, sometimes referred to as a Golden Copy. Properly created, companies can reliably and safely use this Golden Copy to restore their data.

Backup software providers currently employ three processes to detect the presence of malware in backups in order to create this Golden Copy.

Sandbox

A common approach to creating a Golden Copy involves checking for the presence of malware after the backup completes, or post-backup, in a sandbox. Dell EMC represents one provider that employs this post-backup methodology though other backup software vendors also subscribe to this approach.

Using this technique, a company completes its backups as normal. It then creates a sandbox that it isolates from its production environment to test the data in its backups for malware. This sandbox may consist of physical machines, virtual machines, or both, to which it recovers the data originally backed up by Dell EMC Avamar (or whatever backup software a company may use.) Once it restores the data, a company can perform a couple of different tasks.

1. It can scan the data using cybersecurity software such as anti-virus software to examine it for the presence of known strains of malware.
2. It can allow the malware to detonate.

A company may allow the malware to detonate if it suspects its anti-virus software cannot yet identify or detect the malware due to it being a new strain of malware. Allowing the malware detonation to take place in isolation the company can observe how the malware behaves. It can then take steps to identify the malware strain, create a Golden Copy free of malware, and prevent the malware from detonating in the future.

Snapshot Analysis

Another post-backup approach that a company can take to create a Golden Copy involves doing analytics on the snapshots of production data to detect the presence of malware. Rubrik, another representative backup provider, employs this technique though other providers use a similar tactic as well.

In this use case, a company creates snapshots of the production data. After the snapshots complete, the backup software uses data analytics software to examine the snapshots for changes. If the data analytics software detects significant changes between snapshots, it generates an alert that malware may exist. Analyzing each snapshot for changes reduces the need to create a sandbox in which to recover data and test for malware.

Inline Scan

A third approach, employed by Asigra and its Cloud Backup software, incorporates the use of cybersecurity software into the backup process. The cybersecurity software scans incoming backup data and data it restores for the presence of malware. Should it detect any malware signatures in any of this data, Cloud Backup generates alerts and notifies the appropriate individuals based on the notification policies set by the company.

The scan that occurs as part of the recovery re-checks the backup data for any malware signatures that were undiscovered or latent at the time of the original backup. By scanning the data once more during the recovery process, a company further decreases the possibility that recovered data contains any malware.

Methodologies for Creating a Golden Copy

Summary Comparison

METHODOLOGY	INLINE SCAN	SANDBOX	SNAPSHOT ANALYSIS
Representative Product	**Asigra Cloud Backup**	**Dell EMC Avamar**	**Rubrik Cloud Data Management**
How It Works	Scans incoming and restored backup data for malware.	Backups complete as normal. Separate IT sandbox set up to recover data and test for malware.	Takes snapshots of production data. Performs analytics on each snapshot. Results of analytics will inform which snapshots to check for the presence of malware.
Timing of Malware Scans	In real time as backups occur. Any time a recovery occurs.	As often as companies determine need to update Golden Copy of backups.	Analytics will inform which snapshots to scan and when.
Key Benefits	• Cybersecurity software part of backup software. • Detects known malware as backups occurs. • Generates alerts if malware detected. • Malware scans part of the backup and recovery processes. • Rechecks data during recovery for new strains of malware.	• Existing backup processes remain intact. • Malware detonated in isolated environment. • Observe how malware works.	• Snapshots of production data complete quickly. • Present snapshots or snapshot clones to scan them for malware. • Performs analytics to finds changes in files b/t snapshots • May more quickly identify the presence of latent or new malware strains
Cautions	• Malware scan incurs ~10% performance overhead on backup server. • Malware scans only take place when backups and recoveries occur. • May still want to build sandbox to test for latent or new unknown strains of malware.	• May need to acquire cybersecurity software. • May need to setup separate processes to scan for malware. • Company must create appropriate IT environment to recover data and test for malware. • Sandbox testing must occur regularly to maintain a viable Golden Copy. • No guarantee that malware, if present, will detonate. • May still need to rescan data prior to recovery to check for latent or new malware strains.	• May need to acquire cybersecurity software. • May need to setup separate processes to scan for malware. • Must be able to present snapshots to cybersecurity software to scan them. • Backup software must work with OS and applications to create snapshots. • May still need to build sandbox to test for latent malware or to test applications for which only backups can be taken. • May still need to rescan snapshots prior to recovering data to check for latent or new malware strains.

Determining the Best Approach to Confidently Recovering

Each of these three techniques has its own set of considerations that a company should understand prior to implementing any of them. In some cases, a company may want to deploy one or more of these techniques to create a Golden Copy of its backups that contains no malware. Based on the current shipping versions of these products, DCIG recommends that companies should give preference to these three methodologies in the following order as this sequence reflects their respective effectiveness in detecting malware as well as their ease of implementation.

1. Inline Scan

Key Benefits

Backup software that uses cybersecurity software to perform inline scans for malware during backups and recoveries, such as Asigra Cloud Backup does, currently provides key benefits over competing approaches. In almost all cases, inline scans represent the easiest and fastest way for a company to scan its backup data for the presence of known strains of malware as well as positions the company to scan recovered data for yet unknown malware signatures.

Scanning all backup data for malware as part of the backup job serves to alert a company to the presence of malware that slipped past its perimeter cybersecurity defenses. By also scanning data during a recovery, it increases the possibility anti-virus software will detect malware signatures that were latent or undetectable when the backup occurred.

Since cybersecurity software constantly gets updated, the latest version may be able to identify malware signatures during restores that an earlier version did not detect when scanning the data at the time of the backup. This approach also enables a company to restore older backups that were created before the cybersecurity software was in place as it scans backup data for malware when and if the data is restored.

This approach brings backup and cybersecurity software together in a single solution representing perhaps the biggest advantage of using inline scans. It eliminates the need for a company to deploy different backup and cybersecurity software products and manage the processes associated with each. Combined, this approach has the net effect of creating a secondary perimeter around a company's backup repositories.

Key Consideration

There is one key consideration that a company should keep in mind as it looks to adopt inline scans as its preferred methodology. There is performance overhead associated with scanning data as part of the backup job. Asigra finds that an anti-virus scan can incur as much as a ten percent performance penalty which can potentially slow backup jobs.

To avoid this performance hit during the backup, a company may opt to only enable this feature when it restores data. Only scanning data when a recovery occurs will still help ensure a company only restores malware-free data. However, a company will miss its earlier opportunity during the backup to detect the presence of known malware signatures.

2. Snapshot Analysis

Key Benefits

Analyzing snapshots of production data, or clones of snapshots, for abnormal or significant changes between the data of multiple snapshots serves as the next easiest and fastest technique to implement to check for the presence of malware. Since snapshots generally occur more frequently than backups, analyzing multiple snapshots for abnormal or significant data changes can be an ongoing process.

To perform this data analysis, Rubrik leverages its Polaris Radar subscription service to analyze snapshots previously taken by its Cloud Data Management software. Polaris Radar starts by examining existing snapshots to create a baseline against which to compare the changes in future snapshots.

It then examines subsequent snapshots of that system for file properties such as file change rates and abnormal sizes and compares those characteristics to the original baseline. Should Polaris Radar detect any statistically significant variances in file behavior from the baseline, it generates an alert.

The key benefit that this approach offers over competing Sandbox approaches is that it positions a company to discover a previously undetected strain of malware in its environment. Once malware such as ransomware activates in a production environment, it may start to delete or encrypt files.

Polaris Radar should detect these file changes when it compares the snapshots from a system. At that point, it can alert a company to the possible presence of malware in its environment, even if a company's internal cybersecurity software may not yet be aware of this strain of malware.

Key Considerations

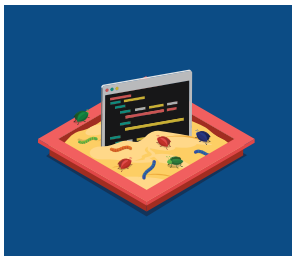
There a few caveats as one considers using snapshot analysis to detect the presence of malware.

First, Polaris Radar only analyzes snapshots for abnormal or significant changes in file activity. It is not cybersecurity software and does not scan snapshots to examine them for the presence of malware. This approach can result in false positives. Systems that legitimately create or modify a lot of files could result in the data analysis software generating an alert that malware may be present and active.

Second, if it generates an alert, a company will still need to scan the snapshot, or a clone or restore of it, for the presence of malware. This will require the company to create a process that first recovers the data in the snapshot and then prompts its anti-virus software to scan the data for the presence of malware.

Third, this approach starts with the premise that the original snapshot of a system is free of malware. The data analysis software compares changes in subsequent snapshots to the original snapshot. But this approach is based on the original snapshot containing no malware. If the original system snapshot contains malware, it is uncertain if analyzing subsequent snapshots from that system will detect the malware present in the original snapshot.

Fourth, there is a performance hit associated with doing the data analysis of the snapshots. Rubrik's Polaris Radar does takes steps to mitigate the performance overhead associated with analyzing the different snapshots. Exactly how many CPU and memory cycles it incurs will vary. One should assume that the greater number of file changes between system snapshots, the more overhead it will create.



3. Sandbox

Key Benefits

There are three key benefits associated with using a sandbox to detect malware and create a Golden Copy backup.

First, there are no limits associated with the applications, files, or operating systems that can be examined for malware in a sandbox. If data can be recovered in the sandbox, it can be tested or scanned for malware. This minimizes the dependency on the backup and snapshot software used to support the application or operating system in order to analyze or scan the data for malware.

Second, all the analysis and scanning for malware occurs after the backup job completes and in environments isolated from the production environment. Using this approach, a company's backups and snapshots continue as configured with no new performance overhead introduced at any point in the production environment.

Third, a company can detonate the malware and observe how it works. This approach can potentially catch and identify either known or unknown strains of malware. In either case, once a company knows malware exists and how it works in the sandbox, it can take steps to detect and eradicate the malware from its production environment. Once eradicated, the company can then create a Golden Copy free of malware.

Key Considerations

Listing all the considerations that a company must account for when setting up a sandbox to test for malware goes beyond the scope of this report. The three reasons listed below should inform a company that it should primarily pursue this methodology as a last resort after it concludes that the prior two methodologies are not options for testing for the presence of malware in its backups.

First, it takes expertise, time, and resources to properly set up a sandbox and then test for malware. A company must first set up a sandbox that appropriately mimics its production environment with the cost, difficulty, and time associated with setting up the sandbox varying by company. Only once the sandbox is configured and all data restored can malware testing begin.

The test may be as simple as scanning the data for the presence of malware. Alternatively, it may be a more robust test that allows the malware to detonate so a company can observe its behavior. In any case, an individual or individuals with the right expertise must be available to conduct the tests and then understand and interpret their results.

Second, a time lapse, perhaps significant, may exist between when the company completes its backups and it finishes its sandbox testing. If a company can complete testing for malware within a reasonable amount of time after its backups complete, perhaps within 24 hours to a week, this approach may suffice. In cases where testing takes so long to complete that a company cannot create a Golden Copy in a time frame that meets its Recovery Point Objective (RPO) or it cannot complete testing on a predictable schedule, it renders the point of doing sandbox testing moot.

Third, a company has no guarantee that malware will detonate in its sandbox. Sandbox evasion technology is becoming more prevalent in malware. When a company attempts to detonate any strains of malware that contain this technology, this malware detects it is in a sandbox and does not detonate. If that occurs, it again makes the point of having a sandbox moot.

Key questions a company should ask to determine the best methodology to confidently recover from a malware attack in its environment:

- How much time, effort, and money does the company want to dedicate to creating a Golden Copy for it to confidently recover?

- Which is a higher priority in the company: quickly recovering data and resuming production with minimal impact or understanding how different strains of malware works?
- Is any performance overhead associated with analyzing backup data for malware during the backup or restore job acceptable? If so, how much?
- What is the company's RPO for data recovery? Does the methodology currently employed to create the current Golden Copy satisfy that RPO?

Automation and Simplification Key Attributes to Ongoing Malware Detection and Prevention

At no time can a company let its guard down when it comes time to detecting and preventing the presence of malware in its environment. Due to the many strains of malware and their constantly changing nature, automation and simplicity are key attributes for a company to incorporate into its processes to detect and prevent malware from infecting its data. A company should only employ manual processes to check for the presence of malware in its environment as a last resort.

The products that Asigra, Dell EMC, and Rubrik offer, and the respective techniques they use to detect the presence of malware in backup repositories, represent the primary methodologies that backup software employs. Of these three, only Asigra and Rubrik provide a company with the means to automate and simplify the process to detect for malware in backups. Of those two, only Asigra currently makes cybersecurity software available as an optional feature that a company can turn on.

Once a company enables this feature in Asigra Cloud Backup, Asigra will automatically scan the data for known malware signatures when the backup occurs. It then scans the data again for malware signatures when a company recovers the data to check for any malware that was unknown by the cybersecurity software at the time of the original backup.

The two competing products from Dell EMC and Rubrik cannot yet natively perform these tasks. The foundation certainly exists for Dell EMC to introduce it should it desire to do so. RSA Security already operates as a division of Dell EMC. Should Dell EMC deem it appropriate, it could make RSA Security's NetWitness Platform an optional feature in one or more of Dell EMC's various data protection products to automatically scan data for malware during backup and recovery. However, a company must currently set up and

Secure the Backups

Regardless of the methodology that a company employs to do backups and then create a Golden Copy from them, it needs to take additional steps to secure this data once created. Since hackers may employ multiple techniques within their malware to compromise, delete, or encrypt this data, there are three additional steps that companies should minimally take to ideally keep both the backups and the Golden Copy safe from malware's reach.

#1—Store the Data in an Immutable Format

Once backups complete or a Golden Copy is created, a company will want to ensure that malware cannot delete or modify this data in any way. All three products examined provide various options to store backup data and the Golden Copy in an immutable format.

A company may configure Asigra to backup and store data in an immutable format in at least three ways. It can store data on disk that is inaccessible over network shares. It can port data to tape. Alternatively, it can store data on shared network folders with random folder names other than the default "/bak" or "/backup" folder names that more sophisticated strains of malware may know about and actively seek out when they detonate. Using folders with randomly created names mitigates the possibility of malware finding the backup data in them.

Asigra also builds multi factor authentication into its Cloud Backup application. If anyone or any program attempts to delete all backup copies, it requires multiple people to authenticate and grant permission for the deletions to occur. This methodology prohibits a single user or program from deleting backup copies, even if that user has elevated privileges.

Dell EMC offers quite a few methods to keep data immutable depending on which of its backup solutions a company uses. If a company uses Avamar, it can turn on its data migration enabler to migrate data to tape. If a company uses Dell EMC Networker, it already native supports tape. If a company uses Dell EMC Data Domain, a company may use its WORM (Write Once Read Many) feature that is available via its Retention Lock Software or a company may opt to copy or migrate data to a public cloud provider and then turn on the WORM functionality available in the cloud.

Rubrik takes any guesswork out of data immutability by immediately making its snapshots inaccessible as soon as it takes one. Further, it never presents the original snapshots to any host. Rather, it creates a clone of the snapshot and presents that to use for testing or recovery. Even if malware does successfully

Continued on next page

Creating a Secondary Perimeter to Detect Malware in Your Enterprise Backup Environment:
A Comparison of How Backup Solutions from Asigra, Dell EMC, and Rubrik Detect and Respond to Malware Attacks

manage a sandbox to scan for malware or test for the presence of malware in their data.

Rubrik's Cloud Data Management and Polaris Radar subscription offerings do come closer to this ideal of automating the process of detecting malware in backups as Polaris Radar will automatically analyze the data in snapshots taken by Rubrik Cloud Data Management.

However, its data analysis does not currently include any native cybersecurity software that would automatically scan and alert to the presence of malware in its snapshots. It only detects anomalies or significant changes in data and its content between snapshots. To conclusively determine if malware exists in its snapshots may still require a company to use third party cybersecurity software to examine the data or build a sandbox to test for malware.

Creating a Secondary Perimeter to Detect Malware Becoming Table Stakes in Enterprise Backup Software

Companies need to have a high degree of confidence that the data in their backup repositories remains free of malware in order to recover from a malware attack in their production environment. That can only happen if companies acquire the appropriate cybersecurity technologies that check for malware, put the needed processes in place to scan for it, and then strictly follow these processes. Any other approach leaves gaps in their ability to quickly identify the presence of malware in their environment and respond to it in a timely manner.

This explains why companies such as Asigra, Dell EMC, and Rubrik each promote their respective methodologies to

Secure the Backups *Continued from previous page*

encrypt or delete a clone, the original snapshot remains inaccessible and unchanged.

The only potential challenge with Rubrik's approach may be found in the permissions it grants to end users to delete snapshots. It is currently unclear how Rubrik manages snapshot deletion, though snapshots are likely deleted once each snapshot reaches the end of the retention policy associated with it. However, the need to override these polices may become paramount if it is discovered that an original snapshot contains a strain of malware that was previously undetected or unknown.

#2—Authenticate Users and Changes to Data

Malware does not necessarily need to find a back door into a company to access its backups. The best and easiest way to compromise its backups may be through the front door. Recent strains of malware have begun to use APIs to access backup software as well as attempting to guess, steal, or, in some fashion, obtain a user name and password to login into the backup application itself.

A company will want to ensure that the individuals administering the backup software and performing tasks such as job scheduling, data recoveries, data placement, and data deletion, among others, have the authority to do so. To help mitigate the possibility of a hacker using malware to access the backup application to compromise backups, enable multi-factor authentication on backup applications and require two or more people to approve any changes or deletions of existing backups.

#3—Send Malware Alerts to Both Backup and Security Admins

Knowing that malware has a presence inside a company is a key first step to take to prevent it from spreading. Yet too often a company may not configure its front of house cybersecurity software such as anti-virus and firewall software to notify backup administrators that is has detected the presence of malware on corporate servers. By failing to notify backup administrators of its presence, backups containing malware may occur.

No matter what software a company uses to scan for malware or where these scans for malware occur (on production data or backup copies,) a company should make provisions to alert both backup and security administrators if malware is detected. As backup software is now a known attack vector, a company's security team or its MSP should be monitoring it in addition to its other perimeter attack vectors. In this way, both sets of individuals can take the appropriate steps to stop malware's spread and remove it from the environment for which they are responsible.

detect malware in backup repositories. They recognize that the ability to detect the presence of malware in backups will soon become a table stakes feature included in enterprise backup software.

Of these three, only Asigra currently offers cybersecurity software as a native feature in its Cloud Backup software that scans data both as it backs the data up and when it recovers data. This approach gives companies, to include MSPs who frequently protect small and midsize businesses, the opportunity to introduce and implement malware detection into their backup environment with little to no extra time, effort, or resources.

More importantly, it gives companies the means to automatically and simply create a secondary perimeter to detect for the presence of malware in their data. While companies should by no means abandon their first line defenses such as anti-virus software and firewalls in their fight against malware, these first lines of defense have their limitations.

By integrating cybersecurity software with backup software such as Asigra has done in its Cloud Backup software, companies can have a higher degree that their most important data—the data they deem worthy of being regularly backed up—has an extra layer of protection around it. In this way, should malware ever penetrate their perimeter defenses and compromise their production data, they can have a high degree of confidence that they can quickly and successfully recover from a malware attack. ■

DCIG
DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552
dcig.com