DCIG

DCIG Top 5
SME Anti-ransomware Backup Solutions

by Jerome Wendt, DCIG President & Founder

SME ANTI-RANSOMWARE BACKUP SOLUTION INCLUSION CRITERIA

- Can detect, prevent, and/or recover from a ransomware attack
- Meets backup and recovery requirements of small and midsized enterprises (SMEs)
- Solution is shipping and available by February 1, 2020
- Information available for DCIG to make an informed, defensible decision

SOLUTIONS EVALUATED

- Acronis Cyber Protect
- Altaro VMBackup
- Arcserve Unifed Data Protection (UDP)
- Asigra Cloud Backup
- Barracuda Backup
- HYCU
- Infrascale Disaster Recovery
- Quest NetVault Plus
- Quest Rapid Recovery
- Quorum OnQ
- StorageCraft OneXafe
- Vembu BDR Suite
- Veritas Backup Exec

SOLUTION FEATURES EVALUATED

- Configuration, licensing, and pricing
- Backup capabilities
- Recovery and replication capabilities
- Anti-ransomware capabilities
- Support

Ransomware: A Clear and Present Danger

Expectations as to the features that a small and midsize enterprise (SME) backup solution *"must"* offer often come about due to technology advancements. Backup appliances, backup-as-a-service (BaaS), cloud connectivity, deduplication, and hyperconverged appliances represent recent advancements that many SME backup solutions now possess. As we enter the 2020's, this has, for the moment, changed. Ransomware, a type of malware, represents an external force driving much of the current innovation occurring in SME backup solutions.

Ransomware represents a clear and present danger against which all SMEs must defend. The latest strains of ransomware increasingly target SMEs in hopes of scoring large paydays with hefty ransoms. Ransom requests often come in at $1M US dollars that must be paid in short timeframes.

While cybersecurity software is the best means to detect and prevent ransomware, it cannot identify every form of it. Here is where SME backup solutions enter the scene. Using these solutions, SMEs may create a secondary perimeter around their backup data. The various features these solutions offer can help to detect, protect, and recover from ransomware attacks.

Legacy Backup Features, New Relevance

All SME backup solutions, by default, offer some means of protection against ransomware. They collectively make copies of production data and store it somewhere else—the cloud, network drives, and/or direct attached storage. These copies of production data ensure some level of protection against ransomware and generally provide a means to recover.

Further, many of these solutions support removable media, such as disk or tape. Removing the media creates an air gap that ransomware cannot bridge. This air gap serves to protect the data from a ransomware attack.

Top 5 SME Anti-ransomware Backup Solutions*

Acronis Cyber Protect
Arcserve UDP
Asigra Cloud Backup
Quest NetVault Plus
StorageCraft OneXafe, ShadowXafe, and Cloud

**Listed in Alphabetical Order*

Those that integrate with Microsoft Active Directory (AD) to authenticate user logins also helps repel ransomware attacks. Some ransomware strains, such as DoppelPaymer, target backup software and attempt to log into it using an admin login and password.

Once logged in, these strains seek to compromise existing backups in at least two ways. They may simply delete or corrupt the backups. Alternatively, they may copy the data and send it to the hacker. The hacker may then threaten to release and publish the data unless the SME pays the hacker a ransom. Using backup software integration with directory services such as LDAP or Microsoft AD, SMEs can more easily implement and manage more sophisticated logins and passwords. They can then use these to better deter ransomware attacks against the backup software itself.

Next Gen Anti-ransomware Features

While legacy features help SMEs respond to ransomware's threats, they only go so far. New technologies exist that better equip organizations to detect, prevent, and recover from

ransomware attacks. These next gen features complement, rather than replace, the legacy approaches in defeating ransomware. Some of these next gen features include:

1. ***Storing data in immutable object stores.*** Immutable object stores may reside in multiple locations. These include on-premises, in general-purpose clouds, purpose-built clouds, or any combination thereof. Using an immutable object store, once data is written to it, the data cannot be erased though it may be overwritten.

   This occurs if the ransomware finds the object store and encrypts the data in it. However, if ransomware does encrypt it, one may configure the object store to retain older, previous versions of the data. In this way, one can recover and restore earlier versions of the data.

2. ***Integration with cybersecurity software.*** A backup solution's integration with cybersecurity software may occur in at least two ways. Some backup solutions partner with cybersecurity software providers to help SMEs better secure their endpoint devices from ransomware attacks. Others integrate cybersecurity software into their offering to scan backup data for ransomware and alert to its presence. In both cases, the cybersecurity software helps SMEs detect and defeat ransomware before it detonates, which is always preferable.

3. ***Artificial intelligence (AI) and machine learning (ML) algorithms.*** Using AI or ML, each scans production and/or backup data and looks for abnormal change rates or unexpected changes to it. Detecting these changes can help alert SMEs to the possible presence of ransomware in their environment.

   Of these three next-gen technologies, AI and ML are perhaps the most immature. Currently, they cannot conclusively determine if ransomware resides in the data. Expect significant advancements in this technology in the coming years. For example, they may more tightly integrate with cybersecurity software to better determine if suspicious data does, in fact, contain ransomware.

Distinguishing Features of SME Anti-ransomware Backup Solutions

DCIG identified over 50 solutions in the marketplace that offer backup capabilities for all size organizations. Of these 50, DCIG identified and classified thirteen of them as meeting DCIG's definition of an SME anti-ransomware backup solution. These thirteen solutions target SME environments based on their documentation. Attributes that distinguish SME solutions from those targeted at large enterprises include support for one or more of the following:

- ***Protect the most common hypervisors and operating systems.*** SME backup solutions support the most common hypervisors and operating systems. They offer support for the Microsoft Hyper-V and VMware vSphere hypervisors and the Linux and Windows operating systems. While these solutions may support other hypervisors (Citrix XenServer, Linux KVM) or versions of UNIX, view support for them as the exception, not the rule.
- ***Primarily protect Microsoft applications.*** These solutions all protect Microsoft applications that SMEs commonly use. These offer support for Active Directory (AD), Exchange, SharePoint, and SQL Server.
- ***Store and manage data on disk.*** These solutions all minimally store and manage backup data on disk-based media such as direct and network storage. A few of these solutions targeted at SMEs came to market in the last ten years. During this time, the demand by SMEs to back up data to removable media (tape or otherwise) dropped. This mitigated the need for more recently released products to offer this functionality.
- ***Offer one or more native data reduction technologies.*** Since all these solutions back up data to disk, they also all offer one or more data reduction technologies. They minimally all offer compression and some form of deduplication. The methods of deduplication each solution offers, and the number of methods offered, do vary by solution. They may offer client–side, media server-based, and perhaps even target-based deduplication options.
- ***Leverage OS- and hypervisor-based snapshot technologies.*** To provide fast backup with minimal application disruption, they each leverage the snapshot technologies natively available from Microsoft and VMware. In performing these backups, by default they each do incremental backups after first doing a full backup.

Similarities Between the Top 5 SME Anti-ransomware Backup Solutions

In addition to the features listed above that all SME anti-ransomware backup solutions generally share, the Top 5 SME solutions have the following anti-ransomware traits in common. They include:

- ***Option to use Linux to host the backup software.*** The Linux OS often gets mentioned as an effective means to deter ransomware attacks on the backup solution itself. All these solutions give SMEs the option to use Linux to host their respective backup software.
- ***Multiple options to secure and validate user logins.*** The latest strains of ransomware, such as DoppelPayer, specifically target and seek to access the backup software. They attempt to access it to compromise, delete, or encrypt existing backups. Each backup solution offers SMEs multiple options to authenticate user logins and validate changes to existing backups. These options may include using complex passwords, two-factor authentication, and integration with directory services.
- ***Making backup data inaccessible to other applications.*** More strains of ransomware now specifically target SMEs. As part of their attack methodology, the ransomware seeks out and encrypts backup files and folders located on network attached devices. To mitigate this type of ransomware attack, all Top 5 solutions make their backup files and folders inaccessible.

The Top 5 SME solutions also all support the following data protection traits, to include:

- The option to license their software per protected server
- Flexibility to change to more favorable software licensing models
- Host their software on either Linux or Windows operating systems
- Protect Linux and Windows network file servers
- Protection for Microsoft 365 (formerly Office 365)

- S3-compatible public cloud backup targets
- Alerting and pro-active restart of failed backup jobs
- Encrypting data at-rest and in-flight
- Bare metal recoveries
- Automating the conversion of VMs

Differences between the Top 5 SME Anti-ransomware Backup Solutions

The Top 5 solutions differ in how they detect, prevent, and recover from ransomware in the following ways:

- ***Detection.*** A few of the solutions use one or both of these two techniques to detect ransomware in backup and production data:
  - ***Integrated anti-malware software*** that scans backup data for the presence of ransomware. This software may scan backups for ransomware as the backup occurs or during a recovery.
  - ***Predictive analytics*** uses artificial intelligence (AI) or machine learning (ML) algorithms to scan data for ransomware. The solution may monitor backup data, production data, or both for changes to the data.

  In both cases, if they detect changes to the data, they alert the SME to the possible presence of ransomware in their environment.
- ***Alerting and notification.*** All five solutions generate notifications if they detect errors or failures when a backup job occurs. Beyond that, they differ significantly in their respective alerting and notification capabilities. This functionality takes on added importance in respect to ransomware. The sooner an SME becomes aware an issue exists, the more quickly it can respond to it.

  For instance, only four Top 5 solutions can detect new virtual machines and proactively schedule backup jobs on them. Without this option, an SME must manually identify and schedule backups on new VMs.

  Only two solutions monitor for and generate alerts if changes or deletions occur in the backup vault. Only one solution can identify and report on other applications that attempt to access and modify their backup vaults. Absent these alerting abilities, the latest ransomware strains may access backup software and encrypt or delete backups without anyone's knowledge.
- ***Multiple deployment options for their solution.*** Some deployment options provide a better defense against ransomware than others. For instance, hosting the backup solution in the cloud or on a hardened physical or virtual appliance can help repel a ransomware attack. These techniques make it more difficult for the ransomware to access and compromise the solution.

  Each solution offers multiple ways for SMEs to deploy it, though none of the solutions offer all the same deployment options. Available deployment options include as a physical or virtual backup appliance, software only, an on-premises software-as-a-service (SaaS), a cloud-based SaaS, or a converged or hyperconverged infrastructure solution.
- ***User login and password management.*** The newest forms of ransomware increasingly target SMEs in hopes of scoring larger paydays. As they do so, these strains may seek to access the backup solutions these SMEs use by logging into them. Minimally, they may use a backup solution's default admin login and password to gain access to it.

  To help repel these attacks, these Top 5 backup solutions offer multiple, but differing, options to create complex user login and passwords combinations. Two solutions give SMEs the option to create a new, specific admin login during setup. Three give SMEs the option to choose and enforce complex admin passwords. Four give SMEs the option to integrate with their existing security infrastructure, such as Microsoft Active Directory (AD).

These solutions also differ in how they deliver on the following data protection traits:

- ***Breadth of hypervisor support.*** The Top 5 solutions differ in their support for hypervisors other than Microsoft HyperV and VMware vSpheere. Only two solutions support Citrix XenServer, Linux KVM, Red Hat Enterprise Virtualization (RHEV), and the Nutanix Acropolis Hypervisor (AHV).
- ***Availability and structure of purpose-built clouds.*** SMEs may want or need the option to recover data or perform disaster recovery in the cloud. They will find more options to do cloud recoveries using these solutions than those targeted at large enterprises. While four of the five solutions offer purpose-built clouds, their respective clouds differ in their respective features and service offerings.
- ***Microsoft 365 data protection.*** All these solutions offer options to protect data residing in Microsoft 365. However, the methods they each use to protect Microsoft 365 data may vary significantly.

Top 5 SME Anti-ransomware Backup Solution Profiles

Each of the Top 5 Anti-ransomware Backup Solution profiles highlights three or more ways each one differentiates itself. These differentiators represent some of the best methods that backup solutions offer to detect, prevent, and recover from ransomware. Within each solution, SMEs will find distinctive features that may better meet their respective needs.

Acronis Cyber Protect

Over the last few years Acronis has largely re-invented itself. This re-invention was motivated, in part, by a realization that it needed to more tightly align backup and cybersecurity software. This foresight led to the development and release of its flagship Cyber Protect software with its Active Protection technology. Three features that help distinguish Acronis Cyber Protect from competitive offerings include:

- ***AI infused backup agent.*** Cyber Protect incorporates artificial intelligence (AI) into the agent that it uses to perform backup and recoveries. It performs real time monitoring and collects data on the I/O's occurring on each machine's system. It compares this data to activities and patterns typically seen in ransomware.

  If it detects a process attempting to encrypt data or inject malicious code, its Active Protection technology stops the process. It notifies an admin who then determines whether to block the

process (blacklist it) or allow it to continue (whitelist it.) In the event the process alters or encrypts some files before Cyber Protect halts it, Cyber Protect automatically restores them.

For Windows users restoring files from the Acronis cloud, Cyber Protect can go one step further. During the restore, an agent in the Acronis cloud can scan each restored file to verify it contains no malware.

- ***Purpose-built cloud for backup and DR.*** Acronis offers a cloud purpose-built for backup and disaster recovery (DR). Used in conjunction with Cyber Protect, an SME may back up and store backups both locally and in the Acronis Cloud. Fully integrated into Cyber Protect, an SME should find storing and retrieving data from the Acronis Cloud a seamless experience.

  The Acronis Cloud data centers meet and exceed the security and safety requirements that most SMEs expect and want. Acronis' 14+ data centers meet ISO 9001, PCI DSS, Tier II, and HIPAA standards, among others, to give SMEs increased confidence to store and recover data in them. This cloud gives SMEs access to Acronis resources (compute, storage, staff, etc.) should they need to quickly perform an offsite DR as a result of a ransomware attack.

- ***Integrated anti-malware, backup, and web protection.*** Acronis Cyber Protect delivers both cybersecurity and data protection software in one integrated solution deploying it as a single agent. Using this agent, Cyber Protect can do URL filtering to help prevent malicious file downloads and block access to suspicious web resources. Any files it identifies as suspicious it quarantines which an SME may delete or recover. Acronis Cyber Protect also equips SMEs to centrally manage Microsoft's native Security Essential and Windows Defender Antivirus applications.

Arcserve Unified Data Protection (UDP)

Arcserve represents one of the two Top 5 SME anti-ransomware backup solution providers that partner with a cybersecurity software provider. Arcserve's partnership with Sophos accomplishes two objectives. Arcserve remains focused on its core backup and recovery competencies while Sophos does the same with its cybersecurity offering. This partnership, combined with Arcserve's native UDP offering, helps distinguish Arcserve from its competitors in the three following ways.

- ***An integrated backup and endpoint data protection appliance.*** The Arcserve Appliances equip SMEs to consolidate their cybersecurity and data protection software on one appliance. The embedded Sophos Intercept X Advanced for Server endpoint protection includes key technologies that prevent ransomware from initially gaining a foothold. Intercept X offers signature-based and signatureless malware detection algorithms to stop ransomware from executing.

  Should ransomware somehow slip past this perimeter and detonate, the embedded UDP software provides multiple options to swift recovery. These include instant VM restores, local and remote virtual standby, granular restores, and full bare metal recovery to same or dissimilar hardware.

- ***Direct-to-cloud backup***. Arcserve's purpose-built cloud, Arcserve Cloud, differentiates itself with its Cloud Direct offering, a direct-to-cloud backup and DRaaS solution. This frees SMEs to back up directly to the Arcserve Cloud without first need ing to cache data on local storage.

  SMEs minimally derive two important benefits from this feature when using it to protect and recover from ransomware. First, by storing backups in Arcserve's purpose-built cloud, it protects the backups from a ransomware attack. Should an SME experience a ransomware attack, the ransomware will not be able to access these backups residing off-premises. Second, the Arcserve Cloud supports VM restores for disaster recovery. An SME may use the Arcserve Cloud to host a recovery and quickly bring an application back online.

- ***Integrated business continuity.*** SMEs can use Sophos to protect their data from ransomware and the Arcserve appliance or cloud to safely store and recover it. The challenge becomes orchestrating a coordinated, integrated recovery for multiple applications across different locations.

  Arcserve delivers on this more robust SME requirement with its UDP Cloud Hybrid offering. This service offering equips SMEs to centralize and manage recoveries of their applications on-premises or in the cloud, Arcserve or otherwise. SMEs can have critical applications running on virtual standby in the cloud with failover and failback capabilities. Further, they can confirm they can meet any service level agreements (SLAs) through automated DR testing and application recoveries.

Asigra Cloud Backup

Asigra Cloud Backup partners with a few independent cybersecurity software providers to detect and protect backup data from ransomware attacks. Asigra combines the cybersecurity software engines' features with its own native data protection features to provide a comprehensive anti-ransomware solution. Three distinctive anti-ransomware features that Asigra Cloud Backup offers include:

- ***Bi-directional malware detection.*** Using Asigra Cloud Backup, SMEs may scan backups for ransomware when they backup data, when they recover it, or both. Asigra Cloud Backup leverages the embedded cybersecurity software to scan data for ransomware when it is backed up or recovered.

  Scanning during backups helps detect ransomware that peripherally focused anti-malware software may have missed. Scanning during recoveries helps detect strains of ransomware that were unknown (zero-day) at the time of their initial backups. SMEs have the option to turn these scans on or off as they do incur some overhead.

- ***Variable file and folder naming.*** Some strains of ransomware specifically target backup solutions and the backups they create. As part of these attacks, it scans network drives. During the scan, the ransomware looks for specific folder names or file extensions (such as a ".bak" extension) created by backup software. If discovered, the ransomware deletes or encrypts this data to hinder or defeat attempts at recovery.

  Asigra Cloud Backup counters these ransomware attacks by providing the option for SMEs to configure it to create randomly generated file and folder names. This tactic prevents ransomware from easily detecting or compromising Asigra backups stored on the network.

- ***Alerts all concerned parties.*** When Asigra detects ransomware during a backup or recovery, SMEs may optionally configure it to alert anyone. Due to the pervasive threat that ransomware poses, backup software should ideally alert more than just backup administrators to its presence. Asigra Cloud Backup may alert server admins, security admins, or any individuals who need to know about ransomware's presence.

Asigra Cloud Backup further distinguishes itself with its *"most favorable"* pricing model. SMEs often must choose how they license software at the worst possible time: when they acquire it. At that time, an SME may not know which licensing option is best or needs flexibility to change later.

Asigra addresses these concerns. Asigra monthly evaluates how the SME utilizes its software. It then automatically applies the best licensing metric (i.e. - most economical) for the SME.

Quest NetVault Plus

Quest NetVault Plus encapsulates two Quest software products, NetVault backup and QoreStor deduplication, into one solution. This solution equips SMEs with backup software along with the flexibility to convert any storage into a deduplication target. The NetVault Plus solution differentiates itself from the Top 5 competitive solutions in the following three ways:

- ***Option to use NetVault-specific login and password.*** Many backup software solutions integrate with Microsoft AD. They offer this integration to simplify user and password management and ensure secure logins to their application. Unfortunately, a few ransomware strains, such as Samas, target Active Directory and seek to assume AD group and user identities.

  NetVault gives SMEs the option to create NetVault-specific logins and passwords to mitigate these attacks. Within NetVault SMEs may create a policy to enforce the creation of complex logins, complex passwords, or both. NetVault then manages these logins and passwords separately from AD. In this way, if ransomware somehow compromises an SME's AD, it cannot access NetVault vis-à-vis AD.
- ***Offers proprietary protocol to securely communicate with QoreStor.*** Many backup software solutions use industry standard network storage protocols to communicate with their storage targets. NetVault supports these protocols as well.

  However, NetVault differs in one important way: it offers its proprietary Rapid Data Access (RDA) protocol to communicate with QoreStor. Quest initially designed RDA as an alternative to industry standard network storage protocols to deliver improved performance during backups. These performance benefits remain.

  Yet as ransomware has become more pervasive, RDA's proprietary nature provides another layer of defense against ransomware attacks. An SME may configure NetVault and QoreStor to only use RDA to communicate with one another. This makes backups stored on QoreStor essentially invisible since no known instances of ransomware support the RDA protocol.
- ***Separate NetVault authentication for QoreStor.*** As part of using the RDA protocol, NetVault uses a separate, distinct login and password to access QoreStor. This addresses the situation where ransomware perchance gains access to NetVault. Should this occur, the ransomware would still need the login and password to access QoreStor using the RDA protocol.

StorageCraft OneXafe, ShadowXafe, and Cloud

StorageCraft brings together its OneXafe appliance, ShadowXafe backup software, and Cloud to create this Top 5 solution. Using StorageCraft, SMEs may do backups, treat it as a storage target, and perform multiple types of recoveries. The StorageCraft solution differentiates itself from the other Top 5 competitive solutions in the following three ways:

- ***Heterogenous storage target with continuous immutable snapshots.*** OneXafe's ability to present itself a storage target to multiple applications distinguishes it from other Top 5 solutions. OneXafe supports standard file networking protocols (SMB and NFS). These free SMEs to deploy OneXafe in multiple ways, including as both a network file server and a backup target.

  Regardless of which application stores data on OneXafe, one may use its continuous immutable snapshot feature to protect this data. This feature takes a snapshot of data every 90 seconds. OneXafe then retains each of these snapshots in an immutable format.

  Stored this way, an SME may recover its data even if ransomware detonates and encrypts files on the OneXafe appliance. Using OneXafe as its common storage repository, an SME may recover data for any application that stores data on it.
- ***Non-disruptive instant recoveries.*** SMEs that opt to use ShadowXafe for backups and OneXafe as their backup target may also perform non-disruptive instant recoveries. Other Top 5 solutions also offer instant recoveries to accelerate recoveries from ransomware attacks. However, StorageCraft includes the technology to do so non-disruptively.

  ShadowXafe uses its proprietary VirtualBoot technology to initiate an application recovery on OneXafe. During an instant recovery, VirtualBoot initially boots the VM using OneXafe as the source. Once booted, VirtualBoot then transparently moves the VM's data back to the production storage even as the VM is running. Other instant recovery methods do something similar. However, they tend to rely on storage vMotion to complete the recovery on production storage which may require application downtime.
- ***Orchestrated DRaaS recovery.*** Like other Top 5 solutions optimized for SMEs, StorageCraft also offers its own cloud purpose-built for disaster recovery. Its Cloud Premium option helps distinguish StorageCraft from other cloud offerings. This option gives SMEs complete control over networking settings and permits full virtualization in the StorageCraft Cloud. Using it, they can create customizable VPN configurations and virtualization policies that facilitate seamless failovers in the event of a disaster.

Inclusion and Evaluation Criteria for SME Anti-ransomware Backup Solutions

In this report DCIG specifically focused on SME anti-ransomware backup solutions that possessed the following characteristics. These include:

- Markets or promotes the capabilities of its backup software to enable SMEs to detect ransomware or prevent and/or recover from a ransomware attack

- Markets or promotes its backup software as being appropriate to meet the backup and recovery requirements of SMEs.
- The solution is shipping and available by February 1, 2020
- Information available for DCIG to make an informed, defensible decision

DCIG identified thirteen different solutions that met these inclusion criteria. DCIG evaluated each of these solutions in the following areas:

1. ***Configuration, licensing, and pricing*** evaluate how SMEs may obtain and host the backup solution and the different licensing options it offers.
2. ***Backup capabilities*** evaluate the types of on-premises and cloud applications it protects; the databases, hypervisors and operating systems it protects; and, the backup targets and techniques it supports.
3. ***Recovery and replication capabilities*** look at the on-premises and cloud recovery options it offers, how it manages replications, and the replication features it offers.
4. ***Anti-ransomware capabilities*** evaluate how the solution detects and prevents ransomware; reports on suspected occurrences of ransomware; and, manages and monitors its backup vaults and user logins and activities.
5. ***Support*** evaluates the availability of and means to access the vendor's support staff, the management options it offers, and how well it integrates with third party management solutions.

DCIG Disclosures

Vendors of some of the solutions covered in this DCIG Top 5 report are or have been DCIG clients. This is not to imply that their solutions were given preferential treatment in this report. In that vein, there are some points to keep in mind when considering the information contained in this Top 5 report and its merit.

- No vendor paid DCIG any fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any vendor that its solution would be included in this Top 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a Top 5 designation.
- All research is based upon publicly available information, information provided by the vendor, and/or the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.
- No negative inferences should be drawn against any vendor or solution not covered in this Top 5 report.
- It is a misuse of this Top 5 report to compare solutions included in this report against solutions not included in it.

DCIG wants to emphasize that no vendor was privy to how DCIG weighted individual features. In every case each vendor only found out the rankings of its solution after the analysis was complete. To arrive at the Top 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible..

1. DCIG established which features would be evaluated.
2. The features were grouped into five general categories.
3. A DCIG analyst internally examined the feature data for each solution and completed a survey for it based upon the analyst's own knowledge of the solution and publicly available information.
4. DCIG identified solutions that met DCIG's definition for an SME Anti-ransomware Backup Solution.
5. DCIG weighted each feature to establish a scoring rubric.
6. DCIG evaluated each solution based on information gathered in its survey.
7. Solutions were ranked using standard scoring techniques.

About DCIG

DCIG empowers the IT industry with actionable analysis that equips individuals within organizations to conduct technology assessments. DCIG delivers informed, insightful, third party analysis and commentary on IT technology. DCIG develops commissioned and licensed content in the form of blog entries, executive white papers, podcasts, competitive intelligence reports, webinars, white papers, and videos. More information is available at **www.dcig.com.**