DCIG

DCIG Top 5
Enterprise Anti-ransomware Backup Solutions

by Jerome Wendt, DCIG President & Founder

ENTERPRISE ANTI-RANSOMWARE BACKUP SOLUTION INCLUSION CRITERIA

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

SOLUTIONS EVALUATED

- Asigra Cloud Backup
- Cobalt Iron Compass
- Cohesity DataProtect
- Commvault Complete Backup and Recovery
- Dell EMC Avamar
- Dell EMC NetWorker
- IBM Spectrum Protect
- Micro Focus Data Protector
- Rubrik Cloud Data Management
- Unitrends Backup and Forever Cloud
- Veritas NetBackup

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 an enterprise 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 enterprise 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 many of the innovations currently occurring in enterprise backup solutions.

Ransomware represents a clear and present danger against which all enterprises must defend. The latest strains of ransomware increasingly target enterprises 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 enterprise backup solutions enter the scene. Using these solutions, enterprises may create a secondary perimeter around backup data. The anti-ransomware features these solutions offer can help to detect, protect, and recover from ransomware attacks.

Legacy Backup Features, New Relevance

All enterprise 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 Enterprise Anti-ransomware Backup Solutions*

Asigra Cloud Backup
Cobalt Iron Compass
Commvault Complete Backup and Recovery
Unitrends Backup and Forever Cloud
Veritas NetBackup

**Listed in Alphabetical Order*

Integration 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, it seeks to compromise existing backups in at least two way. It may simply delete or corrupt the backups. Alternatively, it may copy the data and send it to the hacker. The hacker may then threaten to release and publish the data unless the enterprise pays the hacker a ransom. Using backup software integration with directory services such as LDAP or Microsoft AD, enterprises 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 enterprises 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 can be overwritten.

   Overwrites may occur 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 enterprises 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 organizations 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 enterprises 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 advancement in this technology in the coming years. For example, they may more tightly integrate with cybersecurity software to better determine if anomalous data does, in fact, contain ransomware.

Distinguishing Features of Enterprise Anti-ransomware Backup Solutions

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

1. ***Protecting multiple hypervisors and operating systems.*** Enterprise backup solutions support the most common hypervisors and operating systems as well as legacy operating systems. They all support common hypervisors such as Microsoft Hyper-V and VMware vSphere as well as the Linux and Windows operating systems. However, these solutions will support other hypervisors such as Citrix XenServer, KVM, and Red Hat Enterprise Virtualization (RHEV). They will also support various versions of UNIX such as HP-UX, IBM AIX, and Oracle Solaris.

2. ***Protecting databases other than Microsoft SQL Server.*** The other databases each one protects varies by solution. Most will minimally protect Oracle Database and Sybase databases. However, many support IBM DB2 and Informix, MySQL, and MongoDB, among others.

3. ***Offering multiple deployment options.*** Enterprises may deploy the backup solution in one or more of the following, to include: backup appliance, software only, on-premises software-as-a-service (SaaS), cloud-based SaaS, and, as a hyperconverged infrastructure (HCI) solution.

4. ***Storing and managing data in immutable object stores.*** These solutions interface with immutable object stores through standard S3 application programming interfaces (APIs). These object stores may reside in on-premises or off-premises locations such as general-purpose and purpose-built clouds.

5. ***Storing and managing data on removable media.*** These solutions initially stored backup data to removable disk and/or tape to save money. However, storing data on removable media that is removed and stored elsewhere creates an air gap to better protect data from a ransomware attack.

Similarities between the Top 5 Enterprise Anti-ransomware Backup Solutions

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

- ***Multiple deployment options for their solution.*** Some backup solution deployment options provide a better defense against ransomware than others. Hosting the backup solution in the cloud or on a hardened physical or virtual appliance can help repel a ransomware attack. Further, enterprises differ in how they may want to deploy the backup solution in their environment. Enterprises may deploy each Top 5 solution as a cloud service or as a physical or virtual appliance.
- ***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 enterprises 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 enterprises multiple options to authenticate user logins and validate changes to existing backups. These options include two-factor authentication and integration with directory services.
- ***Making backup data inaccessible to other applications.*** More strains of ransomware specifically target enterprise environments. 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 solutions also deliver on the following data protection traits, which include support for:

- Client OSes to include Windows and the most common distributions of Linux and UNIX
- Linux, Windows, and vendor-specific network file servers
- Microsoft Hyper-V, VMware vSphere, and Red Hat Enterprise Virtualization (RHEV) hypervisors
- Microsoft SQL Server, MySQL, Oracle, and PostgreSQL databases
- Backup targets that include block- and file-based disk storage, cloud, and tape
- Data reduction features such as compression and deduplication
- Full, incremental, and differential backups
- Optimizing bandwidth during replication operations

Differences between the Top 5 Enterprise Anti-ransomware Backup Solutions

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

- ***Detection.*** Backup solutions use the following techniques to detect ransomware:
  - ***AI/ML algorithms*** to monitor changes to backup and production data
  - ***Honey pots*** are files planted in the production environment which the backup solution then monitors for changes
  - ***Integrated anti-malware software*** that scans backup data for ransomware
  - ***Sand boxes*** to allow testing the backups for the presence of ransomware

  Each Top 5 backup solution may use none, one, or multiple of these techniques to search for or detect for the presence of ransomware. The more proactive techniques, such as the AI/ML algorithms or the integrated anti-malware software, will detect ransomware more effectively. Conversely, enterprises will find the honey pot and sand box methodologies less disruptive to production operations to implement.
- ***Alerting and notification.*** All five solutions alert and notify if they detect or suspect ransomware may exist in the environment. However, some solutions only notify the solution's administrators while others can notify anyone. They also differ in the granularity of their reporting and how they configure reporting. Some rely on reporting tools that are part of their portfolio but are not native to their backup solution. Once set up and configured, some only alert if ransomware might exist in the environment. Others alert only when they detect ransomware's actual presence.
- ***Remediation.*** Each backup solution responds to a perceived or real detection of ransomware's presence in the environment differently. Some automatically extend the retention period of all backups under management. Others may lock down or quarantine backup files that they identify as infected. Some may take no actions on files at all.

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

- ***Breadth of hypervisor support.*** The backup solutions vary in their levels of integration and support for protecting Citrix XenServer, Linux KVM, and Nutanix AHV.
- ***Replication capabilities and management.*** Some enterprise may need more advanced forms of data replication. The solutions differ in their abilities to replicate backup data in from or out to two or more remote locations.
- ***Integration with cloud-native applications.*** All these solutions offer options to protect data residing in cloud-native applications such as Microsoft Office 365. However, the methods they use to protect these cloud-native applications vary significantly.

Top 5 Enterprise 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, enterprises will find distinctive features that may better meet their respective needs.

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, enterprise anti-ransomware solution. Three distinctive anti-ransomware features that Asigra Cloud Backup offers include:

- ***Bi-directional malware detection.*** Using Asigra Cloud Backup, enterprises 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. Enterprises have the option to turn these scans on or off as the scans do incur some overhead.
- ***Variable file and folder naming.*** Some strains of ransomware specifically target enterprise backup solutions and the backups they create. As part of these attacks, it scans network drives. During the scan, it looks for specific folder names or file extensions (such as ".bak") created by the backup software. If discovered, the ransomware may attempt to delete or encrypt this data to hinder or defeat attempts at recovery.

Asigra Cloud Backup counters these ransomware attacks by providing the option for 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, enterprises 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. Enterprises often must choose how they license software at the worst possible time: when they acquire it. At that time, enterprises may not know which licensing option is best for them or need flexibility to change later. Asigra addresses these concerns. Asigra monthly evaluates how the enterprise utilizes its software. It then automatically applies which of the licensing metric options is the best fit (i.e. - most economical) for the enterprise.

Cobalt Iron Compass

Founded in 2013, Cobalt Iron Compass provides a remarkably robust enterprise anti-ransomware solution considering its relative newness to the marketplace. Cobalt Iron Compass provides the broader set of core backup and recovery features that enterprises expect and demand. It simultaneously delivers the new set of anti-ransomware features that enterprises want. Three ways that Cobalt Iron differentiates itself from the other Top 5 anti-ransomware solutions include:

- ***Available as a SaaS solution***. Enterprises may choose to host Compass on-premises or with multiple general-purpose cloud providers. Enterprises may choose to host Compass with Alibaba Cloud, Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and the IBM Cloud. Hosted in any of these clouds, enterprises can also take advantage of each cloud's native security features.
- ***Inaccessible backup infrastructure and data.*** Cobalt Iron makes Compass' underlying operating system, backup infrastructure, and data inaccessible. This approach simplifies Compass' administration and mitigates if not eliminates potential points that ransomware may use to attack.

  Cobalt Iron refers to its collection of security features as Compass Cyber Shield. Only Compass software may access its backup files as well as its underlying operating system, backup software and storage. It also encrypts all data in-flight, at-rest, and can store store on WORM media. These technologies mitigate and virtually eliminate any possibility of ransomware compromising backups created by Compass.
- ***Data authentication, validation, and monitoring to check for threats.*** Cobalt Iron Compass distinguishes how it authenticates and validates backup date in at least three ways. Compass first performs checksums and CRCs (cyclic redundancy checks, a specific type of checksum) to catch data transmission and read errors. Once validated, it then compares the newly written data to existing data to check for any anomalies that may indicate the presence of ransomware.

  Finally, Compass constantly monitors the entire backup infrastructure, to include backup data and operations. It looks for any abnormal activity that may indicate the presence of ransomware. During these scans, it creates audit reports and generates notifications that alert to the possibility of a ransomware infection.

Commvault Complete Backup and Recovery

Commvault Complete™ Backup and Recovery represents a long-time stalwart in the enterprise backup market. It has effectively evolved to incorporate cutting-edge anti-ransomware technologies such as AI and ML into its offering. It has supported both cloud and tape technologies for some time that effectively protect data from ransomware attacks. Additionally, Commvault Complete delivers three other technologies that help distinguish it from other anti-ransomware backup solutions. These include:

- ***Data isolation.*** Commvault uses data isolation and air gaps to secure backed up data. Commvault Complete isolates copies of data and can optionally encrypt it, in a FIPS-compliant format. Further, Commvault blocks inbound access to the backup data and only allows restricted outbound access to the source. To secure data communications, Commvault applies end to end encryption, inflight and at rest on the storage device. Commvault can sever device communication automatically by creating an Air Gap.
- ***Application authentication***. To further help repel ransomware attacks, Commvault Complete uses a filter level driver. This filter level driver ensures that only I/O requests originating from Commvault Complete can access backup data. This effectively serves to block any I/O requests from hostile applications, such as ransomware, from accessing any backup data. Commvault further monitors backup data using ML algorithms to alert on anomalous behavior.
- ***User access and data change verification.*** To control access to Complete and validate changes to backup data, Commvault implements multiple features. To first access Complete, enterprises may use: two-factor authentication or integration with third-party authentication services such as LDAP including over SSL/SAML, or both. Once a user accesses Complete, enterprises can opt to also require two-factor authentication for the user to change or delete existing backup data. Commvault again uses ML to detect and identify anomalous events.

Unitrends Backup and Forever Cloud

Unitrends brings its backup appliances, backup software, private cloud, and recovery assurance and testing features together as one offering. Enterprises may use this single solution for backup as well as recovery on- or off-premises.

Its backup software includes artificial intelligence (AI) that helps enterprises analyze the randomness of file changes in backups. Using this feature, enterprises may identify if ransomware resides in their backups and select the best backup to use for restores. Other key features that Unitrends Backup and Forever Cloud offers that help distinguish it include:

- ***Recovery assurance.*** Unitrends stands apart as one of the only providers, Top 5 or otherwise, to formally offer backup testing and verification. Recovery assurance grants enterprises the flexibility to regularly perform testing and verification of their backups.

The backup testing may occur in the Unitrends cloud at any time. This testing gives enterprises the opportunity to scan and check their backups for the presence of ransomware in them. This helps them to proactively identify if ransomware exists in their environment. They may also confirm they have good backups to use in the event they need to perform a recovery. This testing may be performed by either the enterprise's or Unitrends' staff.

- ***Multiple deployment options.*** Hackers increasingly target the OS that enterprises use to host the backup software, with Windows being the most common target. Unitrends largely mitigates this attack vector by hosting its backup software on a Linux system. Unitrends then gives enterprises multiple ways they may deploy its backup software. Enterprises may deploy Unitrends on either a virtual or physical purpose-built backup appliance.
- ***Certified recoveries in the Unitrends Cloud.*** Unitrends' backup software as well as its virtual and physical backup appliances natively integrate with the Unitrends Cloud. While other solutions also integrate with hyperscale and purpose-built clouds, Unitrends differs in an important way. Unitrends can perform recoveries in its cloud on the enterprise's behalf to certify they work. Using this service, enterprises can more regularly test the viability of their backups and have proof their recoveries work. Further, storing data in the Unitrends Cloud creates an air gap that only the Unitrends solution may access and which ransomware cannot.

Veritas NetBackup

Veritas NetBackup represents a widely used enterprise backup solution that offers both native and complementary technologies to detect and recover from ransomware attacks. These include support for multiple cloud and tape interfaces as well as multiple ways to secure user identities and actions. Other technologies and solutions that Veritas NetBackup offers to help enterprises fend off ransomware attacks include:

- ***Hardened NetBackup appliances and secure user profiles.*** The appliance or server that hosts the backup software has become a prime attack vector for ransomware. In this example, the ransomware seeks to compromise the backup server, either its underlying OS or the backup software itself. If the ransomware attack succeeds, it can potentially delete or encrypt the backups.

  To protect NetBackup servers from these attacks, Veritas offers hardened NetBackup appliances. Veritas validates and verifies that no vulnerabilities exist in the appliance's hardware and software when shipped. Veritas regularly updates its appliances as part of its maintenance release cycles. Enterprises may lock these appliances down further by creating stringent user security profiles. These activate Security Technical Implementation Guide (STIG) protocols that harden profiles to align to Defense Information Systems Agency standards.
- ***Backup environment monitoring.*** Veritas offers a set of software tools that observe enterprise environments to help mitigate malware threats. For example, Veritas Information Studio and Data Insight scan for known malware extensions and report on granular data activity, including rename and write interactions. Once infected assets are identified, administrators can take various actions. They may include disabling devices, deleting impacted files and folders, and/or restoring data.
- ***Storing and managing backups in multiple locations.*** Most backup solutions facilitate replication to off-site locations to protect against on-premises ransomware attacks. NetBackup Auto Image Replication (AIR) facilities the management and orchestration of replicating the data off-premises.

  NetBackup AIR supports one-to-one, one-to-many, many-to-one, many-to-many, and cascading replication models between NetBackup domains. Once setup and configured, enterprises can centrally manage the placement of their backup data in any on- or off-premises location. This includes managing the storage of data on air-gapped, immutable cloud, and tape targets.

Inclusion and Evaluation Criteria for Enterprise Anti-ransomware Backup Solutions

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

- Markets or promotes the capabilities of its backup software to enable enterprises 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 large enterprises
- The solution is shipping and available by February 1, 2020
- Information available for DCIG to make an informed, defensible decision

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

1. ***Configuration, licensing, and pricing*** evaluate how enterprises 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 solution was given preferential treatment in this report. In that vein, there are some important facts 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 the vendor only found out the ranking 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 Enterprise 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.**