DCIG

DCIG *Top 5*
SME Anti-ransomware Backup Solution Profile

by Jerome Wendt, DCIG President & Founder

SME 2020-21 DCIG TOP 5 ANTI-RANSOMWARE BACKUP

SOLUTION
Quest NetVault Plus

COMPANY
Quest Software Inc.
4 Polaris Way
Aliso Viejo CA 92656
(800) 306-9329
Quest.com

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 midsize enterprises (SMEs)
- Solution is shipping and available by February 1, 2020
- Information available for DCIG to make an informed, defensible decision

BACKUP SOLUTION FEATURES EVALUATED

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

DISTINGUISHING FEATURES OF QUEST NETVAULT PLUS

- Offers proprietary RDP communication protocol
- Option to use NetVault-specific login and password
- Separate NetVault authentication for QoreStor

Ransomware: A Clear and Present Danger

Expectations as to the features that a small and midsize enterprise (SME) backup solution *"must"* offer often came 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 possess. Ransomware has, for the moment, changed this. It represents an external force driving many innovations occurring in SME backup solutions.

Ransomware presents 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 always stop it. Here is where SME backup solutions enter the scene. Using these solutions, SMEs may create a secondary defensive perimeter. 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.

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

Integration with Microsoft Active Directory (AD) to authenticate user logins also helps repel ransomware attacks. AD integration helps to create more formidable login barriers that ransomware frequently cannot overcome.

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. Next gen features complement, rather than replace, legacy approaches in defeating ransomware. A few 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 original data cannot be erased or encrypted by ransomware.

2. ***Integration with cybersecurity software.*** A backup solution may integrate with cybersecurity software in at least two ways. Some 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.

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 help alert SMEs to the possible presence of ransomware in their environment.

DCIG: Empowering the IT industry with actionable analysis.™

Distinguishing Features of SME Anti-ransomware Backup Solutions

DCIG identified over 50 solutions in the marketplace that offer backup capabilities for businesses and enterprises. Of these 50, DCIG identified and classified thirteen of them as meeting DCIG's definition of an SME anti-ransomware backup solution. Attributes that distinguish SME backup solutions from those targeted at large enterprises include support for the following:

1. ***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 or versions of UNIX, support for them is the exception, not the rule.
2. ***Primarily protect Microsoft applications.*** These solutions all protect commonly used Microsoft applications. They support Active Directory (AD), Exchange, SharePoint, and SQL Server.
3. ***Store and manage data on disk.*** These solutions all store and manage backup data on direct and network-attached disk storage. In the last ten years the demand for these solutions to back up data to removable media (tape or otherwise) has abated.
4. ***Offer one or more means to perform data reduction.*** Since all these solutions back up to disk, they all offer one or more data reduction technologies. They minimally offer compression and some form of deduplication. The methods of deduplication each solution offers, and the number of methods offered, vary by solution. They may offer client-side, media server-based, and perhaps even target-based deduplication.

SME Anti-ransomware Backup Solution Profile

Quest NetVault Plus

Upon DCIG's completion of reviewing the multiple, available SME anti-ransomware solutions, DCIG ranked Quest NetVault Plus as a Top 5 solution. 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. ■

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 custom 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.**