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
Acronis Cyber Protect

COMPANY
Acronis
1 Van de Graaff Drive #301
Burlington, MA 01803
(781) 782-9000
Acronis.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 ACRONIS CYBER PROTECT

- AI infused agent
- Anti-malware and web protection
- Purpose-built cloud for backup and recovery
- Can create organization specific whitelists
- Scans backup data in Acronis cloud for ransomware
- Safe recoveries by applying latest anti-malware defintions

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

Acronis Cyber Protect

Upon DCIG's completion of reviewing the multiple, available SME anti-ransomware solutions, DCIG ranked Acronis Cyber Protect as a Top 5 solution. Over the last few years Acronis has largely re-invented itself. This re-invention entailed Acronis more tightly aligning its backup and cybersecurity software. This 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 its agent that performs 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 goes even further. 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 locally and in the Acronis Cloud. Fully integrated into Cyber Protect, an SME will find storing and retrieving data from the Acronis Cloud a seamless experience.

  Acronis Cloud data centers meet and exceed the security and safety requirements that SMEs expect and want. Its 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.
- ***Anti-malware and web protection.*** Acronis Cyber Protect delivers cybersecurity and data protection software in one integrated solution deployed as a single agent. Using it, 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. ■

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.**