A Comparison of How Acronis Cyber Protect Cloud and StorageCraft Cloud Services Meet MSPs' Baseline BCDR and Cybersecurity Needs

by DCIG President & Founder, Jerome M Wendt

PRODUCTS

Acronis Cyber Protect Cloud

URL ▶ **https://www.acronis.com/en-us/products/cloud/cyber-protect/**

Acronis International, GmbH
1 Van de Graaf Drive, Suite 301
Burlington, MA 01803
(781) 791-4486

StorageCraft Cloud Services

URL ▶ **https://www.storagecraft.com/products/cloud-services**

StorageCraft, an Arcserve Company
380 Data Drive, Suite 300
Draper, UT 84020
(801) 545-4700

COMPARISON USE CASE

MSPs that need a single, integrated data protection and cybersecurity solution to provide their clients with business resilience.

Data Protection's New Mandates

Managed service providers (MSPs) already recognize they must offer robust solutions to protect the diverse environments their clients possess. However, MSPs cannot rest on their laurels. New data protection mandates have emerged with organizations redefining data protection to meet a broader set of their needs.

MSPs cannot ignore their clients' baseline backup and recovery needs. They must still deliver a solution that protects multiple applications, databases, operating systems, hypervisors, and data types.

However, effective protection against malware and ransomware and supporting rapid recoveries from an attack have become new mandates. Existing backup software often fails to meet these latest requirements. Current and prospective customers will demand MSPs offer solutions that:

- ***Secure the environment.*** Customers increasingly expect data protection solutions to secure their data from internal and external threats. Data protection solutions can help meet this expectation. They can scan for and detect threats such as malware and ransomware. They may offer options to validate the integrity of existing backups as well as protect them from ransomware attacks. They may even offer ransomware recovery options and features to keep operating system patches and fixes current.
- ***Protect the edge.*** Customers deploy more applications and generate more data in remote and branch offices, including home offices. Backup requirements may extend to include protecting smartphones, laptops, PCs, and other mobile devices.
- ***Protect multiple cloud environments.*** Customers of all sizes use cloud technologies. These technologies include hybrid, private, and public clouds. Each cloud type typically possesses unique application and data protection requirements.
- ***Deliver on next-gen backup and recovery requirements.*** Automated disaster recovery (DR) and backing up online office suites appear more frequently as requirements.

An MSP Specific Requirement

Identifying a data protection solution that delivers on these new mandates presents a significant challenge. However, MSPs need a solution that also specifically equips them to deploy, monitor, and manage it.

MSPs must cost-effectively and efficiently monitor and manage data protection for all their customers. This dictates they identify solutions that offer open APIs. Open APIs position them to manage data and threat protection from one interface as opposed to using separate consoles.

MSPs also want to minimize their time spent deploying the solution. Further, they want to get paid for services rendered. As such, data protection solutions must simplify deployment while positioning them to bill for services provided.

These multiple different requirements often lead MSPs to consider Acronis Cyber Protect Cloud and StorageCraft Cloud Services. Both offerings contain features that MSPs and their customers respectively care about. However, distinct differences exist between these two offerings. They primarily surface in the following three areas:

- Proactive, natively integrated threat detection and protection
- Comprehensive data protection
- Built for the MSP

#1 – Proactive, Natively Integrated Threat Detection and Protection

It seems almost every day the headlines lead with the consequences of another ransomware attack. Enterprises now regularly pay ransoms over $1 million. Further, new research shows that 80 percent of organizations that pay a ransom experience a subsequent ransomware attack.[1] This may result in additional downtime and ransom payments.

To attack, hackers primarily target edge devices. Analysts forecast that by 2025 enterprises will generate 75% of their data outside of their data center.[2] This data often gets generated or gathered by laptops, PCs, mobile devices, or edge servers. More susceptible to attacks, they provide a gateway for hackers to access organizational data stores.

Organizations look to MSPs for solutions that detect these threats and recover their data should an attack occur. Both StorageCraft and Acronis offer solutions MSPs may use in these roles.

1. https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf. Referenced 6/25/2021.
2. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/. Referenced 5/10/2021.

StorageCraft Cloud Services

StorageCraft's OneXafe solution stores backup data in an immutable format. Should ransomware attack and encrypt backups, OneXafe can recover unencrypted versions of backup data. StorageCraft's ShadowXafe backup software also protects backup data from ransomware. ShadowXafe:

- Creates files or folders only it can access making them inaccessible to other applications
- Generates alerts should anyone or any application attempt to access stored backups
- Automatically extends the retention of previously stored backups

Acronis Cyber Protect Cloud

The Acronis Cyber Protect Cloud shares many characteristics with StorageCraft Cloud Services in how it protects backup data. Acronis:

- Stores backup data in an immutable format on WORM media, with full support coming
- Makes the files and folders it creates inaccessible to other applications
- Generates alerts when someone or some application attempts to access backups
- Automatically extends retention times for previously stored backups should it detect a ransomware attack

Acronis further distinguishes itself by natively integrating cybersecurity software that prevents and detects threats in both production and backup data. Acronis uses a single agent to deliver both its backup and cybersecurity software.

Acronis' Threat Detection and Prevention

The Acronis cybersecurity software actively scans for malware and ransomware in production data in both real-time and on-demand. When running in real-time, it actively scans the operating system and any files in use for malware. If run on-demand, it only scans executable files at the time they get run.

To help prevent ransomware attacks, Acronis performs vulnerability assessments and patch management functions for Windows and over 220 applications. It classifies vulnerabilities using an internal severity scale. Should it identify a system or application vulnerability, the Acronis agent automatically fetches the appropriate update and rolls it out.

The Acronis Smart Protect feature complements its inherent vulnerability assessment features. The Acronis Cyber Protection Operations Center (CPOC) monitors for threats worldwide. As CPOC detects threats, it generates alerts and recommended responses. MSPs may log in at any time to check for threats that apply to their customers and initiate the appropriate actions.

Protection from Zero-day Attacks

Zero-day attacks represent a major threat facing MSPs and their clients. A ransomware attack could occur and spread before anyone recognizes it. Depending on how long this attack occurs undetected, this could make it potentially impossible to recover.

Acronis' integrated cybersecurity and data protection provides MSPs a higher probability of detecting ransomware in the customers' environments. Should they detect an attack in a the environment, they can stop the attack while automatically recovering infected files. This mitigates the need for MSPs to manually intervene.

Acronis also prevents re-occurrences of ransomware during a recovery as latent strains of ransomware may reside in backups. Recovering these files may inadvertently introduce these strains back into the environment. Acronis scans recovered backups for ransomware and auto-updates OS images to ensure ransomware-free restores.

Acronis may additionally diagnose and determine the source of malicious activity. Acronis' Forensic data backup option collects digital evidence to assist in performing forensic investigations. It gathers and analyzes data such as memory dumps and snapshots of running processes and unused disk space. (Table 1.)

TABLE 1

Threat Detection and Protection Capabilities

	Acronis Cyber Protect Cloud	StorageCraft Cloud Services
Integrated backup/cybersecurity agent	✔	●
Backup		
Alerting on backup data access	✔	✔
Automated backup retention extension	✔	✔
Backup data immutability	✔	✔
Inaccessible backup files & folders	✔	✔
Cybersecurity		
Auto recovers infected files	✔	●
Auto updates OS images	✔	Third Party
Forensic data analysis	✔	Third Party
Global threat monitoring	✔	Third Party
OS patch management	✔	●
Scan production data for malware and ransomware	✔	Third Party
Vulnerability assessments	✔	Third Party

✔ Supported ● Undetermined/Unsupported

KEY QUESTIONS TO ASK

- *Are you currently responsible or being called upon to handle endpoint data protection?*
- *Do you get called upon by your customers to help them recover files infected by ransomware? If so, were you able to help them successfully recover?*
- *Have you considered using a single, natively integrated solution that offers backup, cybersecurity, and recovery capabilities?*

#2 – Comprehensive Data Protection

The more customers an MSP has, the more hypervisors and operating systems it encounters and supports. MSPs will minimally back up desktop and server operating systems such as macOS, Linux, and Windows. On the hypervisor side, they should prepare to back up Linux KVM, Microsoft Hyper-V, Red Hat Virtualization (RHV), and VMware vSphere.

A comprehensive backup solution will minimally protect these common hypervisor and operating systems. However, MSPs should also ideally identify a solution that backs up as many hypervisors and operating systems as possible. (Table 2.)

TABLE 2

Supported Hypervisors and Operating Systems

	Acronis Cyber Protect Cloud	StorageCraft Cloud Services
Edge/Mobile Devices		
Android	✓	●
iOS	✓	●
Desktop/Server Operating Systems		
Linux	✓	✓
macOS	✓	●
Windows	✓	✓
Hypervisors		
Citrix XenServer	✓	✓
Linux KVM	✓	✓
Nutanix AHV	✓	●
Oracle VM Server	✓	●
RHV	✓	✓
Scale Computing HC3	✓	●
Virtuozzo	✓	●
VMware vSphere	✓	✓
Windows Hyper-V	✓	✓

✓ Supported ● Undetermined/Unsupported

Edge and Mobile Devices

Almost without exception every employee uses one or more mobile devices. Further, nearly all these mobile devices run either the Android or iOS operating systems. As customers store more sensitive data on these devices, offering an option to back them up becomes an imperative. Of the two solutions, only Acronis offers options to protect both these mobile device **OSs**.

Desktop/Server Operating Systems

The primary difference between Acronis and StorageCraft in their respective support for desktop and server operating systems centers on macOS. Most customers will run either Linux or Windows on their physical and virtual machines. Both solutions back up these OSs.

However, macOS continues to have a substantial market presence. Currently 7.5 percent of desktop operating systems run macOS.[3] Acronis protects macOS which advantages those MSPs who have customers that run macOS and need to protect it.

Hypervisors

Both Acronis and StorageCraft support the most common hypervisors that MSPs will encounter in customer environments. Whether it is Linux KVM, VMware vSphere, Windows Hyper-V, or even hypervisors such as Citrix XenServer or RHV, both these solutions support them.

MSPs wanting a backup solution that prepares them to protect additional hypervisors should again consider Acronis. It also supports Nutanix AHV, Oracle VM Server, and Virtuozzo.

Acronis' support of Nutanix AHV specifically stands out. Nutanix frequently gets mentioned in the same breath in large organizations as Microsoft Hyper-V and VMware vSphere. This increases the probability MSPs will encounter and need to protect applications and data hosted on it.

Cloud and Applications

Any solution must meet baseline cloud and application data protection thresholds for MSPs to consider it viable. On the cloud front, the solution should minimally support Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. The solution may also offer its own cloud locations that MSPs may use to offer disaster recovery-as-a-service (DRaaS).

On the application side, any backup solution should protect all Microsoft applications using application-aware backups. Microsoft applications include Active Directory (AD), Exchange, SharePoint, and SQL Server. The solution should also offer protection for the two leading online Office Suites: Google Workplace and Microsoft 365. Last, but not least, it should protect the widely used enterprise database application Oracle Database.

Both Acronis and StorageCraft deliver on these respective baseline cloud and application data protection options. They support the leading cloud providers, databases, Microsoft applications, and office suites. Further, DCIG has recognized both as TOP 5 DRaaS solutions for their respective abilities to perform disaster recoveries in the cloud. (Table 3.)

3. https://arstechnica.com/gadgets/2021/02/the-worlds-second-most-popular-desktop-operating-system-isnt-macos-anymore/. Referenced 6/28/2021.

TABLE 3

Supported Clouds and Applications

	Acronis Cyber Protect Cloud	StorageCraft Cloud Services
Clouds		
AWS (S3/EC2)	✓ / ✓	✓ / ✓
GCP Cloud Storage	✓	✓
Microsoft Azure (Blob/VMs)	✓ / ✓	✓ / ✓
Provider Cloud Data Centers*	APAC, Europe, LATAM, North America, UK	APAC, Europe, LATAM, North America, UK
Databases		
Oracle Database	✓	✓
SAP HANA	✓	●
Clustered MS SQL Server	✓	●
Microsoft Applications		
Active Directory	✓	✓
Exchange	✓	✓
File Level CDP	✓	●
SharePoint	✓	✓
SQL Server	✓	✓
Office Suites		
Google Workspace	✓	✓
Microsoft 365	✓	✓

* Locations listed provide an overview of each provider's global data center locations

✓ Supported ● Undetermined/Unsupported

Advanced Data Protection Features

The differences between these two solutions primarily lay in their breadth of support of advanced data protection features. Of the two, Acronis better addresses specific requirements that MSPs may encounter in large customer environments.

For instance, MSPs may need to provide near real-time recovery point objectives (RPOs) for their customers' files. Using Acronis Cyber Protect, MSPs may capture all file changes between scheduled backups.

On the database front, only Acronis offers options to protect databases such as SAP HANA and clustered MS SQL Server. Acronis also comes equipped to protect virtual machine (VM) data residing on NetApp NAS filers. MSPs may configure Acronis to create VMware VM backups from snapshots created and residing on NetApp arrays.

If protecting remote offices, Acronis supports client- or source-side deduplication that deduplicates data on the client before transmitting it over the network. MSPs may find this feature particularly desirable when protecting applications and data in remote offices. This feature minimizes WAN bandwidth requirements when sending and receiving backup data. (Table 4.)

TABLE 4

Advanced Data Protection Features

	Acronis Cyber Protect Cloud	StorageCraft Cloud Services
DRaaS	✓	✓
Software-defined Storage (SDS)	✓	●
Source-side Deduplication	✓	●

✓ Supported ● Undetermined/Unsupported

KEY QUESTIONS TO ASK

- *Do you need or want to offer your customers the option to protect their mobile devices?*
- *Do you need or want to manage all applications, clouds, and operating systems using the same solution?*
- *Do you manage backups in remote locations with limited amounts of network bandwidth?*
- *Do you need or want advanced data protection features such as source-side deduplication and software-defined storage?*

Differentiator #3 – Built for MSPs

Many MSPs rely upon professional services automation (PSA) or remote monitoring and management (RMM) software to optimize their daily operations. This makes it imperative any solution integrate with their existing PSA or RMM software solutions which both StorageCraft and Acronis do. However, they differ in their depth of integration.

StorageCraft Cloud Services

StorageCraft's Cloud Public OneSystem offers a centralized management console for its data protection solutions. Hosted in the StorageCraft cloud, MSPs use a browser to access the OneSystem management console.

Once logged in, MSPs may discover, monitor, and manage many of the features found on StorageCraft's three data protection offerings. However, configuring some settings on StorageCraft's offerings may require MSPs to log into a specific StorageCraft device.

StorageCraft's PSA/RMM Integrations

Figure 1

StorageCraft Cloud Services currently integrates with three PSA and RRM tools using a plug-in.[4] The plug-in pushes changes from StorageCraft's MSP Portal to the respective PSA or RMM tool on a schedule or on-demand.

Data pushed includes the number of StorageCraft MSP licenses and cloud storage usage to PSA solutions so they may perform automated billing. MSPs may also use StorageCraft's RMM plug-in to install and update ShadowProtect SPX backup agents.

MSPs wanting to use ShadowProtect APIs to do custom integrations with their PSA or RMM tool will need to contact StorageCraft. It currently does not disclose the ShadowProtect APIs it makes available for custom integrations.

Acronis Cyber Protect Cloud

Acronis demonstrates its commitment to equipping MSPs to centralize management through its integration with multiple PSA and RMM tools. Acronis Cyber Protect Cloud already integrates with Atera; Autotask PSA; CloudBlue; ConnectWise Automate, Control, Command, and Manage; Jamf Pro; Kaseya Virtual System Administrator (VSA); and Matrix42.[5] N-able RMM and N-able Central integrations have been announced by Acronis. Further, Acronis plans to integrate with six more PSA and RMM software solutions.[6] (Figure 2.)

Acronis' PSA/RMM Integrations

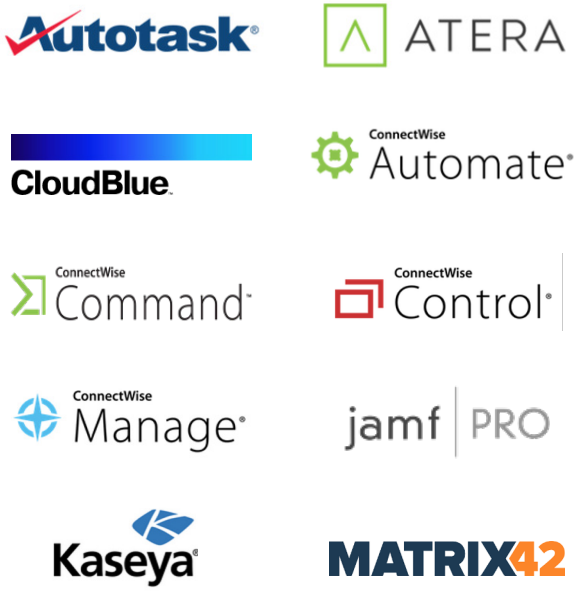

Figure 2

Acronis Cyber Protect Cloud exposes its APIs so MSPs may actively manage Acronis Cyber Protect Cloud using PSA and RMM tools. For example, MSPs may manage Acronis Cyber Protect Cloud with administrative privileges from within the supported PSA and RMM tools.

For example, Acronis' RMM integrations support:

- Fully automated, unattended agent deployments to Windows, Mac and Linux endpoints
- Monitoring of the status of client devices to include agent version, protection status, protection plan name applied, last backup date, next scheduled backup date, and last virus scan, among others. Other RMM-native tools may use this data for endpoint management.
- Synchronizing alerts or tickets generated within the RMM.

Similarly, Acronis' PSA integrations offer:

- Automatically provisioning a Customer tenant in Acronis.
- Mapping product items or SKUs in the PSA to track product start and end dates. Acronis automatically provisions active products associated with active contracts for Customer tenants in Acronis.
- Usage reporting so MSPs may bill customers for the Acronis services they consume, to include prepaid, pay-as-you-go, and prepaid with overage.
- Synchronizing alerts or tickets generated within the PSA.

Acronis Cyber Protect Cloud also exposes its native cybersecurity features through its APIs. This positions MSPs to respond to ransomware attacks as well as notarize and verify file authenticity. (Figure 3.)

Acronis' Hosting Control and Bill System Integrations

Figure 3

MSPs accustomed to hosting control systems such as cPanel or Plesk for server management may manage various Acronis Cyber Protect Cloud backup, restore, security, and admin tasks through these interfaces.[7] MSPs may also use Acronis' integration with Hostbill and WHMCS to perform client billing.[8]

Should MSPs use other PSA or RMM tools, Acronis makes its APIs available for them to create custom integrations. MSPs may alternatively obtain Acronis as a white-labeled solution and apply their branding to it. MSPs operating in different countries or countries with multiple languages may also find Acronis' availability in 25 different languages appealing. (Table 5.)

4. https://www.storagecraft.com/connectwise-solutions; https://www.storagecraft.com/partners/autotask-psa-integration. Referenced 6/23/2021.
5. https://solutions.acronis.com/autotask/. https://solutions.acronis.com/connectwiseautomate/.Referenced 5/28/2021.
6. https://solutions.acronis.com/kaseya/.Referenced 5/28/2021.
7. https://solutions.acronis.com/cpanel/. https://solutions.acronis.com/plesk/. Referenced 6/24/2021.
8. https://solutions.acronis.com/hostbill/. https://solutions.acronis.com/whmcs/ Referenced 6/24/2021.

TABLE 5

PSA and RMM Integrations

	Acronis Cyber Protect Cloud	StorageCraft Cloud Services
PSA/RMM Software	Atera, Autotask PSA, CloudBlue, ConnectWise Automate, Command, Control, & Manage, Jamf Pro, Kaseya VSA, Manage42	Autotask PSA, ConnectWise Automate and Manage
Forthcoming PSA/RMM Product Integrations	6	Undisclosed
PSA/RMM Console Capabilities*	• Backup job scheduling, management • Changes pushed on-demand or on schedule • Cybersecurity management • File authorization & notarization	Changes pushed from ShadowXafe on-demand or on schedule
Hosting Control Systems Providers	cPanel Plesk	●
Third-party Billing Providers	ActivePlatform, HostBill WHMCS	●
Languages Supported	25	1
White Label	✔	●

* Features listed provide a representative sample of each product's capabilities

✔ Supported ● Undetermined/Unsupported

KEY QUESTIONS TO ASK

- *Do you use a PSA, RMM, or other third-party software solution(s) to manage your environment?*
- *Do you want or need to perform administrative tasks using a central management console?*
- *Do you want or need access to APIs to programmatically introduce more features into your PSA or RMM solution?*
- *Do you need to manage the solution using different languages?*

Acronis Delivers on New Mandates for Comprehensive Data Protection

Organizations have redefined their data protection strategy to include new mandates to better protect their IT infrastructure. They want solutions that better back up and recover their applications and data while securing them against ransomware's threat.

Both Acronis and StorageCraft offer solutions that meet the baseline backup and recovery needs of many customers. However, only Acronis Cyber Protect Cloud natively integrates cybersecurity software into its offering to provide a single customer solution.

Acronis Cyber Protect Cloud's native cybersecurity features proactively protect applications and data from malware and ransomware threats. In so doing, Acronis extends its cybersecurity features to protect data in production, backups, or during recovery.

Further, Acronis Cyber Protect Cloud addresses key MSP concerns about deployment, management, and profitability. They may manage all Acronis features using a single agent, with minimal extra training, and through a single management console. MSPs may achieve this final objective thanks to Acronis tight integration with the PSA or RMM console MSPs already possess.

Acronis' integration with leading PSA and RMMs solutions facilitate its ease of adoption and centralized, ongoing management. Once deployed, Acronis backs its solution with APIs, online instructional videos, and top-notch support. These ensure MSPs meet their customer new data protection mandates while maintaining their own quality, service, and profitability objectives. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**