A Comparison of How Acronis and Datto Meet MSP Requirements for Data Protection and Threat Detection and Prevention

by DCIG President & Founder, Jerome M Wendt

PROVIDERS

Acronis

URL ▶ https://www.acronis.com/

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

Datto

URL ▶ https://www.datto.com/

Datto Holding Corp.
101 Merritt 7
Norwalk, CT 06851
(888) 995-1431

COMPARISON USE CASE

MSPs that need a single solution and interface to manage data protection and threat detection in as many of and as much of their customers' environments as possible.

Data Protection's New Mandates

Managed service providers (MSPs) recognize they must address new, more complex cyber protection initiatives in their clients' environments. New mandates have emerged as businesses of all sizes redefine data protection to meet more of their cyber protection needs.

Small and midsize businesses still expect MSPs to deliver solutions that meet their base line backup and recovery needs. MSPs must continue delivering a solution that protects multiple applications, databases, hypervisors, and operating systems.

These features coupled with malware and ransomware protection, along with delivering rapid recoveries, now make up the data protection conversation. Current data protection solutions often fail to meet these new requirements that businesses possess. In response, MSPs must offer solutions that:

- ***Secure the environment.*** Businesses increasingly expect data protection solutions to secure their environment from internal and external threats. New solutions must scan for and detect threats such as malware and ransomware in production environments. These same solutions should also validate the integrity of existing backups as well as protect them from ransomware attacks. Ideally, they will also offer ransomware recovery options as well as features that keep operating system patches and fixes current.
- ***Protect the edge.*** Businesses deploy more applications in remote and branch offices, to include home offices, that generate more data. Backup requirements may also extend to include protecting smartphones, laptops, PCs, and other mobile devices.
- ***Protect multiple cloud environments.*** Businesses of all sizes now routinely 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 now regularly appear as business requirements. Businesses also want options to back up, store, and recover their data on-premises using scalable backup appliances.

MSP Specific Requirements

Identifying a solution that delivers on these new data and threat protection mandates presents a significant challenge. However, MSPs also have requirements specific to them. They need to centrally deploy, monitor, and manage solutions that position them to bill for services provided.

These MSP-specific requirements often lead MSPs to consider available solutions from Acronis and Datto. Both offerings contain features that meet the needs of both MSPs and their customers. However, distinct differences exist between the solutions from these two providers. They primarily surface in the following three areas:

- Proactive, natively integrated threat detection and data protection
- Comprehensive set of features in their data protection solution
- Flexible management options for MSPs

#1 – Proactive, Natively Integrated Threat Detection and Data Protection

The IDC analyst firm recently shared the results of its 2021 enterprise cybersecurity survey at the 2021 Acronis #CyberFit Summit. The survey found 93 percent of enterprises had experienced a cybersecurity attack. IDC's research analyst also surmised all organizations have likely experienced an attack. They either do not know it or cannot acknowledge it, even anonymously.

To attack businesses, hackers often target their edge devices. Analysts forecast that by 2025 organizations will generate 75% of their data outside of their data center.[1] 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.

Should a ransomware attack succeed, organizations may experience devastating results with the average ransomware payment in 2020 exceeding $300K.[2] This amount does not account for the downtime, lost revenue, and missed sales opportunities that a ransomware attack incurs.

These challenges provide MSPs an opportunity to offer solutions that help their customers defend against these attacks. Using data protection solutions that also offer cybersecurity features give them new options to help their customers protect against ransomware. Further, businesses increasingly expect MSPs to provide them with solutions that offer these options.

1. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/. Referenced 5/10/2021..
2. https://www.tripwire.com/state-of-security/featured/average-ransomware-payouts-shoot-up/. Referenced 5/10/2021

Both Acronis and Datto each offer solutions MSPs may use in these roles. However, they each differ in how they deliver their respective offering.

Datto SIRIS and RMM

Datto includes two solutions in its data and threat protection portfolio that target the needs of small and midsized businesses. For data protection, Datto offers its SIRIS backup solution. It delivers SIRIS as a virtual appliance, a physical backup appliance, or in a software-only implementation. SIRIS offers agent-based backups for Windows and Linux OSes and agentless backups for Windows guest OSes hosted on VMware vSphere.[3]

The Datto SIRIS physical backup appliances leverage the Zettabyte File System (ZFS) for storage scalability and data immutability. ZFS's copy-on-write (CoW) snapshot feature gets used by Datto backup appliances to reduce storage consumption and more quickly recover VMs.[4]

To deliver data immutability, Datto SIRIS takes the following steps.

- Stores backup data in the Datto Cloud that mandates two-factor authentication for access to its cloud-based portal.
- Encrypts backup data as it is stored at-rest in the Datto cloud.
- Offers the option to encrypt data stored on its SIRIS backup appliance.
- Performs a post-backup scan to check data for ransomware.[5]
- Offers a Cloud Deletion Defense feature that can recover accidently or maliciously deleted cloud snapshots.[6]

Datto provides threat detection and prevention through its separate Remote Monitoring and Management (RMM) software. RMM resides on and monitors for ransomware on endpoint devices by taking the following steps:

- Generates a notification it has detected ransomware on the endpoint device
- Attempts to terminate the ransomware process
- Attempts to isolate infected device(s) to stop the ransomware from spreading.

RMM also integrates with Datto SIRIS. MSPs may click through from RMM to launch the SIRIS interface. Once in SIRIS, they may use it to recover the affected machine(s) to a prior state.

Datto also acquired BitDam Ltd. in early 2021 to enhance its cybersecurity abilities.[7] It plans to integrate BitDam into its existing platforms to enhance their ransomware detection capabilities.[8] The first integration with BitDam appeared in its SaaS Protection+ offering in late 2021.[9]

Acronis Cyber Protect Cloud

Like Datto, Acronis Cyber Protect Cloud provides a data protection and cyber security solution. Unlike Datto, Acronis offers a single, integrated agent to perform both these tasks. This approach simplifies its deployment and ongoing management.

Acronis' data protection offers:

- ***Options to make backup data inaccessible.*** Cyber Protect performs this task in at least four ways.
  - First, businesses may turn on its immutable storage feature to retain deleted backups in an unchangeable format from 1 to 999 days.[10]
  - Second, it can store backup data on WORM media in an immutable format to prevent ransomware from changing data.
  - Third, it changes security permissions on backup files and folders to make them inaccessible to other applications, to include ransomware.
  - Fourth, Acronis agent has self-protection defenses implemented. These defenses ensure only secured Acronis processes can access backup data.
- ***Alerting and prevention.*** Should someone or some application attempt to access backup data, it generates alerts to inform of potentially nefarious activity and automatically prevents that access.
- ***Extends backup retention periods.*** Should Acronis detect a ransomware attack, it automatically extends retention times for previously stored backups.
- ***Client- and source-side deduplication.*** This gives MSPs more flexibility to decide where data deduplication occurs to meet specific application needs.

Acronis Threat Detection, Prevention, and Remediation

Acronis' use of a single agent provides additional benefits beyond simplified deployment and management. Acronis integrates these two features so if the agent detects malware or ransomware activity it can proactively respond to the attack in multiple ways. Acronis developed its anti-ransomware technology in 2016, introduced it in January of 2017, and has won numerous independent tests since.[11]

For instance, Acronis performs vulnerability assessments and patch management for Windows operating systems (OSes). It also performs the same assessments and patch management for over 270 Windows applications.

Acronis detects, alerts, and automatically recovers any files infected by malware or a ransomware attack. Should it also need to recover OS images infected by an attack, it updates the OS images ***before*** recovering them.

Acronis' global Cyber Protection Operations Centers (CPOC) offer smart protection plans to monitor threats worldwide. As the CPOC detects threats, it assesses their potential impact, generates alerts, and recommends responses to these threats. MSPs may then check in with Acronis' CPOC at any time and initiate actions in customer environments as appropriate.

Protection from Attacks

Acronis also mitigates the potential of any type of attack occurring in customer environments.

A ransomware attack may occur and spread undetected for days, weeks, or even months. During this time, it may silently infect production data and possibly backup data. Infected backups could impede recoveries or even make them impossible. Any recoveries may only serve to re-introduce the ransomware back into the environment.

Acronis helps prevent the re-occurrence of ransomware during a recovery. Acronis scans backup data used in recoveries for the presence of ransomware that previously was undetectable. It also auto-updates recovered OS images to ensure ransomware-free restores.

Acronis' Forensic data backup option further helps with root cause analysis. It collects digital evidence to assist in performing forensic investigations.

3. https://help.datto.com/s/article/KB205931640. Referenced 11/10/2021.
4. https://www.datto.com/technologies/advanced-storage. Referenced 11/10/2021.
5. https://www.datto.com/blog/what-is-immutable-cloud-storage. Referenced 11/10/2021.
6. https://help.datto.com/s/article/KB360050594512. Referenced 9/20/2021.
7. https://www.datto.com/news/datto-acquires-cyber-threat-detection-company-bitdam. Referenced 9/20/2021.
8. https://www.crn.com/news/security/datto-ceo-on-bitdam-buy-the-real-key-is-depth-not-breadth-. Referenced 9/20/2021
9. https://searchitchannel.techtarget.com/news/252508232/DattoCon-Now-points-to-profit-in-SaaS-defense-continuity. Referenced 11/10/2021.
10. https://www.acronis.com/en-us/support/documentation/CyberProtectionService/#enabling-disabling-immutable-storage.html. Referenced 12/23/2021.
11. https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Protect_Cloud_Multilayered_Cybersecurity_EN-US_210129.pdf

It gathers and analyzes data such as memory dumps and snapshots of running processes and unused disk space. This helps businesses diagnose the issue and ideally the source of the ransomware attack. (Table 1.)

TABLE 1

Threat Detection and Protection Capabilities

	Acronis Cyber Protect Cloud	Datto SIRIS and RMM
Single integrated backup/cybersecurity agent	✓	○
Backup		
Alerting on backup data access	✓	○
Automated backup retention extension	✓	○
Backup data immutability	✓	✓
Inaccessible backup files & folders	✓	✓
Prevents access to backup data	✓	○
Cybersecurity		
Auto recovers infected files	✓	○
Auto updates OS images	✓	○
Forensic data analysis	✓	○
Global threat monitoring	✓	○
Infected device isolation	✓	✓
Windows OS rollback	✓	○
OS patch management	✓	○
Scans all production data	✓	○
Scans backup data prior to recovery for malware and ransomware	✓	✓
Vulnerability assessments	✓	✓

✓ 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 single, natively integrated solution that offers backup, cybersecurity, and recovery capabilities?*

#2 – Feature-rich Data Protection Solution

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

MSPs ideally want a single, cost-effective, comprehensive backup solution that addresses these various data protection requirements. However, Acronis and Datto vary in their ability to protect these platforms and the applications and data hosted on them. (Table 2.)

TABLE 2

Supported Hypervisors and Operating Systems

	Acronis Cyber Protect Cloud	Datto SIRIS and RMM
Licensing	All-inclusive Backend TBs	All-inclusive Per Protected Device Front-end TBs *(for archiving & cloud storage)*
Edge/Mobile Devices		
Android	✓	File Synchronization
iOS	✓	File Synchronization
Desktop/Server Operating Systems		
Linux	✓	✓
macOS	✓	✓
Windows	✓	✓
Hypervisors		
Citrix XenServer	Agent-based	Agent-based
Linux KVM	Agent-based	Agent-based
Microsoft Windows Hyper-V	Agentless, Agent-based	Agent-based
Nutanix AHV	Agent-based	○
Oracle VM Server	Agent-based	○
RHV	Agent-based	○
Scale Computing HC3	Agent-based	○
Virtuozzo	Agent-based	○
VMware vSphere	Agentless, Agent-based	Agentless, Agent-based

✓ Supported ○ Undetermined/Unsupported

Software Licensing

Datto licenses its SIRIS solution with a combination of upfront and recurring monthly costs. MSPs may sell Datto SIRIS appliances to their customers for a one-time fixed cost. Customers then subscribe to Datto's monthly service. This service minimally includes unlimited Linux, Mac OSX, and Windows system backup licenses, snapshot support, cloud retention, and capacity-based cloud storage.[12]

Acronis uses a comparable licensing model. It offers backup appliances for a fixed, upfront cost through its partnership with Scale Computing. It then charges a monthly fee for backup and backup storage services. This method includes all necessary software licensing and calculates licensing costs based upon the total amount of stored backup data.

Mobile Devices

Employees almost universally use mobile devices with most running either the Android or iOS operating systems. As businesses generate and store more sensitive data on these devices, offering an option to back them up becomes an imperative.

Datto supports Android and iOS devices at a basic level through its Datto Drive Local. Installed as an app on these devices, it downloads and uploads files to and from these devices.[13] In contrast, Acronis offers automatic, continuous backup for Android and iOS devices. It protects contacts, calendar appointments, photos, videos, and other files stored on them.

Desktop/Server Operating Systems

Both solutions fully protect macOS, Windows OSes, and most Linux distributions whether the OSes run on physical or virtual machines.

Hypervisors

Acronis and Datto share some commonality in hypervisor protection. Both solutions support the native data protection APIs available in VMware vSphere to perform agentless VM backups. They also both use backup agents to protect Linux or Windows VMs hosted on the Linux KVM hypervisor.

However, many MSPs will encounter Microsoft Hyper-V in customer environments. Here is where Acronis differentiates itself.

Acronis capitalizes on the Resilient Change Tracking (RCT) API included in Windows Server 2016, 2019, and 2022. Using RCT, it can perform agentless incremental backups of changed blocks in a Hyper-V VM per a specific point in time.[14] In contrast, Datto SIRIS does not currently support agentless Windows Hyper-V backups and only uses backup agents to protect Hyper-V VMs.[15]

Finally, Acronis formally supports protecting VMs hosted on Nutanix AHV and Virtuozzo hypervisors. This positions MSPs to extend protection to VMs hosted on these hypervisors should they encounter them in customer accounts.

Cloud Data Protection and Support

MSPs increasingly provide support for applications, data, and workloads hosted in the cloud. On the cloud front, any solution they select should minimally support Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. The solution will also ideally protect cloud office suites, offer its own private cloud, and provide disaster recovery-as-a-service (DRaaS).

Datto SIRIS

When it comes to protecting data and VMs hosted with cloud providers, Datto only formally supports two options. It protects data hosted in Microsoft 365 or Google Workspace through its separate SaaS Protection+ software.

Datto also offers its purpose-built Datto Cloud with nine datacenters worldwide. These sites store backed up data and they may host DRs. The Datto Cloud currently consists of two locations in Canada and two in the US. The other five reside in Africa (Madagascar), Australia, Europe (Germany), Iceland, and the UK, respectively.[16]

Datto specifically targets small and midsize businesses (SMBs) with its offerings.[17] DCIG finds SMBs generally possess up to 50 virtual or physical machines in their environment. Datto SIRIS replicates backups of these machines to the Datto Cloud. Once there, MSPs use Datto's DRaaS offering to recover and host VMs to handle production workloads should a disaster occur. (Table 3.)

TABLE 3

Supported Clouds and Applications

	Acronis Cyber Protect Cloud	Datto SIRIS
Cloud Support		
AWS (S3/EC2)	✓ / ✓	● / ●
GCP Cloud Storage	✓	●
Microsoft Azure (Blob/VMs)	✓ / ✓	● / ●
Provider Cloud Data Centers*	APAC, Europe, LATAM, North America, UK (30+)	Africa, Australia, Canada, Iceland, Europe (9)
Cloud Office Suites		
Google Workspace	✓	✓
Microsoft 365	✓	✓
DRaaS		
DRaaS	SMB, SME	SMB
Databases		
Clustered MS SQL Server	Agentless	●
MySQL	Scripting	Scripting
Oracle Database	Agent, Scripting, RMAN	Agent, Scripting, RMAN
SAP HANA	Agent, Scripting	Custom Scripting
Microsoft Applications—On-premises		
Active Directory	✓	✓
Exchange	✓	✓
File Level CDP	Every manual or automate save	Up to every 5-min
SharePoint	✓	✓
SQL Server	✓	✓

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

✓ Supported ● Undetermined/Unsupported

12. hhttps://datto.kfit.ch/wp-content/uploads/Siris_3_3X_KF_Prices.pdf. Referenced 11/10/2021.
13. https://help.datto.com/s/article/KB115005592606. Referenced 11/10/2021.
14. https://www.acronis.com/en-us/solutions/backup/hyper-v/. Referenced 11/11/2021.
15. https://help.datto.com/s/article/KB205931640. Referenced 11/11/2021.
16. https://help.datto.com/s/article/KB210287926; https://help.datto.com/s/article/KB370000003520; https://help.datto.com/s/article/KB360020869131; https://help.datto.com/s/article/KB360020867451; https://help.datto.com/s/article/KB370000002917; https://www.datto.com/blog/simplify-virtual-machine-backup-with-datto-siris Video mark – 2:21. Referenced 11/11/2021.15.
17. https://www.datto.com/about/. Referenced 11/11/2021.

Acronis Cyber Protect Cloud

Acronis officially supports the backup of VMs hosted in the AWS and Microsoft Azure clouds. It also gives MSPs the option to store backup data in cloud storage from AWS, GCP, and Microsoft Azure. If using cloud storage, MSPs will need to deploy an Acronis Backup Gateway in the general-purpose clouds they use.[18]

Like Datto, Acronis supports backing up data hosted in either the Google Workspace or Microsoft 365 cloud office suites.[19]

Acronis also provides its Acronis Cyber Cloud data centers that MSPs may use to store backup data and deliver DRaaS. Acronis has more than 30 data centers worldwide with one on every continent except Antarctica. It also utilizes select GCP and Microsoft Azure datacenters to deliver cloud services.[20]

The Acronis DRaaS offering does distinguish itself in an important way by supporting small and midsized enterprises. These size enterprises typically have anywhere from 50 physical or virtual machines up to perhaps 1,000 or more. Using the Acronis DRaaS and Cyber Cloud offerings, MSPs can realistically explore delivering and hosting DRaaS in the Acronis Cyber Cloud for these size enterprises. This scalability led to its DCIG rank as a TOP 5 All-in-one DRaaS offering.

Application Data Protection and Support

On the application side, modern enterprise backup solutions should protect all Microsoft applications using application-aware backups. Microsoft application support should include Active Directory (AD), Exchange, SharePoint, SQL Server, and Microsoft 365. The solution will ideally also offer protection for widely used enterprise database applications. These include Clustered SQL Server, MySQL, Oracle Database, and SAP HANA.

Microsoft Application Data and File Protection

These two solutions compare favorable in protecting both Microsoft applications and enterprise database applications. Acronis and Datto each capitalize on the Microsoft Windows Volume Shadow Copy Service (VSS) APIs to create application-consistent backups of Microsoft applications. Datto also offers two other options to create crash-consistent backups of Windows applications should the Microsoft Windows VSS writer fail.[21]

Each solution protects files stored on Microsoft Windows using standard full, differential, and incremental backups. Each one also offers continuous data protection (CDP) for Windows files and folders though they differ in their granularity. Datto SIRIS can perform backups as frequently as every five minutes.[22] In contrast, Acronis CDP protects changes after every manual or automatic save.[23] MSPs may find this higher level of protection useful for customers intolerant of data protection gaps.

Database Protection

Both Acronis and Datto offer options to protect Oracle Database and MySQL database instances. The method Datto uses depends upon the OS platform hosting the database. For instance, if protecting Oracle Database hosted on Windows, it can use VSS. Alternatively it can use Oracle RMAN to perform the Oracle Database backup.

If hosting Oracle Database on Linux, Datto provides scripting templates to do backups. However, users will need to create custom scripts to perform pre- and post-processing backup tasks.[24] To protect MySQL on Linux, Datto SIRIS provides a default quiescing script with its Linux agent.[25]

In the case of Acronis Cyber Protect Cloud, it may use either Oracle RMAN or its own agent to natively protect Oracle Database. To protect MySQL, it offers downloadable scripts that run before and after a snapshot of the MySQL data occurs.

Of the two, only Acronis natively backs up clustered Microsoft SQL Server and SAP HANA instances. However, Datto does provide guidance on how to manually configure an environment so it can protect SAP HANA.[26]

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 want or need advanced data protection features such as CDP, DRaaS, and support for general-purpose clouds*?

#3 – Flexible Management Options for MSPs

MSPs rely upon professional services automation (PSA) and remote monitoring and management (RMM) software to optimize their daily operations. This makes it imperative any backup or cybersecurity solution they select integrate with their existing PSA and/or RMM software solutions. Both Acronis and Datto offer RMM and PSA integrations but differ in the breadth and depth of their integration capabilities.

Datto Autotask PSA and RMM

Datto offers its own well-known and widely supported PSA tool, Autotask, as well as its own RMM offering.[27] Datto integrates its RMM and Autotask consoles to unify management of SIRIS backup and recovery as well as endpoint cybersecurity.

Using Datto to meet these varied MSP needs works well assuming Datto's solutions meet all an MSP's needs. In the event Datto does not, an MSPs must select alternative backup and cybersecurity solutions that Datto's manage. This may help explain why Datto's Autotask integrates with and supports other solutions, to include Acronis Cyber Protect Cloud, among others.[28]

Acronis Cyber Protect Cloud

Acronis expects to work and integrate with existing PSA and RMM solutions as MSPs often already have them in place.

Acronis Cyber Protect Cloud integrates with Atera; CloudBlue; ConnectWise Automate, Control, Command, and Manage; Datto Autotask PSA; Jamf Pro; Kaseya Virtual System Administrator (VSA); and Matrix42.[29] It has also announced integrations with N-able RMM and N-able Central and plans to integrate with at least six more PSA and RMM software solutions. (Figure 1.)

By Acronis exposing its APIs to all RMM and PSA tools, MSPs may actively manage Acronis Cyber Protect Cloud using their existing PSA

18. https://dl.acronis.com/u/storage2/html/AcronisStorage_2_quick_start_guide_en-US/connecting-abc-via-abgw/connecting-to-cloud.html. Referenced 11/1/2021.
19. https://www.acronis.com/en-us/solutions/backup/office-365/. Referenced 11/1/2021.
20. https://www.acronis.com/en-us/data-centers/. Referenced 11/12/2021.
21. https://help.datto.com/s/article/KB200554755. Referenced 11/12/2021.
22. https://www.datto.com/technologies/screenshot-verification. Referenced 11/12/2021.
23. https://www.ev-consultech.com/acronis-cyber-protect. Referenced 11/12/2021.
24. https://help.datto.com/s/article/KB115002765583. Referenced 11/12/2021.
25 https://help.datto.com/s/article/KB115001275683. Referenced 11/12/2021.
26. https://help.datto.com/s/article/KB115003282203. Referenced 11/12/2021.
27 https://www.datto.com/products/autotask-psa
28. https://www.n-able.com/products/rmm. Referenced 10/9/2021.
29. https://solutions.acronis.com/autotask/. Referenced 5/28/2021.

Acronis' PSA/RMM Integrations

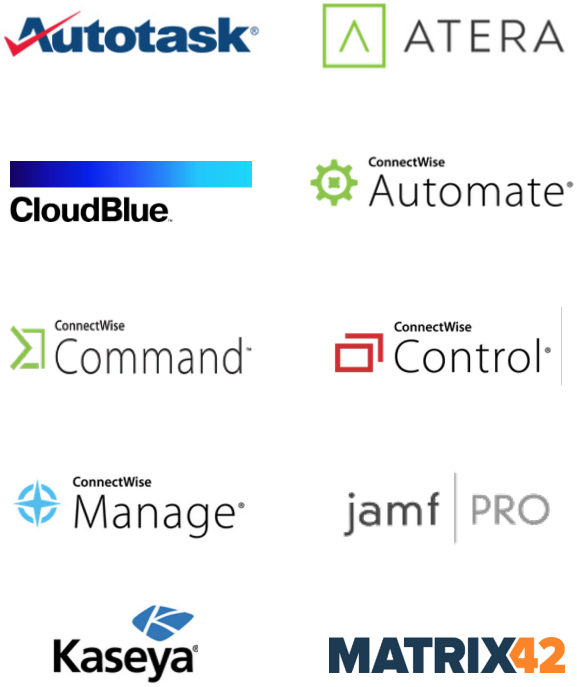

Figure 1

and RMM tools. Through this integration, MSPs may accomplish the following through their RMM console:

- Fully automate unattended agent deployments to Windows, macOS, and Linux endpoints.
- Monitor 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.
- Synchronize 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 using their RMM and PSA tools. (Figure 2.)

MSPs accustomed to hosting control systems such as cPanel or Plesk for server management may manage various Acronis Cyber Protect

Acronis' Hosting Control and Bill System Integrations

Figure 2

Cloud backup, restore, security, and admin tasks through these interfaces. MSPs may also use Acronis' integration with Hostbill and WHMCS to perform client billing.

MSPs may alternatively obtain Acronis as a white-labeled solution and apply their branding to it. MSPs operating in different countries or countries with languages specific to them may also find Acronis' availability in 25 different languages appealing.

KEY QUESTIONS TO ASK

- *Do you already 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 Cyber Protect Cloud: A Flexible, Feature-rich Data Protection and Threat Detection Solution for MSPs

Ransomware has changed how businesses value the protection, security, and recovery of their data. This change has prompted businesses to demand data protection solutions that better protect their IT infrastructure. In short, they want to back up and recover their applications and data while securing them against potential ransomware threats.

Both Acronis and Datto offer solutions that meet the baseline backup, cybersecurity, and recovery needs of most SMB customers. However, only Acronis Cyber Protect Cloud provides a single agent that natively integrates and delivers both backup and cybersecurity features appropriate to the needs of businesses.

Acronis Cyber Protect Cloud's native cybersecurity features proactively protect applications and data from malware and specifically ransomware

threats. In so doing, Acronis extends its cybersecurity features to protect data at all stages of its life cycle: production, backup, and recovery. By scanning and validating backup data during recoveries, Acronis helps ensure ransomware-free recoveries and superior business continuity operations.

Acronis 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 multiple PSA or RMM consoles, one of which MSPs likely already possess.

Acronis' integration with leading PSA and RMMs solutions facilitate its ease of adoption and centralized, ongoing management. Once deployed, Acronis stands behind its solution with APIs, online instructional videos, and top-notch support. These ensure MSPs meet their customers' new demands for better data protection 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.**