A Comparison of How Acronis and N-able 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

N-able™ Backup & EDR

URL ▶ https://www.n-able.com/

N-able, Inc.
301 Edgewater Drive, Suite 306
Wakefield, MA 01880
(781) 328-6490

COMPARISON USE CASE

MSPs that need a single solution and interface to manage threat detection and data protection 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 redefine data protection to meet a broader set of their needs.

Small and midsized 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 data from internal and external threats. New solutions must scan for and detect threats such as malware and ransomware in production environments. They 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 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 multiple MSP-specific requirements often lead MSPs to consider available solutions from Acronis and N-able. 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 solutions
- 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 could not 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

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

options to help their customers protect against ransomware. Further, businesses increasingly expect MSPs to provide them with solutions that offer these options.

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

N-able™ Backup and EDR

N-able offers separate software for threat detection and data protection with each software offering requiring its own agent. For threat detection, N-able offers its Endpoint Detection and Response (EDR) software.

Should EDR detect a threat, it can take any number of steps. These include:

- Stopping malicious processes
- Quarantining executables
- Disconnecting endpoints from the network

It can also remediate the affected endpoint by removing the damage caused by the threat on certain devices. On Windows machines it can roll back to a saved VSS snapshot.

N-able also offers its N-able Backup software. MSPs access N-able Backup as a cloud-based backup-as-a-service (BaaS) offering with no options for on-premises servers or appliances.[3] MSPs then manage it through N-able RMM, its remote monitoring and management solution.

N-able does include backup data storage in its private cloud as part of its Backup offering. It also offers options to store backups locally or in an immutable object store in the cloud. Through Backup, businesses may optionally use its WAN optimization, bandwidth throttling, and native data compression and deduplication features.

Acronis Cyber Protect Cloud

Like N-able, Acronis Cyber Protect Cloud offers both data protection and threat detection. Unlike N-able, 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.[4]
  - 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.[5]

For instance, Acronis performs vulnerability assessments and patch management for macOS and 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 helps MSPs mitigate the potential of any type of attack occurring in their 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. 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.)

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?*

3. https://www.n-able.com/resources/backup-for-it-pros-data-sheet
4. https://www.acronis.com/en-us/support/documentation/CyberProtectionService/#enabling-disabling-immutable-storage.html. Referenced 12/23/2021.
5. https://dl.acronis.com/u/rc/WP_Acronis_Cyber_Protect_Cloud_Multilayered_Cybersecurity_EN-US_210129.pdf

TABLE 1

Threat Detection and Protection Capabilities

	Acronis Cyber Protect Cloud	N-able Backup and EDR
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	✓	○
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

#2 – Feature-rich Data Protection Solution

The more customers an MSP has, the more hypervisors and operating systems it encounters and supports. 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 will want a feature-rich data protection solution. It should minimally protect these common physical operating systems as well as hypervisors and their associated guest operating systems. Ideally, the solution will also back up as many hypervisors and operating systems as possible while remaining affordable and manageable. (Table 2.)

Licensing Costs

N-able primarily licenses its Backup software per protected device. MSPs may add or remove licenses to protect devices as needed. N-able then checks each month to determine which licenses have been active that month and then bills accordingly.[6]

N-able also incurs archiving and cloud storage costs. It calculates these storage costs based on front-end terabyte (TB) licensing.[7] This option calculates total licensing costs by examining the total amount of data protected on each server.

In contrast, Acronis uses back-end TB licensing. This method calculates licensing costs based upon the total amount of stored backup data.

TABLE 2

Supported Hypervisors and Operating Systems

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

✓ Supported ○ Undetermined/Unsupported

6. https://documentation.n-able.com/N-central/userguide/Content/MSP_Backup/MSPBackup licensing.htm. Referenced 11/1/2021.
7. https://www.n-able.com/features/server-backup. Referenced 11/1/2021.

Mobile Devices

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

N-able currently only manages edge and mobile devices through its RMM solution.[8] Of the two solutions, only Acronis offers options to protect both these mobile device OS types.

Desktop/Server Operating Systems

Both solutions protect common desktop and server OSes such as macOS, Linux, and Windows. They both fully protect Windows OSes with varying levels of integration and support for Linux and macOS OSes.

N-able Backup formally supports the CentOS, Debian, and OpenSUSE versions of Linux. N-able Backup will run on any GNU/Linux distribution that meets its minimum hardware and OS requirements.

Both solutions also support macOS though in different ways. N-able Backup supports the backup and recovery on documents on macOS on versions 10.10 and later.[9] Acronis Cyber Protect offers backups, recoveries, antivirus, and antimalware protection for macOS 10.13 and later.[10]

Hypervisors

Both Acronis and N-able protect Microsoft Hyper-V and VMware vSphere, the two hypervisors MSPs will most commonly encounter in customer environments. However, MSPs wanting a backup solution that prepares them to protect additional hypervisors should again consider Acronis.

Acronis support of Linux KVM and Nutanix AHV specifically stand out. Businesses increasingly use variations of the Linux KVM hypervisor to help control costs. Nutanix may get mentioned in the same breath in large businesses as Microsoft Hyper-V and VMware vSphere. The growth in the use of these two hypervisors increases the probability MSPs will encounter and need to protect applications and data hosted on them.

Cloud Data Protection and Support

Growing and enterprise 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 offer its own cloud to store data and provide disaster recovery-as-a-service (DRaaS).

Both Acronis and N-able differ significantly in their support of these various clouds and cloud office suites as well in their cloud offering.

N-able Backup

N-able currently has no plans in place to extend support of Backup to any of the three major clouds' compute or storage platforms. It currently states that *"AWS is not a platform we develop for, test, or officially support."*[11] Its website also makes no mention of either GCP or Microsoft Azure. This suggests it also does not officially support either of these two platforms. While N-able Backup backs up VMs hosted on these platforms, support may fall to the MSP or an N-able partner.

N-able Backup does support Microsoft 365 in an official capacity. It offers back up and recovery for Microsoft 365's Exchange, OneDrive, and SharePoint components.

N-able also offers its own purpose-built cloud with multiple data centers. Though N-able has data centers throughout the world, the majority (11) reside in Europe.[12]

MSPs wanting to use N-able to deliver DRaaS services will find it offers limited capabilities. N-able Backup does support Recovery Testing that facilities testing the recovery of VMs. However, its cloud does not support the recovery of VMs into a production state should a disaster occur.

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.[13]

Acronis also offers backup support for both Google Workspace and Microsoft 365. In the case of Microsoft 365, it protects Exchange, OneDrive, SharePoint, and Microsoft Teams.[14]

Finally, Acronis provides its own purpose-built cloud that MSPs may use for DRaaS. Previously ranked as a TOP 5 DRaaS offering by DCIG, MSPs may leverage the Acronis cloud to host production disaster recoveries for their customers. (Table 3.)

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, and SQL Server. 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 Protection

These two solutions compare favorable in protecting both Microsoft applications and enterprise database applications. Both Acronis and N-able integrate with the Microsoft Windows OS to create application consistent backups of Microsoft applications.

They do differ in their handling of Windows file backups. While both solutions offer full, differential, and incremental backups, only Acronis offers continuous data protection (CDP) for files and folders. MSPs may find this option useful in customer environments that experience frequent data updates or changes and a need to protect this data when manual or automated saves occur.

Database Protection

Both Acronis and N-able equip MSPs to protect their customers' MySQL and Oracle Database instances. In the case of N-able, it relies

8. https://www.n-able.com/features/mobile; Referenced 11/1/2021.
9. https://documentation.n-able.com/remote-management/userguide/Content/osx_supported_operating_system.htm. Referenced 11/1/2021.
10. https://dl.managed-protection.com/u/cyberprotect/help/15/user/en-US/index.html?TocPath=Acronis%2520Cyber%2520Protect%252015%2520editions%2520and%2520licensing%257C_____1#supported-cyber-protect-features-by-operating-system.html. Referenced 11/1/2021.
11. https://www.n-able.com/blog/data-recovery-part-2-targeting-amazon-aws-ec2-for-data-recovery. Referenced 11/1/2021.
12. https://www.n-able.com/features/backup-data-centers. Referenced 11/1/2021.
13. 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.
14. https://www.acronis.com/en-us/solutions/backup/office-365/. Referenced 11/1/2021.

upon Oracle RMAN to perform backups of Oracle Database. To protect MySQL, it natively performs cold, warm, and hot backups of MySQL.[15]

Acronis also uses Oracle RMAN to protect Oracle Database though it can natively protect Oracle Database. To protect MySQL, it offers downloadable scripts that run before and after a snapshot of the MySQL data occurs.

TABLE 3

Supported Clouds and Applications

		Acronis Cyber Protect Cloud	N-able Backup and EDR
Cloud Support			
AWS (S3/EC2)		✓ / ✓	● / ●
GCP Cloud Storage		✓	●
Microsoft Azure (Blob/VMs)		✓ / ✓	● / ●
Provider Cloud Data Centers*		APAC, Europe, LATAM, North America, UK	Australia, Europe, North & South America, UK, South Africa
Cloud Office Suites			
Google Workspace		✓	●
Microsoft 365	*Exchange*	✓	✓
	OneDrive	✓	✓
	SharePoint	✓	✓
	Teams	✓	●
DRaaS			
DRaaS		✓	Testing only
Databases			
Clustered MS SQL Server		✓	●
MySQL		✓	✓
Oracle Database		✓	✓
SAP HANA		✓	●
Microsoft Applications—On-premises			
Active Directory		✓	✓
Exchange		✓	✓
File Level CDP		✓	●
SharePoint		✓	✓
SQL Server		✓	✓

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

✓ Supported ● Undetermined/Unsupported

Of the two, only Acronis backs up clustered Microsoft SQL Server and SAP HANA instances.

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 N-able offer RMM and PSA integrations but differ in the breadth and depth of their integration capabilities.

N-able Backup and EDP

N-able primarily focuses on offering a single, integrated portfolio to meet MSP needs. MSPs may turn to N-able to obtain software such as its Backup and EDR, among others, and then manage them through N-able RMM.

Using only N-able's products to meet these varied MSP needs works as long as they meet all of them. In the event N-able does not, MSPs must select alternative backup and cybersecurity solutions that N-able RMM can manage. This may help explain why N-able RMM integrates with and supports other backup solutions, to include Acronis Cyber Protect.[16] (Table 4.)

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; Autotask PSA; CloudBlue; ConnectWise Automate, Control, Command, and Manage; Jamf Pro; Kaseya Virtual System Administrator (VSA); and Matrix42.[17] 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 and RMM tools. Through this integration, MSPs may accomplish the following through their RMM console:

- Fully automate unattended agent deployments to Windows, Mac, 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.

15. https://www.n-able.com/blog/ultimate-guide-mysql-backup. Referenced 11/1/2021.
16. https://www.n-able.com/products/rmm. Referenced 10/9/2021.
17. https://solutions.acronis.com/autotask/. Referenced 5/28/2021.

TABLE 4

PSA and RMM Integrations

	Acronis Cyber Protect Cloud	N-able Backup and EDR
PSA/RMM Software	Atera; Autotask PSA; CloudBlue; ConnectWise Automate; ConnectWise Command; ConnectWise Control; ConnectWise Manage; jamf PRO; Kaseya VSA; Matrix42	Autotask PSA; Backup Radar; Connectwise Manage; Falanx Cyber; Flexis; Liongard; N-able RMM
Forthcoming PSA/RMM Product Integrations	6	Undisclosed
PSA/RMM Console Capabilities*	• Backup job scheduling, management • Changes pushed from Cyber Protect on-demand or on schedule • Cybersecurity management • File authorization & notarization	• Automated monitoring templates and scripting • Password management • Patch management
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

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.)

Acronis' PSA/RMM Integrations

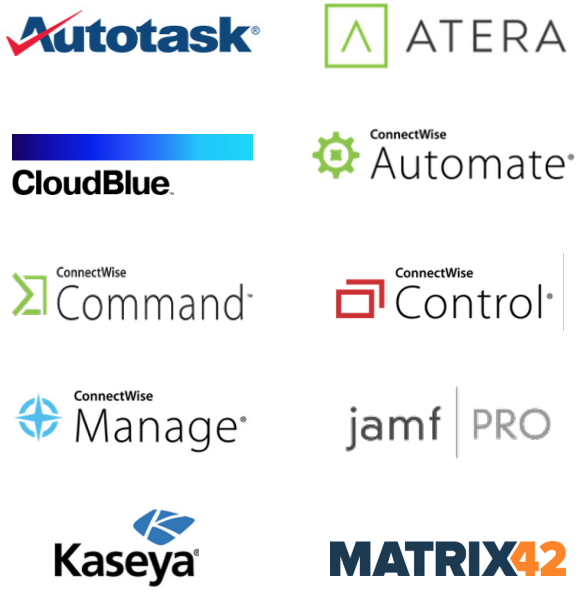

Figure 1

Acronis' Hosting Control and Bill System Integrations

Figure 2

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. 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.

17. https://solutions.acronis.com/autotask/. Referenced 5/28/2021.

KEY QUESTIONS TO ASK

- *Do you already use a PSA, RMM, or other third-party software 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 backup and recover their applications and data while securing them against potential ransomware threats.

Both Acronis and N-able offer solutions that meet the baseline backup, cybersecurity, and recovery needs of many customers. However, only Acronis Cyber Protect Cloud provides a single solution that natively integrates and delivers backup and cybersecurity software as one offering.

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.**

DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552

dcig.com